

Руководство пользователя (CLI)

Серия DGS-1520
Управляемые гигабитные коммутаторы

Версия 1.10

Table of Contents

1. Введение....4
2. Базовые команды интерфейса командной строки....13
3. Команды 802.1X....35
4. Команды ACL (Список управления доступом)....51
5. Команды управления доступом....90
6. Команды предотвращения атак ARP Spoofing....121
7. Команды Asymmetric VLAN....124
8. Команды Authentication, Authorization и Accounting (AAA)....125
9. Базовые команды настройки IPv4....163
10. Базовые команды настройки IPv6....174
11. Команды BPDU Protection....196
12. Команды Cable Diagnostics....200
13. Команды Command Logging....204
14. Команды CPU Access Control List (ACL)....205
15. Команды CPU Port Statistics....210
16. Команды Debug....213
17. Команды DHCP Auto-Configuration....224
18. Команды DHCP Auto-Image....226
19. Команды DHCP Client....229
20. Команды DHCP Relay....233
21. Команды DHCP Server....268
22. Команды DHCP Server Screening....300
23. Команды DHCP Snooping....307
24. Команды DHCPv6 Client....324
25. Команды DHCPv6 Guard....328
26. Команды DHCPv6 Relay....333
27. Команды DHCPv6 Server....357
28. Команды Digital Diagnostics Monitoring (DDM)....377
29. Команды Distance Vector Multicast Routing Protocol (DVMRP)....388
30. Команды клиента D-Link Discovery Protocol (DDP)....395
31. Команды Domain Name System (DNS)....402
32. Команды DoS Prevention....409
33. Команды Dynamic ARP Inspection....413
34. Команды Error Recovery....430
35. Команды Ethernet Ring Protection Switching (ERPS)....434
36. Команды File System....459
37. Команды Filter Database (FDB)....466
38. Команды Filter NetBIOS....482
39. Команды GARP VLAN Registration Protocol (GVRP)....484
40. Команды Gratuitous ARP....494
41. Команды управления интерфейсом....498
42. Команды Internet Group Management Protocol (IGMP)....529
43. Команды Internet Group Management Protocol (IGMP) Proxy....541
44. Команды Internet Group Management Protocol (IGMP) Snooping....547

45. Команды IP Multicast (IPMC).....576
46. Команды IP Multicast Version 6 (IPMCv6).....590
47. Команды IP Source Guard.....597
48. Команды IP Utility.....603
49. Команды IP-MAC-Port Binding (IMPB).....612
50. Команды IPv6 Snooping.....616
51. Команды IPv6 Source Guard.....624
52. Команды Layer 2 Protocol Tunnel (L2PT).....632
53. Команды Link Aggregation Control Protocol (LACP).....640
54. Команды Link Layer Discovery Protocol (LLDP).....648
55. Команды Loopback Detection (LBD).....680
56. Команды Loopback Test.....689
57. Команды аутентификации MAC.....692
58. Команды Mirror.....697
59. Команды Multicast Listener Discovery (MLD).....707
60. Команды Multicast Listener Discovery (MLD) Proxy.....718
61. Команды Multicast Listener Discovery (MLD) Snooping.....725
62. Команды Multicast Source Discovery Protocol (MSDP).....751
63. Команды Multicast VLAN.....774
64. Команды Multiple Spanning Tree Protocol (MSTP).....787
65. Команды Neighbor Discovery (ND) Inspection.....795
66. Команды Network Access Authentication.....801
67. Команды Network Load Balancing (NLB).....818
68. Команды Network Protocol Port Protection.....822
69. Команды Network Time Protocol (NTP).....824
70. Команды Open Shortest Path First Version 2 (OSPFv2).....842
71. Команды Open Shortest Path First Version 3 (OSPFv3).....906
72. Команды Packet Debug.....942
73. Команды Policy-based Routing (PBR).....946
74. Команды Port Security.....950
75. Команды Power over Ethernet (PoE) (только для DGS-1520-28MP и DGS-1520-52MP).....958
76. Команды энергосбережения.....978
77. Команды Priority-based Flow Control (PFC).....985
78. Команды Private VLAN.....988
79. Команды Protocol Independent.....996
80. Команды Protocol Independent Multicast (PIM).....1012
81. Команды Protocol Independent Multicast (PIM) IPv6.....1033
82. Команды Protocol Independent Multicast (PIM) Snooping.....1059
83. Команды Quality of Service (QoS).....1065
84. Команды QoS Amendment Data Center Bridge (DCB).....1106
85. Команды Remote Network MONitoring (RMON).....1115
86. Команды Reset Button.....1124
87. Команды Route Map.....1127
88. Команды Router Advertisement (RA) Guard.....1145
89. Команды Routing Information Protocol (RIP).....1150
90. Команды Routing Information Protocol Next Generation (RIPng).....1164
91. Команды Safeguard Engine.....1178

92. Команды клиента Secure File Transfer Protocol (SFTP).....1187
93. Команды Secure File Transfer Protocol (SFTP) Server.....1190
94. Команды Secure Shell (SSH).....1193
95. Команды sFlow.....1202
96. Команды Simple Mail Transfer Protocol (SMTP).....1210
97. Команды Simple Network Management Protocol (SNMP).....1216
98. Команды Single IP Management (SIM).....1243
99. Команды Spanning Tree Protocol (STP).....1255
100. Команды Stacking.....1272
101. Команды Storm Control.....1280
102. Команды Super VLAN.....1286
103. Команды Surveillance VLAN.....1290
104. Команды портов коммутатора.....1297
105. Команды управления системными файлами.....1302
106. Команды System Log.....1317
107. Команды времени и SNTP.....1332
108. Команды временного диапазона.....1340
109. Команды Traffic Segmentation.....1343
110. Команды Transport Layer Security (TLS).....1346
111. Команды Unicast Reverse Path Forwarding (URPF).....1357
112. Команды Virtual LAN (VLAN).....1361
113. Команды Virtual LAN (VLAN) Counter.....1380
114. Команды Virtual LAN (VLAN) Tunnel.....1384
115. Команды Virtual Router Redundancy Protocol (VRRP).....1398
116. Команды Virtual Router Redundancy Protocol Version 3 (VRRPv3).....1412
117. Команды Voice VLAN.....1421
118. Команды Web-аутентификации.....1430
119. Команды Weighted Random Early Detection (WRED).....1436
120. Команды Zone Defense.....1442
Приложение A. Восстановление пароля (Password Recovery).....1444
Приложение B. Записи системного журнала.....1446
Приложение C. Записи trap-сообщений.....1496
Приложение D. Назначение атрибутов RADIUS.....1509
Приложение E. Поддержка атрибутов IETF RADIUS.....1515
Приложение F. Информация ERPS.....1518
Приложение G. Информация по стекированию.....1519

1. Введение

Описание команд в данном руководстве основано на программном обеспечении версии **1.00**. Представленный здесь список является подмножеством команд, поддерживаемых коммутаторами серии DGS-1520.

Целевая аудитория

Руководство предназначено для сетевых администраторов и других IT-специалистов, использующих для управления коммутатором интерфейс командной строки (CLI). Это основной интерфейс управления коммутаторами серии DGS-1520. Настоящее руководство рассчитано на пользователей, знакомых с основными принципами работы Ethernet и организации сетей LAN.

Прочая документация

Руководства, указанные ниже, являются дополнительным источником информации по настройке коммутатора и выявлению неисправностей. Документы доступны на веб-сайте D-Link:

Краткое руководство по установке коммутаторов серии DGS-1520

Руководство пользователя по веб-интерфейсу коммутаторов серии DGS-1520

Условное обозначение	**Описание**
Полужирный шрифт	Команды, опции команд и ключевые слова. Ключевые слова в командной строке необходимо вводить именно так, как они представлены в данном документе.
КУРСИВ ЗАГЛАВНЫМИ	Параметры или значения, которые необходимо указать. При вводе параметров в командной строке необходимо подставить фактические значения, для которых требуется выполнение данной команды.
Квадратные скобки [ ]	Дополнительное значение или набор дополнительных аргументов.
Фигурные скобки { }	Альтернативные ключевые слова заключаются в фигурные скобки и разделяются вертикальной чертой. Как правило, необходимо выбрать один из вариантов, разделенных вертикальной чертой.
Вертикальная черта |	Дополнительные значения или аргументы заключаются в квадратные скобки и разделяются вертикальной чертой. Как правило, необходимо указать одно или несколько значений/аргументов, разделенных вертикальной чертой.
`Цветной шрифт Courier`	Используется для иллюстрации работы с командной строкой, включая примеры команд с соответствующим выводом. Все примеры в данном руководстве основаны на работе с коммутатором DGS-1520-28MP серии DGS-1520.

Предупреждения и примечания

При использовании данного руководства для управления коммутатором обращайте внимание на следующее:



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



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



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

Подключение к консольному порту

Консольный порт используется для доступа к интерфейсу командной строки (CLI). Подключите консольный кабель (входит в комплект поставки) стороной с разъемом DB9 к последовательному (COM) порту компьютера и стороной с разъемом RJ45 к консольному порту коммутатора.

Для доступа к интерфейсу командной строки (CLI) через консольный порт необходимо использовать эмулятор терминала, например, PuTTY или Tera Term. При этом требуются скорость передачи данных **115200** бод и выключенная функция Flow control.

После завершения загрузки появится окно для входа CLI.

Описания команд

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

Описание – краткое описание функционала команды.

Синтаксис – точная форма команды и правила ее написания.

Параметры – таблица с кратким описанием необязательных или обязательных для ввода параметров и их использованием в команде.

По умолчанию – если команда задает новое значение конфигурации или административное состояние коммутатора, которые отличаются от настроек по умолчанию, то это указывается в данном поле.

Режим ввода команды – режим, в котором возможно использование команды. Режимы описаны в разделе «Режимы ввода команд».

Уровень команды по умолчанию – уровень привилегий пользователя, необходимый для использования команды.

Использование команды – детальное описание команды и различных сценариев ее использования.

Пример (-ы) – пример использования команды в подходящем сценарии.

Режимы ввода команд

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

Интерфейс командной строки поддерживает три уровня привилегий учетной записи пользователя:

Basic User – 1-й уровень привилегий. Данный уровень учетной записи обладает самым низким приоритетом среди учетных записей и позволяет получить доступ к просмотру базовой информации о системе. Пользователь может получить доступ к информации, не относящейся к безопасности.

Operator – 12-й уровень привилегий. Данный уровень учетной записи позволяет отслеживать или менять настройки, за исключением относящихся к безопасности, как например, настройки учетных записей пользователей, учетных записей SNMP и т. д.

Administrator – 15-й уровень привилегий. Учетная запись уровня Administrator позволяет получить доступ ко всей информации о системе и системным настройкам, представленным в данном руководстве.

В интерфейсе командной строки (CLI) доступно три базовых режима в следующем иерархическом порядке:
User EXEC Mode (Пользовательский режим EXEC);

Privileged EXEC Mode (Привилегированный режим EXEC);

Global Configuration Mode (Режим глобальной конфигурации).

Переход в специальные режимы конфигурирования выполняется 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**.

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

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

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

Доступные командные режимы и уровни привилегий:

Режим ввода команд / Уровень привилегий	**Описание**
User EXEC Mode / Уровень Basic User	Самый низкий уровень приоритета среди пользовательских учетных записей. Доступен только просмотр базовых настроек системы.

Privileged EXEC Mode / Уровень Operator	Изменение локальных и глобальных настроек терминала, контроль и выполнение некоторых задач администрирования. Исключен доступ к информации, относящейся к безопасности.
Privileged EXEC Mode / Уровень Administrator	Те же права, что и для уровня Operator, при этом пользователь также может просматривать и вносить изменения в настройки безопасности.
Global Configuration Mode / Уровень Operator	Применение глобальных настроек, за исключением настроек безопасности, для всей системы. Также используется для перехода к специальным режимам.
Global Configuration Mode / Уровень Administrator	Применение глобальных настроек для всей системы. Также используется для перехода к специальным режимам.
Interface Configuration Mode / Уровень Administrator	Режим настройки интерфейса.

User EXEC Mode с базовым уровнем доступа Basic User

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

Privileged EXEC Mode с 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 при наличии 12-ого уровня привилегий.

Privileged EXEC Mode с уровнем доступа Administrator

Вход в данный режим можно получить при наличии 15-ого уровня 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 (Режим глобальной конфигурации)

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

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

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

Команда **exit** используется для выхода из режима глобальной конфигурации и возвращения в режим Privileged EXEC:

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

Порядок действий для входа в специальные режимы конфигурирования 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.

Создание пользовательской учетной записи

Можно создать несколько учетных записей для разного уровня привилегий. Этот раздел поможет пользователю создать учетную запись с помощью интерфейса командной строки.



Примечание: по умолчанию на коммутаторе настроена одна учетная запись. Имя пользователя и пароль: admin, уровень привилегий: 15.

Рассмотрим следующий пример:

```
Switch#enable
Switch#configure terminal
Switch(config)#username user1 password 1234
Switch(config)#username user1 privilege 15
Switch(config)#line console
Switch(config-line)#login local
Switch(config-line)#
```

В данном примере получен доступ к команде username.

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

Далее используется команда **configure terminal** для перехода к глобальному режиму конфигурации. Данный режим позволяет использовать команду **username**.

С помощью команды **username user1 password 1234** создается учетная запись пользователя с именем *user1* и паролем *1234.*

Команда **username user1 privilege 15** назначает 15-й уровень привилегий для учетной записи user1.

Команда **line console** обеспечивает доступ к режиму конфигурации строки для консоли (Line Configuration Mode).

Команда **login local** объявляет коммутатору, что для получения доступа к консоли пользователю необходимо ввести учетные данные из локальной базы данных.

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

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

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

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

Switch#
```

После перезагрузки коммутатора или выхода из учетной записи можно будет зайти в интерфейс командной строки с новым именем пользователя и паролем, как показано в примере ниже:

```
                    DGS-1520-28MP Gigabit Ethernet Smart Managed Switch

                                  Command Line Interface
                                 Firmware: Build 1.00.022
                 Copyright(C) 2020 D-Link Corporation. All rights reserved.

User Access Verification

Username:user1
Password:****

Switch#
```

Конфигурирование интерфейса

При конфигурировании физических портов коммутатора используется особое обозначение.

В следующем примере показан вход в режим глобальной конфигурации, далее переход в режим конфигурации интерфейса (Interface Configuration Mode) с использованием обозначения **1/0/1**. После входа в режим Interface Configuration Mode для порта 1 необходимо установить скорость 1 Гбит/с, используя команду **speed 1000**.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
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. Коммутатор серии DGS-1520 не поддерживает слоты расширения, поэтому для данного параметра всегда будет использоваться значение «0». 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. В таблице ниже указаны возможные сообщения об ошибках с описанием проблемы.

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

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

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

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

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

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

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

Функции редактирования

Интерфейс командной строки коммутатора поддерживает следующие клавиши для редактирования.

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

ESC	Выход из отображаемой страницы.

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

```
Switch#show running-config | begin interface ethernet 1/0/27
interface ethernet 1/0/27
!
interface ethernet 1/0/28
!
interface Vlan1
!
interface Null0
!
ntp access-group default nomodify noquery
!
!
end


Switch#
```

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

```
Switch#show running-config | include line
line console
line telnet
line ssh


Switch#
```

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

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

Current configuration : 1502 bytes


line console
line telnet
line ssh
network-protocol-port protect tcp
network-protocol-port protect udp
configure terminal
end
interface Mgmt0
interface ethernet 1/0/1
interface ethernet 1/0/2
interface ethernet 1/0/3
interface ethernet 1/0/4
interface ethernet 1/0/5
interface ethernet 1/0/6
interface ethernet 1/0/7
interface ethernet 1/0/8
interface ethernet 1/0/9
interface ethernet 1/0/10
interface ethernet 1/0/11
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

2. Базовые команды интерфейса командной строки

2.1 help

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

help

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда **help** применяется для получения краткой справочной информации, включая следующее:

- 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), так как 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), так как 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#
```

В примере ниже показано использование справки **по слову** для отображения команд режима Privileged EXEC Mode, 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
```

В следующем примере показано использование справки **по синтаксису команды**, позволяющей получить недостающий аргумент для частично введенной команды **stack**. Символы, введенные перед вопросительным знаком (?), также отображаются на следующей строке, что позволяет пользователю продолжить ввод команды.

```
Switch#stack ?
  <1-8>      Specifies current box ID
  bandwidth  Stacking port bandwidth
  preempt    Preempt the master role play
  <cr>

Switch#stack
```

2.2 enable

Данная команда используется для изменения уровня привилегий активной сессии.

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если привилегированный уровень требует пароля, введите его в предусмотренном для этого поле. Разрешено только три попытки. При неудачном вводе пользователь будет возвращен к текущему уровню.

Пример

В данном примере показано, как изменить уровень привилегий активной сессии на 15-ый 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 привилегий пользователя на более низкий.

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

Параметры

PRIVILEGE-LEVEL	(Опционально.) Укажите уровень привилегий в диапазоне от 1 до 15. 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 применяется для изменения уровня привилегий пользователя на более низкий.

Пример

В данном примере показано, как изменить уровень активной сессии CLI на 1-ый 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 применяется для входа в режим глобальной конфигурации.

Пример

В данном примере показано, как войти 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 применяется для смены пользователя и входа в систему с новой учетной записью. Разрешено 3 попытки входа в интерфейс коммутатора. При использовании Telnet, если все попытки будут неудачными, пользователь вернется к приглашению на ввод команды. Если в течение 60 секунд не вводится никаких данных, сессия вернется в состояние выхода из учетной записи.

Пример

В данном примере показано, как войти в учетную запись с именем пользователя «user1».

```
Switch#login

Username: user1
Password: xxxxx

Switch#
```

2.6 login (Line)

Данная команда используется, чтобы настроить метод входа для указанного типа подключения. Для отключения требования авторизации воспользуйтесь формой **no** этой команды.

login [local]
no login

Параметры

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

По умолчанию

По умолчанию для доступа через **консоль**, **Telnet** и **SSH** используется локальная база данных (имя пользователя и пароль).

Режим ввода команды

Line Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

- При выключении авторизации пользователь войдет в систему с уровнем привилегий 1.
- При выборе опции **by password** после ввода того же пароля, что в команде **password,** пользователь войдет в строку на уровне 1. Если пароль не был сконфигурирован, 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 три типа аутентификации:

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

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

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

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

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

  - При выборе опции **password** имя пользователя игнорируется, но требуется ввод пароля, 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 примере ниже 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 следующем 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#
```

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

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

В данном примере показан процесс конфигурации метода входа login local.

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

2.7 logout

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

logout

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

В данном примере показано, как выйти из системы.

```
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 конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для возврата 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 eth1/0/1
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 применяется 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 показано, как вернуться из режима конфигурирования интерфейса (Interface Configuration Mode) в режим глобальной конфигурации (Global Configuration Mode).

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

2.10 show history

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

show history

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Навигация по командам в истории выполняется следующими комбинациями клавиш:

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

Пример

В данном примере показан процесс вызова буфера истории.

```
Switch#show history

 help
 history

Switch#
```

2.11 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, так как 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 (start-up configuration).

Пример

В данном примере показано, как использовать функцию 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 о состоянии вентиляторов, температуре и питании.

show environment [fan | power | temperature]

Параметры

fan	(Опционально.) Укажите для отображения подробной информации о состоянии вентиляторов.
power	(Опционально.) Укажите для отображения подробной информации о питании.
temperature	(Опционально.) Укажите для отображения подробной информации о температуре.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если параметры не заданы, будут отображаться все типы информации.

Пример

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

```
Switch#show environment

Detail Temperature Status:
Unit     Temperature Descr/ID          Current/Threshold Range
-----   ----------------------------------------------------
1        Central Temperature/1         23C/11~79C
Status code: * temperature is out of threshold range

Detail Fan Status:
-------------------------------------------------------------
Unit 1:
  Right Fan 1 (OK)      Right Fan 2 (OK)      Right Fan 3 (OK)
  Right Fan 4 (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 корректно. **empty**: источник питания не подключен.

2.13 show unit

Данная команда позволяет получить общую информацию по устройствам стека.

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

Параметры

UNIT-ID	(Опционально.) Укажите Unit ID устройства, информацию о котором необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации об устройствах стека. Если параметр *UNIT-ID* не указан, выводится информация по всем устройствам.

Пример

В данном примере показано, как отобразить информацию об устройствах в стеке.

```
Switch#show unit

Unit: 1
Model Descr: 20 ports GE PoE + 4 ports 2.5 GE PoE + 2 10GE ports + 2 SFP+ Smart Managed Sw
itch
Model Name: DGS-1520-28MP
Serial-Number: DGS1520-28MPA
Status: OK
Up Time: 0DT1H39M47S
DRAM      524288 K total,   223786 K used,   300502 K free
FLASH      60823 K total,    59384 K used,     1439 K free

Switch#
```

2.14 show cpu utilization

Данная команда позволяет получить информацию об использовании ЦПУ.

show cpu utilization [history {15_minute [slot *INDEX*] **| 1_day [slot** *INDEX*]}]

Параметры

history	(Опционально.) Укажите для отображения архивной информации об использовании ЦПУ.
15_minute	(Опционально.) Укажите для отображения статистики за прошедшие 15 минут.
1_day	(Опционально.) Укажите для отображения статистики за прошедшие сутки.

slot *INDEX*	(Опционально.) Укажите номер слота, информацию о котором необходимо отобразить. Для статистики за 15 минут используется диапазон от 1 до 5. Для статистики за сутки – диапазон от 1 до 2. Если слот не указан, будет отображаться информация по всем слотам.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения данных по загрузке центрального процессора с интервалами 5 секунд, 1 минута и 5 минут.

Существует два типа отображения архивной информации об использовании ЦПУ: за 15 минут и за сутки. В первом случае (15 минут) слот 1 используется для отображения статистики за прошедшие 15 минут, а слот 2 – статистики для интервала, который начался 30 минут назад и завершился 15 минут назад, и т.д. Во втором случае (сутки) слот 1 используется для отображения статистики за прошедшие 24 часа, а слот 2 – статистики для интервала, который начался 48 часов назад и закончился 24 часа назад.

Пример

В данном примере показано, как получить информацию о загрузке процессора.

```
Switch#show cpu utilization

CPU Utilization

Five seconds -  14 %         One minute -  14 %         Five minutes -  14 %


Switch#
```

В данном примере показано, как получить информацию о загрузке процессора за 15 минут.

```
Switch#show cpu utilization history 15_minute

CPU Utilization:
12 Dec 2019  10:00:08 - 12 Dec 2019  09:45:08  : 5   %
12 Dec 2019  09:45:08 - 12 Dec 2019  09:30:08  : 6   %
12 Dec 2019  09:30:08 - 12 Dec 2019  09:15:08  : 6   %
12 Dec 2019  09:15:08 - 12 Dec 2019  09:00:08  : 6   %
12 Dec 2019  09:00:08 - 12 Dec 2019  08:45:08  : 9   %

Switch#
```

2.15 show version

Данная команда используется для отображения информации о версии коммутатора.

show version

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о версии коммутатора.

Пример

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

```
Switch#show version

System MAC Address: 80-26-89-15-28-00

Unit ID    Module Name                    Versions
-------  ----------------------------  ---------------------
   1      DGS-1520-28MP                 H/W:A1
                                        Bootloader:1.00.010
                                        Runtime:1.00.022


Switch#
```

2.16 snmp-server enable traps environment

Данная команда используется для включения отправки trap-сообщений о состоянии питания, температуре и работе вентиляторов. Чтобы отключить отправку trap-сообщений, воспользуйтесь формой **no** этой команды.

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

Параметры

fan	(Опционально.) Укажите для отправки предупреждающих trap-сообщений о событиях (остановка вентилятора или восстановление работы вентилятора).
power	(Опционально.) Укажите для отправки предупреждающих trap-сообщений о событиях (отказ питания или восстановление питания).
temperature	(Опционально.) Укажите для отправки предупреждающих trap-сообщений о событиях (превышение пороговых значений температуры или восстановление температуры).

По умолчанию

По умолчанию поддержка trap-сообщений для всех параметров отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для включения отправки trap-сообщений о состоянии питания,

температуре и работе вентиляторов. Если параметры не указаны, будет включена или отключена поддержка trap-сообщений для всех параметров.

Пример

В данном примере показано, как включить отправку trap-сообщений.

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

2.17 environment temperature threshold

Данная команда используется, чтобы настроить пороговые значения температур для срабатывания термодатчика. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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. Значение – 1.
high	(Опционально.) Укажите верхнюю границу температуры в градусах Цельсия. Диапазон значений: от -100 до 200.
low	(Опционально.) Укажите нижнюю границу температуры в градусах Цельсия. Диапазон значений: от -100 до 200. Нижняя граница не может быть выше верхней границы.

По умолчанию

По умолчанию корректным является указанный рабочий диапазон.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить пороговые значения температуры, соответствующие корректному диапазону рабочих температур, определенных для датчика. Нижняя граница температурного диапазона не может быть выше верхней. Настроенный диапазон должен быть в

пределах минимума и максимума разрешенных температур, определенных для датчика. При превышении заданного порога будет отправлено уведомление.

Пример

В данном примере показано, как настроить диапазон температур для термодатчика с ID 1 на устройстве Unit 1.

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

2.18 show memory utilization

Данная команда используется для отображения информации об использовании памяти.

show memory utilization [history {15_minute [slot *INDEX*] **| 1_day [slot** *INDEX*]}]

Параметры

history	(Опционально.) Укажите для отображения архивной информации об использовании памяти.
15_minute	(Опционально.) Укажите для отображения статистики за прошедшие 15 минут.
1_day	(Опционально.) Укажите для отображения статистики за прошедшие сутки.
slot *INDEX*	(Опционально.) Укажите номер слота для отображения информации. Для статистики за 15 минут используется диапазон от 1 до 5. Для статистики за сутки – диапазон от 1 до 2. Если слот не указан, будет отображаться информация по всем слотам.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации об использовании памяти коммутатора.

Существует два типа отображения архивной информации об использовании памяти: за 15 минут и за сутки. В первом случае (15 минут) слот 1 используется для отображения статистики за прошедшие 15 минут, а слот 2 – статистики для интервала, который начался 30 минут назад и завершился 15 минут назад, и т.д. Во втором случае (сутки) слот 1 используется для отображения статистики за прошедшие 24 часа, а слот 2 – статистики для интервала, который начался 48 часов назад и закончился 24 часа назад.

Архивная информация отображается только для памяти DRAM.

Пример

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

```
SSwitch#show memory utilization

Unit: 1
DRAM      524288 K total,   223606 K used,   300682 K free
FLASH      60823 K total,    44847 K used,    15976 K free

Switch#
```

В данном примере показано, как отобразить информацию об использовании памяти за 15 минут.

```
Switch#show memory utilization history 15_minute

Unit 1 DRAM Utilization:
1  Jan 2019  01:24:25 - 1  Jan 2019  01:09:25  : 42  %
1  Jan 2019  01:09:25 - 1  Jan 2019  00:54:25  : 42  %
1  Jan 2019  00:54:25 - 1  Jan 2019  00:39:25  : 42  %
1  Jan 2019  00:39:25 - 1  Jan 2019  00:24:25  : 42  %
1  Jan 2019  00:24:25 - 1  Jan 2019  00:09:25  : 42  %

Switch#
```

2.19 privilege

Данная команда используется, чтобы настроить уровни привилегий для команд. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

MODE	Укажите режим ввода команды.
level *PRIVILEGE-LEVEL*	Укажите уровень привилегий, необходимый для выполнения команды, в диапазоне от 1 до 15.
reset	Укажите, чтобы вернуть уровень привилегий для команды к значению по умолчанию.

COMMAND-STRING	Укажите команду, которую необходимо конфигурировать.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Команда используется для настройки уровня привилегий для команд. When this command is used, the command string used must exist at current command level. Если с указанной строки начинаются несколько команд, будет изменен уровень для всех этих команд.

Пример

В данном примере показано, как изменить уровень команды **configure terminal**, выбрав уровень 12.

```
Switch#enable 15
Switch#configure terminal
Switch(config)#privilege exec level 12 configure terminal
Switch(config)#
```

2.20 show privilege

Данная команда используется для отображения текущего уровня привилегий.

show privilege

Параметры

Нет**.**

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда используется для отображения текущего уровня привилегий.

Пример

В данном примере показано, как отобразить текущий уровень привилегий.

```
Switch#show privilege

Current privilege level is 15

Switch#
```

3. Команды 802.1X

3.1 clear dot1x counters

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

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для сброса всех счетчиков 802.1X (диагностика, статистика и статистика сессии).

Пример

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

```
Switch#clear dot1x counters interface eth1/0/1
Switch#
```

3.2 dot1x control-direction

Данная команда используется для настройки типа трафика на порту как однонаправленного (in) или двунаправленного (both). Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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

Параметры

both	Укажите для включения контроля трафика в двух направлениях.
in	Укажите для включения 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 применима исключительно для настройки интерфейсов 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, что 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. Направление **in** является действующим только при режиме **multi-host**, настроенном с использованием команды **authentication host-mode**.

Пример

В данном примере показано, как настроить контроль трафика на интерфейсе Ethernet 1/0/1 в качестве однонаправленного.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x control-direction in
Switch(config-if)#
```

3.3 dot1x default

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

dot1x default

Параметры

Нет.

По умолчанию

Аутентификация IEEE 802.1X отключена.

Двунаправленный режим потока.

Управление портом – автоматическое.

Forward PDU на порту отключено.

Максимальное количество запросов – 2.

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 применима исключительно для настройки интерфейсов физического порта.

Пример

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

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x default
Switch(config-if)#
```

3.4 dot1x port-control

Данная команда используется для управления состоянием авторизации порта. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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

Параметры

auto	Укажите, чтобы включить аутентификацию IEEE 802.1X для порта.
force-authorized	Укажите, чтобы порт считался принудительно авторизованным.
force-unauthorized	Укажите, чтобы порт считался принудительно неавторизованным.

По умолчанию

Параметр по умолчанию – **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.

Команда применима исключительно для настройки интерфейсов физического порта.

При выборе параметра **force-authorized** контроль трафика в обоих направлениях не осуществляется. При выборе параметра **auto** для контроля трафика в заданном направлении необходимо пройти процедуру аутентификации. При выборе параметра **force-unauthorized** управление портом в указанном направлении заблокировано.

Пример

В данном примере показано, как запретить доступ на интерфейс Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
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. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

dot1x forward-pdu
no dot1x forward-pdu

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена**.**

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. Команда действует, 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 eth1/0/1
Switch(config-if)#dot1x forward-pdu
Switch(config-if)#
```

3.6 dot1x initialize

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

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

В режиме multi-host укажите ID интерфейса для инициализации определенного порта.

В режиме multi-auth укажите MAC-адрес для инициализации определенного MAC-адреса.

Пример

В данном примере показано, как инициализировать режим аутентификатора для интерфейса Ethernet 1/0/1.

```
Switch#dot1x initialize interface eth1/0/1
Switch#
```

3.7 dot1x max-req

Данная команда используется, чтобы задать максимальное количество попыток для передачи клиенту запроса EAP (Extensive Authentication Protocol) от внутреннего сервера аутентификации, прежде чем инициировать повторную аутентификацию. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

По умолчанию используется значение 2.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. Если клиент не отвечает на запрос аутентификации в течение периода, заданного командой **dot1x timeout tx-period** *SECONDS,* коммутатор отправит повторный запрос. Используйте команду, чтобы 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. Указанное значение – 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x max-req 3
Switch(config-if)#
```

3.8 dot1x pae authenticator

Данная команда используется для конфигурирования определенного порта в качестве аутентификатора IEEE 802.1X PAE (Port Access Entity). Чтобы отключить использование порта в качестве аутентификатора IEEE 802.1X, воспользуйтесь формой **no** этой команды.

dot1x pae authenticator
no dot1x pae authenticator

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. 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 показано, как настроить интерфейс Ethernet 1/0/1 в качестве аутентификатора IEEE 802.1X PAE.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#
```

В примере ниже показано, как отключить аутентификацию IEEE 802.1X для интерфейса Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no dot1x pae authenticator
Switch(config-if)#
```

3.9 dot1x re-authenticate

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

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

Параметры

interface *INTERFACE-ID*	Укажите порт для повторной аутентификации. Доступными интерфейсами являются физические порты.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
mac-address *MAC-ADDRESS*	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 применяется 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 показано, как включить повторную аутентификацию для интерфейса Ethernet 1/0/1.

```
Switch#dot1x re-authenticate interface eth1/0/1
Switch#
```

3.10 dot1x system-auth-control

Данная команда используется для глобального включения аутентификации IEEE 802.1X на коммутаторе. Чтобы отключить аутентификацию IEEE 802.1X, воспользуйтесь формой **no** этой команды.

dot1x system-auth-control

no dot1x 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

При включении функции аутентификации IEEE 802.1X неавторизованные узлы не смогут 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 показано, как включить аутентификацию IEEE 802.1X глобально на коммутаторе.

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

3.11 dot1x timeout

Данная команда используется для настройки таймеров IEEE 802.1X. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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

Параметры

server-timeout *SECONDS*	Укажите период времени в секундах, в течение которого коммутатор ожидает запрос от сервера аутентификации. По истечении времени ожидания аутентификатор отправит клиенту пакет EAP-Request. Диапазон значений: от 1 до 65535.
supp-timeout *SECONDS*	Укажите период времени в секундах, в течение которого коммутатор ожидает ответ от запрашивающего устройства. По истечении времени ожидания все сообщения от запрашивающего устройства, кроме запроса EAP request ID, будут недействительны. Диапазон значений от 1 до 65535.
tx-period *SECONDS*	Укажите период времени в секундах, в течение которого коммутатор ожидает ответ на запрос EAP-Request/Identity от клиента перед повторной отправкой запроса. 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 применима исключительно для настройки интерфейсов 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 eth1/0/1
Switch(config-if)#dot1x timeout server-timeout 15
Switch(config-if)#dot1x timeout supp-timeout 15
Switch(config-if)#dot1x timeout tx-period 10
Switch(config-if)#
```

3.12 show dot1x

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

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения глобальной конфигурации или конфигурации интерфейса. Если параметры не указаны, будет отображаться 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 примере ниже показано, как включить отображение конфигурации dot1X для интерфейса Ethernet 1/0/1.

```
Switch#show dot1x interface eth1/0/1


Interface          : eth1/0/1
PAE                : Authenticator
Control Direction  : Both
Port Control       : Auto
Tx Period          : 30    sec
Supp Timeout       : 30    sec
Server Timeout     : 30    sec
Max-req            : 2     times
Forward PDU        : 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.) Укажите интерфейс или группу интерфейсов, для которых будут отображаться данные диагностики dot1x. Если значение не указано, отображается информация обо всех интерфейсах.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

```
Switch#show dot1x diagnostics interface eth1/0/1

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.) Укажите интерфейс или группу интерфейсов, для которых будет отображаться статистика dot1x. Если значение не указано, будет отображаться информация для всех интерфейсов.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения статистики IEEE 802.1X. Если значение не указано, отображается статистика для всех интерфейсов.

Пример

В данном примере показано, как отобразить статистику dot1X для интерфейса Ethernet 1/0/1.

```
Switch#show dot1x statistics interface eth1/0/1

 eth1/0/1 dot1x statistics information:
 EAPOL Frames RX                    : 2
 EAPOL Frames TX                    : 3
 EAPOL-Start Frames RX              : 0
 EAPOL-Req/Id Frames TX             : 1
 EAPOL-Logoff Frames RX             : 0
 EAPOL-Req Frames TX                : 1
 EAPOL-Resp/Id Frames RX            : 1
 EAPOL-Resp Frames RX               : 1
 Invalid EAPOL Frames RX            : 0
 EAP-Length Error Frames RX         : 0
 Last EAPOL Frame Version           : 1
 Last EAPOL Frame Source            : 00-0D-88-11-8B-6A

Switch#
```

3.15 show dot1x session-statistics

Данная команда используется для отображения статистики сессий IEEE 802.1X.

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

В данном примере показано, как отобразить статистику по сессиям dot1X для интерфейса Ethernet 1/0/1.

```
Switch#show dot1x session-statistics interface eth1/0/1

Eth1/0/1 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, чтобы включить отправку SNMP-уведомлений для аутентификации 802.1X. Для отключения отправки SNMP-уведомлений воспользуйтесь формой **no** этой команды.

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

Используйте данную команду, чтобы включить/отключить отправку SNMP-уведомлений для аутентификации 802.1X

Пример

В данном примере показано, как включить отправку trap-сообщений 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 изменения нумерации записей в списке доступа. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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

no access-list resequence

Параметры

NAME	Укажите имя конфигурируемого списка доступа. Максимальное количество символов – 32.
NUMBER	Укажите номер конфигурируемого списка доступа.
STARTING-SEQUENCE-NUMBER	Укажите начальное значение, в соответствии с которым будут перегруппированы записи в списке. Значение по умолчанию – 10. Диапазон значений: от 1 до 65535.
INCREMENT	Укажите шаг для присвоения порядковых номеров. Значение по умолчанию – 10. Например, если значение шага равно 5, а начальный номер – 20, то последующим записям будут присвоены номера 25, 30, 35, 40 и т. д. 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 применяется для изменения нумерации записей для указанного списка доступа в соответствии с начальным номером из параметра *STARTING-SEQUENCE-NUMBER* и шагом, заданным с помощью параметра *INCREMENT*. Если сгенерированный порядковый номер превышает максимально допустимое значение, то существующая нумерация записей не изменится.

Если правило создано без указания определенного порядкового номера, он будет присвоен автоматически. Первой записи в списке присваивается начальный порядковый номер, а каждая новая

запись получает последующий номер с учетом заданного шага и помещается в конец списка.

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

Пример

В данном примере показано, как изменить нумерацию записей для списка доступа на основе IP-адресации с именем R&D.

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

4.2 acl-hardware-counter

Данная команда используется, чтобы включить аппаратный счетчик ACL указанного списка доступа (access-list) для функций ограничения доступа (access group) или access map для фильтрации на основе VLAN. Для отключения аппаратных счетчиков воспользуйтесь формой **no** этой команды.

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

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

Параметры

access-group	*ACCESS-LIST-NAME*	Укажите имя конфигурируемого списка доступа.
access-group	*ACCESS-LIST-NUMBER*	Укажите номер конфигурируемого списка доступа.
vlan-filter	*ACCESS-MAP-NAME*	Укажите имя конфигурируемой access map.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

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

Пример

В данном примере показано, как включить функцию аппаратного счетчика ACL.

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

4.3 action

Данная команда используется для настройки действий продвижения, отбрасывания или переадресации из sub-map в режиме VLAN Access-map Sub-map Configuration Mode. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

Параметр по умолчанию – **forward**.

Режим ввода команды

VLAN Access-map Sub-map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

В данном примере показано, как настроить действие на sub-map.

```
Switch#show vlan access-map
VLAN access-map vlan-map 20
  match mac access list: ext_mac(ID: 7999)
  action: forward
Switch#configure terminal
Switch(config)#vlan access-map vlan-map 20
Switch(config-access-map)#action redirect eth1/0/5
Switch(config-access-map)#end
Switch#show vlan access-map
VLAN access-map vlan-map 20
  match mac access list:  ext_mac(ID: 7999)
  action: redirect eth1/0/5
Switch#
```

4.4 clear acl-hardware-counter

Данная команда используется для сброса аппаратных счетчиков ACL.

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

Параметры

access-group	*ACCESS-LIST-NAME*	Укажите название списка доступа для удаления.
access-group	*ACCESS-LIST-NUMBER*	Укажите номер списка доступа для удаления.
vlan-filter	*ACCESS-MAP-NAME*	Укажите название access map для удаления.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если в параметре **access-group** не указано определенное название (access-list name) или номер списка доступа (access-list number), данная команда обнулит аппаратные счетчики сразу для всех списков управления доступом (access-group hardware counters). Если в параметре **vlan-filter** не указано название access map, будут сброшены все аппаратные счетчики для фильтрации на основе VLAN.

Пример

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

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

4.5 expert access-group

Данная команда используется для применения указанных списков управления доступом expert (expert ACL) к интерфейсу. Чтобы отменить применение, воспользуйтесь формой **no** этой команды.

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

Параметры

NAME	Укажите имя настраиваемого списка управления доступом expert (expert access-list). Максимальное количество символов – 32.
NUMBER	Укажите номер настраиваемого списка управления доступом expert (expert access-list).
in	(Опционально.) Укажите для фильтрации входящих пакетов на интерфейс. Если направление не указано, используется значение **in**.
out	(Опционально.) Укажите, чтобы включить фильтрацию исходящих пакетов для передачи интерфейсу.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

 PROMPT: The remaining applicable EXPERT related access entries are 1664, remaining range
entries are 32.
Switch(config-if)#
```

4.6 expert access-list

Данная команда используется для создания или изменения расширенного списка управления доступом expert (extended expert ACL). Использование данной команды осуществляет вход в режим Extended Expert Access-list Configuration Mode. Чтобы удалить расширенный список доступа expert, воспользуйтесь формой **no** этой команды.

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

Параметры

NAME	Укажите имя конфигурируемого расширенного списка доступа expert. Максимальное количество символов – 32.
NUMBER	Укажите идентификационный номер (ID number) списка доступа expert. 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 number).

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)#
```

4.7 ip access-group

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

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

Параметры

NAME	Укажите имя используемого списка доступа IP. Максимальное количество символов – 32.
NUMBER	Укажите номер используемого списка доступа IP.
in	(Опционально.) Укажите, чтобы список доступа IP применялся для проверки пакетов во входящем направлении. Если направление не указано, используется **in**.
out	(Опционально.) Укажите, чтобы список доступа IP применялся для проверки пакетов в исходящем направлении.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

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

Пример

В данном примере показано, как настроить список доступа IP «Strict-Control» в качестве группы доступа IP для порта Ethernet 1/0/2.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#ip access-group Strict-Control

 PROMPT: The remaining applicable IP related access entries are 3327, remaining range entries
are 32.
Switch(config-if)#
```

4.8 ip access-list

Данная команда используется для создания или изменения списка доступа IP (IP access list). При использовании команды произойдет вход в режим IP Access List Configuration Mode. Чтобы удалить список доступа IP, воспользуйтесь формой **no** этой команды.

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

Параметры

extended	(Опционально.) Укажите для использования расширенного списка доступа IP (extended IP access list) и возможности применить больше опций фильтрации. Если параметр не указан, список доступа будет считаться стандартным.
NAME	Укажите имя списка доступа IP. Максимальное количество символов – 32. Первым символом должна быть буква.
NUMBER	Укажите ID-номер (ID number) списка доступа IP. Диапазон значений для стандартных списков доступа IP: от 1 до 1999; для расширенных списков доступа IP: от 2000 до 3999.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

4.9 ipv6 access-group

Данная команда используется для назначения списка доступа IPv6 (IPv6 access list), который будет применяться к интерфейсу. Чтобы удалить список доступа IPv6, воспользуйтесь формой **no** этой команды.

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

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

Параметры

NAME	Укажите имя используемого списка доступа IPv6.
NUMBER	Укажите номер используемого списка доступа IPv6.
in	(Опционально.) Укажите, чтобы список доступа IPv6 применялся для проверки пакетов во входящем направлении. Если направление не указано, используется **in**.
out	(Опционально.) Укажите, чтобы список доступа IPv6 применялся для проверки пакетов в исходящем направлении.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

К одному и тому же интерфейсу нельзя применить несколько списков доступа одинакового типа, при этом могут применяться списки доступа разных типов. Привязка группы доступа (access group) к интерфейсу будет расходовать ресурсы коммутатора для записей фильтрации. Если для активации команды не хватает ресурсов, появится сообщение об ошибке.

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

Пример

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

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 access-group ip6-control in

 PROMPT: The remaining applicable IPv6 related access entries are 767, remaining range entries
are 32.
Switch(config-if)#
```

4.10 ipv6 access-list

Данная команда используется для создания или изменения списка доступа IPv6 (IPv6 access list). При использовании команды произойдет вход в режим IPv6 Access List Configuration Mode. Чтобы удалить список доступа IPv6, воспользуйтесь формой **no** этой команды.

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

Параметры

extended	(Опционально.) Укажите для использования расширенного списка доступа IPv6 и возможности применить больше опций фильтрации. Если параметр не указан, список доступа IPv6 будет считаться стандартным.
NAME	Укажите имя списка доступа IPv6. Максимальное количество символов – 32.
NUMBER	Укажите номер ID (ID number) списка доступа IPv6. Диапазон значений для стандартных списков доступа IPv6: от 11000 до 12999; для расширенных списков доступа IPv6: от 13000 до 14999

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

4.11 list-remark

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

list-remark *TEXT*

no list-remark

Параметры

TEXT	Укажите текст комментария (не более 256 символов).

По умолчанию

Нет.

Режим ввода команды

Access-list Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда доступна в режимах MAC, IP, IPv6 и Expert Access-list Configure Mode.

Пример

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

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

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

Switch#
```

4.12 mac access-group

Данная команда используется для определения списка MAC-адресов, применяемого к интерфейсу. Чтобы удалить группу доступа с интерфейса, воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

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

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

Пример

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

```
Switch#configure terminal
Switch(config)#interface eth1/0/4
Switch(config-if)#mac access-group daily-profile in

 PROMPT: The remaining applicable MAC related access entries are 1535, remaining range entries
are 32.
Switch(config-if)#
```

4.13 mac access-list

Данная команда используется для создания или изменения списков управления доступом на базе MAC-адресации. Команда позволяет войти в режим MAC Access List Configuration Mode. Чтобы удалить список управления доступом MAC, воспользуйтесь формой **no** этой команды.

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

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

Параметры

NAME	Укажите имя списка управления доступом MAC (MAC access list). Максимальное количество символов – 32.
NUMBER	Укажите номер ID (ID number) списка управления доступом на основе MAC. Диапазон значений для расширенных списков доступа MAC: от 6000 до 7999.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы войти в режим MAC Access-list Configuration Mode, и введите команду **permit** или **deny**, чтобы указать правила. Указанное имя должно быть уникальным среди всех списков доступа. Имя чувствительно к регистру. Если номер списка доступа не задан, автоматически будет назначен самый большой неиспользуемый номер из диапазона номеров списков доступа на основе MAC.

Пример

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

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

4.14 match ip address

Данная команда используется для сопоставления списка доступа IP с настраиваемой sub-map. Чтобы удалить совпадающую запись, воспользуйтесь формой **no** этой команды.

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

no match ip address

Параметры

ACL-NAME	Укажите имя списка управления доступом (ACL access list). Максимальное количество символов – 32.
ACL-NUMBER	Укажите номер списка управления доступом IP (IP ACL).

По умолчанию

Нет.

Режим ввода команды

VLAN Access-map Sub-map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы сопоставить список доступа IP с настроенной sub-map. С одной

sub-map может быть сопоставлен только один список доступа (IP access list, IPv6 access list или MAC access list). IP sub-map проверяет только IP-пакеты. При вводе новой команды предыдущие настройки будут перезаписаны.

Пример

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

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

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

Switch#
```

4.15 match ipv6 address

Данная команда используется для сопоставления списков доступа IPv6 с настраиваемыми sub-maps. Чтобы удалить соответствующую запись, воспользуйтесь формой **no** этой команды.

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

Параметры

ACL-NAME	Укажите имя списка управления доступом IPv6 (IPv6 ACL). Максимальное количество символов – 32.
ACL-NUMBER	Укажите номер списка управления доступом IPv6 (IPv6 ACL).

По умолчанию

Нет.

Режим ввода команды

VLAN Access-map Sub-map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы сопоставить список доступа IPv6 с настроенной sub-map. С

одной sub-map может быть сопоставлен только один список доступа (IP access list, IPv6 access list или MAC access list). IPv6 sub-map проверяет только IPv6-пакеты. При вводе новой команды предыдущие настройки будут перезаписаны.

Пример

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

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

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

Switch#
```

4.16 match mac address

Данная команда используется для сопоставления списков доступа MAC (MAC access lists) с настраиваемыми sub-maps. Чтобы удалить соответствующую запись, воспользуйтесь формой **no** этой команды.

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

no match mac address

Параметры

ACL-NAME	Укажите имя списка управления доступом MAC (ACL MAC). Максимальное количество символов – 32.
ACL-NUMBER	Укажите номер списка управления доступом MAC.

По умолчанию

Нет.

Режим ввода команды

VLAN Access-map Sub-map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

VLAN access-map vlan-map 20
  match ip access list: sp1(ID: 3999)
  action: forward
VLAN access-map vlan-map 30
  match mac access list:  ext_mac(ID: 7999)
  action: forward

Switch#
```

4.17 permit | deny | deny-cpu (expert access-list)

Данная команда используется для создания разрешающих или запрещающих правил фильтрации в списке ACL. Чтобы удалить запись, воспользуйтесь формой **no** этой команды.

Расширенный список управления доступом expert (Extended Expert ACL):

[*SEQUENCE-NUMBER***] {permit | deny | deny-cpu}** *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* **[***MASK***] [inner** *INNER-COS* **[***MASK***]]] [{vlan** *OUTER-VLAN* **[***MASK***] | vlan-range** *MIN-VID MAX-VID***} [inner** *INNER-VLAN* **[***MASK***]]] [fragments] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny | deny-cpu} 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* **| mask** *PORT MASK***] {***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* **| mask** *PORT MASK***] [***TCP-FLAG***] [cos** *OUTER-COS* **[***MASK***] [inner** *INNER-COS* **[***MASK***]]] [{vlan** *OUTER-VLAN* **[***MASK***] | vlan-range** *MIN-VID MAX-VID***} [inner** *INNER-VLAN* **[***MASK***]]] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [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* **| mask** *PORT MASK***] {***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* **| mask** *PORT MASK***] [cos** *OUTER-COS* **[***MASK***] [inner** *INNER-COS* **[***MASK***]]] [{vlan** *OUTER-VLAN* **[***MASK***] | vlan-range** *MIN-VID MAX-VID***} [inner** *INNER-VLAN* **[***MASK***]]] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny | deny-cpu} 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* **[***MASK***] [inner** *INNER-COS* **[***MASK***]]] [{vlan** *OUTER-VLAN* **[***MASK***] | vlan-range** *MIN-VID MAX-VID***} [inner** *INNER-VLAN* **[***MASK***]]] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

no *SEQUENCE-NUMBER*

Параметры

SEQUENCE-NUMBER	Укажите порядковый номер. Диапазон значений: от 1 до 65535. Чем меньше номер, тем выше приоритет правила permit/deny.
PROTOCOL	(Опционально.) Укажите ID IP-протокола или один из следующих протоколов: **eigrp, esp, gre, igmp, ospf, pim, vrrp, pcp** и **ipinip**. Если ID протокола указан, параметр *MASK* (0x0-0xff) является опциональным. Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
cos *OUTER-COS*	(Опционально.) Укажите значение внешнего приоритета (outer priority). Диапазон значений: от 0 до 7.
MASK	(Опционально.) Укажите маску внешнего приоритета (outer priority mask) (0x0-0x7). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
inner *INNER-COS*	(Опционально.) Укажите значение внутреннего приоритета (inner priority). Диапазон значений: от 0 до 7.
MASK	(Опционально.) Укажите маску внутреннего приоритета (inner priority mask) (0x0-0x7). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
vlan *OUTER-VLAN*	(Опционально.) Укажите outer VLAN ID.
MASK	(Опционально.) Укажите маску outer VLAN ID (0x0-0xfff). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.

vlan-range *MIN-VID MAX-VID*	(Опционально.) Укажите диапазон VLAN.
inner *INNER-VLAN*	(Опционально.) Укажите inner VLAN ID.
MASK	(Опционально.) Укажите маску inner VLAN ID (0x0-0xfff). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
any	Укажите для использования любого MAC-адреса источника, любого MAC-адреса назначения, любого IP-адреса источника или любого IP-адреса назначения.
host *SRC-MAC-ADDR*	Укажите определенный MAC-адрес узла источника.
SRC-MAC-ADDR SRC-MAC-WILDCARD	Укажите группу MAC-адресов источника, используя значение битовой маски (wildcard). Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
host *DST-MAC-ADDR*	Укажите определенный MAC-адрес узла назначения.
DST-MAC-ADDR DST-MAC-WILDCARD	Укажите группу MAC-адресов назначения, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
host *SRC-IP-ADDR*	Укажите определенный IP-адрес узла источника.
SRC-IP-ADDR SRC-IP-WILDCARD	Укажите группу IP-адресов источника, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
host *DST-IP-ADDR*	Укажите определенный IP-адрес узла назначения.
DST-IP-ADDR DST-IP-WILDCARD	Укажите группу IP-адресов назначения, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
precedence *PRECEDENCE*	(Опционально.) Укажите, чтобы пакеты могли фильтроваться по уровню приоритета (precedence). Диапазон значений: от 0 до 7.
MASK	(Опционально.) Укажите маску приоритета (precedence mask) (0x0-0x7). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
tos *TOS*	(Опционально.) Укажите, чтобы пакеты могли фильтроваться по уровню type of service. Диапазон значений: от 0 до 15.
MASK	(Опционально.) Укажите маску ToS (0x0-0xf). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.

dscp *DSCP*	(Опционально.) Укажите DSCP-код для совпадений с заголовком IP. Диапазон значений: от 0 до 63 или выбор из следующих имен DSCP: af11 - 001010, af12 -001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 – 110000, cs7 - 111000, default (по умолчанию) - 000000, ef – 101110.
MASK	(Опционально.) Укажите маску DSCP (0x0-0x3f). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
lt *PORT*	(Опционально.) Укажите для сопоставления, если значение порта меньше указанного.
gt *PORT*	(Опционально.) Укажите для сопоставления, если значение порта больше указанного.
eq *PORT*	(Опционально.) Укажите для сопоставления, если значение порта равно указанному.
neq *PORT*	(Опционально.) Укажите для сопоставления, если значение порта не равно указанному.
range *MIN-PORT MAX-PORT*	(Опционально.) Укажите для сопоставления, если значение попадает в указанный диапазон портов.
mask *PORT MASK*	(Опционально.) Укажите для сопоставления портов, определенных маской. Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
TCP-FLAG	(Опционально.) Укажите поля TCP flag и указанные биты заголовка TCP с именем **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize) или **urg** (urgent).
fragments	(Опционально.) Укажите для фильтрации фрагментов пакета.
time-range *PROFILE-NAME*	(Опционально.) Укажите имя профиля временного интервала, связанного со списком доступа и определяющего период его активации.
ICMP-TYPE	(Опционально.) Укажите тип сообщения ICMP. Доступны номера типа сообщений от 0 до 255.
ICMP-CODE	(Опционально.) Укажите код сообщения ICMP. Доступны номера кода сообщений от 0 до 255.

ICMP-MESSAGE	(Опционально.) Укажите сообщение ICMP. Для выбора доступны следующие предустановленные параметры: beyond-scope, destination-unreachable, echo-reply, echo-request, header, hop-limit, mld-query, mld-reduction, mld-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, parameter-option, parameter-problem, port-unreachable, reassembly-timeout, redirect, renum-command, renum-result, renum-seq-number, router-advertisement, router-renumbering, router-solicitation, time-exceeded, unreachable.

По умолчанию

Нет.

Режим ввода команды

Extended Expert Access-list Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

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

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

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

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

4.18 permit | deny | deny-cpu (ip access-list)

Данная команда используется для добавления записи permit или deny. Чтобы удалить запись, воспользуйтесь формой **no** этой команды.

Расширенный список управления доступом (Extended Access List):

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

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

[*SEQUENCE-NUMBER***] {permit | deny | deny-cpu} 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* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

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

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

Стандартный список доступа IP (Standard IP Access List):

[*SEQUENCE-NUMBER***] {permit | deny | deny-cpu} {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. Диапазон значений: от 1 до 65535. Чем меньше номер, тем выше приоритет правила permit/deny.
any	Укажите для использования любого IP-адреса источника или IP-адреса назначения.

host *SRC-IP-ADDR*	Укажите определенный IP-адрес узла источника.
SRC-IP-ADDR *SRC-IP-WILDCARD*	Укажите группу IP-адресов источника, используя значение битовой маски (wildcard). Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
host *DST-IP-ADDR*	Укажите определенный IP-адрес узла назначения.
DST-IP-ADDR *DST-IP-WILDCARD*	Укажите группу IP-адресов назначения, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
precedence *PRECEDENCE*	(Опционально.) Укажите, чтобы пакеты могли фильтроваться по уровню приоритета (precedence). Доступны значения от 0 до 7.
MASK	(Опционально.) Укажите маску приоритета (precedence mask) (0x0-0x7). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
dscp *DSCP*	(Опционально.) Укажите DSCP-код для совпадений с заголовком IP. Диапазон значений: от 0 до 63 или выбор из следующих имен DSCP: af11 - 001010, af12 -001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default - 000000, ef - 101110.
MASK	(Опционально.) Укажите маску DSCP (0x0-0x3f). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
tos *TOS*	(Опционально.) Укажите, чтобы пакеты могли фильтроваться по уровню type of service. Доступны значения от 0 до 15.
MASK	(Опционально.) Укажите маску ToS (0x0-0xf). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
lt *PORT*	(Опционально.) Укажите для сопоставления, если значение порта меньше указанного.
gt *PORT*	(Опционально.) Укажите для сопоставления, если значение порта больше указанного.
eq *PORT*	(Опционально.) Укажите для сопоставления, если значение порта равно указанному.
neq *PORT*	(Опционально.) Укажите для сопоставления, если значение порта не равно указанному.

range *MIN-PORT MAX-PORT*	(Опционально.) Укажите для сопоставления, если значение попадает в указанный диапазон портов.
mask *PORT MASK*	(Опционально.) Укажите для сопоставления с портами, определенными маской. Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
TCP-FLAG	(Опционально.) Укажите поля TCP flag и указанные биты заголовка TCP с именем **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize) или **urg** (urgent).
fragments	(Опционально.) Укажите для фильтрации фрагментов пакета.
time-range *PROFILE-NAME*	(Опционально.) Укажите имя профиля временного интервала time-range, связанного со списком доступа и определяющего период его активации.
tcp, udp, icmp, igmp, ipinip, gre, esp, eigrp, ospf, pcp, pim, vrrp	Укажите протоколы 4 уровня.
PROTOCOL-ID	(Опционально.) Укажите Protocol ID. Диапазон значений: от 0 до 255. Чтобы запретить/разрешить protocol ID, укажите значение 255.
MASK	(Опционально.) Укажите маску protocol ID (0x0-0xff). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
ICMP-TYPE	(Опционально.) Укажите тип сообщения ICMP. Доступны номера для типа сообщений от 0 до 255.
ICMP-CODE	(Опционально.) Укажите код сообщения ICMP. Доступны номера для кода сообщений от 0 до 255.
ICMP-MESSAGE	(Опционально.) Укажите сообщение ICMP. Для выбора доступны следующие предустановленные параметры: administratively-prohibited, alternate-address, conversion-error, host-prohibited, net-prohibited, echo, echo-reply, pointer-indicates-error, host-isolated, host-precedence-violation, host-redirect, host-tos-redirect, host-tos-unreachable, host-unknown, host-unreachable, information-reply, information-request, mask-reply, mask-request, mobile-redirect, net-redirect, net-tos-redirect, net-tos-unreachable, net-unreachable, net-unknown, bad-length, option-missing, packet-fragment, parameter-problem, port-unreachable, precedence-cutoff, protocol-unreachable, reassembly-timeout, redirect-message, router-advertisement, router-solicitation, source-quench, source-route-failed, time-exceeded, timestamp-reply, timestamp-request, traceroute, ttl-expired, unreachable.

По умолчанию

Нет.

Режим ввода команды

IP Access-list Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

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

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

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

При создании правила сопоставления для стандартного списка доступа IP (IP standard access list) указываются только поля IP-адреса источника и назначения.

Пример

В данном примере показано, как создать 4 записи для расширенного списка доступа IP с названием «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 следующем примере показано, как создать 2 записи для стандартного списка доступа IP с названием «std-acl». Это следующие записи: разрешить IP-пакеты для сети 10.20.0.0, разрешить IP-пакеты для узла 10.100.1.2.

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

4.19 permit | deny | deny-cpu (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 | deny-cpu} tcp {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR/PREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDR/PREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] [***TCP-FLAG***] [dscp** *VALUE [MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny | deny-cpu} udp {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR/PREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDR/PREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] [dscp** *VALUE [MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny | deny-cpu} 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* **[***MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

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

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

Стандартный список доступа IPv6 (Standard IPv6 Access List):

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

no *SEQUENCE-NUMBER*

Параметры

SEQUENCE-NUMBER	Укажите порядковый номер. Диапазон значений: от 1 до 65535. Чем меньше номер, тем выше приоритет правила permit/deny.
any	Укажите для использования любого IPv6-адреса источника или IPv6-адреса назначения.
host *SRC-IPv6-ADDR*	Укажите определенный IPv6-адрес узла источника.

SRC-IPV6-ADDR/PREFIX-LENGTH	Укажите IPv6-адрес сети источника.
host *DST-IPV6-ADDR*	Укажите определенный IPv6-адрес узла назначения.
DST-IPV6-ADDR/PREFIX-LENGTH	Укажите IPv6-адрес сети назначения.
tcp, udp, icmp, esp, pcp ,sctp	Укажите тип протокола 4 уровня.
dscp *VALUE*	(Опционально.) Укажите совпадающее значение класса трафика в заголовке IPv6. Диапазон значений: 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.
MASK	(Опционально.) Укажите маску DSCP (0x0-0x3f). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
traffic-class *VALUE*	(Опционально.) Укажите значение совпадающего класса трафика в заголовке IPv6. Диапазон значений: от 0 до 255.
MASK	(Опционально.) Укажите маску класса трафика (0x0-0xff). Если значение не указано, используется 0xff.
lt *PORT*	(Опционально.) Укажите для сопоставления, если значение порта меньше указанного.
gt *PORT*	(Опционально.) Укажите для сопоставления, если значение порта больше указанного.
eq *PORT*	(Опционально.) Укажите для сопоставления, если значение порта равно указанному.
neq *PORT*	(Опционально.) Укажите для сопоставления, если значение порта не равно указанному.
range *MIN-PORT MAX-PORT*	(Опционально.) Укажите для сопоставления, если значение попадает в указанный диапазон портов.
mask *PORT MASK*	(Опционально.) Укажите для сопоставления с портами, определенными маской. Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
PROTOCOL-ID	(Опционально.) Укажите Protocol ID. Диапазон значений: от 0 до 255.

MASK	(Опционально.) Укажите маску Protocol ID (0x0-0xff). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
ICMP-TYPE	(Опционально.) Укажите тип сообщения ICMP. Доступны номера типа сообщений от 0 до 255.
ICMP-CODE	(Опционально) Укажите код сообщения ICMP. Доступны номера кода сообщений от 0 до 255.
ICMP-MESSAGE	(Опционально.) Укажите сообщение ICMP. Для выбора доступны следующие предустановленные параметры: beyond-scope, destination-unreachable, echo-reply, echo-request, erroneous_header, hop-limit, multicast-listener-query, multicast-listener-done, multicast-listener-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, parameter-option, parameter-problem, port-unreachable, reassembly-timeout, redirect, renum-command, renum-result, renum-seq-number, router-advertisement, router-renumbering, router-solicitation, time-exceeded, unreachable.
TCP-FLAG	(Опционально.) Укажите поля TCP flag и указанные биты заголовка TCP с именем **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize) или **urg** (urgent).
flow-label *FLOW-LABEL*	(Опционально.) Укажите значение flow label. Диапазон значений: от 0 до 1048575.
MASK	(Опционально.) Укажите маску flow label (0x0-0xfffff). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
fragments	(Опционально.) Укажите для фильтрации фрагментов пакета.
time-range *PROFILE-NAME*	(Опционально.) Укажите имя профиля временного интервала, связанного со списком доступа и определяющего период его активации.

По умолчанию

Нет.

Режим ввода команды

IPv6 Access-list Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

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

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

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

Пример

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

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

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

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

4.20 permit | deny | deny-cpu (mac access-list)

Данная команда используется для назначения правила, которое будет разрешать или запрещать продвижение пакетов. Чтобы удалить запись, воспользуйтесь формой **no** этой команды.

[*SEQUENCE-NUMBER***] {permit | deny | deny-cpu} {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* **[***MASK***] [inner** *INNER-COS* **[***MASK***]]] [{vlan** *VLAN-ID* **[***MASK***] | vlan-range** *MIN-VID MAX-VID***} [inner** *INNER-VLAN* **[***MASK***]]] [time-range** *PROFILE-NAME***]**

no *SEQUENCE-NUMBER*

Параметры

SEQUENCE-NUMBER	Укажите порядковый номер. Диапазон значений: от 1 до 65535. Чем меньше номер, тем выше приоритет правила permit/deny.
any	Укажите для использования любого MAC-адреса источника или MAC-адреса назначения.
host *SRC-MAC-ADDR*	Укажите определенный MAC-адрес узла источника.
SRC-MAC-ADDR SRC-MAC-WILDCARD	Укажите группу MAC-адресов источника, используя значение битовой маски (wildcard). Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
host *DST-MAC-ADDR*	Укажите определенный MAC-адрес узла назначения.
DST-MAC-ADDR DST-MAC-WILDCARD	Укажите группу MAC-адресов назначения, используя значение wildcard. Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
ethernet-type *TYPE MASK*	(Опционально.) Укажите Ethernet-тип фильтруемых пакетов в виде шестнадцатеричного числа с диапазоном значений от 0 до FFFF или используйте имя типа Ethernet. Доступны следующие имена: aarp, appletalk, decnet-iv, etype-6000, etype-8042, lat, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp или arp.
cos *VALUE*	(Опционально.) Укажите значение приоритета от 0 до 7.
MASK	(Опционально.) Укажите маску внешнего приоритета (outer priority mask) (0x0-0x7). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться. Если значение не указано, используется 0x7.
inner *INNER-COS*	(Опционально.) Укажите внутренний приоритет (inner priority). Диапазон значений: от 0 до 7.
MASK	(Опционально.) Укажите маску внутреннего приоритета (inner priority mask) (0x0-0x7). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN ID.
MASK	(Опционально.) Укажите маску outer VLAN ID (0x0-0x0fff). Если значение не указано, используется 0x0fff.
vlan-range *MIN-VID MAX-VID*	(Опционально.) Укажите диапазон VLAN.
inner *INNER-VLAN*	(Опционально) Укажите inner VLAN ID.

MASK	(Опционально.) Укажите маску inner VLAN ID (0x0-0x0fff). Если значение не указано, используется 0x0fff.
time-range *PROFILE-NAME*	(Опционально.) Укажите имя профиля временного интервала, связанного со списком доступа и определяющего период его активации.

По умолчанию

Нет.

Режим ввода команды

MAC Access-list Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

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

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

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

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

Пример

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

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

4.21 show access-group

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

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

В данном примере показано, как отобразить списки доступа, применяемые ко всем интерфейсам.

```
Switch#show access-group

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

Switch#
```

4.22 show access-list

Данная команда используется для отображения информации о настройках списка доступа.

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

Параметры

ip	(Опционально.) Укажите для отображения всех списков доступа IP.

mac	(Опционально.) Укажите для отображения всех списков доступа MAC.
ipv6	(Опционально.) Укажите для отображения всех списков доступа IPv6.
expert	(Опционально.) Укажите для отображения всех списков доступа expert.
arp	(Опционально.) Укажите для отображения всех списков доступа ARP.
NAME	(Опционально.) Укажите имя списка доступа для отображения.
NUMBER	(Опционально.) Укажите ID списка доступа для отображения.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о списках доступа. Если не указан определенный параметр, отображается перечень всех настроенных списков доступа. Если указан тип списка доступа, будет отображена подробная информация о соответствующем ему списке доступа. Если включен аппаратный счетчик ACL (ACL hardware counter) для списка доступа (access list), счетчик будет отображен на основе каждой записи списка доступа.

Пример

В данном примере показано, как отобразить все списки 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 примере ниже показано, как отобразить списки 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 следующем примере показано, как отобразить содержимое списка доступа с включенным аппаратным счетчиком.

```
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#
```

4.23 show vlan access-map

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

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

Параметры

MAP-NAME	(Опционально.) Укажите имя настраиваемой VLAN access map. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

В данном примере показано, как отобразить 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 отобразить содержимое VLAN access-map, если включен аппаратный счетчик.

```
Switch#show vlan access-map

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

Switch#
```

4.24 show vlan filter

Данная команда используется для отображения информации о настройках фильтрации VLAN для VLAN-интерфейсов.

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

Параметры

access-map *MAP-NAME*	(Опционально.) Укажите имя VLAN access-map. Максимальное количество символов – 32.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN ID.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

В данном примере показано, как отобразить информацию о фильтрации VLAN.

```
Switch#show vlan filter

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

Switch#

Switch#show vlan filter vlan 5

VLAN ID 5
  VLAN Access Map: aa

Switch#
```

4.25 vlan access-map

Данная команда используется, чтобы создать sub-map для VLAN access-map и войти в режим VLAN Access-map Sub-map Configure Mode. Для удаления access map или ее sub-map воспользуйтесь формой **no** этой команды.

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

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

Параметры

MAP-NAME	Укажите имя VLAN access-map. Максимальное количество символов – 32.
SEQUENCE-NUM	(Опционально.) Укажите порядковый номер sub-map. 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-map. Для каждой sub-map может быть указан один список доступа (IP access list, IPv6 access list или MAC access list) и одно действие. После создания VLAN access map пользователь может использовать команду **vlan filter** для применения access map к VLAN.

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

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

При использовании формы **no** без указания порядковых номеров будет удалена вся информация о sub-map указанной access map.

Пример

В данном примере показано, как создать VLAN access map.

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

4.26 vlan filter

Данная команда используется для применения VLAN access map к VLAN. Чтобы удалить VLAN access map, воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

5. Команды управления доступом

5.1 access-class

Данная команда используется для указания списка, которому необходимо ограничить доступ к сессии. Чтобы отменить проверку указанного списка доступа, воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

Line Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда применяется для указания списка, 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** данной команды.

Пример

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

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

5.2 banner login

Данная команда используется для входа в режим Banner Login Mode и настройки отображения баннера приветствия. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

banner login *cMESSAGEc*
no banner login

Параметры

c	Укажите разделитель текста баннера приветствия, например, знак решетки (#). Употребление символа-разделителя в тексте баннера приветствия недопустимо.
MESSAGE	Укажите текст баннера приветствия, отображаемый до появления приглашения на ввод имени пользователя и пароля.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить текст баннера, который будет отображаться после успешного входа пользователя в систему. После команды **banner login** введите как минимум один пробел и любой символ-разделитель на выбор. Далее введите одну или несколько строк текста, закончив сообщение вторым разделителем.

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



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

Пример

В данном примере показано, как настроить баннер приветствия. Символ «#» является разделителем. Первый разделитель, сообщение баннера и последний разделитель вводятся до первого нажатия клавиши Enter.

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

В примере ниже показано, как настроить баннер приветствия. Символ «#» является разделителем. Только первый разделитель вводится до первого нажатия клавиши Enter.

```
Switch#configure terminal
Switch(config)#banner login #
Enter TEXT message.  End with the character '#'.
Enter Command Line Interface
#
Switch(config)#
```

5.3 do

Данная команда используется для выполнения команд, изначально находящихся в режиме User/Privileged EXEC Mode, из режима глобальной конфигурации или других режимов конфигурации.

do *COMMAND*

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для выполнения команд, изначально находящихся в режиме User/Privileged EXEC Mode (таких как **show**, **clear** или **debug**) при настройке коммутатора. После выполнения команды произойдет возврат системы к используемому режиму конфигурации.



Примечание: в команде можно использовать знак вопроса (?) и клавишу Tab.

Пример

В данном примере показано, как выполнить команду **show privilege** в режиме Global Configuration Mode.

```
Switch#configure terminal
Switch(config)#do show privilege

Current privilege level is 15

Switch(config)#
```

5.4 prompt

Данная команда используется для изменения приглашения на ввод команды в командной строке CLI. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

prompt *STRING*
no prompt

Параметры

STRING	Укажите строку для определения настраиваемой подсказки. Подсказка будет основываться на определенных символах или следующих символах управления (пробел в строке игнорируется): **%h** – подстановка имени сервера SNMP; **%s** – пробел; **%%** – подстановка символа %.

По умолчанию

По умолчанию в строке зашифровано имя SNMP-сервера.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для настройки приглашения командной строки. Если в качестве приглашения выбрать зашифрованное имя сервера SNMP, то зашифрованы будут только первые 15 символов. Подсказка может отобразить только 15 символов. Символ уровня привилегий в приглашении будет отображаться последним.

Символы определяются по следующим правилам:

> – для приглашения пользовательского режима;

– для приглашения привилегированного режима.

Пример

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

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

5.5 enable password

Данная команда используется, чтобы включить пароль для входа на различные уровни привилегии. Для возврата к пустому значению воспользуйтесь формой **no** этой команды.

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

Параметры

level *PRIVILEGE-LEVEL*	(Опционально.) Укажите уровень привилегий пользователя в диапазоне от 1 до 15. Если данный параметр не указан или используется форма **no**, уровнем по умолчанию считается 15.
0	(Опционально.) Укажите пароль в открытом незашифрованном тексте. Пароль чувствителен к регистру и может содержать от 1 до 32 символов, а также пробелы. Если невозможно указать синтаксис пароля, остается незашифрованный текст.
7	(Опционально.) Укажите зашифрованный пароль на основе SHA-1. Длина пароля ограничена 35 байтами. Пароль чувствителен к регистру и зашифрован. Если синтаксис пароля не указан, используется незашифрованный текст.
15	(Опционально.) Укажите зашифрованный пароль на основе MD5. Длина пароля ограничена 31 байтом. Пароль чувствителен к регистру и зашифрован. Если синтаксис пароля не указан, используется незашифрованный текст.
PASSWORD	Укажите пароль для пользователя.

По умолчанию

По умолчанию пароль не задан. Данная строка остается пустой.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

В привилегированном режиме для входа на определенный уровень привилегий используется соответствующий данному уровню пароль. Для каждого уровня можно задать только один пароль.

Пример

В данном примере показано, как назначить пароль «MyEnablePassword» для уровня привилегий 15.

```
Switch#configure terminal
Switch(config)#enable password MyEnablePassword
Switch(config)#
```

5.6 ip http server

Данная команда используется для включения сервера HTTP. Чтобы отключить сервер HTTP, воспользуйтесь формой **no** этой команды.

ip http server
no ip http server

Параметры

Нет.

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для включения сервера HTTP. Управление интерфейсом доступа HTTPS выполняется отдельно с помощью команд SSL.

Пример

В данном примере показано, как включить сервер HTTP.

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

5.7 ip http secure-server

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

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

Параметры

ssl-service-policy *NAME*	*POLICY-*	(Опционально.) Укажите имя политики сервиса SSL. Используйте параметр **ssl-service-policy**, только если политика сервиса SSL уже указана с помощью команды **ssl-service-policy**.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда позволяет включить сервер HTTPS и использовать определенную политику сервиса SSL для HTTPS. Если данный параметр не указан, для HTTPS будет использоваться встроенный локальный сертификат.

Пример

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

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

5.8 ip {http | https} access-class

Данная команда позволяет назначить список, которому необходимо ограничить доступ к HTTP- или HTTPs-серверу. Для отмены проверки указанного списка доступа воспользуйтесь формой **no** этой команды.

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

Параметры

IP-ACL	Укажите стандартный список доступа IP-адресов. Поле адреса источника в правиле определяет, является ли узел доверенным.

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- или HTTPS-серверу. Если указанный список доступа не существует, команда не будет выполнена и ни один из списков доступа не будет проверяться при доступе к HTTP или HTTPS.

Пример

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

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

5.9 ip http service-port

Данная команда позволяет указать порт для HTTP-соединения. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

TCP-PORT	Укажите номер порта TCP в диапазоне от 1 до 65535. Как правило,

	для протокола HTTP назначается TCP-порт 80.

По умолчанию

По умолчанию используется порт 80.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

5.10 ip http timeout-policy idle

Данная команда позволяет задать значение тайм-аута для подключения к серверу HTTP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

INT	Укажите значение таймера. Диапазон значений: от 60 до 36000 секунд.

По умолчанию

По умолчанию значение составляет 180 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы задать значение тайм-аута для подключения к серверу HTTP.

Пример

В данном примере показано, как настроить тайм-аут. Заданное значение – 100 секунд.

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

5.11 ip telnet server

Данная команда используется для включения сервера Telnet. Чтобы отключить сервер Telnet, воспользуйтесь формой **no** этой команды.

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.

Пример

В данном примере показано, как включить сервер Telnet.

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

5.12 ip telnet service port

Данная команда используется, чтобы задать порт, используемый Telnet-сервером. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

TCP-PORT	Укажите номер TCP-порта. Диапазон значений: 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

Используйте данную команду, чтобы указать TCP-порт для доступа по Telnet.

Пример

В данном примере показано, как настроить сервисный порт 3000 для Telnet.

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

5.13 line

Данная команда используется, чтобы задать тип сессии для конфигурации и войти в режим Line Configuration Mode.

line {console | telnet | ssh}

Параметры

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

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда позволяет войти в режим Line Configuration Mode.

Пример

В данном примере показано, как войти в режим Line Configuration Mode для сессии терминала SSH и настроить класс 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. Для отключения данной функции воспользуйтесь формой **no** этой команды.

service password-recovery
no service password-recovery

Параметры

Нет.

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить функцию восстановления пароля. Функция восстановления пароля включена по умолчанию.

Пример

В данном примере показано, как отключить функцию восстановления пароля.

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

5.15 service password-encryption

Данная команда используется, чтобы включить шифрование пароля перед сохранением в файле конфигурации. Для отключения шифрования воспользуйтесь формой **no** этой команды.

service password-encryption [7 | 15]

no service password-encryption

Параметры

7	(Опционально.) Укажите пароль, зашифрованный на основе SHA-1. Если параметр не указан, это опция по умолчанию.
15	(Опционально.) Укажите пароль, зашифрованный на основе MD5.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

Если функция 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 без возможности обратного перевода в простую текстовую форму.

Данная команда применяется к паролю учетной записи пользователя, паролю для повышенного уровня привилегий (enable) и паролю аутентификации.

Пример

В данном примере показано, как включить шифрование пароля перед сохранением в файле конфигурации.

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

5.16 show terminal

Данная команда используется, чтобы отобразить информацию о настройках параметров конфигурации терминала для текущей сессии терминала.

show terminal

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о настройках терминала для текущей сессии.

Пример

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

```
Switch#show terminal
Terminal Settings:
 Length: 24 lines
 Width: 80 columns
 Default Length: 24 lines
 Default Width: 80 columns
 Baud Rate: 115200 bps

Switch#
```

5.17 show ip telnet server

Данная команда используется для отображения информации о состоянии сервера Telnet.

show ip telnet server

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения информации о состоянии сервера Telnet.

Пример

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

```
Switch#show ip telnet server

Server State: Enabled

Switch#
```

5.18 show ip http server

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

show ip http server

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

```
Switch#show ip http server

ip http server state :  Enabled
Switch#
```

5.19 show ip http secure-server

Данная команда используется для отображения информации о состоянии SSL.

show ip http secure-server

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения информации о состоянии SSL.

Пример

В данном примере показано, как отобразить информацию о состоянии SSL.

```
Switch#show ip http secure-server

ip http secure-server state :  Disabled
Switch#
```

5.20 show password-recovery

Данная команда используется для отображения настроек восстановления пароля.

show password-recovery

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения настроек восстановления пароля.

Пример

В данном примере показано, как отобразить настройки восстановления пароля.

```
Switch#show password-recovery

 Running Configuration  :Enabled
 NV-RAM Configuration   :Enabled

Switch#
```

5.21 show users

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

show users

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

```
Switch#show users

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

Total Entries: 3

Switch#
```

5.22 telnet

Данная команда используется для подключения к другому устройству с поддержкой Telnet.

telnet {*IP-ADDRESS* **|** *IPV6-ADDRESS* **|** *DOMAIN-NAME***} [***TCP-PORT***]**

Параметры

IP-ADDRESS	Укажите IPv4-адрес узла.
IPV6-ADDRESS	Укажите IPv6-адрес узла.
DOMAIN-NAME	Укажите имя узла назначения Telnet.
TCP-PORT	(Опционально.) Укажите номер TCP-порта. Диапазон значений: 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.
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 показано, как подключиться к IP-адресу 10.90.90.91 с помощью порта 23. IP-адрес 10.90.90.91 является интерфейсом управления DGS-1520-28MP, позволяющим пользователю войти в учетную запись.

```
Switch#telnet 10.90.90.91

                DGS-1520-28 Gigabit Ethernet Smart Managed Switch

                          Command Line Interface
                         Firmware: Build 1.00.022
          Copyright(C) 2020 D-Link Corporation. All rights reserved.

User Access Verification

Username:
```

В следующем примере показана неудачная попытка подключения по Telnet к IP-адресу 10.90.90.91 через порт 23. Далее для входа в интерфейс управления используется порт 3500.

```
Switch#telnet 10.90.90.91 23

 ERROR: Could not open a connection to host on server port 23.
Switch#telnet 10.90.90.91 3500

                    DGS-3630-28TC Gigabit Ethernet Switch

                          Command Line Interface
                         Firmware: Build 2.20.B007
          Copyright(C) 2018 D-Link Corporation. All rights reserved.

Password required, but none set

Switch#
```

5.23 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. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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

Параметры

NUMBER	Укажите количество строк, отображаемых на экране. Диапазон значений: от 0 до 512. При значении 0 отображение не прекратится, пока не будет достигнут конец отображаемого материала.

По умолчанию

Значение по умолчанию – 24.

Режим ввода команды

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

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

Уровень команды по умолчанию

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

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

Использование команды

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

Если в команде **terminal length** указано значение, отличное от 0 (например, 50), то вывод приостанавливается после каждых 50 строк. Используйте данную команду, чтобы настроить количество отображаемых строк во время текущей сессии. Команда также применяется для сессий Telnet и SSH. Доступны значения от 0 до 512. По умолчанию используется значение 24. При выборе 0 коммутатор будет автоматически выводить всю информацию без пауз.

Если вывод одной команды выходит за границы экрана, то такой вывод приостанавливается и в нижней части экрана появляется приглашение **--More--**. При появлении приглашения **--More--** нажмите CTRL+C, q, Q или ESC, чтобы прервать вывод и вернуться к приглашению. Нажмите пробел для отображения дополнительного экрана вывода или нажмите Return для отображения еще одной строки вывода. При настройке длины экрана на 0 отключается функция прокручивания, из-за чего весь вывод

экрана отображается сразу. Пока не будет использовано ключевое слово **default**, изменения значения terminal length будут применяться только к текущей сессии. При использовании формы **no** данной команды количество строк на экране терминала сбрасывается к 24.

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

Пример

В данном примере показано, как изменить количество строк. Указанное значение – 60.

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

5.24 terminal speed

Данная команда используется для настройки скорости терминала. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

terminal speed *BPS*
no terminal speed

Параметры

BPS	Укажите 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 применяется для настройки скорости подключения терминала. Некоторые скорости передачи данных, доступные на подключенных устройствах, не поддерживаются коммутатором.

Пример

В данном примере показано, как изменить скорость последовательного порта, указав значение 9600 бит/с.

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

5.25 session-timeout

Данная команда используется, чтобы задать значение тайм-аута сессии. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

session-timeout *MINUTES*
no session-timeout

Параметры

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

По умолчанию

Значение по умолчанию – 3 минуты.

Режим ввода команды

Line Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы задать значение тайм-аута сессии, по истечении которого произойдет автоматический выход из учетной записи.

Пример

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

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

5.26 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. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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

Параметры

NUMBER	Укажите количество символов, отображаемых на экране. Диапазон значений: от 40 до 255.

По умолчанию

Значение по умолчанию – 80.

Режим ввода команды

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

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

Уровень команды по умолчанию

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

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

Использование команды

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

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

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

Пример

В данном примере показано, как изменить текущую ширину терминала, указав значение 120.

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

5.27 username

Данная команда используется для создания учетной записи пользователя. Чтобы удалить учетную запись пользователя, воспользуйтесь формой **no** этой команды.

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

no username [*NAME***]**

Параметры

NAME	Укажите имя пользователя. Максимальное количество символов – 32.
privilege *LEVEL*	(Опционально.) Укажите уровень привилегий для каждого пользователя. Диапазон значений: от 1 до 15. Если параметр не указан, используется значение 1.
nopassword	(Опционально.) Укажите, чтобы для данной учетной записи не применялся пароль.
password	(Опционально.) Укажите, чтобы для данной учетной записи применялся пароль.
0	(Опционально.) Укажите пароль в обычном текстовом виде. Пароль может содержать от 1 до 32 символов. Допустимо использование пробелов. Допустимо использование пробелов. Пароль чувствителен к регистру. Если синтаксис пароля не указан, используется обычный текст.
7	(Опционально.) Укажите пароль, зашифрованный на основе SHA-1. Длина пароля ограничена 35 байтами. Пароль чувствителен к регистру. Пароль зашифрован. Если синтаксис пароля не указан, используется обычный текст.
15	(Опционально.) Укажите пароль, зашифрованный на основе MD5. Длина пароля ограничена 31 байтом. Пароль чувствителен к регистру. Пароль зашифрован. Если синтаксис пароля не указан, используется обычный текст.
PASSWORD	(Опционально.) Укажите пароль на основе одного из указанных выше параметров.

По умолчанию

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

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда применяется для создания учетной записи пользователя с различными уровнями

доступа. При входе в систему с уровнем привилегий 1 будет включен режим User EXEC Mode. Чтобы перейти в режим Privileged EXEC Mode, необходимо использовать команду **enable**.

Если вход совершается с уровнем привилегий 2 или выше, пользователь сразу же будет переведен в режим Privileged EXEC Mode. Данный режим доступен уровням от 2 до 15.

Пользователь может указать пароль в зашифрованной форме или в виде обычного текста. Пароль, который был задан в виде обычного текста, при включенной функции шифрования пароля будет изменен на зашифрованный.

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

По умолчанию учетная запись пользователя пустая. Когда учетная запись пустая, пользователю будет сразу назначен режим User EXEC Mode и уровень 1. После этого пользователь может перейти в режим Privileged EXEC Mode с помощью команды **enable**.

Пример

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

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

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

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

5.28 password

Данная команда используется для создания нового пароля. Чтобы удалить пароль, воспользуйтесь формой **no** этой команды.

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

Параметры

0	(Опционально.) Укажите пароль в обычном текстовом виде. Пароль может содержать от 1 до 32 символов. Допустимо использование пробелов. Пароль чувствителен к регистру. Если синтаксис пароля не указан, используется обычный текст.
7	(Опционально.) Укажите пароль, зашифрованный на основе SHA-1. Длина пароля ограничена 35 байтами. Пароль чувствителен к регистру. Пароль зашифрован. Если синтаксис пароля не указан, используется обычный текст.

15	(Опционально.) Укажите пароль, зашифрованный на основе MD5. Длина пароля ограничена 31 байтами. Пароль чувствителен к регистру. Пароль зашифрован. Если синтаксис пароля не указан, используется обычный текст.
PASSWORD	Укажите 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 показано, как создать пароль для сессии консоли.

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

5.29 clear line

Данная команда используется для завершения сессии подключения.

clear line *LINE-ID*

Параметры

LINE-ID	Укажите идентификатор line ID сессии соединения, которую необходимо отключить.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда применяется для отключения активной сессии коммутатора. Идентификатор (line ID) присваивается при создании сессии подключения. Используйте команду **show users** для просмотра активных сессий.

Данная команда может отключить только сессии SSH и Telnet.

Пример

В данном примере показано, как отключить сессию 1.

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

5.30 banner exec

Данная команда используется для настройки текста баннера, отображаемого при входе в режим EXEC. Чтобы удалить настроенный баннер EXEC, воспользуйтесь формой **no** этой команды.

banner exec *cMESSAGEc*
no banner exec

Параметры

c	Укажите разделитель текста баннера EXEC, например, знак решетки (#). Употребление символа-разделителя в тексте баннера приветствия недопустимо.
MESSAGE	Укажите текст баннера EXEC, отображаемый после появления приглашения на ввод имени пользователя и пароля, но до входа в режим EXEC Mode.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для настройки баннера, отображаемого перед приглашением на вход в режим EXEC Mode.

При настройке сообщения баннера разрешается использовать специальные символы со знаком $ для отображения текущей конфигурации или системной информации:

- **$(hostname)** – строка, используемая для подсказки;
- **$(line)** – идентификатор сессии (line ID).

Пример

В данном примере показано, как настроить баннер EXEC. Вместо маркера ($) будет подставлена соответствующая информация.

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

5.31 exec-banner

Данная команда позволяет включить отображение баннера EXEC в указанных сессиях. Чтобы отключить отображение баннера EXEC, воспользуйтесь формой **no** этой команды.

exec-banner
no exec-banner

Параметры

Нет.

По умолчанию

По умолчанию баннер отображается во всех типах сессий.

Режим ввода команды

Line Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда определяет, будет ли коммутатор отображать баннер EXEC при создании сессии EXEC.

Пример

В данном примере показано, как отключить отображение баннера EXEC при установлении сессии SSH.

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

5.32 outgoing-session-timeout

Данная команда позволяет задать значение таймаута исходящей сессии. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

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

Параметры

MINUTES	Укажите тайм-аут в минутах. При использовании значения 0 тайм-аут не истекает никогда. Диапазон значений: от 0 до 1439.

По умолчанию

Значение по умолчанию – 0.

Режим ввода команды

Line Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда позволяет задать значение тайм-аута исходящей сессии, используемое для отключения исходящих Telnet-соединений с другим устройством с помощью командной строки коммутатора.
Если тайм-аут истечет при подключении по виртуальной линии (Telnet/SSH), сессия вернется к режиму Privileged EXEC Mode.
Если тайм-аут истечет при подключении по физической линии (подключение к консоли коммутатора), произойдет выход из сессии и сеанс подключения будет возвращен в режим ожидания.
Функция тайм-аута исходящей сессии имеет более высокий приоритет, чем функция тайм-аута (подключения к коммутатору), настроенная с помощью команды **session-timeout**. Локальная сессия не может быть закрыта, если исходящая сессия еще активна.

Пример

В данном примере показано, как настроить значение тайм-аута исходящей сессии для SSH.

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

5.33 terminal monitor

Данная команда используется для включения сообщений отладки (debug) и системного журнала (system log) для текущих сессий Telnet/SSH. Используйте форму **no**, чтобы отключить данную функцию.

terminal monitor
terminal no monitor

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для включения/отключения сообщений отладки и системного журнала для текущих сессий Telnet/SSH.

Пример

В данном примере показано, как включить сообщения отладки и системного журнала для текущей сессии Telnet/SSH.

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

6. Команды предотвращения атак ARP Spoofing

6.1 ip arp spoofing-prevention

Данная команда используется для настройки записи ARP Spoofing Prevention (ASP), используемой для предотвращения атак ARP Spoofing. Для удаления записи ARP Spoofing Prevention воспользуйтесь формой **no** этой команды.

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

Параметры

GATEWAY-IP	Укажите IP-адрес шлюза.
GATEWAY-MAC	Укажите MAC-адрес шлюза. Настройки MAC-адреса заменят последнюю конфигурацию для того же IP-адреса шлюза.
interface *INTERFACE-ID*	Укажите интерфейс, который будет активирован или удален из числа активных интерфейсов (при использовании формы **no**). Запись ARP не будет проверяться, если принимающий порт не включен в указанный список интерфейсов.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) 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 применима исключительно для настройки интерфейсов физического порта и port-channel.Команда используется для создания записи ARP Spoofing Prevention (ASP), чтобы предотвратить спуфинг MAC-адреса защищенного шлюза. После создания записи ARP-пакеты, у которых IP-адрес источника совпадает с IP-адресом шлюза, а MAC-адрес источника не совпадает с MAC-адресом шлюза, будут отбрасываться. ASP игнорирует ARP-пакеты, если IP-адрес источника не совпадает с настроенным IP-адресом шлюза.

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

Пример

В данном примере показано, как настроить запись ARP Spoofing Prevention с IP-адресом 10.254.254.251 и MAC-адресом 00-00-00-11-11-11 для Ethernet-порта 1/0/10.

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

6.2 ip arp spoofing-prevention logging enable

Данная команда используется для включения логирования информации об атаках, если IP-адрес, с которого производится атака, совпадает с адресом шлюза. Для отключения функции воспользуйтесь формой **no** этой команды.

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

Параметры

Нет.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для включения или отключения логирования информации об атаках, если IP-адрес, с которого производится атака, совпадает с адресом шлюза.

Пример

В данном примере показано, как включить логирование информации об атаках, если IP-адрес, с которого производится атака, совпадает со шлюзом.

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

6.3 show ip arp spoofing-prevention

Данная команда используется для отображения настроек ARP Spoofing Prevention.

show ip arp spoofing-prevention

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения всех записей ARP Spoofing Prevention.

Пример

В данном примере показано, как отобразить записи 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 включения функции Asymmetric VLAN. Для отключения функции воспользуйтесь формой **no** этой команды.

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

Данная команда применяется для включения/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 позволяет настроить список методов аккаунтинга, используемый для всех команд на указанном уровне привилегий. Для удаления списка методов аккаунтинга воспользуйтесь формой **no** этой команды.

aaa accounting commands *LEVEL* **{default |** *LIST-NAME***} start-stop** *METHOD1* **[***METHOD2***…] | none}**

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

Параметры

LEVEL	Укажите уровень привилегий, на котором необходимо активировать аккаунтинг для всех команд **configure**. Допустимые уровни привилегий: от 1 до 15.
default	Укажите для использования списка методов аккаунтинга по умолчанию.
LIST-NAME	Укажите название списка методов (не более 32 символов).
start-stop	Укажите для отправки accounting-сообщений при входе и выходе из системы. Пользователям разрешен доступ к сети независимо от того, успешно ли активирован акккаунтинг при отправке начального accounting-сообщения.
METHOD1 **[***METHOD2***...]**	Укажите список методов, который необходимо выполнить алгоритму аккаунтинга в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода. **group tacacs+** – используются серверы, определенные командой TACACS+ server host. **group** *GROUP-NAME* – используются группы серверов, определенных командой **aaa group server tacacs+**.
none	Укажите, чтобы аккаунтинг не выполнялся.

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 привилегий 15, используя TACACS+, который будет отправлять accounting-сообщения, когда пользователь входит и выходит из системы.

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

8-2 aaa accounting exec

Данная команда позволяет настроить список методов, используемый для аккаунтинга сессий EXEC для конкретного терминала. Для отключения аккаунтинга EXEC воспользуйтесь формой **no** этой команды.

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

Параметры

default	Укажите для использования списка методов аккаунтинга EXEC по умолчанию.
LIST-NAME	Укажите название списка методов (не более 32 символов).
start-stop	Укажите для отправки accounting-сообщений при входе и выходе из системы. Пользователям будет разрешен доступ независимо от того, успешно ли активирован акккаунтинг при отправке начального accounting-сообщения.
METHOD1 **[***METHOD2***...]**	Укажите список методов, который 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** – используются серверы, определенные командой RADIUS server host. **group tacacs+** – используются серверы, определенные командой TACACS+ server host. **group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server.
none	Укажите, чтобы аккаунтинг не выполнялся.

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 для аккаунтинга действий пользователей, используя RADIUS, который будет отправлять accounting-сообщения, когда пользователь входит и выходит из системы.

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

8.3 aaa accounting network

Данная команда позволяет настроить список методов аккаунтинга, используемый для всех команд на определенном уровне привилегий. Для удаления списка методов аккаунтинга воспользуйтесь формой **no** этой команды.

aaa accounting network default {start-stop *METHOD1* **[***METHOD2***…] | none}**
no aaa accounting network default

Параметры

network	Укажите для выполнения аккаунтинга сервисных запросов, касающихся сети.
default	Укажите для настройки списка методов аккаунтинга по умолчанию.
start-stop	Укажите для отправки accounting-сообщений при входе и выходе из системы. Пользователям будет разрешен доступ к сети независимо от того, успешно ли активирован акккаунтинг при отправке начального accounting-сообщения.

METHOD1 **[***METHOD2***...]**	Укажите список методов, который 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** – используются серверы, определенные командой RADIUS server host. **group tacacs+** – используются серверы, определенные командой TACACS+ server host. **group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server.
none	Укажите, чтобы аккаунтинг не выполнялся.

По умолчанию

Метод аккаунтинга AAA не настроен.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду для настройки списка методов аккаунтинга для платы за обеспечение доступа к сети. Чтобы список методов по умолчанию вступил в силу, предварительно включите AAA, используя команду **aaa new-model**. Система аккаунтинга выключена, если 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, когда пользователь входит и выходит из системы.

```
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 системных событий. Для удаления списка методов аккаунтинга воспользуйтесь формой **no** этой команды.

aaa accounting system default {start-stop *METHOD1* **[***METHOD2***…] | none}**

no aaa accounting system default

Параметры

system	Укажите для выполнения аккаунтинга событий системного уровня.
default	Укажите для настройки списка методов аккаунтинга по умолчанию.
start-stop	Укажите для отправки accounting-сообщений при входе и выходе из системы. Пользователям будет разрешен доступ к сети независимо от того, успешно ли активирован акккаунтинг при отправке начального accounting-сообщения.
METHOD1 **[***METHOD2***...]**	Укажите список методов, который 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** – используются серверы, определенные командой RADIUS server host. **group tacacs+** – используются серверы, определенные командой TACACS+ server host. **group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server.
none	Укажите, чтобы аккаунтинг не выполнялся.

По умолчанию

Метод аккаунтинга AAA не настроен.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда позволяет настроить список методов аккаунтинга для системных событий, таких как перезагрузка, восстановление заводских настроек по умолчанию и т. п. Чтобы список методов по умолчанию вступил в силу, предварительно включите AAA, используя команду **aaa new-model**. Система аккаунтинга отключена, если список методов по умолчанию не настроен.

Пример

В данном примере показано, как включить аккаунтинг системных событий, 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, чтобы настроить список методов аутентификации по умолчанию для определения доступа к привилегированному уровню EXEC. Для удаления списка методов по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

METHOD1 **[***METHOD2***...]**	Укажите список методов, который необходимо выполнить алгоритму аутентификации в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода. **enable** – для аутентификации используется локальный пароль. **group radius** – используются серверы, определенные командой RADIUS server host. **group tacacs+** – используются серверы, определенные командой TACACS+ server host. **group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server. **none** – как правило, данный метод указывается в списке последним. Пользователь пройдет аутентификацию, если это не запрещено 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, чтобы настроить список методов аутентификации по умолчанию для определения доступа к привилегированному уровню EXEC при вводе команды **enable [privilege** *LEVEL***]**. Аутентификация с использованием RADIUS-сервера основана на уровне привилегий и использует «enable12» или «enable15» в качестве имени пользователя.

Пример

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

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

8.6 aaa authentication dot1x

Данная команда позволяет настроить список методов по умолчанию, используемый для аутентификации 802.1X. Для удаления списка методов по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

METHOD1 **[***METHOD2***...]**	Укажите список методов, который необходимо выполнить алгоритму аутентификации в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода. **local** – для аутентификации используется локальная база данных. **group radius** – используются серверы, определенные командой RADIUS server host. **group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server. **none** – как правило, данный метод указывается в списке последним. Пользователь пройдет аутентификацию, если это не запрещено 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, чтобы настроить список методов по умолчанию для аутентификации 802.1X. Аутентификация запросов 802.1X будет выполняться на основе локальной базы данных.

Пример

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

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

8.7 aaa authentication igmp-auth

Данная команда позволяет настроить список методов по умолчанию, используемый для аутентификации IGMP. Для удаления списка методов по умолчанию воспользуйтесь формой **no** этой команды.

aaa authentication igmp-auth default group radius
no aaa authentication igmp-auth default

Параметры

Нет.

По умолчанию

Метод ведения учета AAA не настроен.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы настроить список методов 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 аутентификации при входе в систему. Для удаления списка методов воспользуйтесь формой **no** этой команды.

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

Параметры

default	Укажите, чтобы использовать для аутентификации список методов по умолчанию.
LIST-NAME	Укажите название списка методов, отличного от списка методов по умолчанию. Максимальное количество символов – 32.
METHOD1 **[***METHOD2***...]**	Укажите список методов, который необходимо выполнить алгоритму аутентификации в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода. **local** – для аутентификации используется локальная база данных. **group radius** – используются серверы, определенные командой RADIUS server host. **group tacacs+** – используются серверы, определенные командой TACACS+ server host. **group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server. **none** – как правило, данный метод указывается в списке последним. Пользователь пройдет аутентификацию, если это не запрещено 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 позволяет настроить список методов, используемый для аутентификации при входе в систему. Можно настроить несколько списков методов. Для определения списка по умолчанию используется параметр **default**.

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

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

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

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

Пример

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

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

8.9 aaa authentication mac-auth

Данная команда позволяет настроить список методов по умолчанию, используемый для аутентификации по MAC-адресам. Для удаления списка методов по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

METHOD1 **[***METHOD2***...]**	Укажите список методов, который необходимо выполнить алгоритму аутентификации в данной последовательности. Введите от одного до четырех методов. Ниже приведены ключевые слова, которые могут использоваться для указания метода. **local** – для аутентификации используется локальная база данных. **group radius** – используются серверы, определенные командой RADIUS server host. **group** *GROUP-NAME* – используются группы серверов, определенные командой AAA group server. **none** – как правило, данный метод указывается в списке последним. Пользователь пройдет аутентификацию, если это не запрещено 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 позволяет настроить список методов по умолчанию, используемый для аутентификации по MAC-адресам. Изначально список методов по умолчанию не настроен. Аутентификация запросов MAC будет выполняться на основе локальной базы данных.

Пример

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

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

8.10 aaa authentication web-auth

Данная команда позволяет настроить список методов по умолчанию, используемый для web-аутентификации. Для удаления списка методов по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

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

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 позволяет настроить список методов по умолчанию, используемый для web-аутентификации. Изначально список методов по умолчанию не настроен. Аутентификация запросов web-auth будет выполняться на основе локальной базы данных.

Пример

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

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

8.11 aaa group server radius

Данная команда используется для входа в режим настройки группы серверов RADIUS и привязки серверов к группе. Для удаления группы серверов RADIUS воспользуйтесь формой **no** этой команды.

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

Параметры

GROUP-NAME	Укажите название группы серверов. Максимальное количество символов – 32. Синтаксисом является обычная строка, пробелы недопустимы.

По умолчанию

Группа серверов AAA не настроена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда позволяет определить группу серверов RADIUS. Созданная группа серверов используется для установки списков методов, используемых для аутентификации или аккаунтинга с помощью команд **aaa authentication** и **aaa accounting**. Также команда применяется, чтобы войти в режим настройки группы серверов RADIUS (RADIUS Group Server Configuration Mode). Используйте команду **server** для привязки серверов RADIUS к группе.

Пример

В данном примере показано, как создать группу серверов RADIUS с двумя записями. Второй узел выступает в качестве резервного сервера.

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

8.12 aaa group server tacacs+

Данная команда используется для входа в режим настройки группы серверов TACACS+ и привязки серверов к группе. Для удаления группы серверов TACACS+ воспользуйтесь формой **no** этой команды.

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

Параметры

GROUP-NAME	Укажите название группы серверов. Максимальное количество символов – 32. Синтаксисом является обычная строка, 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, чтобы войти в режим настройки группы серверов TACACS+. Для привязки серверов TACACS+ к группе применяется команда **server**. Заданная группа серверов может быть указана в качестве списка методов для аутентификации или аккаунтинга с помощью команд **aaa authentication** и **aaa accounting**.

Пример

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

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

8.13 aaa new-model

Данная команда используется, чтобы включить функцию AAA для аутентификации и аккаунтинга. Для отключения данной функции воспользуйтесь формой **no** этой команды.

aaa new-model
no aaa new-model

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

Пример

В данном примере показано, как включить функцию AAA.

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

8.14 aaa server radius dynamic-author

Данная команда используется для настройки коммутатора в качестве сервера AAA, чтобы обеспечить взаимодействие с внешним сервером политик. Для отключения функции воспользуйтесь формой **no** этой команды.

aaa server radius dynamic-author

no aaa server radius dynamic-author

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Динамическая авторизация позволяет внешнему серверу политик динамически отправлять обновления авторизации на устройство. Используйте команду для настройки коммутатора в качестве сервера AAA, а также для входа в режим Dynamic Authorization Local Server Configuration Mode.

Пример

В примере показано, как войти в режим Dynamic Authorization Local Server Configuration Mode.

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

8.15 accounting commands

Данная команда позволяет настроить список методов, используемый для аккаунтинга команд через конкретную сессию. Для отключения аккаунтинга команд воспользуйтесь формой **no** этой команды.

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

no accounting commands *LEVEL*

Параметры

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

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Line Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

Пример

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

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

8.16 accounting exec

Данная команда позволяет настроить список методов, используемый для аккаунтинга EXEC для конкретной сессии. Чтобы отключить данную опцию, воспользуйтесь формой **no** этой команды.

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

Параметры

default	Укажите для использования списка методов по умолчанию.
METHOD-LIST	Укажите название списка методов.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Line Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Для вступления в силу аккаунтинга по списку методов предварительно включите функцию AAA с помощью команды **aaa new-model**. Заранее создайте список методов, используя команду **aaa accounting exec**. Если список методов отсутствует, команда не будет применена.

Пример

В данном примере показано, как настроить список методов аккаунтинга EXEC под названием «list-1», использующий сервер RADIUS. Если сервер безопасности не отвечает, аккаунтинг не выполняется. После настройки аккаунтинг EXEC применяется к консоли.

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

8.17 clear aaa counters servers

Данная команда используется для сброса счетчиков статистики серверов AAA.

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

Параметры

all	Укажите, чтобы сбросить счетчики для всех серверов.
radius *IP-ADDRESS*	Укажите, чтобы сбросить счетчики для заданного сервера RADIUS IPv4.
radius *IPV6-ADDRESS*	Укажите, чтобы сбросить счетчики для заданного сервера RADIUS IPv6.

radius all	Укажите, чтобы сбросить счетчики для всех серверов RADIUS.
tacacs *IP-ADDRESS*	Укажите, чтобы сбросить счетчики для заданного сервера TACACS IPv4.
tacacs *IPV6-ADDRESS*	Укажите, чтобы сбросить счетчики для заданного сервера TACACS IPv6.
tacacs all	Укажите, чтобы сбросить счетчики для всех серверов TACACS.
sg *NAME*	Укажите, чтобы сбросить счетчики для всех серверов в указанной группе.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

Пример

В данном примере показано, как сбросить счетчики серверов AAA.

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

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

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

8.18 client

Данная команда используется для конфигурирования клиента RADIUS, от которого коммутатор может принимать запросы на изменение авторизации (CoA) и разрыв сессии (disconnect). Для удаления конфигурации воспользуйтесь формой **no** этой команды.

client {*IP-ADDRESS* **|** *HOST-NAME***} server-key [0 | 7]** *STRING*

no client {*HOST-NAME* **|** *IP-ADDRESS***}**

Параметры

IP-ADDRESS	Укажите IP-адрес клиента RADIUS.
HOST-NAME	Укажите имя клиента RADIUS.
server-key	Общий ключ RADIUS, который будет использоваться между коммутатором и клиентом RADIUS.
0	(Опционально.) Укажите, чтобы передать ключ в виде открытого текста. Это опция по умолчанию, если не указаны ни параметр **0**, ни параметр **7**.
7	(Опционально.) Укажите, чтобы передать ключ в зашифрованном виде.
STRING	Введите общий ключ.

По умолчанию

По умолчанию запросы CoA и disconnect отбрасываются.

Режим ввода команды

Dynamic Authorization Local Server Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Коммутатор можно настроить таким образом, чтобы динамически принимать обновления от внешнего сервера политик. Такой функционал обеспечивается расширением CoA RADIUS. CoA дает возможность коммутатору выступать в качестве сервера, а внешнему серверу политик – в качестве клиента.

Используйте эту команду для конфигурирования клиентов RADIUS, для которых коммутатор может выступать в качестве RADIUS-сервера.

Пример

В примере показано, как настроить коммутатор, чтобы он принимал запросы от клиента RADIUS.

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

8.19 ip http authentication aaa login-authentication

Данная команда используется, чтобы назначить список методов аутентификации AAA для аутентификации пользователей HTTP-сервера. Для возврата к списку методов по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

default	Укажите для аутентификации на основе списка методов по умолчанию.
METHOD-LIST	Укажите название списка методов.

По умолчанию

По умолчанию используется опция **default**.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

Пример

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

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

8.20 ip http accounting exec

Данная команда используется, чтобы назначить метод аккаунтинга AAA для пользователей HTTP-сервера. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

default	Укажите для аккаунтинга на основе списка методов по умолчанию.
METHOD-LIST	Укажите название списка методов.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Для вступления в силу аккаунтинга по списку методов предварительно включите функцию AAA с помощью команды **aaa new-model**. Заранее создайте список методов, используя команду **aaa accounting exec**. Если список методов отсутствует, то команда не будет действовать.

Пример

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

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

8.21 ip radius source-interface

Данная команда позволяет указать интерфейс, IP-адрес которого будет использоваться в качестве IP-адреса источника для отправки пакетов RADIUS. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode.

Server Group Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

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

Пример

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

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

8.22 ip tacacs source-interface

Данная команда позволяет указать интерфейс, IP-адрес которого будет использоваться в качестве IP-адреса источника для отправки пакетов TACACS. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip tacacs source-interface *INTERFACE-ID*

no ip tacacs source-interface

Параметры

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

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode.

Server Group Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

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

Пример

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

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

8.23 ipv6 radius source-interface

Данная команда позволяет указать интерфейс, IPv6-адрес которого будет использоваться в качестве IPv6-адреса источника для отправки пакетов RADIUS. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 radius source-interface *INTERFACE-ID*

no ipv6 radius source-interface

Параметры

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

По умолчанию

По умолчанию используется IPv6-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode.

Server Group Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

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

Пример

В данном примере показано, как указать интерфейс VLAN100, IPv6-адрес которого будет использоваться в качестве адреса источника для отправки пакетов RADIUS.

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

8.24 ipv6 tacacs source-interface

Данная команда позволяет указать интерфейс, IPv6-адрес которого будет использоваться в качестве IPv6-адреса источника для отправки пакетов TACACS. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 tacacs source-interface *INTERFACE-ID*

no ipv6 tacacs source-interface

Параметры

INTERFACE-ID	Укажите интерфейс, IPv6-адрес которого будет использоваться как IPv6-адрес источника для отправки пакетов TACACS.

По умолчанию

По умолчанию используется IPv6-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode.

Server Group Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда применяется для указания интерфейса, IPv6-адрес которого будет использоваться в качестве IPv6-адреса источника для отправки пакетов TACACS. Если интерфейс источника указан в режиме глобальной конфигурации и в режиме конфигурации группы серверов, то приоритетом обладает интерфейс источника, указанный в режиме конфигурации группы серверов.

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

Пример

В данном примере показано, как указать интерфейс VLAN100, IPv6-адрес которого будет использоваться в качестве адреса источника для отправки пакетов TACACS.

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

8.25 login authentication

Данная команда позволяет настроить список методов, используемый для аутентификации при входе для конкретной сессии. Для возврата к списку методов по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

default	Укажите для аутентификации на основе списка методов по умолчанию.
METHOD-LIST	Укажите название списка методов.

По умолчанию

По умолчанию используется параметр **default**.

Режим ввода команды

Line Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Для вступления в силу аутентификации по списку методов предварительно включите функцию AAA с помощью команды **aaa new-model**. Заранее создайте список методов, используя команду **aaa authentication login**. Если список методов отсутствует, то команда не вступает в силу, и аутентификация будет выполняться по списку методов по умолчанию.

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

Пример

В данном примере показано, как настроить локальную сессию консоли с использованием списка методов «CONSOLE-LINE-METHOD» для аутентификации при входе.

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

8.26 port

Данная команда используется для настройки порта, который слушает запросы от клиентов RADIUS. Для возвращения к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

port *PORT-NUMBER*
no port

Параметры

PORT-NUMBER	Укажите номер порта.

По умолчанию

По умолчанию используется порт 3799.

Режим ввода команды

Dynamic Authorization Local Server Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте команду для настройки порта, который слушает запросы от клиентов RADIUS.

Пример

В примере показано, как изменить порт, который слушает запросы от клиентов RADIUS, выбрав

порт 1650.

```
Switch#configure terminal
Switch(config)#aaa server radius dynamic-author
Switch(config-locsvr-da-radius)#port 1650
Switch(config-locsvr-da-radius)#
```

8.27 radius-server attribute 4

Данная команда применяется для назначения IP-адреса, используемого в качестве адреса RADIUS-атрибута 4. Для удаления IP-адреса воспользуйтесь формой **no** этой команды.

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

Параметры

IP-ADDRESS	Укажите IP-адрес для RADIUS-атрибута 4.

По умолчанию

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

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Как правило, если настроена команда **ip radius source-interface**, указанный IP-адрес используется в IP-заголовках, а также в качестве адреса RADIUS-атрибута 4 в пакетах RADIUS.

Однако, если настроена команда **radius-server attribute 4**, то в качестве адреса атрибута 4 в пакетах RADIUS используется указанный IP-адрес. На адрес в IP-заголовках пакетов RADIUS он не влияет.

Пример

В данном примере показано, как указать IP-адрес 10.0.0.21 в качестве адреса RADIUS-атрибута 4.

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

8.28 radius-server attribute 55 include-in-acct-req

Данная команда используется для включения отправки RADIUS-атрибута 55 (Event-Timestamp) в пакетах аккаунтинга. Для выключения функции воспользуйтесь формой **no** этой команды.

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

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда позволяет включить или выключить отправку RADIUS-атрибута 55 в пакетах аккаунтинга.

Пример

В данном примере показано, как включить отправку RADIUS-атрибута 55.

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

8.29 radius-server deadtime

Данная команда используется для назначения интервала времени, в течение которого разрешается пропускать опрос недоступного сервера. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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

Параметры

MINUTES	Укажите время простоя. Диапазон значений: от 0 до 1440 (24 часа). Если установлено значение 0, недоступный сервер не будет помечен как недействующий.

По умолчанию

По умолчанию используется значение 0.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда позволяет оптимизировать время обработки данных аутентификации с помощью установки времени простоя (dead time), в течение которого недоступные серверы опрашиваться не будут.

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

Пример

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

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

8.30 radius-server host

Данная команда используется для добавления RADIUS-сервера в список используемых серверов. Чтобы удалить сервер, воспользуйтесь формой **no** этой команды.

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

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

Параметры

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

acct-port *PORT*	(Опционально.) Укажите номер UDP-порта назначения для отправки пакетов аккаунтинга. Диапазон значений: от 0 до 65535. Установите ноль в качестве значения номера порта, если сервер не предназначен для аккаунтинга. Значение по умолчанию – 1813.
timeout *SECONDS*	(Опционально.) Укажите значение тайм-аута сервера. Диапазон значений: от 1 до 255 секунд. Если значение не указано, по умолчанию используется 5 секунд.
retransmit *COUNT*	(Опционально.) Укажите количество повторных передач запросов на сервер, когда ответ не получен. Диапазон значений: от 0 до 20. Используйте 0 для отключения повторной передачи. Если значение не указано, по умолчанию используется 2.
Key 0 *KEY-STRING*	Укажите незашифрованный (открытый текст) общий ключ длиной от 1 до 254 символов.
Key 0 *KEY-STRING*	Укажите общий ключ в зашифрованной форме длиной от 24 до 344 символов.

По умолчанию

По умолчанию сервер не настроен.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

Пример

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

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

8.31 server (RADIUS)

Данная команда используется для привязки RADIUS-сервера к группе RADIUS-серверов. Для удаления сервера из группы воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

По умолчанию сервер не настроен.

Режим ввода команды

RADIUS Group Server Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Команда **server** применяется для привязки RADIUS-сервера к группе серверов RADIUS. Определенная группа серверов может быть указана в качестве списка методов аутентификации или аккаунтинга с помощью команд **aaa authentication** и **aaa accounting**. Команда **radius-server host** позволяет создать запись сервера. Данная запись идентифицируется по IP-адресу.

Пример

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

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

8.32 server (TACACS+)

Данная команда используется для привязки сервера TACACS+ к группе серверов. Для удаления сервера из группы воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

По умолчанию сервер не настроен.

Режим ввода команды

TACACS+ Group Server Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Команда **server** применяется для привязки сервера TACACS+ к группе серверов TACACS+. Определенная группа серверов может быть указана в качестве списка методов для аутентификации или аккаунтинга с помощью команд **aaa authentication** и **aaa accounting**. Серверы в группе будут применяться по порядку. Команда **tacacs-server host** позволяет создать запись сервера. Данная запись идентифицируется по IP-адресу.

Пример

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

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

8.33 show aaa

Данная команда используется для отображения глобального состояния AAA.

show aaa

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения глобального состояния AAA.

Пример

В данном примере показано, как отобразить глобальное состояние AAA.

```
Switch#show aaa

AAA is enabled.

Switch#
```

8.34 tacacs-server host

Данная команда используется для создания сервера TACACS+. Чтобы удалить сервер, воспользуйтесь формой **no** этой команды.

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

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

Параметры

IP-ADDRESS	Укажите IPv4-адрес сервера TACACS+.
IPV6-ADDRESS	Укажите IPv6-адрес сервера TACACS+.
port *PORT-NUMBER*	(Опционально.) Укажите номер UDP-порта назначения для отправки request-пакетов. Номер порта по умолчанию – 49. Диапазон значений: от 1 до 65535.
timeout *SECONDS*	(Опционально.) Укажите значение тайм-аута сервера. Диапазон значений: от 1 до 255 секунд. Значение по умолчанию – 5 секунд.
0	(Опционально.) Пароль в форме обычного незашифрованного текста. Данный параметр используется по умолчанию.

7	(Опционально.) Пароль в зашифрованной форме.
key *KEY-STRING*	Укажите ключ, используемый для связи с сервером. Ключ может содержать от 1 до 254 символов.

По умолчанию

По умолчанию сервер TACACS+ не настроен.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

Пример

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

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

8.35 show radius statistics

Данная команда используется, чтобы отобразить статистику RADIUS для пакетов аккаунтинга и аутентификации.

show radius statistics

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

```
Switch#show radius statistics

 RADIUS Server: 10.90.90.211: Auth-Port 1812, Acct-Port 1813
 State is Up
                         Auth.       Acct.
 Round Trip Time:        2           0
 Access Requests:        2           NA
 Access Accepts:         1           NA
 Access Rejects:         0           NA
 Access Challenges:      1           NA
 Acct Request:           NA          0
 Acct Response:          NA          0
 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


Switch#
```

Отображаемые параметры

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

Access Challenges	Количество пакетов RADIUS Access-Challenge (действительных или недействительных), полученных с данного сервера.
Acct Request	Количество отправленных пакетов RADIUS Accounting-Request. Не включает повторные передачи.
Acct Response	Количество пакетов RADIUS, полученных на accounting-порту от данного сервера.
Retransmissions	Количество пакетов RADIUS Request, повторно переданных данному RADIUS-серверу. Повторные передачи включают попытки, при которых поля Identifier и Acct-Delay были обновлены, а также попытки, при которых они остаются без изменений.
Malformed Responses	Количество ошибочных пакетов RADIUS Response, полученных от данного сервера. Ошибочные пакеты включают пакеты с некорректной длиной. Неверные аутентификаторы, атрибуты Signature или неизвестные типы не учитываются.
Bad Authenticators	Количество пакетов RADIUS Response, полученных от данного сервера и содержащих некорректные аутентификаторы или атрибуты Signature.
Pending Requests	Количество пакетов RADIUS Request, предназначенных для данного сервера, время которых еще не истекло, или которые не получили ответ. Эта переменная увеличивается, когда запрос отправляется, и уменьшается из-за получения ответа, тайм-аута или повторной передачи.
Timeouts	Количество тайм-аутов для данного сервера. По истечении тайм-аута клиент может повторить попытку подключения к данному серверу, отправить запрос на аутентификацию другому серверу или прекратить попытки. Повторная попытка подключиться к этому же серверу считается повторной передачей, также как и тайм-аут. Попытка подключиться к другому серверу рассматривается как запрос, точно также как и тайм-аут.
Unknown Types	Количество пакетов RADIUS неизвестного типа, полученных от данного сервера.
Packets Dropped	Количество пакетов RADIUS, полученных от данного сервера и отброшенных по какой-либо причине.

8.36 show tacacs statistics

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

show tacacs statistics

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

```
Switch#show tacacs statistics

 TACACS+ Server: 10.90.90.5/49, State is Up
 Socket Opens: 0
 Socket Closes: 0
 Total Packets Sent: 0
 Total Packets Recv: 0
 Reference Count: 0


Switch#
```

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 на сервер 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). Для удаления статической записи из кэша ARP воспользуйтесь формой **no** этой команды.

arp *IP-ADDRESS HARDWARE-ADDRESS*
no arp *IP-ADDRESS HARDWARE-ADDRESS*

Параметры

IP-ADDRESS	Укажите IP-адрес.
HARDWARE-ADDRESS	Укажите MAC-адрес (48-битный).

По умолчанию

В кэше ARP нет ни одной статической записи.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

В данном примере показано, как добавить статическую ARP-запись для 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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

arp timeout *MINUTES*
no arp timeout

Параметры

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

По умолчанию

Значение по умолчанию – 240 минут.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для настройки времени устаревания ARP-записей в таблице ARP.

Пример

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

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

9.3 clear arp-cache

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

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

Параметры

all	Укажите, чтобы полностью очистить кэш динамических ARP-записей, связанных со всеми интерфейсами.
INTERFACE-ID	Укажите идентификатор интерфейса.
IP-ADDRESS	Укажите IP-адрес динамической ARP-записи, которую необходимо удалить.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

9.4 ip address

Данная команда используется для назначения интерфейсу основного или второстепенного адреса IPv4, а также для автоматического получения IP-адреса от DHCP-сервера. Чтобы удалить настройки IP-адреса или отключить DHCP на интерфейсе, воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

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

IP-адрес по умолчанию порта управления (MGMT) – 192.168.0.1/24.

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 одной VLAN сразу несколько сетей с IP-адресом для каждой. Один из этих IP-адресов должен быть основным, а остальные – второстепенными. Основной адрес используется в качестве IP-адреса источника для отправленных с интерфейса сообщений SNMP trap или syslog.

Параметр **dhcp** не поддерживается на порту MGMT.

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 default-gateway

Данная команда используется для настройки IP-адреса шлюза по умолчанию на порту управления. Для удаления IP-адреса шлюза по умолчанию воспользуйтесь формой **no** этой команды.

ip default-gateway *IP-ADDRESS*
no ip default-gateway *IP-ADDRESS*

Параметры

IP-ADDRESS	Укажите IPv4-адрес шлюза по умолчанию.

По умолчанию

IP-адрес шлюза по умолчанию – 0.0.0.0.

Режим ввода команды

MGMT Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

IP-пакеты, предназначенные для других подсетей IP, отправляются на шлюз по умолчанию. Данная команда может использоваться только в режиме MGMT Interface Configuration Mode.

Пример

В данном примере показано, как указать адрес 192.168.0.254 в качестве IP-адреса шлюза по умолчанию MGMT-интерфейса.

```
Switch#configure terminal
Switch(config)#interface mgmt0
Switch(config-if)#ip default-gateway 192.168.0.254
Switch(config-if)#
```

9.6 ip proxy-arp

Данная команда используется для включения опции Proxy ARP на интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip proxy-arp

no ip proxy-arp

Параметры

Нет.

По умолчанию

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

9.7 ip local-proxy-arp

Данная команда используется для включения на интерфейсе опции Local Proxy ARP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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 второстенными сетями VLAN или изолированными портами в пределах домена. Команда сработает только после включения опции **ip proxy arp**.

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)#
```

9.8 ip mtu

Данная команда используется для настройки значения MTU. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip mtu *BYTES*
no ip mtu

Параметры

BYTES	Укажите значение IP MTU. Диапазон значений: от 512 до 16383 байт.

По умолчанию

По умолчанию установлено значение MTU, равное 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

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

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы 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.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения заданного времени устаревания ARP-записей.

Пример

В данном примере показано, как отобразить время устаревания 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-интерфейсам.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите, чтобы отобразить информацию по определенному IP-интерфейсу.
brief	(Опционально.) Укажите, чтобы отобразить краткую информацию по IP-интерфейсам.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если параметры не указаны, будет отображаться информация для всех интерфейсов.

Пример

В данном примере показано, как отобразить краткую информацию по IP-интерфейсам. **(Только для DGS-1520-28 и DGS-1520-52.)**

```
Switch#show ip interface brief


Interface    IP Address      Link Status
----------  ---------------  -----------
vlan1       10.90.90.90      up
mgmt_ipif   192.168.0.1      down

Total Entries: 2

Switch#
```

В данном примере показано, как отобразить краткую информацию по IP-интерфейсам. **(Только для DGS-1520-28MP и DGS-1520-52MP.)**

```
Switch#show ip interface brief


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

Total Entries: 1

Switch#
```

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

```
Switch#show ip interface vlan 1

Interface vlan1 is enabled, Link status is up
  IP address is 10.90.90.90/8 (Manual)
  ARP timeout is 240 minutes.
  IP MTU is 1500 bytes
  Helper Address is not set
  Proxy ARP is disabled
  IP Local Proxy ARP is disabled
  IP Directed Broadcast is disabled
  gratuitous-send is disabled, interval is 0 seconds

Total Entries: 1

Switch#
```

В следующем 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#
```

10. Базовые команды настройки IPv6

10.1 clear ipv6 neighbors

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

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

Параметры

all	Укажите, чтобы удалить динамические записи из IPv6 neighbor cache для всех интерфейсов.
interface *INTERFACE-ID*	Укажите, чтобы удалить динамические записи из IPv6 neighbor cache для конкретного интерфейса.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется 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 interface vlan 1
Switch#
```

10.2 ipv6 address

Данная команда используется для настройки IPv6-адреса вручную на интерфейсе. Чтобы удалить заданный вручную IPv6-адрес, воспользуйтесь формой **no** этой команды.

ipv6 address {*IPV6-ADDRESS/PREFIX-LENGTH* **|** *PREFIX-NAME SUB-BITS/PREFIX-LENGTH* **|** *IPV6-ADDRESS* **link-local}**

no ipv6 address {*IPV6-ADDRESS/PREFIX-LENGTH* **|** *PREFIX-NAME SUB-BITS/PREFIX-LENGTH* **|** *IPV6-ADDRESS* **link-local}**

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес и длину префикса для подсети.
PREFIX-LENGTH	Укажите длину префикса. Префикс IPv6-адреса также является локальной подсетью на интерфейсе.
PREFIX-NAME	Укажите имя префикса, используя не более 12 символов без пробелов.
SUB-BITS	Укажите сетевую и узловую части IPv6-адреса.
link-local	Укажите адрес Link-Local.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

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

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

Пример

В данном примере показано, как задать IPv6-адрес.

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

В примере ниже 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 следующем 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 нижеприведенном 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 позволяет настроить на интерфейсе IPv6-адрес с использованием идентификатора интерфейса EUI-64 (Interface ID). Для удаления IPv6-адреса, сгенерированного с использованием идентификатора интерфейса EUI-64, воспользуйтесь формой **no** этой команды.

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

Параметры

IPV6-PREFIX	Укажите IPv6-префикс для конфигурируемого IPv6-адреса.
PREFIX-LENGTH	Укажите длину префикса. Префикс IPv6-адреса также является локальной подсетью на интерфейсе. Максимальная длина префикса – 64.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для настройки на интерфейсе IPv6-адреса с использованием идентификатора интерфейса EUI-64 (Interface ID).

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. Чтобы отключить использование DHCPv6 для получения IPv6-адреса, воспользуйтесь формой **no** этой команды.

ipv6 address dhcp [rapid-commit]

no ipv6 address dhcp

Параметры

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

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить на интерфейсе получение сетевых настроек IPv6 от DHCPv6-сервера.

Стандартный обмен сообщениями между маршрутизаторами Delegating Router (DR) и Requesting Router (RR) включает в себя четыре сообщения: *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** как на DR, так 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 получение IPv6-адреса от DHCPv6-сервера на интерфейсе VLAN 1.

```
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 Auto-Configuration. Чтобы удалить IPv6-адрес, сгенерированный с помощью механизма автоконфигурации, воспользуйтесь формой **no** этой команды.

ipv6 address autoconfig [default]
no ipv6 address autoconfig

Параметры

default	(Опционально.) Если на данном интерфейсе выбран шлюз по умолчанию, то с указанием параметра default будет установлен маршрут по умолчанию с использованием этого шлюза по умолчанию. Параметр можно указать только на одном интерфейсе.

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 интерфейса VLAN IPv6. Опция автоконфигурации по умолчанию отключена.

При включении автоконфигурации интерфейс включает обработку IPv6 и получает анонс от маршрутизатора IPv6 с назначенным префиксом глобального адреса. Далее итоговый адрес, состоящий из префикса и идентификатора интерфейса, назначается данному интерфейсу. В случае отключения этой опции полученный Global Unicast-адрес будет удален из интерфейса.

Применение опции **default** позволит использовать анонс маршрутизатора для добавления маршрута по умолчанию в таблицу маршрутизации IPv6. Данный маршрут по умолчанию получен с помощью SLAAC и обладает более высоким приоритетом по сравнению с другими динамическими маршрутами, полученными по протоколам RIPng и OSPFv3.

Если автоконфигурация уже была включена, то перед вводом команды **ipv6 address autoconfig default** необходимо выполнить команду **no**.

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. Чтобы отключить обработку IPv6 на интерфейсах, у которых нет явно настроенного IPv6-адреса, воспользуйтесь формой **no** этой команды.

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

Если IPv6-адрес задан на интерфейсе явно, автоматически генерируется IPv6-адрес Link-Local и начинается обработка IPv6. Если на интерфейсе нет явно настроенного IPv6-адреса, IPv6-адрес

Link-Local не генерируется и обработка IPv6 не запускается. Используйте команду **ipv6 enable** для автоматической генерации IPv6-адреса Link-Local 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, чтобы настроить параметр hop limit (предельное число шагов) для IPv6 на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 hop-limit *VALUE*
no ipv6 hop-limit

Параметры

VALUE	Укажите значение для параметра IPv6 hop limit. 0 означает, что для отправки пакета используются настройки по умолчанию. Диапазон значений: 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 этот параметр в качестве начального значения 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, чтобы настроить значение MTU для IPv6. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mtu *BYTES*
no ipv6 mtu

Параметры

BYTES	Укажите, чтобы задать значение MTU для IPv6. Диапазон значений: от 1280 до 65534 байт.

По умолчанию

По умолчанию для IPv6 установлено значение MTU, равное 1500 байт.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима для настройки интерфейсов L3. Используйте эту команду, чтобы настроить значение 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 примере ниже показано, как восстановить значение IPv6 MTU 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 Address Configuration (M) в анонсируемых сообщениях RA. Чтобы отключить флаг, воспользуйтесь формой **no** этой команды.

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. Чтобы отключить флаг, воспользуйтесь формой **no** этой команды.

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 в сообщениях RA, анонсируемых в VLAN 1.

```
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. Чтобы удалить префикс, воспользуйтесь формой **no** этой команды.

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

no ipv6 nd prefix *IPV6-PREFIX/PREFIX-LENGTH*

Параметры

IPV6-PREFIX/PREFIX-LENGTH	Укажите IPv6-префикс, который будет сгенерирован или анонсирован в сообщении RA на интерфейсе.
VALID-LIFETIME	(Опционально.) Укажите период времени в секундах, в течение которого префикс будет действителен. Диапазон значений: от 0 до 4294967295. Если значение не задано, устанавливается значение по умолчанию – 2592000 секунд (30 дней).

PREFERRED-LIFETIME	(Опционально.) Укажите предпочтительное время жизни префикса в секундах. Диапазон значений: от 0 до 4294967295. Если значение не задано, устанавливается значение по умолчанию – 604 800 секунд (7 дней).
off-link	(Опционально.) Укажите, чтобы отключить флаг наличия соединения on-link. Если значение не задано, по умолчанию устанавливается флаг off-link.
no-autoconfig	(Опционально.) Укажите, чтобы отключить флаг auto-configure. Если значение не задано, флаг auto-configure включается по умолчанию.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Статус префикса представлен следующими комбинациями:

- Комбинация 1: параметры **off-link** и **no-autoconfig** не заданы.
  - Префикс добавляется в таблицу маршрутизации. Бит L = 1, бит A = 1.
- Комбинация 2: задан параметр **no-autoconfig**.
  - Префикс добавляется в таблицу маршрутизации. Бит L = 1, бит A = 0.
- Комбинация 3: задан параметр **off-link**.
  - Префикс не добавляется в таблицу маршрутизации. Бит L = 0, бит A = 1.

Значение допустимого времени жизни (Valid Lifetime) для префикса должно превышать значение предпочтительного времени жизни (Preferred Lifetime). Данные значения влияют на префикс, в котором включен бит A. Полученный узел будет конфигурировать адреса на основе префикса, используя механизм Stateless Configuration. Если время жизни префикса превысило значение предпочтительного времени (Preferred Lifetime), тогда IPv6-адрес, сконфигурированный на основе этого префикса, будет признан устаревшим. Если время жизни префикса превысило значение Valid Lifetime, то IPv6-адрес, сконфигурированный на основе этого префикса, будет удален.

Пример

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

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

10.12 ipv6 nd ra interval

Данная команда используется для настройки временного интервала между сообщениями RA для IPv6-интерфейса. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 nd ra interval *MAX-SECS* **[***MIN-SECS***]**

no ipv6 nd ra interval

Параметры

MAX-SECS	Укажите максимальный временной интервал для повторной передачи сообщения RA (в секундах). Диапазон значений: от 4 до 1800 секунд.
MIN-SECS	(Опционально.) Укажите минимальный временной интервал для повторной передачи сообщения RA (в секундах). Диапазон значений: 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 IPv6.

```
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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

SECONDS	Укажите продолжительность использования маршрутизатора в качестве маршрутизатора по умолчанию (в секундах). Диапазон значений: 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 значение Lifetime 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. Чтобы включить отправку сообщений RA, воспользуйтесь формой **no** этой команды.

ipv6 nd suppress-ra
no ipv6 nd suppress-ra

Параметры

Нет.

По умолчанию

Анонсирование RA на VLAN-интерфейсе 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. Воспользуйтесь командой **no ipv6 nd suppress-ra** для включения отправки 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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

MILLI-SECONDS	Укажите время доступности для отправляемых анонсов маршрутизатора (в миллисекундах). Диапазон значений: 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 значение Reachable Time продолжительностью 3600 секунд для интерфейса VLAN 1.

```
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 отправками сообщений NS. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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

Параметры

MILLI-SECONDS	Укажите временной интервал отправки запросов NS (в миллисекундах). Диапазон значений: от 0 до 3600000 миллисекунд, кратно 1000.

По умолчанию

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

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

10.17 ipv6 neighbor

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

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

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес для записи в IPv6 neighbor cache.
interface *INTERFACE-ID*	Укажите интерфейс для создания статической записи в IPv6 neighbor cache.
MAC-ADDRESS	Укажите MAC-адрес для записи в IPv6 neighbor cache.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для создания статической записи в таблице IPv6 neighbor cache на интерфейсе. Отслеживание доступности соседних узлов к статическим записям не применяется.

Команда **clear ipv6 neighbors** позволяет удалять динамические записи из таблицы IPv6 neighbor. Для удаления статической записи воспользуйтесь командой **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 interface vlan 1 00-01-80-11-22-99
Switch(config)#
```

10.18 ipv6 optimistic dad

Данная команда используется для включения алгоритма IPv6 Optimistic Duplicate Address Detection (DAD). Для отключения данного алгоритма воспользуйтесь формой **no** этой команды.

ipv6 optimistic dad

no ipv6 optimistic dad

Параметры

Нет.

По умолчанию

По умолчанию данный алгоритм выключен.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для включения или отключения IPv6 Optimistic DAD.

Пример

В данном примере показано, как включить IPv6 Optimistic DAD.

```
Switch#configure terminal
Switch(config)#ipv6 optimistic dad
Switch(config)#
```

10.19 show ipv6 general-prefix

Данная команда используется для отображения информации по основному IPv6-префиксу.

show ipv6 general-prefix [*PREFIX-NAME***]**

Параметры

PREFIX-NAME	(Опционально.) Укажите имя основного префикса, для которого необходимо отобразить информацию. Если имя основного префикса не указано, будет отображаться информация по всем основным префиксам. Максимальное количество символов – 12.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

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#
```

10.20 show ipv6 interface

Данная команда используется для отображения информации по IPv6-интерфейсу.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейс, для которого необходимо получить информацию.

brief	(Опционально.) Укажите, чтобы получить краткую информацию.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки конфигурации IPv6-интерфейса.

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 примере ниже 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#
```

10.21 show ipv6 neighbors

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

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

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс для отображения информации о записях в таблице IPv6 neighbor cache.
IPV6-ADDRESS	(Опционально.) Укажите IPv6-адрес, для которого необходимо получить информацию из таблицы IPv6 neighbor cache.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

```
Switch# show ipv6 neighbors

IPv6 Address                            Link-Layer Addr   Interface Type State
--------------------------------------- ----------------- --------- ---- -----
FE80::200:11FF:FE22:3344                00-00-11-22-33-44 vlan 1     D   REACH

Total Entries: 1

Switch#
```

Отображаемые параметры

Type	**D** – динамическая изученная запись. **S** – статическая neighbor-запись.
State	**INCMP** (неполное) – состояние, когда запрос на получение адреса для записи отправлен, но ответное сообщение neighbor advertisement еще не получено. **REACH** (достижимое) – состояние, когда сообщение neighbor advertisement уже получено, а время таймера Reachable Time (в миллисекундах) еще не истекло. Это означает, что соседнее устройство работает корректно. **STALE** – состояние, в которое переходит запись, если с момента получения последнего подтверждения прошло больше заданного таймером Reachable Time времени (в миллисекундах). **PROBE** – состояние записи, при котором устройство отправляет сообщение neighbor solicitation, чтобы подтвердить достижимость. **DELAY –** больше неизвестно, доступно ли соседнее устройство, которому недавно был отправлен трафик. Немедленная проверка с помощью отправки тестовых сообщений будет ненадолго отложена, чтобы дать возможность протоколам верхнего уровня подтвердить достижимость.

10.22 show ipv6 optimistic dad

Данная команда используется для отображения состояния IPv6 Optimistic DAD.

show ipv6 optimistic dad

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения состояния IPv6 Optimistic DAD.

Пример

В примере ниже показано, как отобразить состояние IPv6 Optimistic DAD.

```
Switch#show ipv6 optimistic dad

IPv6 Optimistic DAD State: Enabled

Switch#
```

11. Команды BPDU Protection

11.1 spanning-tree bpdu-protection (global)

Данная команда используется для глобального включения функции BPDU protection. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

spanning-tree bpdu-protection
no spanning-tree bpdu-protection

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 1.

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, как глобально включить функцию BPDU Protection.

```
Switch#configure terminal
Switch(config)#spanning-tree bpdu-protection
Switch(config)#
```

11.2 spanning-tree bpdu-protection (interface)

Данная команда используется для включения функции BPDU Protection на порту. Для отключения данной функции воспользуйтесь формой **no** этой команды.

spanning-tree bpdu-protection {drop | block | shutdown}

no spanning-tree bpdu-protection

Параметры

drop	Укажите, чтобы отбросить все принимаемые BPDU-пакеты при обнаружении атаки.
block	Укажите, чтобы отбросить все пакеты (включая BPDU и обычные пакеты) при обнаружении атаки.
shutdown	Укажите, чтобы отключить интерфейс при обнаружении атаки.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Используйте данную команду для включения и настройки режима работы BPDU Protection (BPDU Protection Operational Mode).

Пример

В данном примере показано, как включить функцию BPDU Protection в режиме block на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#spanning-tree bpdu-protection block
Switch(config-if)#
```

11.3 show spanning-tree bpdu-protection

Данная команда предназначена для отображения информации BPDU Protection.

show spanning-tree bpdu-protection [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите ID интерфейса для отображения.

,	(Опционально.) Используется для перечисления нескольких или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после запятой недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения информации BPDU Protection. Если ID интерфейса не указан, будет отображена информация для всех интерфейсов.

Пример

В данном примере показано, как отобразить информацию BPDU Protection и статус интерфейсов.

```
Switch#show spanning-tree bpdu-protection

 Global State:      Enabled

Interface          State        Mode         Status
--------------     --------     --------     ------------
eth1/0/1           Enabled      Shutdown     Under Attack
eth1/0/2           Enabled      Drop         Normal
eth1/0/3           Disabled     Block        -
eth1/0/4           Disabled     Shutdown     Normal
eth1/0/5           Disabled     Shutdown     Normal
eth1/0/6           Disabled     Shutdown     Normal
eth1/0/7           Disabled     Shutdown     Normal
eth1/0/8           Disabled     Shutdown     Normal
eth1/0/9           Disabled     Shutdown     Normal
eth1/0/10          Disabled     Shutdown     Normal
eth1/0/11          Disabled     Shutdown     Normal
eth1/0/12          Disabled     Shutdown     Normal
eth1/0/13          Disabled     Shutdown     Normal
eth1/0/14          Disabled     Shutdown     Normal
eth1/0/15          Disabled     Shutdown     Normal
eth1/0/16          Disabled     Shutdown     Normal
eth1/0/17          Disabled     Shutdown     Normal
eth1/0/18          Disabled     Shutdown     Normal
eth1/0/19          Disabled     Shutdown     Normal
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В примере ниже показано, как отобразить информацию BPDU Protection для интерфейса Ethernet 1/0/1.

```
Switch#show spanning-tree bpdu-protection interface eth1/0/1

Interface          State        Mode         Status
--------------     --------     --------     ------------
eth1/0/1           Enabled      Shutdown     Under Attack

Switch#
```

Отображаемые параметры

Interface	Интерфейс, на котором включена функция BPDU Protection.
State	Состояние конфигурации интерфейса.
Mode	Режим работы интерфейса.
Status	Отображает, находится ли интерфейс в состоянии защиты.

11.4 snmp-server enable traps stp-bpdu-protection

Данная команда используется, чтобы включить отправку SNMP-уведомлений для BPDU Protection. Для отключения отправки SNMP-уведомлений воспользуйтесь формой **no** этой команды.

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

Данная команда используется, чтобы включить отправку SNMP-уведомлений для BPDU Protection.

Пример

В данном примере показано, как включить отправку SNMP-уведомлений 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, чтобы проверить состояние и длину медного кабеля.

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда используется для диагностики кабеля на физическом порту. Диагностика кабеля позволяет выявить проблемы с подключением на медных портах. Для запуска диагностики используйте команду **test cable-diagnostics**.

Пример

В данном примере показано, как запустить диагностику для проверки статуса и длины медного кабеля.

```
Switch#test cable-diagnostics interface eth1/0/1
Switch#
```

12.2 show cable-diagnostics

Данная команда используется для отображения результатов диагностики кабеля.

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

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите ID интерфейса. Интерфейс должен быть физическим портом.
,	(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.

Медный порт может находиться в одном из следующих состояний:

- **Open**: пара в кабеле не имеет подключения в указанной позиции;
- **Short**: короткое замыкание в кабеле в указанной позиции;
- **Open or Short**: нет подключения или короткое замыкание, не удается определить тип неисправности;
- **Crosstalk**: перекрестные помехи между парами в кабеле в указанной позиции;
- **Shutdown**: удаленное устройство отключено;
- **Unknown**: состояние неизвестно;
- **OK**: неисправностей пары или кабеля не выявлено;
- **No cable**: кабель не подключен к порту.

Пример

В данном примере показано, как отобразить результаты диагностики кабеля для интерфейса Ethernet 1/0/1.

```
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 позволяет удалить результаты диагностики кабеля.

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

Параметры

all	Укажите, чтобы удалить результаты диагностики кабеля для всех интерфейсов.
interface *INTERFACE-ID*	Укажите ID интерфейса. Интерфейс должен быть физическим портом.
,	(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, чтобы удалить результаты диагностики кабеля на физическом порту. При выполнении диагностики на интерфейсе будет отображено сообщение об ошибке.

Пример

В данном примере показано, как удалить результаты диагностики кабеля.

```
Switch#clear cable-diagnostics interface eth1/0/1
Switch#
```

13. Команды Command Logging

13.1 command logging enable

Данная команда используется для включения функции логирования выполненных команд. Для отключения функции логирования воспользуйтесь формой **no** этой команды.

command logging enable
no command logging enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команды логирования используются для записи команд, успешно выполненных через интерфейс командной строки. В журнале ведется запись введенных команд и информации об учетной записи пользователя, в которой была введена команда. Команды, не изменяющие конфигурацию или работу коммутатора (например, **show**), не записываются. Информация о сохранении и просмотре системного журнала описана в характеристиках sys-log.



Примечание: если коммутатор находится в режиме BAT (процедура загрузки, загрузка конфигурационного файла и т.д.), ни одна из команд конфигурации не логируется (не будет записана в журнал).

Пример

В данном примере показан процесс включения функции логирования.

```
Switch#configure terminal
Switch(config)#command logging enable
Switch(config)#
```

14. Команды CPU Access Control List (ACL)

14.1 soft-acl filter-map

Данная команда используется для создания или изменения программных списков управления доступом (software ACL filter map). При использовании этой команды осуществляется вход в режим Software ACL Filter Map Configuration Mode. Для удаления программных списков управления доступом воспользуйтесь формой **no** этой команды.

soft-acl filter-map *NAME*
no soft-acl filter-map *NAME*

Параметры

NAME	Укажите имя программного списка управления доступом (software ACL filter map). Имя может содержать до 32 символов в длину.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы перейти в режим Software ACL Filter Map Configuration Mode и создать привязку из нескольких предварительно заданных списков ACL для фильтрации пакетов, получаемых ЦПУ. Можно настроить несколько программных списков управления доступом (software ACL filter map).

Пример

В данном примере показано, как создать программный список ACL filter map с именем «cpu_filter».

```
Switch#configure terminal
Switch(config)#soft-acl filter-map cpu_filter
Switch(config-soft-acl)#
```

14.2 match access-group

Данная команда используется для привязки списка доступа к программному списку управления доступом (software ACL filter map). Для удаления привязки воспользуйтесь формой **no** этой команды.

SEQUENCE-NUMBER **match mac access-group** *NAME*
SEQUENCE-NUMBER **match ip access-group** *NAME*

SEQUENCE-NUMBER **match ipv6 access-group** *NAME*
SEQUENCE-NUMBER **match expert access-group** *NAME*
no match {mac | ip | ipv6 | expert} access-group

Параметры

SEQUENCE-NUMBER	Укажите порядковый номер соответствующей записи совпадения. Диапазон значений: от 1 до 65535. Чем меньше номер, тем выше приоритет списка доступа.
NAME	Укажите имя списка доступа ACL, которое должно совпадать.

По умолчанию

Нет.

Режим ввода команды

Software ACL Filter Map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для привязки списка доступа к программному списку управления доступом (software ACL filter map). К одному программному списку могут быть привязаны несколько списков доступа, при условии что они относятся к разным типам (expert, MAC, IP и IPv6). В случае привязки списков доступа одинакового типа каждая последующая команда перезаписывает предыдущую.

Порядковые номера определяют приоритет обработки связанного списка доступа в filter map. Список доступа с меньшим порядковым номером обладает более высоким приоритетом. Связанные списки доступа с одинаковым порядковым номером обрабатываются в следующем порядке: список доступа expert, список доступа MAC, список доступа IP, список доступа IPv6.

Пример

В данном примере показано, как привязать список доступа IP с именем «cpu-acl» и список доступа MAC с именем mac4001 к программному списку управления доступом (software ACL filter map) «cpu_filter».

```
Switch#configure terminal
Switch(config)#ip access-list cpu-acl
Switch(config-ip-acl)#permit 10.20.0.0 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)#
```

14.3 match interface

Данная команда используется для настройки соответствующих входных интерфейсов (ingress interface). Для удаления соответствующих входных интерфейсов воспользуйтесь формой **no** этой команды.

match interface *INTERFACE-ID* **[, | -]**
no match interface {all | *INTERFACE-ID* **[, | -]}**

Параметры

INTERFACE-ID	Укажите соответствующий идентификатор интерфейса (Interface ID). Корректными интерфейсами являются физические интерфейсы.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
all	Указывается в форме **no** этой команды, чтобы удалить все совместимые входные интерфейсы.

По умолчанию

Нет.

Режим ввода команды

Software ACL Filter Map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Программный список управления доступом (software ACL filter map) будет активирован, когда настроен

один или несколько совместимых интерфейсов. Если совместимый интерфейс не настроен, программный список не вступит в силу.

Когда пакет принимается CPU, и входной интерфейс настроен в программном списке управления доступом (software ACL filter map), коммутатор будет автоматически выполнять поиск связанных списков доступа соответствующего списка.

Связанный список доступа с наивысшим приоритетом в программном списке будет проверен в первую очередь. При обнаружении совпадения другие списки доступа будут проигнорированы. В противном случае, будет выполняться поиск списка доступа со следующим наивысшим приоритетом и так далее.

Внутри списка доступа используется похожая проверка номеров. Правило с меньшим порядковым номером получает более высокий приоритет. При обнаружении совпадения другие правила будут проигнорированы.

В итоге, если совпадение не обнаружено, пакет будет разрешен, и он может непрерывно обрабатываться другими функциями.

Если действием является ‘permit’, он будет пропущен к другим функциям. Если действием является ‘drop’, пакет будет отброшен.

Другими словами, действие программного списка основано на явно настроенной записи «разрешить/запретить». Пакет разрешен, если он не соответствует какому-либо явно заданному правилу «разрешить» или «запретить».

Интерфейс может принадлежать только одному списку. Если интерфейс настроен для нового программного списка, он будет удален из предыдущего списка.

Пример

В данном примере показано, как настроить совместимый интерфейс 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 eth1/0/1
Switch(config-soft-acl)#
```

14.4 show soft-acl

Данная команда используется для отображения информации о программных списках управления доступом (software ACL filter map).

show soft-acl filter-map [*NAME***]**

Параметры

NAME	(Опционально.) Укажите имя отображаемого программного списка управления доступом.

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):cpu-acl
      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.

15. Команды CPU Port Statistics

15.1 debug show cpu port

Данная команда используется для отображения статистики по пакетам Layer 2 или Layer 3, полученным ЦПУ.

debug show cpu port [l2 | l3 [unicast | multicast] | protocol *NAME***]**

Параметры

l2	(Опционально.) Укажите, чтобы отобразить счетчики статистики по пакетам Layer 2.
l3	(Опционально.) Укажите, чтобы отобразить счетчики статистики по пакетам Layer 3.
unicast	(Опционально.) Укажите, чтобы отобразить счетчики статистики по пакетам Layer 3 и одноадресной маршрутизации Layer 3.
multicast	(Опционально.) Укажите, чтобы отобразить счетчики статистики по пакетам Layer 3 и многоадресной маршрутизации Layer 3.
protocol *NAME*	(Опционально.) Укажите имя протокола.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда применяется для отображения статистики по пакетам Layer 2 и Layer 3, полученным ЦПУ.

Пример

В данном примере показано, как отобразить статистику по пакетам Layer 2 и Layer 3, полученным ЦПУ.

```
Switch#debug show cpu port

Type                              PPS        Total       Drop
--------------------------------- ---------- ----------- -----------
802.1X                            0          0           0
ARP                               0          2           0
CTP                               0          0           0
DHCP                              0          0           0
DHCPv6                            0          0           0
DNS                               0          0           0
DVMRP                             0          0           0
ERPS                              0          0           0
GVRP                              0          0           0
ICMP                              0          0           0
ICMPv6                            0          0           0
IGMP                              0          0           0
LACP                              0          0           0
LLDP                              0          0           0
MLD                               0          0           0
NDP                               0          0           0
OSPFv2                            0          0           0
OSPFv3                            0          0           0
PIM-IPv4                          0          0           0
PIM-IPv6                          0          0           0
Reserved-IPv4-IPMC                0          0           0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

15.2 debug clear cpu port

Данная команда используется для сброса всех счетчиков по пакетам Layer 2 или Layer 3, полученным ЦПУ.

debug clear cpu port

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда используется для сброса всех счетчиков по пакетам Layer 2 или Layer 3, полученным ЦПУ.

Пример

В данном примере показано, как сбросить все счетчики статистики.

```
Switch#debug clear cpu port
Switch#
```

16. Команды Debug

16.1 debug enable

Данная команда используется для включения функции вывода сообщения отладки (Debug). Для отключения данной функции воспользуйтесь формой **no** этой команды.

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, чтобы включить функцию 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)#
```

16.2 debug output

Используйте данную команду, чтобы обозначить индивидуальные модули, для которых необходимо вывести сообщение отладки (Debug). Для отключения данной функции воспользуйтесь формой **no** этой команды.

debug output {module *MODULE-LIST* **| all} {buffer | console | monitor}**
no debug output {module *MODULE-LIST* **| all}**

Параметры

MODULE-LIST	Укажите список модулей, для которых необходимо вывести сообщение отладки (Debug). Заключите названия модулей в двойные кавычки, разделив 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.
monitor	Укажите, чтобы вывести сообщение отладки (Debug) в терминал (например, Telnet или SSH).

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 сообщения отладки (Debug) MSTP на локальную консоль.

```
Switch#debug output module "MSTP" console
Switch#
```

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. Для отключения режима воспользуйтесь формой **no** этой команды.

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

SOURCE-URL	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.
DESTINATION-URL	Укажите URL-адрес назначения.
LOCATION	Укажите IPv4- или IPv6-адрес 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. Если скопирована информация **tech-support** и в стеке более одного коммутатора, будет сгенерировано несколько файлов, содержащих unit ID коммутатора в качестве суффикса в имени файла.

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
Clear debug-buffer? (y/n) [n]  y
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.

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
OSPFV2                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.

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 : 2020/01/11 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 : 2020/01/11 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 [unit *UNIT-ID***]**

Параметры

unit *UNIT-ID*	(Опционально.) Укажите unit ID в стеке.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

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. Если параметры не указаны, будет отображена информация обо всех устройствах.

Пример

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

```
Switch#debug show tech-support

#------------------------------------------------------------------------------
#                DGS-1520-28MP Gigabit Ethernet Smart Managed Switch
#                          Technical Support Information
#
#                            Firmware: Build 1.00.022
#    Copyright(C) 2020  D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------


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

[SYS 2019-1-1 00:03:10]

Boot Time           : 1 Jan 2019  00:00:00
RTC Time            : 2019/01/01 00:03:10
Boot PROM Version   : Build 1.00.010
Firmware Version    : Build 1.00.022
Hardware Version    : A1
Serial number       : DGS1520-28MPA
MAC Address         : 80-26-89-15-28-00
MAC Address Number  : 29

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 ЦПУ, а также коэффициента загрузки ЦПУ с разбивкой на процессы.

debug show cpu utilization

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы отобразить информацию по загрузке ЦПУ и загрузке по каждому процессу.

Пример

В данном примере показано, как отобразить информацию о загрузке ЦПУ с разбивкой на процессы.

```
Switch#debug show cpu utilization

Five seconds -   7 %         One minute -   6 %         Five minutes -  17 %

Process Name          5Sec     1Min     5Min
-----------------    ------   ------   ------
tIdleTask0           93 %     94 %     83 %
bcmL2X.0              1 %      1 %      1 %
bcmCNTR.0             1 %      1 %      1 %
cpuprotect            0 %      0 %      0 %
bcmLINK.0             0 %      0 %      0 %
hisr1                 0 %      0 %      0 %
socdmadesc.0          0 %      0 %      0 %
poe_task              0 %      0 %      0 %
MAUMIB_TASK           0 %      0 %      0 %
FWD-ETH               0 %      0 %      0 %
IP-Msg                0 %      0 %      0 %
bcmRX                 0 %      0 %      0 %
web                   0 %      0 %      0 %
CNT_TASK              0 %      0 %      0 %
bcmMEM_SCAN.0         0 %      0 %      0 %
CLI                   0 %      0 %      0 %
OS_TIMER              0 %      0 %      0 %
8021xCtrl             0 %      0 %      0 %
HISTORCNT_TASK        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. Для отключения данной функции воспользуйтесь формой **no** этой команды.

autoconfig enable
no autoconfig enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

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 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.

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 Auto-Image

18.1 autoimage enable

Данная команда используется для включения функции Auto-Image. Для отключения данной функции воспользуйтесь формой **no** этой команды.

autoimage enable
no autoimage enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

При запуске коммутатора данная функция позволяет получить файл образа с внешнего TFTP-сервера, чей IP-адрес и имя файла содержатся в сообщении DHCP OFFER, полученном от DHCP-сервера. Полученный файл используется системой в качестве загрузочного. Если функция Auto-Image включена, при загрузке системы коммутатор автоматически становится DHCP-клиентом.

DHCP-клиент будет активирован для получения сетевых настроек от DHCP-сервера, который добавит в сообщение IP-адрес TFTP-сервера и имя файла образа. После получения данной информации коммутатор запустит функцию загрузки с указанного TFTP-сервера. На данном этапе в консоли будут отображены параметры конфигурации загрузки – так же, как при использовании команды **download firmware**.

После завершения загрузки программного обеспечения будет выполнена перезагрузка коммутатора.

Если одновременно включены функция Auto-Configuration и функция Auto-Image, сначала будет выполнена загрузка файла образа, а затем загрузка конфигурации. Коммутатор выполнит сохранение настроек, а затем – перезагрузку.

Полученное программное обеспечивание проходит проверку. Если версия нового программного обеспечения совпадает с версией текущего программного обеспечения, коммутатор завершит процесс Auto-Image. Однако если включена функция Auto-Configuration, загрузка конфигурации продолжится.

Функция Auto-Image аналогична функции Auto-Configuration. IP-адрес TFTP-сервера также размещен в полях siaddr DHCP Option 66 или Option 150. Если ответное DHCP-сообщение содержит одновременно поля Option 66, Option 150 и siaddr, сначала будет обработано поле Option 150. Если системе не удается подключиться к TFTP-серверу, будет обработано поле Option 66. Если подключиться снова не удается, будет обработано поле siaddr.

Если коммутатор использует Option 66 для получения имени TFTP-сервера, сначала будет обработано Option 6, что позволит получить IP-адрес DNS-сервера. Если коммутатору не удается подключиться к DNS-серверу или ответное сообщение не содержит Option 6, коммутатор попытается подключиться к DNS-серверу, уже установленному в системе вручную.

Так как поля DHCP Option используются не только в функции Auto-Image, но и в функции Auto-Configuration, файл образа и файл конфигурации должны быть размещены на одном TFTP-сервере.

При указании имени файла образа необходимо использовать DHCP Option 125 (RFC 3925). Коммутатор проверяет поле enterprise-number1. Если его значение не совпадает с указанным D-Link Vendor ID (171), процесс будет остановлен. При наличии нескольких данных будут использоваться только первые данные enterprise-number1.

Пример

В данном примере показано, как включить функцию Auto-Image.

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

18.2 autoimage timeout

Данная команда используется для указания тайм-аута, в течение которого будет получен файл образа.

autoimage timeout *SECONDS*

Параметры

SECONDS	Укажите тайм-аут в диапазоне от 1 до 65535 секунд.

По умолчанию

Значение по умолчанию – 50 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы указать тайм-аут, в течение которого будет получен файл образа.

Пример

В данном примере показано, как настроить тайм-аут 60 секунд.

```
Switch#configure terminal
Switch(config)#autoimage timeout 60
Switch(config)#
```

18.3 show autoimage

Данная команда используется для отображения статуса Auto-Image.

show autoimage

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статус Auto-Image.

Пример

В данном примере показано, как отобразить статус Auto-Image.

```
Switch#show autoimage

Autoimage State: Disabled
Timeout        : 60

Switch#
```

19. Команды DHCP Client

19.1 ip dhcp client class-id

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

ip dhcp client class-id {*STRING* **| hex** *HEX-STRING***}**

no ip dhcp client class-id

Параметры

STRING	Укажите Vendor Class Identifier в формате строки. Максимальная длина строки – 32 символа.
hex *HEX-STRING*	Укажите Vendor Class Identifier в шестнадцатеричном формате. Максимальная длина строки – 64 символа.

По умолчанию

По умолчанию в качестве ID класса используется тип устройства.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

19.2 ip dhcp client client-id

Данная команда используется для обозначения интерфейса VLAN, шестнадцатеричный MAC-адрес которого будет использован в качестве ID клиента, отправляемого в сообщении Discover. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

INTERFACE-ID	Укажите интерфейс VLAN, шестнадцатеричный MAC-адрес которого 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)#
```

19.3 ip dhcp client hostname

Используйте данную команду, чтобы указать значение опции имени узла (Host Name) для отправки в сообщении DHCP Discover. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip dhcp client hostname *HOST-NAME*
no ip dhcp client hostname

Параметры

HOST-NAME	Укажите имя узла. Максимальная длина строки – 64 символа. Имя узла должно начинаться с буквы, заканчиваться буквой или цифрой, внутри можно использовать буквы, цифры 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)#
```

19.4 ip dhcp client lease

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

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

Параметры

DAYS	Укажите продолжительность аренды в днях. Допустимый диапазон: от 0 до 10000 дней.
HOURS	(Опционально.) Укажите продолжительность аренды в часах. Допустимый диапазон: от 0 до 23 часов.
MINUTES	(Опционально.) Укажите продолжительность аренды в минутах. Допустимый диапазон: от 0 до 59 минут.

По умолчанию

Время аренды не запрашивается.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

20. Команды DHCP Relay

20.1 class (DHCP Relay)

Данная команда используется для входа в режим DHCP Pool Class Configuration Mode и привязки диапазона IP-адресов к DHCP-классу. Для удаления привязки воспользуйтесь формой **no** этой команды.

class *NAME*
no class *NAME*

Параметры

NAME	Укажите имя DHCP-класса. Максимальная длина – 32 символа.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для привязки пула DHCP relay pool к DHCP pool class. Используйте команду **relay target**, чтобы указать список адресов relay target для перенаправления DHCP-пакета. Если запрос DHCP-клиента совпадает с пулом relay, настроенным с классами, клиент должен соответствовать классу, настроенному в пуле, для ретрансляции. Если DHCP-класс не настроен, запрос будет сопоставляться только с пулом relay и будет ретранслироваться на сервер назначения relay, указанный для соответствующего пула relay.

Пример

В данном примере показано, как настроить DHCP-класс, «Service-A», определенный шаблоном соответствия DHCP Option 60 в виде 0x112233 и 0x102030, классифицированным для пула relay, «pool1», и связанный с relay target «10.2.1.2».

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

20.2 ip dhcp class (DHCP Relay)

Данная команда используется для указания DHCP-класса и входа в режим DHCP Class Configuration Mode. Для удаления DHCP-класса воспользуйтесь формой **no** этой команды.

ip dhcp class *NAME*
no ip dhcp class *NAME*

Параметры

NAME	Укажите имя DHCP-класса, содержащее не более 32 символов в длину.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для входа в режим DHCP Class Configuration Mode и команду **option hex** для указания шаблона соответствия для DHCP-класса. Если у класса нет связанной с ним шестнадцатеричной опции, то классу будет соответствовать любой пакет.

Пример

В данном примере показано, как настроить DHCP-класс Service-A и указать шаблон соответствия DHCP Option 60 в виде 0x112233.

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

20.3 ip dhcp pool (DHCP Relay)

Данная команда используется для настройки пула DHCP Relay на DHCP Relay Agent и входа в режим DHCP Pool Configuration Mode. Для удаления пула DHCP Relay воспользуйтесь формой **no** данной команды.

ip dhcp pool *NAME*
no ip dhcp pool *NAME*

Параметры

NAME	Укажите имя пула адресов. Максимальное 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 с помощью команды **ip dhcp pool**, затем при помощи команды **relay source** укажите подсеть-источник (source) запросов клиента, далее 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.

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)#
```

20.4 ip dhcp relay information check

Данная команда позволяет включить в DHCP Relay Agent проверку/удаление информации Relay Agent Information Option (Option 82) в полученном пакете DHCP-ответа. Для глобального отключения функции Check для Option 82 воспользуйтесь формой **no** этой команды.

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), то 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 глобальное включение функции Check DHCP Relay Agent.

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

20.5 ip dhcp relay information check-reply

Данная команда используется для настройки в DHCP Relay Agent проверки информации Relay Agent Information Option (Option 82) в полученном пакете DHCP-ответа. Для удаления данных настройки для интерфейса воспользуйтесь формой **no** этой команды.

ip dhcp relay information check-reply [none]

no ip dhcp relay information check-reply [none]

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 глобально отключить 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)#
```

20.6 ip dhcp relay information option

Данная команда используется, чтобы включить вставку информации о Relay Agent (Option 82) в ретранслируемых пакетах DHCP-запроса. Для отключения данной функции воспользуйтесь формой **no** этой команды.

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 действует при включенной команде **service dhcp**.

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

Администраторы могут использовать команду **ip dhcp relay information option remote-id**, чтобы указать строку, заданную 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)#
```

20.7 ip dhcp relay information option-insert

Данная команда используется для включения/выключения встраивания Option 82 для интерфейса в ретранслируемые пакеты DHCP-запроса. Для удаления настроек данной функции воспользуйтесь формой **no** этой команды.

ip dhcp relay information option-insert [none]

no ip dhcp relay information option-insert [none]

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)#
```

20.8 ip dhcp relay information policy

Данная команда используется для настройки алгоритма перенаправления Option 82 для DHCP Relay Agent. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 действует при включенной команде **service dhcp**.

Используйте данную команду для настройки общего алгоритма встраивания Option 82 в пакеты, у которых уже есть Option 82.

Если сконфигурирована данная команда, а команда **ip dhcp relay information policy-action** сконфигурирорвана не в режиме Interface Configuration Mode, настройки будут применены ко всем интерфейсам.

Пример

В данном примере показано, как настроить алгоритм перенаправления Relay Agent Option (Option 82) с помощью параметра keep.

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

20.9 ip dhcp relay information policy-action

Данная команда используется, чтобы настроить алгоритм перенаправления Option 82 для DHCP Relay Agent на интерфейсе. Для отмены конфигурации воспользуйтесь формой **no** этой команды.

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 действует, если запущена команда **service 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)#
```

20.10 ip dhcp relay information option format remote-id

Данная команда используется для настройки sub-опции Remote ID DHCP. Для применения настроек по умолчанию воспользуйтесь формой **no** этой команды.

ip dhcp relay information option format remote-id {default| string *STRING* **| vendor2 | vendor3}**

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  |
|-------------------------------------------------|
```

string *STRING*	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.** *Тип sub-опции*: число 2 указывает, что это remote ID. **b**. *Длина*: длина значения. **c**. *Значение*: строка символов. Системное имя коммутатора.
vendor3	Укажите, чтобы использовать vendor 3. Оригинальный формат Remote ID представлен ниже: |-----|-----|-----| | a. | b. | c. | |-----|-----|-----| | 2 | n | User Defined | |-----|-----|-----| | 1 byte | 1 byte | Max. 251 bytes | |-----|-----|-----| **a.** *Тип sub-опции*: число 2 указывает, что это 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 команды **ip dhcp relay information option format-type remote-id vendor3 string** *STRING*. Максимальная длина строки – 32 символа.

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 примере ниже 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)#
```

20.11 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. Для удаления sub-опции Remote ID как строки формата vendor воспользуйтесь формой **no** этой команды.

ip dhcp relay information option format-type remote-id vendor3 string *STRING*

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

Параметры

vendor3	Укажите строку vendor 3, задаваемую пользователем. Максимальная длина строки – 32 символа.
STRING	Укажите строку, задаваемую vendor-ом.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применима исключительно для настройки интерфейсов физического порта и 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 vendor 3 remote-id для интерфейса Ethernet 1/0/1. В примере используется строка «switch1».

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip dhcp relay information option format-type remote-id vendor3 string
switch1
Switch(config-if)#
```

20.12 ip dhcp relay information option format circuit-id

Данная команда используется для настройки sub-опции Circuit ID DHCP. Для применения настроек по умолчанию воспользуйтесь формой **no** этой команды.

ip dhcp relay information option format circuit-id {default | string *STRING* **| vendor1 | vendor2 | vendor3 | vendor4 | vendor5 | vendor6}**

no ip dhcp relay information option format circuit-id

Параметры

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

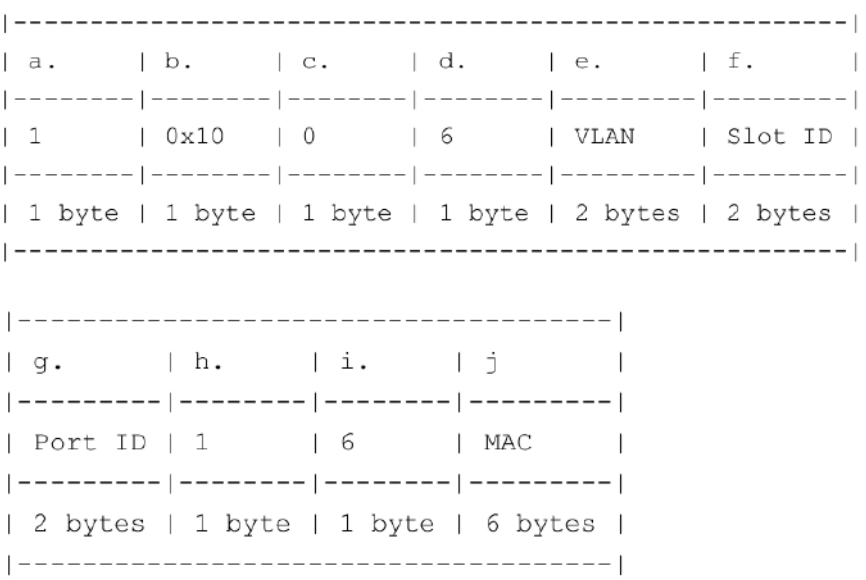
a.	b.	c.	d.	e.	f.	g.
1	0x6	0	4	VLAN	Module ID	Port ID
1 byte	1 byte	1 byte	1 byte	2 bytes	1 byte	1 byte

a. *Тип sub-опции*: число 1 свидетельствует о том, что тип данного 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.
STRING	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.** *Тип sub-опции*: число 1 свидетельствует о том, что тип данного 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 в стеке. **g**. *ID порта*: номер порта для каждого Unit ID. **h.** *Второй тег sub-опции Circuit ID*: необходимое значение – 1. **i**. *Длина второго тега*: необходимое значение – 6. **j**. *MAC-адрес*: системный MAC-адрес коммутатора.

vendor2	Укажите, чтобы использовать vendor2. Формат Circuit ID представлен ниже: |----------|----------|----------| | a. | b. | c. | |----------|----------|----------| | 1 | n | Port Number | |----------|----------|----------| | 1 byte | 1 byte | n byte | |----------|----------|----------| **a.** *Тип sub-опции*: число 1 свидетельствует о том, что тип данного ID – Circuit ID. **b**. *Длина*: длина значения. **c**. *Значение*: строка символов. Номер входящего порта в пакете DHCP Client формируется в формате строки и начинается с символа «p». Например, «p02» используется для обозначения порта 2. (При отсутствии типа sub-опции Circuit ID значение заполняется напрямую.) Формат порта 1 для портов стекирования на коммутаторе unit 3 – p 129. Максимальное количество портов, предназначенных для одного коммутатора – 64.
vendor3	Укажите, чтобы использовать vendor3. Формат Circuit ID представлен ниже: |----------|----------|----------| | a. | b. | c. | |----------|----------|----------| | 1 | n | User Defined | |----------|----------|----------| | 1 byte | 1 byte | Max. 32 bytes | |----------|----------|----------| **a.** *Тип sub-опции*: число 1 свидетельствует о том, что тип данного ID – Circuit 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 команды **ip dhcp relay information option format-type remote-id vendor3 string** *STRING*. Максимальная длина строки – 32 символа. (При отсутствии типа sub-опции Circuit ID значение заполняется напрямую.)

vendor4	Укажите, чтобы использовать vendor4. Формат Circuit ID представлен ниже:

a.	b.	c.	d.	e.	f.	g.	h.
1	n	System Name	-	Module ID	/	Port ID	-
1 byte	1 byte	0 to 128 bytes	1 byte	1 byte	1 byte	1 to 2 bytes	1 byte

i.
CVID
1 to 4 bytes

a. *Тип sub-опции*: число 1 свидетельствует о том, что тип данного ID – Circuit ID.

b. *Длина*: общая длина всех следующих строк.

c. Системное имя.

d. *Отдельный символ.*

e. *ID модуля*: необходимое значение для автономных коммутаторов – 1, для стекированных коммутаторов – Unit ID.

f. *Отдельный символ.*

g. *ID порта*: номер порта для каждого Unit ID.

h. *Отдельный символ.*

i. *CVID*: VLAN ID клиента. Если включена технология Q-in-Q, VLAN является внутренней. В противном случае – VLAN является внешней.

vendor5	Укажите, чтобы использовать vendor5. Формат Circuit ID представлен ниже:

a.	b.	c.	d.	e.	f.	g.	h.
1	n	System Name	space (0x20)	e (0x65)	t (0x74)	h (0x68)	space (0x20)
1 byte	1 byte	0 to 128 bytes	1 byte	1 byte	1 byte	1 byte	1 byte

i.	j.	k.	l.	m.	n.	o.
Chassis ID	/ (0x2F)	Slot ID	/ (0x2F)	Port Number	: (0x3A)	VLAN ID
1 to 2 bytes	1 byte	1 to 2 bytes	1 byte	1 byte	1 byte	1 to 4 bytes

a. *Тип sub-опции*: число 1 свидетельствует о том, что тип данного ID – Circuit ID.

b. *Длина*.

c. *Системное имя*: системное имя коммутатора. Если длина имени превышает 128 байт, будут использованы только первые 128 байт.

d. *Пробел.*

e. *e:* код ASCII – 0x65.

f. t*:* код ASCII – 0x74.

g. h*:* код ASCII – 0x68.

h. *Пробел:* код ASCII – 0x20.

i. *ID шасси:* номер шасси. ID шасси для автономных коммутаторов – 0. ID шасси для стекированных коммутаторов – Unit ID.

j. *Косая черта (/):* код ASCII – 0x2F.

k. *ID слота*: номер слота шасси. ID слота для устройств без шасси – ID модуля. Начальное значение – 0.

l. *Косая черта (/):* код ASCII – 0x2F.

m. *Номер порта:* номер порта клиента.

n. *Двоеточие (:):* код ASCII – 0x3A.

o. *VLAN ID:* ID VLAN клиента.

vendor6

Укажите, чтобы использовать vendor6. Формат Circuit ID представлен ниже:

F01	F02	F03	F04	F05	F06	F07	F08
1	Length	E	t	h	e	r	n
		(0x45)	(0x74)	(0x68)	(0x65)	(0x72)	(0x6E)
1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte

F09	F10	F11	F12	F13	F14	F15	F16
e	t	Chassis	/	0	/	Port	:
(0x65)	(0x74)	ID	(0x2F)	(0x30)	(0x2F)	Number	(0x3A)
1 byte	1 byte	1 to 2 bytes	1 byte	1 byte	1 byte	1 to 2 bytes	1 byte

F17	F18	F19	F20	F21	F22	F23	F24
cvlan	.	0	Space	System	/	0	/
	(0x2E)	(0x30)	(0x20)	Name	(0x2F)	(0x30)	(0x2F)
1 to 4 bytes	1 byte	1 byte	1 byte	1 to 128 bytes	1 byte	1 byte	1 byte

F25	F26	F27	F28	F29	F30	F31
0	/	Chassis	/	0	/	Port
(0x30)	(0x2F)	ID	(0x2F)	(0x30)	(0x2F)	Number
1 byte	1 byte	1 to 2 bytes	1 byte	1 byte	1 byte	1 to 2 bytes

F01. *Тип sub-опции*: число 1 свидетельствует о том, что тип данного ID – Circuit ID.
F02. *Длина*
F03. *E:* код ASCII – 0x45.
F04. *t*: код ASCII – 0x74.
F05. *h:* код ASCII – 0x68.
F06. *e:* код ASCII – 0x65.
F07. *r:* код ASCII – 0x72.
F08. *n*: код ASCII – 0x6E.
F09. *e*: код ASCII – 0x65.
F10. *t*: код ASCII – 0x74.
F11. *ID шасси:* номер шасси. Формат строки – ASCII. ID шасси для автономных коммутаторов – 1. ID шасси для стекированных коммутаторов – Unit ID.
F12. *Косая черта (/):* код ASCII – 0x2F.

F13. *0:* Код ASCII – 0x30.
F14. *Косая черта (/):* код ASCII – 0x2F.
F15. *Номер порта:* номер входящего порта в пакете DHCP Client. Формат строки – ASCII.
F16. *Двоеточие (:):* код ASCII – 0x3A.
F17. *cvlan:* VLAN ID клиента. Диапазон значений: от 1 до 4094.
F18. *Точка (.):* код ASCII – 0x2E.
F19. *0:* код ASCII – 0x30.
F20. *Пробел:* код ASCII – 0x20.
F21. *Системное имя:* системное имя коммутатора. Если длина имени превышает 128 байт, будут использованы только первые 128 байт.
F22. *Косая черта (/):* код ASCII – 0x2F.
F23. *0:* Код ASCII – 0x30.
F24. *Косая черта (/):* код ASCII – 0x2F.
F25. *0:* Код ASCII – 0x30.
F26. *Косая черта (/):* код ASCII – 0x2F.
F27. *ID шасси:* номер шасси. Формат строки – ASCII. ID шасси для автономных коммутаторов – 1. ID шасси для стекированных коммутаторов – Unit ID.
F28. *Косая черта (/):* код ASCII – 0x2F.
F29. *0:* Код ASCII – 0x30.
F30. *Косая черта (/):* код ASCII – 0x2F.
F31. *Номер порта*: номер входящего порта в пакете DHCP Client. Формат строки – ASCII.

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 примере ниже 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)#
```

20.13 ip dhcp relay information option format-type circuit-id

Данная команда используется для настройки sub-опции Circuit ID DHCP. Для удаления sub-опции Circuit ID воспользуйтесь формой **no** этой команды.

ip dhcp relay information option format-type circuit-id vendor3 string *STRING*
no ip dhcp relay information option format-type circuit-id vendor3 string

Параметры

vendor3	Укажите строку vendor3, задаваемую пользователем. Максимальное количество символов – 32.
STRING	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 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 vendor3 «abc» для интерфейса Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)# ip dhcp relay information option format-type circuit-id vendor3 string abc
Switch(config-if)#
```

20.14 ip dhcp relay information trust-all

Данная команда позволяет назначить на DHCP Relay Agent все интерфейсы, отправляющие информацию об IP DHCP Relay, доверенными. Для отключения функции Trust для всех интерфейсов воспользуйтесь формой **no** этой команды.

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.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information trust-all
Switch(config)#
```

20.15 ip dhcp relay information trusted

Данная команда позволяет назначить на DHCP Relay Agent определенный интерфейс, отправляющий информацию об IP DHCP Relay, в качестве доверенного. Для отключения функции Trust воспользуйтесь формой **no** этой команды.

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 снять статус trust для всех интерфейсов на DHCP Relay Agent 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)#
```

20.16 ip dhcp local-relay vlan

Данная команда используется для включения Local Relay на одной из VLAN или группе VLAN. Для отключения данной функции воспользуйтесь формой **no** этой команды.

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 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

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 member-порты 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)#
```

20.17 ip dhcp smart-relay

Данная команда используется для включения Smart Relay DHCP Relay Agent. Для отключения функции воспользуйтесь формой **no** данной команды.

ip dhcp smart-relay

no ip dhcp smart-relay

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если у полученного интерфейса пакета есть второстепенные адреса, по умолчанию Relay Agent установит поле адреса шлюза пакета в основной адрес интерфейса. Если включена функция Smart Relay, Relay Agent будет подсчитывать количество попыток отправить сообщение DISCOVER, предпринятых клиентом. По истечении трех попыток Relay Agent изменит адрес шлюза на второстепенный адрес полученного интерфейса.

Пример

В данном примере показано, как включить Smart Relay.

```
Switch#configure terminal
Switch(config)#ip dhcp smart-relay
Switch(config)#
```

20.18 option hex (DHCP Relay)

Данная команда используется, чтобы указать шаблон соответствия DHCP option для DHCP-класса. Для удаления указанного шаблона соответствия для DHCP-класса воспользуйтесь формой **no** этой команды.

option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

no option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

Параметры

CODE	Укажите номер DHCP option.
PATTERN	Укажите шестнадцатеричный шаблон определенной DHCP option. Шаблон должен содержать четное количество символов.

*	Укажите оставшиеся биты, которые не будут соответствовать. Если параметр * не указан, количество битов шаблона должно быть таким же, что и количество битов опции.
MASK	Укажите шестнадцатеричную битовую маску для шаблона. Биты маски шаблона будут соответствующими. Если маска не указана, все биты, указанные шаблоном, будут проверены. Набор битов, например, 1, будет проверен. Формат ввода должен быть таким же, как и у шаблона. Маска поддерживает только 00 или FF.

По умолчанию

Нет.

Режим ввода команды

DHCP Class Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Пользователь может использовать команду **ip dhcp class** наряду с командой **option hex**, чтобы указать DHCP-класс. Классы в пуле распределяются в том порядке, в котором они настроены в пуле адресов.

Команда **option hex** применяется для указания номера DHCP-опции с шаблоном соответствия для DHCP-класса. Для одного DHCP-класса можно указать несколько шаблонов опции. Если пакет соответствует какому-либо из указанных шаблонов DHCP-класса, он будет причислен к DHCP-классу и передан в указанное место назначения

Ниже приведены некоторые часто используемые номера 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 с шаблоном соответствия DHCP Option 60 в виде 0x112233 и 0x102030.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#option 60 hex 102030
Switch(config-dhcp-class)#
```

В примере ниже показано, как настроить DHCP-класс Service-B с шаблоном соответствия DHCP Option 60 в виде 0x5566 * и 0x5060 *.

```
Switch#configure terminal
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)#
```

В данном примере показано, как настроить DHCP-класс Service-C с шаблоном соответствия DHCP Option 60 в виде 0x506007 с битовой маской 00FF00.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-C
Switch(config-dhcp-class)#option 60 hex 506007 bitmask 00FF00
Switch(config-dhcp-class)#
```

20.19 relay destination

Данная команда используется для указания IP-адреса назначения DHCP Relay Destination, ассоциированного с пулом Relay. Для удаления Relay Destination из пула DHCP Relay воспользуйтесь формой **no** этой команды.

relay destination *IP-ADDRESS*
no relay destination *IP-ADDRESS*

Параметры

IP-ADDRESS	Укажите IP-адрес DHCP Relay Destination Server.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Relay Destination DHCP-сервера можно указать в пуле DHCP Relay. Для этого войдите в режим настройки пула DHCP при помощи команды **ip dhcp pool**, далее при помощи команды **relay source** укажите подсеть-источник (source) запросов клиента. После чего с помощью команды **relay destination** укажите адрес Relay Destination Server. В пуле можно указать несколько адресов Relay Source и Relay Destination. Если пакет соответствует какому-либо из адресов Relay Source, он будет отправлен на все адреса Relay Destination.

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)#
```

20.20 relay source

Данная команда используется для указания подсети-источника (source) пакетов клиента. Для удаления подсети-источника воспользуйтесь формой **no** этой команды.

relay source *IP-ADDRESS SUBNET-MASK*
no relay source *IP-ADDRESS SUBNET-MASK*

Параметры

IP-ADDRESS	Укажите исходную подсеть-источник (source) пакетов клиента.
SUBNET-MASK	Укажите маску подсети-источника (source).

По умолчанию

Нет.

Режим ввода команды

Global Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Наряду с пакетами DHCP Relay, подчиняющимися команде **ip helper-address**, Relay Destination DHCP-Relay-сервера можно указать в пуле DHCP Relay. Для этого войдите в режим настройки пула

DHCP при помощи команды **ip dhcp pool**, затем при помощи команды **relay source** укажите подсеть-источник (source) запросов клиента, после чего при помощи команды **relay destination** укажите адрес Relay Destination Server. В пуле можно указать несколько адресов Relay Source и Relay Destination. Если пакет соответствует какому-либо из адресов Relay Source, он будет отправлен на все адреса Relay Destination.

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.

Пример

В данном примере показано, как создать пул DHCP relay под именем «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)#
```

20.21 relay target

Данная команда используется, чтобы указать DHCP Relay Target для ретранслируемых пакетов в соответствии с шаблоном значений опции, установленной в классе. Для удаления Relay Target воспользуйтесь формой **no** этой команды.

relay target *IP-ADDRESS*
no relay target *IP-ADDRESS*

Параметры

IP-ADDRESS	Укажите IP-адрес сервера relay target для класса.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Class Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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)#
```

20.22 service dhcp (DHCP Relay)

Данная команда используется для включения сервиса DHCP Relay на коммутаторе. Для отключения сервиса DHCP Relay воспользуйтесь формой **no** этой команды.

service dhcp
no service dhcp

Параметры

Нет.

По умолчанию

По умолчанию сервис отключен.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применяется для включения DHCP-сервера и сервиса DHCP Relay на коммутаторе.

Пример

В данном примере показано, как отключить DHCP-сервер и сервис DHCP Relay.

```
Switch#configure terminal
Switch(config)#no service dhcp
Switch(config)#
```

20.23 show ip dhcp relay information trusted-sources

Данная команда используется для отображения всех интерфейсов, настроенных в качестве доверенных источников для опции DHCP Relay.

show ip dhcp relay information trusted-sources

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда применяется 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:
vlan100             vlan200             vlan300             vlan400
vlan500

Total Entries: 5

Switch#
```

В примере ниже 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#
```

20.24 show ip dhcp relay information option format-type

Данная команда используется для отображения настроек формата опций интерфейса.

show ip dhcp relay information option format-type [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите для отображения информации об интерфейсе.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда позволяет отобразить настройки формата опций интерфейса. Если параметр не указан, будет отображена информация обо всех интерфейсах.

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#
```

20.25 show ip dhcp relay information option-insert

Данная команда используется для отображения настройки встраивания Relay Option.

show ip dhcp relay information option-insert

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения Relay Information Option и информации о настройке встраивания.

Пример

В данном примере показано, как отобразить информацию об Option 82 и информацию о настройке встраивания этой опции для всех VLAN.

```
Switch#show ip dhcp relay information option-insert

Interface     Option-Insert
------------ ----------
vlan1         Enabled
vlan2         Disabled
vlan3         Not Configured

Total Entries: 3

Switch#
```

20.26 show ip dhcp relay information policy-action

Данная команда позволяет отобразить информацию об алгоритме перенаправления Relay Option для интерфейса.

show ip dhcp relay information policy-action

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения информации об алгоритме перенаправления Relay Option.

Пример

В данном примере показано, как отобразить информацию об алгоритме перенаправления Option 82 для всех VLAN.

```
Switch#show ip dhcp relay information policy-action

Interface      Policy
-------------- ----------
vlan1          Keep
vlan2          Drop
vlan3          Replace
vlan4          Not configured

Total Entries: 3

Switch#
```

20.27 ip dhcp relay unicast

Данная команда позволяет настроить DHCP Relay и Local Relay Agent для обработки одноадресных DHCP-пакетов. Для отмены обработки одноадресных DHCP-пакетов воспользуйтесь формой **no** этой команды.

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, то 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)#
```

20.28 ip dhcp relay

Данная команда используется для включения DHCP Relay на интерфейсе. Для отключения функции воспользуйтесь формой **no** этой команды.

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

Используйте команду для включения/отключения DHCP Relay на интерфейсе.

Пример

В данном примере показано, как включить обработку одноадресных пакетов DHCP-клиента на коммутаторе.

```
Switch#configure terminal
Switch(config)#service dhcp
Switch(config)#interface eth1/0/2
Switch(config-if)#ip dhcp relay
Switch(config-if)#
```

21. Команды DHCP Server

21.1 address range

Данная команда используется для обозначения диапазона IP-адресов, которые необходимо ассоциировать с DHCP-классом в пуле DHCP-адресов. Чтобы удалить диапазон адресов, которые необходимо ассоциировать с DHCP-классом, воспользуйтесь формой **no** этой команды.

address range *START-IP-ADDRESS END-IP-ADDRESS*
no address range *START-IP-ADDRESS END-IP-ADDRESS*

Параметры

START-IP-ADDRESS	Укажите адрес или первый адрес в диапазоне адресов.
END-IP-ADDRESS	Укажите последний адрес в диапазоне адресов.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Class Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команды **address range** и **class** в конфигурации пула DHCP используются для того, чтобы ограничить выделение IP-адресов из подсети. Сеть разбивается на разделы на основе значения опции DHCP-запроса. Если в пуле адресов определены классы и применена команда **ip dhcp use class**, назначение адреса будет основано на классе этого адресного пула.

Когда сервер пытается выделить адрес из пула адресов, и если у пула определены классы, то сервер сначала проверит, содержит ли пул запрашиваемую подсеть. Если подсеть пула адресов содержит GIADDR (не равно нулю) или подсеть принимаемого интерфейса, то сервер будет выделять из пула адрес, соответствующий определенному классу.

Для удаления диапазона адресов можно указать только точный диапазон адресов, который уже был ранее настроен.

Пример

В данном примере показано, как создать DHCP-класс «Customer-A» с шаблоном, соответствующим Relay Information Option (Option 82). Он ассоциирован с диапазоном адресов DHCP «pool1».

```
Switch# configure terminal
Switch(config)# ip dhcp class Customer-A
Switch(config-dhcp-class)# option 82 hex 1234 *
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# network 172.28.5.0/24
Switch(config-dhcp-pool)# class Customer-A
Switch(config-dhcp-pool-class)# address range 172.28.5.1 172.28.5.12
witch(config-dhcp-pool-class)#
```

21.2 bootfile

Используйте данную команду, чтобы указать файл конфигурации для загрузки на устройство DHCP-клиента. Для удаления загрузочного файла воспользуйтесь формой **no** этой команды.

bootfile *URL*
no bootfile

Параметры

URL	Укажите URL файла загрузки. Максимальное количество символов – 64.

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 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.cfg» для DHCP-пула «pool1» в качестве загрузочного.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#bootfile mdubootfile.cfg
Switch(config-dhcp-pool)#
```

21.3 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 указан IP-адрес, то автоматическая запись привязки, относящаяся к IP-адресу, будет удалена независимо от пула. 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 примере ниже показано, как удалить все привязки изо всех пулов.

```
Switch# clear ip dhcp all binding *
Switch#
```

В следующем 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#
```

21.4 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 удалить.

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 проверки ping.

Если задан параметр **pool**, а значение IP-адреса – «*», то все записи конфликта, относящиеся к пулу, будут удалены. Если значение параметра **pool** – all, и указан IP-адрес, то указанная запись конфликта будет удалена независимо от пула. 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 примере ниже показано, как удалить все адресные конфликты из базы данных DHCP-сервера.

```
Switch# clear ip dhcp all conflict *
Switch#
```

В следующем примере показано, как удалить все адресные конфликты из пула адресов «pool1».

```
Switch# clear ip dhcp pool pool1 conflict *
Switch#
```

В нижеприведенном 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#
```

21.5 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 сбросить все счетчики DHCP.

```
Switch# clear ip dhcp server statistics
Switch#
```

21.6 class (DHCP Server)

Данная команда используется для привязки диапазона IP-адресов к DHCP-классу. Чтобы удалить привязку, воспользуйтесь формой **no** этой команды.

class *NAME*
no class *NAME*

Параметры

NAME	Укажите имя DHCP-класса. Максимальное 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.

Пример

В данном примере показано, как создать два DHCP-класса «Customer-A» и «Customer-B» с шаблонами соответствия Option 82. Они ассоциированы с диапазонами адресов DHCP-сервера «srv-pool1».

```
Switch#configure terminal
Switch(config)#ip dhcp class Customer-A
Switch(config-dhcp-class)#option 82 hex 1234 *
Switch(config-dhcp-class)#exit
Switch(config)#ip dhcp class Customer-B
Switch(config-dhcp-class)#option 82 hex 5678 *
Switch(config-dhcp-class)#exit
Switch(config)#ip dhcp pool srv-pool1
Switch(config-dhcp-pool)#network 172.28.5.0/24
Switch(config-dhcp-pool)#class Customer-A
Switch(config-dhcp-pool-class)#address range 172.28.5.1 172.28.5.12
witch(config-dhcp-pool-class)#exit
Switch(config-dhcp-pool)#class Customer-B
Switch(config-dhcp-pool-class)#address range 172.28.5.18 172.28.5.32
Switch(config-dhcp-pool-class)#
```

В примере ниже показано, как настроить DHCP-класс «Service-A» и задать шаблоны соответствия Option 60 DHCP в виде 0x112233 и 0x102030. Другой класс «Service-B» настроен и задан с шаблонами

соответствия Option 60 DHCP в виде 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 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)#class Service-A
Switch(config-dhcp-pool-class)#relay target 10.2.1.2
Switch(config-dhcp-pool-class)#exit
Switch(config-dhcp-pool)#class Service-B
Switch(config-dhcp-pool-class)#relay target 10.2.1.5
Switch(config-dhcp-pool)#exit
Switch(config-dhcp-pool)#class Default-class
Switch(config-dhcp-pool-class)#relay target 10.2.1.32
Switch(config-dhcp-pool)#
```

21.7 client-identifier

Данная команда используется для указания уникального ID DHCP-клиента в записи ручной привязки пула DHCP-адресов. Чтобы удалить ID клиента, воспользуйтесь формой **no** этой команды.

client-identifier *IDENTIFIER*
no client-identifier

Параметры

IDENTIFIER	Укажите ID 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. ID 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 аппаратным адресом узла.

Используйте команды **client-identifier** и **host**, чтобы указать запись привязки, созданной вручную на основе ID 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 01524153203124.

```
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)#
```

21.8 default-router

Данная команда используется, чтобы указать шлюзы по умолчанию для DHCP-клиента. Для удаления шлюза по умолчанию воспользуйтесь формой **no** этой команды.

default-router *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**
no default-router *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**

Параметры

IP-ADDRESS	Укажите IP-адрес шлюза по умолчанию для DHCP-клиента.
IP-ADDRESS2...IP-ADDRESS8	Укажите несколько IP-адресов, разделяя их при помощи пробелов. Максимально допустимое количество адресов – 8.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется, чтобы настроить шлюз по умолчанию для клиента. IP-адрес шлюза должен принадлежать той же сети, что и подсеть клиента. Шлюзы перечисляются в порядке приоритетности. Если шлюзы по умолчанию уже настроены, то шлюзы, настраиваемые позже, будут добавлены в список.

Пример

В данном примере показано, как указать IP-адрес шлюза по умолчанию в пуле DHCP-адресов. Настроенный 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
```

21.9 domain-name

Данная команда используется, чтобы указать доменное имя для DHCP-клиента. Используйте форму **no** для удаления доменного имени.

domain-name *NAME*
no domain-name

Параметры

NAME	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 применяется, чтобы настроить доменное имя для DHCP-клиента. Можно указать не более одного доменного имени.

Пример

В данном примере показано, как указать доменное имя в пуле DHCP-адресов. Настроенное доменное имя – domain.com.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# domain-name domain.com
```

21.10 dns-server

Данная команда используется, чтобы указать DNS-серверы для DHCP-клиента. Для удаления указанного DNS-сервера воспользуйтесь формой **no** этой команды.

dns-server *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**

no dns-server *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**

Параметры

IP-ADDRESS	Укажите IP-адреса, которые будут использованы DHCP-клиентом в качестве DNS-сервера.
IP-ADDRESS2...IP-ADDRESS8	Укажите несколько IP-адресов, используя пробелы. Максимальное 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.

Пример

В данном примере показано, как указать IP-адрес DNS-сервера в пуле DHCP-адресов. Настроенный IP-адрес – 10.1.1.1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# dns-server 10.1.1.1
```

21.11 hardware-address

Данная команда используется для указания аппаратного адреса в созданной вручную записи привязки пула DHCP-адресов. Чтобы удалить аппаратный адрес созданной вручную записи привязки, воспользуйтесь формой **no** этой команды.

hardware-address *HARDWARE-ADDRESS*
no hardware-address

Параметры

HARDWARE-ADDRESS	Укажите MAC-адрес клиента.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Запись привязки – это сопоставление IP-адреса с аппаратным адресом оборудования или ID клиента. При создании записи привязки IP-адрес присваивается клиенту вручную.

В пуле DHCP-адресов может быть указано не более одной записи привязки. С помощью записи привязки IP-адрес может быть связан с ID клиента или с аппаратным адресом узла.

Используйте команды **client-identifier** и **host**, чтобы настроить вручную запись привязки на основе ID клиента в DHCP-пакете. Команды **hardware-address** и **host** используются для настройки вручную записи привязки на основе аппаратного адреса.

Пример

В данном примере показано, как создать пул DHCP-адресов с настроенной вручную записью привязки, которая связывает IP-адрес 10.1.2.100/24 с MAC-адресом C2:F3:22:0A:12:F4. Указанное имя пула – pool1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# hardware-address C2F3.220A.12F4
Switch(config-dhcp-pool)# host 10.1.2.100/24
Switch(config-dhcp-pool)#
```

21.12 host

Данная команда используется для указания IP-адреса в настроенной вручную записи привязки пула DHCP-адресов. Чтобы удалить IP-адрес из записи, воспользуйтесь формой **no** этой команды.

host {*IP-ADDRESS MASK* **|** *IP-ADDRESS**|**PREFIX-LENGTH***}**
no host

Параметры

IP-ADDRESS	Укажите IP-адрес в настроенной вручную записи привязки.
MASK	Укажите биты, определяющие сетевую маску.
PREFIX-LENGTH	Укажите длину префикса сети. Это альтернативный способ указать сетевую маску.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

В пуле DHCP-адресов может быть указано не более одной записи привязки. С помощью записи привязки IP-адрес может быть связан с ID 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** применяются, чтобы настроить 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)#
```

21.13 ip dhcp class (DHCP Server)

Данная команда используется для настройки DHCP-класса и входа в режим DHCP Class Configuration Mode. Чтобы удалить DHCP-класс, воспользуйтесь формой **no** этой команды.

ip dhcp class *NAME*
no ip dhcp class *NAME*

Параметры

NAME	Укажите имя DHCP-класса. Максимальное 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 DHCP Class Configuration Mode и команду **option hex** для настройки соответствия шаблона опции с DHCP-классом. Если у класса отсутствует связка с шестнадцатеричной опцией, то классу будет соответствовать любой пакет.

Пример

В данном примере показано, как настроить DHCP-класс «Service-A» и установить шаблон соответствия DHCP Option 60 в виде 0x112233.

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

21.14 ip dhcp excluded-address

Данная команда используется, чтобы исключить диапазон IP-адресов для назначения клиенту. Для удаления исключенных адресов воспользуйтесь формой **no** этой команды.

ip dhcp excluded-address *START-IP-ADDRESS END-IP-ADDRESS*
no ip dhcp excluded-address *START-IP-ADDRESS END-IP-ADDRESS*

Параметры

START-IP-ADDRESS	Укажите адрес или первый адрес диапазона адресов, которые необходимо исключить.
END-IP-ADDRESS	Укажите последний адрес диапазона адресов, которые необходимо исключить.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

DHCP-сервер автоматически распределяет адреса из пула DHCP-адресов по DHCP-клиентам. Для распределения доступны все адреса, кроме IP-адреса интерфейса коммутатора и исключенных адресов, которые обозначены при помощи команды **ip dhcp excluded-address**. Можно задать несколько диапазонов исключенных адресов. Для удаления 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
```

21.15 ip dhcp ping packets

Данная команда используется для указания количества пакетов, которые будет отправлять DHCP-сервер в рамках проверки ping. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip dhcp ping packets *COUNT*
no ip dhcp ping packets

Параметры

COUNT	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 применяется для указания количества пакетов, отправляемых DHCP-сервером в рамках проверки ping. Проверка ping, 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 IP-адрес будет занесен в запись конфликта.

Укажите «0», чтобы отключить проверку ping.

Пример

В данном примере показано, как указать количество ping-пакетов. Заданное количество – 3.

```
Switch# configure terminal
Switch(config)# ip dhcp ping packets 3
Switch(config)#
```

21.16 ip dhcp ping timeout

Данная команда используется для указания времени ожидания ответного ping-пакета DHCP-сервером. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip dhcp ping timeout *MILLI-SECONDS*
no ip dhcp ping timeout

Параметры

MILLI-SECONDS	Укажите период ожидания ответного ping-пакета DHCP-сервером. Максимальный период ожидания – 10000 миллисекунд (10 секунд). Указанное значение должно быть кратным 100.

По умолчанию

Значение по умолчанию – 500 миллисекунд (0,5 секунды).

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для настройки периода ожидания проверки ping. DHCP-сервер отправляет 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 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)#
```

21.17 ip dhcp pool (DHCP Server)

Данная команда используется для настройки пула DHCP-адресов DHCP-сервера и входа в режим настройки DHCP Pool Configuration Mode. Чтобы удалить пул DHCP-адресов, воспользуйтесь формой **no** этой команды.

ip dhcp pool *NAME*
no ip dhcp pool *NAME*

Параметры

NAME	Укажите имя пула. Максимальное 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)#
```

21.18 ip dhcp use class

Данная команда применяется, чтобы позволить DHCP-серверу использовать DHCP-классы при распределении адресов. Для отключения использования DHCP-классов воспользуйтесь формой **no** этой команды.

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 применяется для того, чтобы позволить DHCP-серверу использовать DHCP-классы при распределении адресов.

Пример

В данном примере показано, как отключить использование DHCP-классов.

```
Switch# configure terminal
Switch(config)# no ip dhcp use class
Switch(config)#
```

21.19 lease

Данная команда используется для настройки периода аренды IP-адреса, назначаемого из пула адресов. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

lease {*DAYS* **[***HOURS* **[***MINUTES***]] | infinite}**
no lease

Параметры

DAYS	Укажите период аренды в днях.
HOURS	(Опционально.) Укажите период аренды в часах.
MINUTES	(Опционально.) Укажите период аренды в минутах.
infinite	Период аренды не ограничен.

По умолчанию

Период аренды по умолчанию – 1 день.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется 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 pool1. Указанное время аренды – 1 день.

```
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 pool1. Указанное время

аренды – 1 час.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# lease 0 1
```

21.20 netbios-node-type

Данная команда используется, чтобы настроить тип узла NetBIOS для DHCP-клиентов Microsoft. Для удаления настроек типа NetBIOS воспользуйтесь формой **no** этой команды.

netbios-node-type *NTYPE*
no netbios-node-type

Параметры

NTYPE	Укажите тип узла NetBIOS для клиента Microsoft. Используются следующие типы: **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 применяется, чтобы настроить тип 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. Указанный 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)#
```

21.21 netbios-name-server

Данная команда используется, чтобы указать WINS-серверы для DHCP-клиента Microsoft. Для удаления настроек указанных WINS-серверов воспользуйтесь формой **no** этой команды.

netbios-name-server *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**
no netbios-name-server *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**

Параметры

IP-ADDRESS	Укажите IP-адрес WINS-сервера для DHCP-клиента.
IP-ADDRESS2...IP-ADDRESS8	Укажите несколько IP-адресов, разделяя их пробелами. Максимальное количество серверов – 8.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для настройки IP-адресов WINS-сервера, доступных клиенту Microsoft. Максимальное количество серверов – 8. Серверы указываются в порядке приоритетности. Если серверы уже настроены, то серверы, настраиваемые позже, будут добавлены в список.

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)#
```

21.22 next-server

Данная команда используется, чтобы указать boot-сервер для DHCP-клиента. Для удаления boot-серверов воспользуйтесь формой **no** этой команды.

next-server *IP-ADDRESS*
no next-server

Параметры

IP-ADDRESS	Укажите IP-адрес boot-сервера, чтобы клиент получил файл загрузки.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для указания IP-адреса сервера для загрузки клиентом файла образа или конфигурации. Обычно используется TFTP-сервер. Максимальное количество boot-серверов – 1.

Пример

В данном примере показано, как настроить IP-адрес next-server в процессе загрузки DHCP-клиента в пуле «pool1». Указанный 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
```

21.23 network

Данная команда используется, чтобы настроить подсеть для пула DHCP-адресов. Для удаления подсети воспользуйтесь формой **no** этой команды.

network {*NETWORK-ADDRESS MASK* **|** *NETWORK-ADDRESS***/***PREFIX-LENGTH***}**
no network

Параметры

NETWORK-ADDRESS	Укажите адрес подсети для пула адресов.

MASK	Укажите биты, определяющие сетевую маску.
PREFIX-LENGTH	Укажите длину префикса сети (это альтернативный способ указать сетевую маску).

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется 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)#
```

21.24 option

Данная команда используется для настройки опций DHCP-сервера. Чтобы удалить определенную опцию, воспользуйтесь формой **no** этой команды.

option *CODE* **{ascii** *STRING* **| hex {***HEX-STRING* **| none} | ip** *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]}**

no option *CODE*

Параметры

CODE	Укажите номер опции в десятичном виде.
ascii *STRING*	Укажите формат строки ASCII для DHCP-опции. Максимальное количество байт – 255.
hex	Укажите шестнадцатеричный формат для DHCP-опции. Максимальное количество символов – 254.
HEX-STRING	Укажите шестнадцатеричную строку для DHCP-опции.
none	Укажите шестнадцатеричную строку нулевой длины.
ip *IP-ADDRESS*	Укажите IP-адрес. Максимальное количество IP-адресов – 8.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется 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. 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 примере ниже 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
```

21.25 option hex (DHCP Server)

Данная команда используется, чтобы настроить шаблон соответствия опции DHCP для DHCP-класса. Для удаления указанного шаблона соответствия воспользуйтесь формой **no** этой команды.

option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**
no option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

Параметры

CODE	Укажите номер DHCP-опции.
PATTERN	Укажите шестнадцатеричный шаблон указанной DHCP-опции. Длина должна быть выражена при помощи четного числа.
*	Укажите биты опции, которые не будут проверяться на соответствие. При отсутствии отметки со знаком * длина шаблона опции должна быть равна битовой длине опции.
MASK	Укажите 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. Маска каждого байта поддерживает только 00 или FF.

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 сопоставляются в порядке настройки.

С помощью команды **option hex** пользователь может указать номер DHCP-опции с шаблоном соответствия для 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 перенаправлен в указанное место назначения.

Ниже перечислены некоторые часто используемые номера 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 шаблоны соответствия DHCP Option 60 в виде 0x112233 и 0x102030.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#option 60 hex 102030
Switch(config-dhcp-class)#
```

В следующем примере показано, как настроить класс «Service-B» с шаблонами соответствия DHCP Option 60 в виде 0x5566* и 0x5060*.

```
Switch#configure terminal
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)#
```

В примере ниже показано, как настроить DHCP-класс «Service-C» с шаблоном соответствия DHCP Option 60 0x506007 с битовой маской 00FF00.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-C
Switch(config-dhcp-class)#option 60 hex 506007 bitmask 00FF00
Switch(config-dhcp-class)#
```

21.26 service dhcp (DHCP Server)

Данная команда используется для включения DHCP-сервера и Relay Service. Чтобы отключить DHCP-сервер и Relay Service, воспользуйтесь формой **no** этой команды.

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)#
```

21.27 show ip dhcp binding

Данная команда используется для отображения записей привязки адресов DHCP-сервера.

show ip dhcp binding [*IP-ADDRESS***]**

Параметры

IP-ADDRESS	(Опционально.) Укажите, чтобы отобразить запись привязки. Если IP-адрес не указан, отображаются все записи привязки или записи привязки указанного пула.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1

Использование команды

Будет отображен IP-адрес, аппаратный адрес и срок истечения периода аренды.

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 примере ниже 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#
```

21.28 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

IP-ADDRESS	(Опционально.) Укажите, чтобы отобразить запись конфликта. Если IP-адрес не указан, отображаются все записи конфликта или записи конфликта указанного пула.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

DHCP-сервер обнаруживает конфликт IP-адресов при помощи проверки ping. 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 примере ниже 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#
```

21.29 show ip dhcp pool

Данная команда используется для отображения информации о DHCP-пуле.

show ip dhcp pool [*NAME***]**

Параметры

NAME	(Опционально.) Укажите, чтобы отобразить информацию о DHCP-пуле.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы просмотреть параметры настроек пула. Если значение не задано, будут отображены параметры конфигурации всех пулов.

Пример

В данном примере показано, как отобразить информацию о настройках DHCP-пула «pool1».

```
Switch#show ip dhcp pool pool1

 Pool name: pool1
   Network: 10.0.0.0/8
   Boot file:
   Default router:
   DNS server:
   NetBIOS server:
   Domain name:
   Lease: 1 days 0 hours 0 minutes
   NetBIOS node type:
   Next server: 0.0.0.0
   Remaining unallocated address number: 1023
   Number of leased addresses: 1


Switch#
```

21.30 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.

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: Disabled
 Ping packets number: 2
 Ping timeout: 500 ms
 Excluded Addresses
  10.0.1.1 - 10.1.1.1
 List of DHCP server configured address pool
  pool10  pool11  pool12  pool13  pool14  pool2  pool3  pool4  pool5  pool6  pool7  pool8
pool9

Switch#
```

21.31 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.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить счетчики DHCP. Все счетчики суммируются.

Пример

В данном примере показано, как отобразить статистику DHCP-сервера.

```
Switch# show ip dhcp server statistics

Address pools              3
Automatic bindings         100
Manual binding             2
Malformed messages         0
Renew messages             0

Message             Received
BOOTREQUEST                12
DHCPDISCOVER               200
DHCPREQUEST                178
DHCPDECLINE                0
DHCPRELEASE                0
DHCPINFORM                 0

Message                 Sent
BOOTREPLY               12
DHCPOFFER               190
DHCPACK                 172
DHCPNAK                  6

Switch#
```

Отображаемые параметры

Address pools	Количество пулов, настроенных в базе данных DHCP.
Malformed messages	Количество поврежденных сообщений, полученных DHCP-сервером.
Renew messages	Количество renew-сообщений для времени аренды DHCP. Счетчик увеличивается, когда поступает новое renew-сообщение о продлении аренды.
Message	Тип DHCP-сообщения.
Received	Количество DHCP-сообщений, полученных DHCP-сервером.
Sent	Количество DHCP-сообщений, отправленных DHCP-сервером.

22. Команды DHCP Server Screening

22.1 based-on hardware-address

Данная команда используется для добавления записи профиля DHCP Server Screen. Чтобы удалить запись, воспользуйтесь формой **no** этой команды.

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

Параметры

CLIENT-HARDWARE-ADDRESS	Укажите MAC-адрес клиента.

По умолчанию

Нет.

Режим ввода команды

DHCP Server Screen Configure 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)#
```

22.2 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. Последующие пакеты из той же сессии не будут отправляться в модуль журнала событий, пока его запись в буфере не будет удалена.

Пример

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

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

22.3 dhcp-server-screen profile

Данная команда используется для настройки профиля Server Screen и входа в режим DHCP Server Screen Configure Mode. Используйте форму **no** для удаления профиля Server Screen.

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

Параметры

PROFILE-NAME	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)#
```

22.4 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

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

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применима исключительно 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 позволяет защитить сеть в случае, когда пакеты DHCP-сервера отправляются вредоносным узлом.

Если IP-адрес сервера не указан, на интерфейсе будет включен/отключен DHCP Server Screen. По умолчанию функция DHCP Server Screening отключена на всех интерфейсах. При ее включении 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 порта 3.

```
Switch#configure terminal
Switch(config)#dhcp-server-screen profile campus-profile
Switch(config-dhcp-server-screen)#based-on hardware-address 00-08-01-02-03-04
Switch(config-dhcp-server-screen)#based-on hardware-address 00-08-01-03-00-01
Switch(config-dhcp-server-screen)#exit
Switch(config)#interface eth1/0/3
Switch(config-if)#ip dhcp snooping server-screen 10.1.1.2 profile campus-profile
Switch(config-if)#
```

22.5 ip dhcp snooping server-screen log-buffer

Данная команда используется для настройки буфера журнала событий DHCP Server Screen. 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

NUMBER	Укажите количество записей в буфере. Максимальное значение – 1024.

По умолчанию

Значение по умолчанию – 32.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для настройки максимального количества записей в буфере журнала 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. Последующие пакеты из той же сессии не будут отправлены в модуль журнала событий, пока его запись в буфере не будет удалена.

Если буфер журнала событий заполнен, а события (нарушения) продолжают поступать, пакеты будут отброшены, но 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)#
```

22.6 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.

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#
```

22.7 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 отправку SNMP-уведомлений о подобных событиях.

Пример

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

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

23. Команды DHCP Snooping

23.1 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 в VLAN. С помощью данной функции DHCP-пакеты с недоверенного интерфейса могут получить статус проверенных и будет создана таблица привязки DHCP Snooping в 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)#
```

23.2 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 в VLAN, на которой включена функция DHCP Snooping. По умолчанию при проверке будут отброшены пакеты, если 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)#
```

23.3 ip dhcp snooping database

Данная команда используется для настройки хранения записей привязки DHCP Snooping на удаленном узле. Для отключения хранения или возврата к настройкам по умолчанию используйте команду **no**.

ip dhcp snooping database {*URL* **| write-delay** *SECONDS***}**

no ip dhcp snooping database [write-delay]

Параметры

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

По умолчанию

По умолчанию URL-адрес агента базы данных не установлен.

Значение времени задержки для записи по умолчанию составляет 300 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для сохранения записей привязки DHCP на удаленном узле через TFTP.

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.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch(config)#
```

23.4 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#
```

23.5 clear ip dhcp snooping binding

Данная команда используется для удаления привязки DHCP.

clear ip dhcp snooping binding [*MAC-ADDRESS***] [***IP-ADDRESS***] [vlan** *VLAN-ID***] [interface** *INTERFACE-ID***]**

Параметры

MAC-ADDRESS	(Опционально.) Укажите MAC-адрес, который необходимо удалить.
IP-ADDRESS	(Опционально.) Укажите IP-адрес, который необходимо удалить.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN ID, который необходимо удалить.
interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс, который необходимо удалить.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда позволяет удалить запись привязки DHCP, включая заданные вручную записи привязки.

Пример

В данном примере показано, как удалить все записи привязки DHCP Snooping.

```
Switch#clear ip dhcp snooping binding
Switch#
```

23.6 renew ip dhcp snooping database

Данная команда используется для обновления таблицы привязки DHCP.

renew ip dhcp snooping database *URL*

Параметры

URL	Укажите URL для обновления таблицы привязки DHCP в следующем формате: • tftp://location/filename

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для обновления таблицы привязки DHCP с URL-адреса и добавления записей в таблицу привязки DHCP Snooping. Записи с удаленного узла загружаются через TFTP.

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#
```

23.7 ip dhcp snooping binding

Данная команда используется для настройки привязки DHCP Snooping вручную.

ip dhcp snooping binding *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **expiry** *SECONDS*

Параметры

MAC-ADDRESS	Укажите MAC-адрес записи, которую необходимо добавить или удалить.
vlan *VLAN-ID*	Укажите VLAN ID записи, которую необходимо добавить или удалить.
IP-ADDRESS	Укажите IP-адрес записи, которую необходимо добавить или удалить.

interface *INTERFACE-ID*	Укажите интерфейс, на котором необходимо добавить или удалить запись привязки.
expiry *SECONDS*	Укажите интервал, после которого привязки не будут действительны. Доступен диапазон значений от 60 до 4294967295 секунд.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Даннакая команда применима исключительно для настройки интерфейсов физических портов и port-channel.
Команда используется для создания динамической записи DHCP Snooping.

Пример

В данном примере показано, как настроить запись DHCP Snooping с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 для VLAN 2 и интерфейса Ethernet 1/0/10 с expiry time 100 секунд.

```
Switch#ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10 expiry
100
Switch#
```

23.8 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 применима исключительно для настройки интерфейсов физических портов и port-channel.

Порты, подключенные к DHCP-серверу или к другим коммутаторам, должны быть настроены как доверенные интерфейсы. Порты, подключенные к DHCP-клиентам, должны быть настроены как недоверенные интерфейсы. DHCP Snooping работает в качестве межсетевого экрана между недоверенными интерфейсами и DHCP-серверами.

Если порт настроен как недоверенный интерфейс, сообщение DHCP придет на порт в ту VLAN, в которой включен DHCP Snooping. Коммутатор перенаправит пакеты DHCP, если только не будет соблюдаться любое из следующих условий (в таком случае пакеты будут отбрасываться):

- Порт коммутатора получает пакет (например, пакет DHCPOFFER, DHCPACK, DHCPNAK или DHCPLEASEQUERY) от DHCP-сервера за пределами межсетевого экрана.
- Если включена команда **ip dhcp snooping verify mac-address**, чтобы пройти проверку, MAC-адрес источника в заголовке Ethernet должен быть таким же, как и аппаратный адрес DHCP-клиента.
- Недоверенный интерфейс получает DHCP-пакет, включающий в себя IP-адрес агента ретрансляции (Relay Agent), отличный от 0.0.0.0, или Relay Agent перенаправляет пакет, включающий в себя Option 82 на недоверенный интерфейс.
- Маршрутизатор получает сообщение DHCPRELEASE или DHCPDECLINE от недоверенного узла с записью в таблице привязки DHCP 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 в таблице привязки на основе IP-адреса, назначенного клиенту сервером. 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 интерфейс Ethernet 1/0/3 в качестве доверенного для DHCP Snooping.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#
```

23.9 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 ограничения записей DHCP.

ip dhcp snooping limit entries {*NUMBER* **| no-limit}**
no ip dhcp snooping limit entries

Параметры

NUMBER	Укажите ограничение количества привязок DHCP Snooping на порт. Диапазон 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 применима исключительно для настройки интерфейсов физических портов и 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) на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip dhcp snooping limit entries 100
Switch(config-if)#
```

23.10 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 ограничения сообщений DHCP.

ip dhcp snooping limit rate {*VALUE* **| no-limit}**
no ip dhcp snooping limit rate

Параметры

VALUE	Укажите количество DHCP-сообщений, которое может быть обработано за секунду. Диапазон допустимых значений: от 1 до 300.
no-limit	Укажите для снятия ограничения количества сообщений.

По умолчанию

По умолчанию ограничений нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При превышении указанного 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 интерфейсе Ethernet 1/0/3 за одну секунду.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ip dhcp snooping limit rate 100
Switch(config-if)#
```

23.11 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)#
```

23.12 ip dhcp snooping verify mac-address

Данная команда используется для включения проверки совпадения MAC-адреса источника в DHCP-пакете 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 в VLAN, на которой включена функция DHCP Snooping. По умолчанию DHCP Snooping проверяет, совпадает ли MAC-адрес источника в пакете с аппаратным адресом DHCP-клиента.

Пример

В данном примере показано, как включить проверку на соответствие MAC-адреса источника в DHCP-пакете 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 в VLAN или группе VLAN. При использовании формы **no** команда отключит DHCP Snooping в VLAN или группе VLAN.

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

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

Параметры

VLAN-ID	Укажите VLAN, в которой необходимо включить или отключить функцию DHCP Snooping.
,	(Опционально.) 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

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 включения DHCP Snooping для VLAN. Функция DHCP Snooping отслеживает пакеты DHCP, поступающие на недоверенный интерфейс в VLAN. С помощью данной функции DHCP-пакеты с недоверенного интерфейса могут получить статус проверенных и будет создана таблица привязки DHCP Snooping в 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 в VLAN 10.

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

В следующем примере показано, как включить DHCP Snooping в нескольких VLAN.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping vlan 10,15-18
Switch(config)#
```

23.14 show ip dhcp snooping

Данная команда используется для отображения настроек DHCP Snooping.

show ip dhcp snooping

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения настроек DHCP Snooping.

Пример

В данном примере показано, как отобразить конфигурацию 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#
```

23.15 show ip dhcp snooping binding

Данная команда используется для отображения записей привязки DHCP Snooping.

show ip dhcp snooping binding [*IP-ADDRESS***] [***MAC-ADDRESS***] [vlan** *VLAN-ID***] [interface** *INTERFACE-ID* **[[, | -]]]**

Параметры

IP-ADDRESS	(Опционально.) Укажите, если необходимо отображать привязки на основе IP-адреса.
MAC-ADDRESS	(Опционально.) Укажите, если необходимо отображать привязки на основе MAC-адреса.
vlan *VLAN-ID*	(Опционально.) Укажите, если необходимо отображать привязки на основе VLAN.
interface *INTERFACE-ID*	(Опционально.) Укажите, если необходимо отображать привязки на основе ID порта (port ID).
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения записей привязки DHCP Snooping.

Пример

В данном примере показано, как отобразить все записи 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 отобразить запись 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 следующем примере показано, как отобразить запись привязки DHCP Snooping для 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 следующем примере показано, как отобразить запись привязки DHCP Snooping для IP 10.1.1.1 и MAC 00-01-02-03-04-05 в VLAN 100.

```
Switch#show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05 vlan 100

MAC Address       IP Address      Lease(seconds) Type          VLAN Interface
----------------- --------------- -------------- ------------- ---- --------------
00-01-02-03-04-05 10.1.1.1        1500           dhcp-snooping 100  eth1/0/5

Total Entries: 1

Switch#
```

В примере ниже показано, как отобразить записи привязки DHCP Snooping в 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 примере ниже показано, как отобразить записи привязки DHCP Snooping на интерфейсе Ethernet 1/0/5.

```
Switch#show ip dhcp snooping binding interface eth1/0/5

MAC Address       IP Address      Lease(seconds) Type          VLAN Interface
----------------- --------------- -------------- ------------- ---- --------------
00-01-02-03-04-05 10.1.1.10       1500           dhcp-snooping 100  eth1/0/5
00-01-02-00-00-05 10.1.1.11       495            dhcp-snooping 100  eth1/0/5

Total Entries: 2

Switch#
```

Отображаемые параметры

MAC Address	Аппаратный MAC-адрес клиента.
IP Address	IP-адрес клиента, назначенный DHCP-сервером.
Lease (seconds)	Время аренды IP-адреса.
Type	Тип привязки, настроенный через интерфейс командной строки или изученный динамически.
VLAN	VLAN ID.
Interface	Интерфейс, к которому подключен DHCP-клиент.

23.16 show ip dhcp snooping database

Данная команда используется для отображения статистики таблицы привязок DHCP Snooping.

show ip dhcp snooping database

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения статистики таблицы привязок DHCP Snooping.

Пример

В данном примере показано, как отобразить статистику таблицы привязок 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 привязок DHCP Snooping.
Expired leases	Количество записей с истекшим сроком аренды в таблице привязок DHCP Snooping.
Invalid interfaces	Количество интерфейсов, получивших сообщение DHCP, для которых не выполняется DHCP Snooping.
Parse failures	Количество недопустимых пакетов DHCP.

Checksum errors	Количество подсчитанных значений контрольной суммы, отличных от сохраненного значения контрольной суммы.
Unsupported vlans	Количество записей, для которых VLAN отключена.

24. Команды DHCPv6 Client

24.1 clear ipv6 dhcp client

Данная команда используется для перезапуска клиента DHCPv6 на интерфейсе.

clear ipv6 dhcp client *INTERFACE-ID*

Параметры

INTERFACE-ID	Укажите интерфейс VLAN, на котором необходимо перезапустить клиент DHCPv6.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов VLAN.

Команда используется для перезапуска клиента DHCPv6 на указанном интерфейсе.

Пример

В данном примере показано, как перезапустить клиент DHCPv6 на интерфейсе VLAN 1.

```
Switch#clear ipv6 dhcp client vlan1
Switch#
```

24.2 ipv6 dhcp client pd

Данная команда используется, чтобы включить запрос клиента DHCPv6 для делегирования префикса (Prefix Delegation) через указанный интерфейс. Используйте форму **no**, чтобы отключить запрос.

ipv6 dhcp client pd {*PREFIX-NAME***} [rapid-commit] | hint** *IPV6-PREFIX***}**

no ipv6 dhcp client pd

Параметры

PREFIX-NAME	Укажите имя основного префикса IPv6. Максимально допустимое количество символов – 12.

rapid-commit	(Опционально.) Укажите, чтобы получать сетевые настройки от DHCPv6-сервера посредством быстрого обмена двумя сообщениями вместо стандартных четырех между Requesting Router (RR) и Delegating Router (DR).
hint *IPV6-PREFIX*	Укажите IPv6-префикс для отправки в сообщении в качестве хинта (hint).

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** как на DR, так и на RR.

Если клиент получает advertisement от нескольких серверов, будет выбран сервер с наивысшим приоритетом. Клиент может принять несколько префиксов, делегированных сервером.

Функции клиента DHCPv6, сервера DHCPv6 и DHCPv6 Relay являются взаимоисключающими 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 vlan2
Switch(config-if)#ipv6 address dhcp-prefix 0:0:0:7272::72/64
Switch(config-if)#exit
Switch(config)#interface vlan1
Switch(config-if)#ipv6 dhcp client pd dhcp-prefix rapid-commit
Switch(config-if)#
```

24.3 show ipv6 dhcp

Данная команда используется для отображения настроек DHCPv6 на интерфейсе.

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

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 на интерфейсах. 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 следующем примере показано, как отобразить настройки DHCPv6 для интерфейса VLAN 1. При этом функция DHCPv6 на VLAN1 отключена.

```
Switch#show ipv6 dhcp interface vlan1

vlan1 is not in DHCPv6 mode.

Switch#
```

В примере ниже показано, как отобразить настройки DHCPv6 для всех VLAN. Отображаются только те VLAN, на которых включена функция DHCPv6.

```
Switch#show ipv6 dhcp interface

vlan1 is in client mode
  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#
```

25. Команды DHCPv6 Guard

25.1 ipv6 dhcp guard policy

Данная команда используется для создания или изменения политики DHCPv6 Guard. Команда позволяет войти в режим DHCPv6 Guard Configuration Mode. Для удаления политики DHCPv6 Guard воспользуйтесь формой **no** этой команды.

ipv6 dhcp guard policy *POLICY-NAME*

no ipv6 dhcp guard policy *POLICY-NAME*

Параметры

POLICY-NAME	Укажите имя политики DHCPv6 Guard.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для создания или изменения политики DHCPv6 Guard. Команда позволяет войти в режим DHCPv6 Guard Configuration Mode. Политики DHCPv6 Guard могут использоваться для блокировки ответов DHCPv6 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)#
```

25.2 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)#
```

25.3 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 сообщений сервера DHCPv6 на основе IP-адреса источника. Если не настроена команда **match ipv6 access-list,** все сообщения сервера пропускаются. 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)#
```

25.4 ipv6 dhcp guard attach-policy

Данная команда используется для применения политики DHCPv6 Guard на определенном интерфейсе. Для удаления привязки воспользуйтесь формой **no** этой команды.

ipv6 dhcp guard attach-policy [*POLICY-NAME***]**

no ipv6 dhcp guard attach-policy

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики DHCPv6 Guard.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для применения политики DHCPv6 Guard на интерфейсе. Политики DHCPv6 Guard используются для блокировки DHCPv6-сообщений сервера или фильтрации сообщений сервера на основе IP-адреса источника. Если имя политики не указано, то политика по умолчанию настроит устройство в качестве клиента.

Пример

В данном примере показано, как применить политику DHCPv6 Guard «pol1» для интерфейса Ethernet 1/0/3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 dhcp guard attach-policy pol1
Switch(config-if)#
```

25.5 show ipv6 dhcp guard policy

Данная команда позволяет отобразить информацию о DHCPv6 Guard.

show ipv6 dhcp guard policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики DHCPv6 Guard.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если имя политики не указано, будет отображаться информация для всех политик.

Пример

В данном примере показано, как отобразить информацию для всех политик.

```
Switch#show ipv6 dhcp guard policy

DHCP guard policy: default
   Device Role: DHCP client
   Target: eth1/0/3

DHCP guard policy: test1
   Device Role: DHCP server
   Source Address Match Access List: acl1
   Target: eth1/0/1

Switch#
```

Отображаемые параметры

Device Role	Роль устройства: клиент или сервер.
Target	Название интерфейса.
Source Address Match Access List	Список доступа IPv6 определенной политики.

26. Команды DHCPv6 Relay

26.1 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. Для удаления Relay Destination воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay destination *IPV6-ADDRESS* **[***INTERFACE-ID***]**
no ipv6 dhcp relay destination *IPV6-ADDRESS* **[***INTERFACE-ID***]**

Параметры

IPV6-ADDRESS	Укажите адрес DHCPv6 Relay Destination.
INTERFACE-ID	(Опционально.) Укажите выходной интерфейс для Relay Destination.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Чтобы включить на интерфейсе функцию DHCPv6 Relay, настройте адрес Relay Destination при помощи команды **ipv6 dhcp relay destination**. Чтобы удалить адрес Relay, используйте команду **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 vlan1
Switch(config-if)#ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 vlan1
Switch(config-if)#ipv6 dhcp relay destination FE80::22:33 vlan2
Switch(config-if)#
```

26.2 ipv6 dhcp relay remote-id format

Данная команда используется для настройки sub-опции Remote ID. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 — В качестве Remote ID используется системный MAC-адрес коммутатора. 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

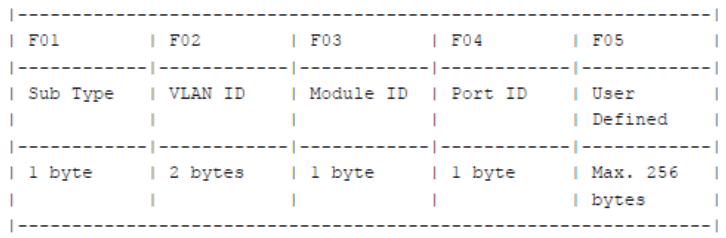
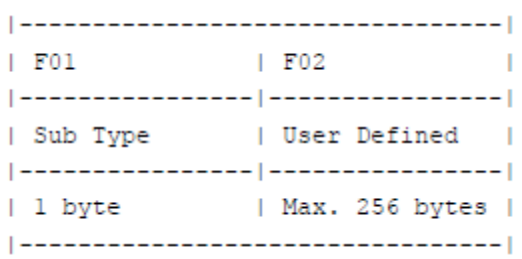
F01. *Тип sub-опции:* число 1 свидетельствует о данном типе Remote ID.

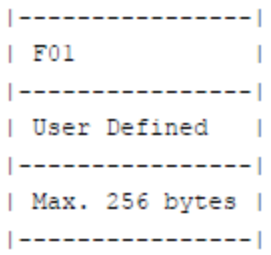
F02. *VLAN ID:* входящий VLAN ID в пакете DHCP Client.

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	В качестве Remote ID используется CID со строкой, заданной пользователем. Формат Remote ID представлен ниже:  **F01.** *Тип sub-опции:* число 2 свидетельствует о данном типе 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 relay remote-id udf**. По умолчанию данное поле не заполнено.
user-define	Remote ID задается самостоятельно. Формат Remote ID представлен ниже:  **F01.** *Тип sub-опции:* число 3 свидетельствует о данном типе Remote ID. **F02.** *Задать самостоятельно:* заданная пользователем строка, настраиваемая при помощи команды **ipv6 dhcp relay remote-id udf**.

expert-udf	Remote ID задается пользователем самостоятельно в виде произвольной строки. Формат Remote ID представлен ниже:  **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)#
```

26.3 ipv6 dhcp relay remote-id option

Данная команда используется для того, чтобы включить встраивание Relay Agent Remote ID Option 37 в ретранслируемых пакетах запроса DHCP IPv6. Для отключения данной функции воспользуйтесь формой **no** этой команды.

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)#
```

26.4 ipv6 dhcp relay remote-id policy

Данная команда используется для настройки политики перенаправления Option 37 для DHCPv6 Relay Agent. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 ретранслировать пакет запроса DHCPv6, в котором уже есть опция Remote ID, 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 присутствует опция Remote ID, будет отброшен. При выборе политики **keep** коммутатор не будет проверять, присутствует ли в полученном пакете опция Remote ID.

Пример

В данном примере показано, как настроить политику DHCPv6 Relay Agent Remote ID Option так, чтобы пакет был отброшен при наличии в нем опции Remote ID.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id policy drop
Switch(config)#
```

26.5 ipv6 dhcp relay remote-id udf

Используйте данную команду, чтобы настроить User Define Field (UDF) для Remote ID. Для удаления записи UDF воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay remote-id udf {ascii *STRING* **| hex** *HEX-STRING***}**

no ipv6 dhcp relay remote-id udf

Параметры

ascii *STRING*	Укажите строку ASCII для UDF Remote ID. Максимальное количество символов – 128.
hex *HEX-STRING*	Укажите шестнадцатеричную строку для UDF Remote ID. Максимальное 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 следующем примере показано, как настроить UDF (шестнадцатеричная строка ASCII) «010c08».

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id udf hex 010c08
Switch(config)#
```

26.6 show ipv6 dhcp

Данная команда используется для отображения настроек DHCPv6 на интерфейсе.

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

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 интерфейса VLAN 1, на котором включен режим DHCPv6 Relay.

```
Switch#show ipv6 dhcp interface vlan1

vlan1 is in relay mode
    Relay destinations:
      FE80::20A:BBFF:FECC:102 via vlan2

Switch#
```

В данном примере показано, как отобразить информацию о DHCPv6 для интерфейса VLAN 1, на котором отключен режим DHCPv6.

```
Switch#show ipv6 dhcp interface vlan1

Vlan1 is not in DHCPv6 mode

Switch#
```

26.7 show ipv6 dhcp relay information option

Данная команда используется для отображения настроек DHCPv6 Relay Information Options.

show ipv6 dhcp relay information option

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки DHCPv6 Relay Information Options.

Пример

В данном примере показано, как отобразить настройки DHCPv6 Relay Remote ID.

```
Switch#show ipv6 dhcp relay information option

IPv6 DHCP relay remote-id
  Insert : disabled
  Policy : keep
  Format : default
  UDF is ascii string

IPv6 DHCP relay interface-id
  Insert : enabled
  Policy : keep
  Format : default


Switch#
```

26.8 ipv6 dhcp relay interface-id format

Данная команда используется для настройки sub-опции Interface ID. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay interface-id format {default | cid | vendor1 | expert-udf [standalone_unit_format {0 | 1}] }

no ipv6 dhcp relay interface-id format

Параметры

default	В качестве Interface ID используется VLAN ID. Формат Interface ID представлен ниже: |-------------------------| | F01 | F02 | |------------|------------| | Sub Type | VLAN ID | |------------|------------| | 1 byte | 2 bytes | |-------------------------| **F01.** *Тип sub-опции:* число 1 свидетельствует о данном типе Interface ID. **F02.** *VLAN ID:* входящий VLAN ID в пакете от клиента DHCP.
cid	В качестве Interface ID используется CID. 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.** *Тип sub-опции:* число 2 свидетельствует о данном типе Interface ID. **F02.** *VLAN ID:* входящий VLAN ID в пакете от клиента DHCP. **F03.** *ID модуля:* ID модуля для автономных коммутаторов – 0. ID модуля для стекированных коммутаторов – Unit ID. **F04.** *ID порта*: номер входящего порта для пакета от клиента DHCP. Номера портов начинаются с 1.

vendor1

В качестве Interface ID используется 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	:	cvlan
(0x30)	(0x2F)	Number	(0x3A)	
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. *Слэш (/):* код ASCII – 0x2F.

F11. *0:* Код ASCII – 0x30.

F12. *Слэш (/):* код ASCII – 0x2F.

F13. *Номер порта:* номер входящего порта для пакета от клиента DHCP.

F14. *Двоеточие (:):* код ASCII – 0x3A.

F15. *cvlan:* 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. *Слэш (/):* код ASCII – 0x2F.

F21. *0:* Код ASCII – 0x30.

F22. *Слэш (/):* код ASCII – 0x2F.

F23. *0:* Код ASCII – 0x30.

F24. *Слэш (/):* код ASCII – 0x2F.

F25. *ID шасси:* номер шасси. ID шасси для автономных коммутаторов – 0. ID шасси для стекированных коммутаторов – Unit ID.

F26. *Слэш (/):* код ASCII – 0x2F.

F27. *0:* Код ASCII – 0x30.

F28. *Слэш (/):* код ASCII – 0x2F.

F29. *Номер порта*: номер входящего порта для пакета от клиента DHCP.

expert-udf	Interface ID задается пользователем 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.
standalone_unit_format	Укажите Unit ID для автономного коммутатора. Значение по умолчанию – 0.

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 в формате «cid».

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay interface-id format cid
Switch(config)#
```

26.9 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. Для отключения данной функции воспользуйтесь формой **no** этой команды.

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 опции DHCPv6 Relay Agent Interface ID.

Пример

В данном примере показано, как включить встраивание опции DHCPv6 Relay Agent Interface ID.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay interface-id option
Switch(config)#
```

26.10 ipv6 dhcp relay interface-id policy

Данная команда используется для настройки политики перенаправления Option 18 для DHCPv6 Relay Agent. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 ретранслировать пакет запроса DHCPv6, в котором уже есть Relay Agent Interface ID Option, на сервер DHCPv6 в неизменном виде.

По умолчанию

Политика 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 опции Interface ID.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay interface-id policy drop
Switch(config)#
```

26.11 ipv6 dhcp local-relay vlan

Данная команда используется для включения DHCPv6 Local Relay на VLAN или группе VLAN. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ipv6 dhcp local-relay vlan *VLAN-ID* **[, | -]**
no ipv6 dhcp local-relay vlan *VLAN-ID* **[, | -]**

Параметры

VLAN-ID	Укажите VLAN ID для конфигурации.
,	(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 включена проверка Option 37, коммутатор проверит запрос от клиента и отбросит пакет, уже

содержащий Option 37.

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)#
```

26.12 ipv6 dhcp relay enable

Данная команда используется для включения функции DHCPv6 Relay на порту. Для отключения данной функции воспользуйтесь формой **no** этой команды.

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 на портах.

Пример

В данном примере показано, как отключить функцию DHCPv6 Relay на порту 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no ipv6 dhcp relay enable
Switch(config-if)#
```

26.13 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. Для удаления профиля воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay remote-id profile *NAME*
no ipv6 dhcp relay remote-id profile *NAME*

Параметры

NAME	Укажите имя профиля. Максимальное количество символов – 32. Максимальное 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)#
```

26.14 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. Для удаления профиля воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay interface-id profile *NAME*
no ipv6 dhcp relay interface-id profile *NAME*

Параметры

NAME	Укажите имя профиля. Максимальное количество символов – 32. Максимальное 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)#
```

26.15 format string

Данная команда используется для настройки заданной пользователем строки для Option 18 или Option 37. Для удаления записи воспользуйтесь формой **no** этой команды.

format string *STRING*
no format string

Параметры

STRING	Введите строку для использования в Option 18 или Option 37. 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 инкапсулирована в пакет. 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 (**0**) – настройка по умолчанию.

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.

keyword – для преобразования будет использовано ключевое слово на основе фактических системных значений. При обнаружении неизвестных или неподдерживаемых ключевых слов команда будет отклонена. Доступны следующие ключевые слова:

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 получен при помощи специальной команды (например, **ipv6 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 получен при помощи команд CLI (например, **ipv6 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 экранирования. 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

DHCPv6 Profile Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить строку пользователя для Option 18 или Option 37.

Пример

В данном примере показано, как настроить строку пользователя для 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:%05svlan"
Switch(config-dhcp-profile)#
```

26.16 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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 для задаваемого пользователем профиля Option 18 или Option 37: aa-bb-cc-dd-ee-ff.
uppercase	Укажите, чтобы использовать верхний регистр при записи MAC-адреса для задаваемого пользователем профиля Option 18 или Option 37: AA-BB-CC-DD-EE-FF.
hyphen	Укажите, чтобы использовать «-» в качестве разделителя данных: AA-BB-CC-DD-EE-FF.
colon	Укажите, чтобы использовать «:» в качестве разделителя данных: AA:BB:CC:DD:EE:FF.
dot	Укажите, чтобы использовать «.» в качестве разделителя данных: AA.BB.CC.DD.EE.FF.
none	Укажите для ввода данных без разделителя: AABBCCDDEEFF.
number	Укажите количество разделителей: **1:** один разделитель: AABBCC.DDEEFF. **2:** два разделителя: AABB.CCDD.EEFF. **5:** 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)#
```

26.17 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.

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#
```

26.18 ipv6 dhcp relay remote-id format-type expert-udf

Данная команда используется для настройки строки Option 37 expert UDF на порту. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay remote-id format-type expert-udf *STRING*
no ipv6 dhcp relay remote-id format-type expert-udf

Параметры

STRING	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 1, выбрав профиль «profile1».

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ipv6 dhcp relay remote-id format-type expert-udf profile1
Switch(config-if)#
```

26.19 ipv6 dhcp relay interface-id format-type expert-udf

Данная команда используется для настройки строки Option 18 expert UDF на порту. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay interface-id format-type expert-udf *STRING*
no ipv6 dhcp relay interface-id format-type expert-udf

Параметры

STRING	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 1, выбрав профиль «profile2».

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ipv6 dhcp relay interface-id format-type expert-udf profile2
Switch(config-if)#
```

26.20 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.

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#
```

26.21 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.

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#
```

27. Команды DHCPv6 Server

27.1 address prefix

Данная команда используется для указания префикса адреса, который будет присвоен клиенту. Используйте форму **no**, чтобы удалить префикс адреса.

address prefix *IPV6-PREFIXIPREFIX-LENGTH* **[lifetime** *VALID-LIFETIME PREFERRED-LIFETIME***]**

no address prefix

Параметры

IPV6-PREFIX	Укажите префикс IPv6-адреса, который необходимо присвоить клиенту.
PREFIX-LENGTH	Укажите длину префикса IPv6-адреса.
lifetime *VALID-LIFETIME*	(Опционально) Укажите значение допустимого времени жизни (Valid Lifetime) для префикса адреса в секундах. Значение Valid Lifetime должно превышать значение предпочтительного времени жизни (Preferred Lifetime). Доступный диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение Valid Lifetime по умолчанию– 2592000 секунд (30 дней).
PREFERRED-LIFETIME	(Опционально) Укажите значение Preferred Lifetime для префикса 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)#
```

27.2 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 CLIENT-DUID* **[iaid** *IAID***] [lifetime** *VALID-LIFETIME PRE-FERRED-LIFETIME***]**

no address-assignment *IPV6-ADDRESS CLIENT-DUID* **[iaid** *IAID***]**

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес, который необходимо присвоить обозначенному клиенту.
CLIENT-DUID	Укажите DHCP Unique Identifier (DUID) клиента, которому необходимо присвоить адрес.
iaid *IAID*	(Опционально.) Укажите Identity Association Identifier (IAID). IAID используется для обозначения серии Non-Temporary Addresses (IANA), присвоенных клиенту.
lifetime *VALID-LIFETIME*	(Опционально.) Укажите значение допустимого времени жизни (Valid Lifetime) для адреса в секундах. Значение Valid Lifetime должно превышать значение предпочтительного времени жизни (Preferred Lifetime). 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.
PREFERRED-LIFETIME	(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 для присвоения адреса обозначенному клиенту.

Получив запрос от клиента, сервер проверит пул IPv6 DHCP, ассоциированный с полученным интерфейсом. Если запрос содержит опцию IANA и имеются свободные статические записи, настроенные с IAID и совпадающие с DUID и IAID сообщения, будет присвоен соответствующий адрес. Если соответствующая запись отсутствует, но имеются свободные статические записи без указанных IAID, которые совпадают с DUID сообщения, будет отправлен ответ в соответствии с записью.

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(config-dhcp)#address prefix 2001:0DB8::0/64 lifetime 200 100
Switch(config-dhcp)#address-assignment 2001:0DB8::1:2 000300010506BBCCDDEE
Switch(config-dhcp)#exit
Switch(config)#interface vlan100
Switch(config-if)#ipv6 dhcp server pool1
Switch(config-if)#
```

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(config-dhcp)#address prefix 2001:AAB8::0/64 lifetime 200 100
Switch(config-dhcp)#address-assignment 2001:AAB8::2:2 00030001050611223344 iaid 1234
Switch(config-dhcp)#exit
Switch(config)#interface vlan200
Switch(config-if)#ipv6 dhcp server pool2
Switch(config-if)#
```

27.3 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, из которого был назначен.

Пример

В данном примере показано, как удалить все записи привязки DHCPv6-сервера.

```
Switch#clear ipv6 dhcp binding all
Switch#
```

27.4 domain-name

Данная команда используется для назначения имени домена запрашивающему DHCPv6-клиенту. Используйте форму **no**, чтобы удалить настройки имени домена.

domain-name *DOMAIN-NAME*

no domain-name

Параметры

DOMAIN-NAME	Укажите имя домена.

По умолчанию

Нет.

Режим ввода команды

DHCPv6 Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы назначить имя домена запрашивающему DHCPv6-клиенту. Можно указать только одно имя домена.

Пример

В данном примере показано, как настроить имя домена в пуле DHCPv6-сервера «pool1».

```
Switch#configure terminal
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#domain-name v6domain
Switch(config-dhcp)#
```

27.5 dns-server

Данная команда используется для назначения списка серверов DNS IPv6 запрашивающему IPv6-клиенту. Используйте форму **no**, чтобы удалить DNS-сервер из списка серверов.

dns-server *IPV6-ADDRESS*

no dns-server *IPV6-ADDRESS*

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес DNS-сервера.

По умолчанию

Нет.

Режим ввода команды

DHCPv6 Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы присвоить IPv6-адрес DNS-сервера запрашивающему DHCPv6-клиенту. Если необходимо присвоить несколько адресов, введите команду несколько раз.

Пример

В данном примере показано, как настроить сервер DNS IPv6 в пуле DHCPv6-сервера «pool1».

```
Switch#configure terminal
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#dns-server 2001:0DB8:3000:3000::42
Switch(config-dhcp)#
```

27.6 ipv6 dhcp excluded-address

Данная команда используется для указания IPv6-адресов, которые DHCPv6-сервер не должен присваивать DHCP-клиентам. Используйте форму **no**, чтобы удалить исключенные IPv6-адреса.

ipv6 dhcp excluded-address *LOW-ADDRESS* **[***HIGH-ADDRESS***]**

no ipv6 dhcp excluded-address *LOW-ADDRESS* **[***HIGH-ADDRESS***]**

Параметры

LOW-ADDRESS	Укажите исключенный IPv6-адрес или первый IPv6-адрес в диапазоне исключенных адресов.
HIGH-ADDRESS	(Опционально.) Укажите последний IPv6-адрес в диапазоне исключенных адресов.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Сервер DHCPv6 допускает назначение любого адреса клиенту (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)#
```

27.7 ipv6 dhcp pool

Данная команда используется для входа в режим DHCP Pool Configuration Mode и настройки пула IPv6 DHCP. Используйте форму **no**, чтобы удалить пул IPv6 DHCP.

ipv6 dhcp pool *POOL-NAME*

no ipv6 dhcp pool *POOL-NAME*

Параметры

POOL-NAME	Укажите имя пула адресов. Максимальное количество символов – 12.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для входа в режим IPv6 DHCP Pool Configuration Mode и настройки пула IPv6 DHCP. Используйте команду **ipv6 dhcp server**, чтобы включить сервер DHCPv6 на интерфейсе и указать пул IPv6 DHCP, используемый для обслуживания DHCP-запроса.

Пример

В данном примере показано, как настроить пул адресов «pool1».

```
Switch#configure terminal
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#
```

27.8 ipv6 dhcp server

Данная команда используется для включения сервера DHCPv6 на интерфейсе. Используйте форму **no**, чтобы отключить сервер DHCPv6.

ipv6 dhcp server *POOL-NAME* **[rapid-commit] [preference** *VALUE***] [allow-hint]**

no ipv6 dhcp server

Параметры

POOL-NAME	Укажите имя пула IPv6 DHCP, обслуживающего запрос, полученный на интерфейсе.

rapid-commit	(Опционально.) Укажите, чтобы получать сетевые настройки от DHCP-сервера посредством быстрого обмена двумя сообщениями вместо стандартных четырех между Requesting Router (RR) и Delegating Router (DR). По умолчанию обмен двумя сообщениями отключен.
preference *VALUE*	(Опционально.) Значение приоритета, предлагаемое сервером из диапазона от 0 до 255. Значение по умолчанию – 0. Чем больше значение, тем выше приоритет.
allow-hint	(Опционально.) Укажите, чтобы разрешить делегировать префикс на основе хинта (prefix hint), который был предложен клиентом. По умолчанию хинт игнорируется.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда предназначена для включения сервера DHCPv6 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. Функции клиента, сервера и DHCP-Relay являются взаимоисключающими 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** как на DR, так и на RR.

Если команда сконфигурирована со значением **preference** отличным от 0, то данное значение будет указано в виде опции в оповещении. Оповещение без опции является эквивалентом оповещения со значением приоритета 0. Чем больше значение, тем выше приоритет.

Если команда сконфигурирована с опцией **allow-hint**, то сервер будет делегировать префикс на основе хинта (prefix hint) от клиента. В противном случае префикс hint от клиента будет проигнорирован.

Пример

В данном примере показано как создать DHCP-пул «pool1», включить сервер DHCPv6 на интерфейсе VLAN 100 и использовать «pool1» для передачи префиксов.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#exit
Switch(config)#interface vlan100
Switch(config-if)#ipv6 dhcp server pool1
Switch(config-if)#
```

27.9 ipv6 local pool

Данная команда используется для настройки локального пула IPv6-префиксов. Используйте форму **no**, чтобы удалить пул.

ipv6 local pool *POOL-NAME IPV6-PREFIX/PREFIX-LENGTH ASSIGNED-LENGTH*

no ipv6 local pool *POOL-NAME*

Параметры

POOL-NAME	Укажите имя локального пула IPv6-префиксов. Максимально допустимое количество символов – 12.
IPV6-PREFIX	Укажите адрес IPv6-префикса в локальном пуле.
PREFIX-LENGTH	Укажите длину IPv6-префикса в локальном пуле.
ASSIGNED-LENGTH	Укажите длину префикса, который необходимо делегировать из пула пользователю. Заданная длина не может быть меньше длины префикса.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Локальный пул IPv6-префиксов определяет блок префиксов. Настройте пул с префиксами, которые пересекаются с другими пулами. Чтобы изменить префикс в локальном пуле, удалите локальный пул, а затем создайте его заново. Все префиксы данного пула, которые уже были распределены, будут свободны.

Пример

В данном примере показано, как создать локальный пул IPv6-префиксов «prefix-pool» и использовать локальный пул в DHCP-пуле «pool1».

```
Switch#configure terminal
Switch(config)#ipv6 local pool prefix-pool 3004:DB8::/48 64
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#prefix-delegation pool prefix-pool lifetime 300 200
Switch(config-dhcp)#
```

27.10 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-LIFETIME PREFERRED-LIFETIME***]**

no prefix-delegation *IPV6-PREFIX/PREFIX-LENGTH CLIENT-DUID* **[iaid** *IAID***]**

Параметры

IPV6-PREFIX	Укажите IPv6-префикс, который необходимо делегировать обозначенному клиенту.
PREFIX-LENGTH	Укажите длину IPv6-префикса.
CLIENT-DUID	Укажите DHCP Unique Identifier (DUID) клиента, которому необходимо делегировать префикс.
iaid *IAID*	(Опционально.) Укажите Identity Association Identifier (IAID). IAID используется для обозначения серии префиксов, присвоенных Requesting Router (RR).
lifetime *VALID-LIFETIME*	(Опционально.) Укажите значение Valid Lifetime (допустимое время жизни) для префикса в секундах. Значение Valid Lifetime должно превышать значение Preferred Lifetime (предпочтительное время жизни). Доступный диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение Valid Lifetime по умолчанию – 2592000 секунд (30 дней).
PREFERRED-LIFETIME	(Опционально.) Укажите значение Preferred Lifetime для префикса в секундах. Доступный диапазон значений: от 60 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 для указания префикса, 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 IAID, которые соответствуют DUID сообщения, данные записи будут отправлены в ответ. Если в сообщении request отсутствует опция IAID, а в наличии есть свободные статические записи без IAID, которые соответствуют DUID сообщения, такие записи также будут отправлены в 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 local pool prefix-pool 2001:DB8::/48 64
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#prefix-delegation pool prefix-pool lifetime 300 200
Switch(config-dhcp)#prefix-delegation 2001:0DB8::/64 0003000010506BBCCDDEE
Switch(config-dhcp)#exit
Switch(config)#interface vlan 100
Switch(config-if)#ipv6 dhcp server pool1
Switch(config-if)#
```

27.11 prefix-delegation pool

Данная команда используется для указания локального пула IPv6, из которого могут быть делегированы префиксы. Используйте форму **no**, чтобы удалить локальный пул IPv6-префиксов.

prefix-delegation pool *POOL-NAME* **[lifetime** *VALID-LIFETIME PREFERRED-LIFETIME***]**
no prefix-delegation pool *POOL-NAME*

Параметры

POOL-NAME	Укажите имя локального пула IPv6-префиксов.

lifetime *VALID-LIFETIME*	(Опционально.) Укажите значение Valid Lifetime (допустимое время жизни) для префикса в секундах. Значение Valid Lifetime должно превышать значение Preferred Lifetime (предпочтительное время жизни). Доступный диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение Valid Lifetime по умолчанию – 2592000 секунд (30 дней).
lifetime *PREFERRED-LIFETIME*	(Опционально.) Укажите значение Preferred Lifetime для префикса в секундах. Доступный диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение Preferred Lifetime по умолчанию – 604800 секунд (7 дней).

По умолчанию

Нет.

Режим ввода команды

DHCPv6 Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для указания локального пула IPv6-префиксов в пуле IPv6 DHCP, чтобы делегировать префикс клиентам. В пуле IPv6 DHCP можно указать только один локальный пул IPv6-префиксов.

Получив запрос от клиента, сервер проверит пул IPv6 DHCP, ассоциированный с 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 vlan100
Switch(config-if)#ipv6 dhcp server pool1
Switch(config-if)#
```

27.12 service ipv6 dhcp

Данная команда используется для включения сервера DHCPv6 и службы DHCPv6 Relay на коммутаторе. Используйте форму **no** для отключения сервера DHCPv6 и DHCPv6 Relay.

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 DHCPv6 и службу DHCPv6 Relay на коммутаторе. Чтобы настройки вступили в силу, необходимо отключить, а затем снова включить сервер.

Пример

В данном примере показано, как включить сервер IPv6 DHCP и DHCPv6 Relay.

```
Switch#configure terminal
Switch(config)#service ipv6 dhcp
Switch(config)#
```

27.13 show ipv6 dhcp

Данная команда используется для отображения настроек DHCPv6 для интерфейсов.

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить DHCPv6 DUID устройства. 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. При этом DHCPv6 на VLAN1 отключен.

```
Switch#show ipv6 dhcp interface vlan1

vlan1 is not in DHCPv6 mode

Switch#
```

В следующем примере показано, как отобразить информацию о DHCPv6 для интерфейса VLAN 1. На VLAN1 включен сервер DHCPv6.

```
Switch#show ipv6 dhcp interface vlan1

vlan1 is in server mode
  IPv6 DHCP pool is test
  Preference value: 0
  Hint from client: ignored
  Rapid-Commit is disabled

Switch#
```

27.14 show ipv6 dhcp binding

Данная команда используется для отображения записи привязки IPv6-префикса.

show ipv6 dhcp binding [*IPV6-PREFIX***]**

Параметры

IPV6-PREFIX	(Опционально.) Укажите, чтобы отобразить запись привязки.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

При использовании данной команды без указания параметра *IPV6-PREFIX* будут отображены все записи привязки префикса DHCPv6. При указании параметра *IPV6-PREFIX* будет отображена только привязка префикса указанного клиента.

Пример

В данном примере показано, как отобразить записи 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#
```

27.15 show ipv6 dhcp pool

Данная команда используется для отображения информации о настройках пула DHCPv6-сервера.

show ipv6 dhcp pool [*POOL-NAME***]**

Параметры

POOL-NAME	(Опционально.) Укажите пул IPv6 DHCP для отображения.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

При использовании данной команды без указания параметра *POOL-NAME* будет отображена информация о настройках всех пулов DHCPv6-сервера. При указании параметра *POOL-NAME* будет отображена информация только об указанном пуле.

Пример

В данном примере показано, как отобразить информацию о DHCPv6-пуле.

```
Switch#show ipv6 dhcp pool

DHCPv6 pool: pool1
        Static bindings:
           Binding for client 00030001aabbcd000080
           IA PD: IA ID 0x0001
              Prefix: 3000:0:300::/48
               preferred lifetime 604800, valid lifetime 2592000
        Prefix delegation pool: abc
              preferred lifetime 604800, valid lifetime 2592000
        DNS server: 2345::2
        Domain name: pool1.com
        Active clients: 0

DHCPv6 pool: pool2
        DNS server: 6000::2
        DNS server: 6000::9
        Domain name: pool2.com
        Active clients: 0

DHCPv6 pool: test
        Static bindings:
           Binding for client 00030001aabbcd001234
           IA NA: IA ID not specified
              Address: 1234::1234
               preferred lifetime 604800, valid lifetime 2592000
        Address prefix: 1234::/64
              preferred lifetime 200, valid lifetime 300
        DNS server:
        Domain name:
        Active clients: 3

Switch#
```

Отображаемые параметры

DHCPv6 pool	Имя пула.
Binding for client 000300010002FCA5C01C	Статическая привязка для клиента с DUID 000300010002FCA5C01C.
IAPD	Серия префиксов, присвоенных клиенту.
IAID	Идентификатор данной IAPD.
Prefix	Префиксы, которые необходимо делегировать.
preferred lifetime, valid lifetime	Значения Preferred Lifetime и Valid Lifetime для префикса, присвоенные клиенту.
DNS server	Список адресов DNS-серверов.
Domain name	Список доменных имен, назначаемых клиентам.

Active clients	Общее количество активных клиентов.

27.16 show ipv6 excluded-address

Данная команда используется для отображения информации о настройках исключенных IPv6-адресов.

show ipv6 excluded-address

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить диапазон исключенных адресов.

Пример

В данном примере показано, как отобразить исключенные адреса.

```
Switch#show ipv6 excluded-address

 IPv6 excluded address:
       1.      2000::123
       2.      2000::237 - 2000::333

 Total Entries: 2

Switch#
```

27.17 show ipv6 local pool

Данная команда используется для отображения информации о настройках локального пула IPv6-префиксов.

show ipv6 local pool [*POOL-NAME***]**

Параметры

POOL-NAME	(Опционально.) Укажите, чтобы отобразить локальный пул IPv6-префиксов.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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 без указания имени пула.

```
Switch#show ipv6 local pool

Pool         Prefix                                    Free In use
------------ ----------------------------------------- ---- ------
prefix-pool  3004:DB8::/48                             65536 0
------------ ----------------------------------------- ---- ------
Total Entries: 1

Switch#
```

В следующем примере показано, как отобразить информацию о локальном пуле «PP1».

```
Switch#show ipv6 local pool PP1

Prefix is 3004:DB8::/48 assign /64 prefix
1 entries in use, 65536 available, 0 rejected
User                Prefix                                    Interface
------------------- ----------------------------------------- ----------
000300010002FCA5C01C 2003::/64                                vlan1

Switch#
```

27.18 show ipv6 dhcp operation

Данная команда используется для того, чтобы отобразить эксплуатационные данные для DHCPv6-сервера.

show ipv6 dhcp operation

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить эксплуатационные данные для DHCPv6-сервера.

Пример

В данном примере показано, как отобразить эксплуатационные данные для DHCPv6-сервера.

```
switch#show ipv6 dhcp operation

DHCPv6 pool: pool1
        Prefix delegation pool: abc, prefix is 3000::/32 48
        Static bindings:
           Binding for client 00030001aabbcd000080
             IA PD: IA ID 0x0001
             Prefix: 3000:0:300::/48
             preferred lifetime 604800, valid lifetime 2592000
        preferred lifetime 604800, valid lifetime 2592000
        DNS server: 2345::2
        Domain name: pool1.com

DHCPv6 pool: test
        Address prefix: 1234::/64
        Static bindings:
           Binding for client 00030001aabbcd001234
            IA NA: IA ID not specified
              Address: 1234::1234
               preferred lifetime 604800, valid lifetime 2592000
        preferred lifetime 200, valid lifetime 300
        DNS server: 2000::2
        Domain name: test.com

switch#
```

28. Команды Digital Diagnostics Monitoring (DDM)

28.1 show interfaces transceiver

Данная команда используется для отображения текущих операционных параметров модуля SFP/SFP+.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейсы, для которых необходимо отобразить состояние трансиверов. Если Interface ID не указаны, будут отображены статусы трансиверов 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.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить текущие операционные параметры модулей SFP/SFP+ на указанных портах.

Пример

В данном примере показано, как отобразить текущие операционные параметры модулей SFP/SFP+ для всех портов.

```
Switch#show interfaces transceiver

 ++ : high alarm, +  : high warning, -  : low warning, -- : low alarm
 mA: milliamperes, mW: milliwatts

Transceiver Monitoring traps: None

           Temperature  Voltage      Bias Current TX Power     RX Power
port       (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 следующем примере показано, как отобразить подробную информацию о состоянии трансиверов 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#
```

28.2 snmp-server enable traps transceiver-monitoring

Данная команда используется для того, чтобы включить отправку всех или определенных SNMP-уведомлений мониторинга оптических трансиверов. 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 мониторинга трансиверов.

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)#
```

28.3 transceiver-monitoring action shutdown

Используйте данную команду, чтобы отключить порт при обнаружении события alarm (тревога) или warning (предупреждение). Используйте форму **no**, чтобы отключить данную функцию.

transceiver-monitoring action shutdown {alarm | warning}
no transceiver-monitoring action shutdown

Параметры

alarm	Укажите, чтобы отключить порт при обнаружении события alarm.
warning	Укажите, чтобы отключить порт при обнаружении события warning.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки физических портов.

Команда позволяет указать, будет ли отключаться порт при обнаружении события alarm или warning. При включении мониторинга события alarm или warning происходят, если отслеживаемые параметры выходят за пределы соответствующих верхних или нижних порогов.

Отключение порта контролируется модулем Error Disable без таймера восстановления (recovery). Пользователь может включить порт вручную, применив команду **shutdown**, а затем команду **no shutdown**.

Пример

В данном примере показано, как настроить отключение порта 1 при обнаружении события alarm.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#transceiver-monitoring action shutdown alarm
Switch(config-if)#
```

28.4 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

INTERFACE-ID	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.

VALUE	Укажите порог в диапазоне от 0 до 131 мА.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данный функционал доступен только для портов SFP+ с оптическими модулями, поддерживающими функцию мониторинга.

Команда позволяет настроить пороги тока смещения на указанных портах. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, куда будут перезаписаны в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен только в системе. Отображаться будут заданные пользователем настройки. 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 интерфейсе Ethernet 1/0/21. Указанное значение: 10,237 мА.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring bias-current eth1/0/21 high warning 10.237

WARNING: A closest value 10.236 is chosen according to the transceiver-monitoring precision
definition

Switch(config)#
```

28.5 transceiver-monitoring enable

Данная команда используется для включения функции мониторинга оптических трансиверов на порту SFP/SFP+. Используйте форму **no**, чтобы отключить функцию мониторинга.

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

Данная команда применима исключительно для настройки интерфейсов физического порта.

Данная команда позволяет включить/отключить функцию мониторинга оптических трансиверов на порту SFP/SFP+. При включении мониторинга отслеживаются события alarm и warning. События alarm или warning происходят, если отслеживаемые параметры выходят за пределы соответствующих верхних или нижних порогов.

Если трансивер SFP/SFP+, поддерживающий функцию мониторинга, 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 **show interfaces transceiver**.

Пример

В данном примере показано, как включить функцию мониторинга трансивера на порту 21.

```
Switch#configure terminal
Switch(config)#interface eth1/0/21
Switch(config-if)#transceiver-monitoring enable
Switch(config-if)#
```

28.6 transceiver-monitoring rx-power

Данная команда используется для настройки порогов входной мощности на указанном порту.
Используйте форму **no**, чтобы удалить заданные настройки.

transceiver-monitoring rx-power *INTERFACE-ID* **{high | low} {alarm | warning} {mwatt** *VALUE* **| dbm** *VALUE***}**

no transceiver-monitoring rx-power *INTERFACE-ID* **{high | low} {alarm | warning}**

Параметры

INTERFACE ID	Укажите интерфейс, который необходимо настроить.

high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
mwatt *VALUE*	Укажите порог входной мощности в диапазоне от 0 до 6,5535 мВт.
dbm V*ALUE*	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 портов SFP+ с оптическими модулями, поддерживающими функцию мониторинга.

Команда позволяет настроить пороги входной мощности на указанном порту. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, куда будут перезаписаны в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен только в системе. Отображаться будут заданные пользователем настройки. 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 интерфейсе Ethernet 1/0/21. Указанное значение – 0,135 мВт.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring rx-power eth1/0/21 low warning mwatt 0.135
Switch(config)#
```

28.7 transceiver-monitoring temperature

Данная команда используется для настройки порогов температуры на указанном порту. Используйте форму **no**, чтобы удалить заданные настройки.

transceiver-monitoring temperature *INTERFACE-ID* **{high | low} {alarm | warning}** *VALUE*
no transceiver-monitoring temperature *INTERFACE-ID* **{high | low} {alarm | warning}**

Параметры

INTERFACE ID	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
VALUE	Укажите порог температуры в диапазоне от -128 до +127,996 °C.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данный функционал доступен только для интерфейсов портов SFP+ с оптическими модулями, поддерживающими функцию мониторинга.

Данная команда позволяет настроить пороги температуры на указанном порту. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, куда будут перезаписаны в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен только в системе. Отображаться будут заданные пользователем настройки. 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 alarm для температуры на интерфейсе Ethernet 1/0/21. Указанное значение: 127,994 °C.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring temperature eth1/0/21 high alarm 127.994

WARNING: A closer value of 127.992 is chosen according to the transceiver-monitoring precision
definition

Switch(config)#
```

28.8 transceiver-monitoring tx-power

Данная команда используется для настройки порогов выходной мощности на указанном порту. Используйте форму **no**, чтобы удалить заданные настройки.

transceiver-monitoring tx-power *INTERFACE-ID* **{high | low} {alarm | warning} {mwatt** *VALUE* **| dbm** *VALUE***}**

no transceiver-monitoring tx-power *INTERFACE-ID* **{high | low} {alarm | warning}**

Параметры

INTERFACE ID	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
mwatt *VALUE*	Укажите порог выходной мощности в диапазоне от 0 до 6,5535 мВт.
dbm V*ALUE*	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 портов SFP+ с оптическими модулями, поддерживающими функцию мониторинга.

Команда позволяет настроить пороги выходной мощности на указанном порту. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, куда будут перезаписаны в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен только в системе. Отображаться будут заданные пользователем настройки. 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 выходной мощности на интерфейсе Ethernet 1/0/21. Указанное значение: 0,181 мВт.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring tx-power eth1/0/21 low warning mwatt 0.181
Switch(config)#
```

28.9 transceiver-monitoring voltage

Данная команда используется для настройки порогов напряжения на указанном порту. Используйте форму **no**, чтобы удалить заданные настройки.

transceiver-monitoring voltage *INTERFACE-ID* **{high | low} {alarm | warning}** *VALUE*
no transceiver-monitoring voltage *INTERFACE-ID* **{high | low} {alarm | warning}**

Параметры

INTERFACE ID	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
VALUE	Укажите порог напряжения в диапазоне от 0 до 6,55 В.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данный функционал доступен только для портов SFP+ с оптическими модулями, поддерживающими функцию мониторинга.

Команда позволяет настроить пороги напряжения на указанном порту. Заданные значения сохраняются как в системе, так и в трансиверах SFP/SFP+, куда будут перезаписаны в 16-битном формате.

Если конфигурируемый модуль SFP/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен только в системе. Отображаться будут заданные пользователем настройки. 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 alarm для напряжения на интерфейсе Ethernet 1/0/21. Указанное значение: 0,005 В.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring voltage eth1/0/21 low alarm 0.005
Switch(config)#
```

29. Команды Distance Vector Multicast Routing Protocol (DVMRP)

29.1 ip dvmrp

Данная команда используется для включения DVMRP на текущем интерфейсе. Для отключения DVMRP на интерфейсе воспользуйтесь формой **no** этой команды.

ip dvmrp
no ip dvmrp

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды
Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды
Можно запустить (или остановить) протокол DVMRP на интерфейсе. Перед включением функции DVMRP на интерфейсе необходимо включить многоадресную IP-маршрутизацию, используя команду **ip multicast-routing** в режиме Global Configuration Mode. На интерфейсе можно включить только один протокол многоадресной маршрутизации. При запуске нескольких протоколов появится сообщение об ошибке.

Пример
В данном примере показано, как включить протокол DVMRP на интерфейсе VLAN1.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip dvmrp
```

29.2 ip dvmrp metric

Данная команда используется для настройки метрики, ассоциируемой с маршрутом для отчетов DVMRP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip dvmrp metric *METRIC*
no ip dvmrp metric

Параметры

METRIC	Укажите значение метрики в диапазоне от 1 до 32. Значение 32 означает бесконечность (недоступность).

По умолчанию

Значение метрики по умолчанию – 1.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для каждого сетевого источника метрика маршрута ассоциируется с отчетным маршрутом. Метрика представляет собой сумму метрик интерфейсов между маршрутизатором, отправляющим отчет, и сетью-источником. Для DVMRP метрика со значением 32 означает бесконечность (недоступность). Это позволяет ограничить размер сети DVMRP и устанавливает верхнюю границу времени сходимости протокола.

Пример

В данном примере показано, как изменить значение метрики интерфейса, указав значение 2.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip dvmrp metric 2
```

29.3 ip dvmrp neighbor-timeout

Данная команда используется, чтобы настроить время жизни для соседнего устройства DVMRP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip dvmrp neighbor-timeout *SECONDS*
no ip dvmrp neighbor-timeout

Параметры

SECONDS	Укажите время жизни соседнего устройства (от 1 до 65535 секунд).

По умолчанию

Значение по умолчанию – 35 секунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если по истечении тайм-аута маршрутизатор не получил сообщение probe от соседнего устройства, то соседнее устройство считается отключенным.

Пример

В данном примере показано, как установить тайм-аут для соседнего устройства. Указанное значение – 60 секунд.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip dvmrp neighbor-timeout 60
```

29.4 ip dvmrp probe-time

Данная команда используется, чтобы указать интервал DVMRP probe. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip dvmrp probe-time *SECONDS*
no ip dvmrp probe-time

Параметры

SECONDS	Укажите значение интервала DVMRP probe в диапазоне от 1 до 65535 секунд.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для указания временного интервала, используемого маршрутизатором DVMRP для отправки сообщений DVMRP probe.

Пример

В данном примере показано, как установить интервал DVMRP probe. Указанное значение – 20 секунд.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip dvmrp probe-time 20
```

29.5 show ip dvmrp interface

Данная команда используется для отображения информации о настройках DVMRP на интерфейсе.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейс VLAN.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о DVMRP на интерфейсах с активным DVMRP. Если интерфейс не отображается, можно использовать команду **show running-config** для дальнейшей проверки конфигурации DVMRP. Если интерфейс не указан, будут отображены все интерфейсы с активным DVMRP.

Пример

В данном примере показано, как отобразить информацию о настройках DVMRP для интерфейса VLAN1000.

```
Switch#show ip dvmrp interface vlan1000

NT = Neighbor Timeout
Interface  Address          NT   Probe    Metric  Generation ID  State
---------  ---------------- ----  -----  ------  -------------   ------
vlan1000   10.0.0.254      35      10    1       1234567890     Enabled

Total Entries: 1

Switch#
```

29.6 show ip dvmrp neighbor

Данная команда используется для отображения информации о соседнем устройстве DVMRP.

show ip dvmrp neighbor [*INTERFACE-ID* **|** *IP-ADDRESS***]**

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса.
IP-ADDRESS	(Опционально.) Укажите IP-адрес соседнего устройства.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о соседнем устройстве DVMRP. Если параметры не указаны, будет отображена информация обо всех соседних устройствах.

Пример

В данном примере показано, как отобразить информацию о соседнем устройстве.

```
Switch#show ip dvmrp neighbor

Interface        Neighbor Address  Generation ID  ExpTime
---------------  ----------------  -------------  -----------
vlan1            10.10.10.11       35ef6d         0DT00H00M29S

Total Entries: 1

Switch#
```

Отображаемые параметры

Interface	Интерфейс маршрутизации, соответствующий VLAN-интерфейсу.
Neighbor Address	После того как система получает от соседнего устройства сообщение probe, содержащее адрес системы в списке соседних устройств, с данным маршрутизатором устанавливается двустороннее соединение.
Generation ID	После перезапуска маршрутизатора DVMRP информация о предыдущих входящих/исходящих сообщениях prune будет удалена. Для обнаружения соседями перезапуска маршрутизатора в сообщениях probe используется неубывающее число, которое называется Generation ID. При обнаружении изменения в Generation ID любое сообщение prune, полученное от маршрутизатора, больше не действительно и его необходимо удалить.

ExpTime	Значение интервала Neighbor Timeout должно составлять 35 секунд. Это позволяет достаточно оперативно обнаружить соседнее устройство, соединение с которым было прервано, не перегружая при этом работой многоадресные маршрутизаторы. Данные значения необходимо согласовать между всеми маршрутизаторами DVMRP в физическом сегменте сети. Значение Expire-Time показывает время, оставшееся до истечения тайм-аута.

29.7 show ip dvmrp route

Данная команда используется для отображения информации о маршрутах DVMRP.

show ip dvmrp route [*NETWORK-ADDRESS***]**

Параметры

NETWORK-ADDRESS	(Опционально.) Укажите адрес и маску сети-источника. Если сетевой адрес не указан, отображаются все маршруты DVMRP.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о маршрутах DVMRP.

Пример

В данном примере показано, как отобразить информацию о маршрутах DVMRP.

```
Switch#show ip dvmrp route

State: H = Hold-down
Source Network     Upstream Neighbor  Metric  Learned  Interface  State  ExpTime
---------------  -----------------  ------  -------  ---------  -----  ------
10.10.11.0/24     10.10.11.11        1       Local    vlan1      -      -

Total Entries: 1

Switch#
```

Отображаемые параметры

Source Network	Сеть источника.
Upstream Neighbor	Следующий узел в сети источника. Если интерфейс представляет собой локальную запись, будет отображен IP-адрес интерфейса.
Learned	Показывает, что маршрут локальный или изучается динамически.
Interface	Интерфейс в сети источника.
State	Если статус маршрута DVMRP «Hold-down», то в статусе отображается «H». Для локального интерфейса отображается «-».
ExpTime	Количество времени, оставшееся до удаления записи из таблицы маршрутизации DVMRP. Знак тире означает, что данная запись не будет удалена (так как это локальный интерфейс).

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

30.1 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 включена.

Режим ввода команды

Global Configuration Mode.

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию клиента DDP глобально или на физическом порту.

Если на порту отключена функция DDP, данный порт не будет ни обрабатывать, ни генерировать DDP-сообщения. Полученные портом DDP-сообщения распространяются в рамках широковещательного домена.

Пример

В данном примере показано, как включить DDP глобально.

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

В следующем примере показано, как включить DDP на интерфейсе Ethernet 1/0/1.

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

30.2 ddp report-timer

Данная команда используется для настройки интервала между двумя последовательными

сообщениями DDP report. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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)#
```

30.3 show ddp

Данная команда используется для отображения настроек DDP на коммутаторе.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о DDP на коммутаторе.

Пример

В данном примере показано, как отобразить общую информацию о DDP.

```
Switch#show ddp

D-Link Discovery Protocol state: Enabled
DDP Version:  5
Report timer: Never

Switch#
```

В следующем примере показано, как отобразить информацию о DDP на интерфейсе Ethernet 1/0/1.

```
Switch#show ddp interface eth1/0/1

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

Switch#
```

30.4 show ddp neighbors

Данная команда используется для отображения информации о соседних устройствах DDP.

show ddp neighbors [interface *INTERFACE-ID* **[, | -]] [detail]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите ID интерфейса для отображения.
,	(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.
detail	(Опционально.) Укажите для отображения подробной информации.

По умолчанию
Нет.

Режим ввода команды
User/Privileged EXEC Mode.

Уровень команды по умолчанию
Уровень 1.

Использование команды
Данная команда применяется для отображения информации о соседних устройствах DDP.

Пример
В данном примере показано, как отобразить информацию о соседних устройствах DDP.

```
Switch#show ddp neighbors
Total Entries: 2

Interface MAC Address       IP Address                              Product  DDP
                                                                    Category Ver
--------- ----------------- --------------------------------------- -------- ---
eth1/0/8  28-3B-82-7F-5A-08 10.90.90.90                             Switch   5
eth1/0/10 28-3B-82-AA-BB-CC 3FFE:22:33:44::55                       Switch   5

Switch#
```

Отображаемые параметры

Interface	Интерфейс, на котором получена и изучена запись.
MAC Address	MAC-адрес устройства.
IP Address	IPv4/IPv6-адрес устройства.

Product Category	Идентификация типа продукта. **Switch (Коммутатор)** **AP**: Access point (Точка доступа) **NC**: Network camera (Сетевая камера) **VE**: Video encoder (Видеокодер) **NVR**: Network video recorder (Сетевой видеорегистратор) **NAS**: Network attached storage (Сетевой накопитель) **SR**: Service router (Сервисный маршрутизатор) **WC**: Wireless controller (Беспроводной контроллер) **WS**: Wireless switch (Беспроводной коммутатор) **WR**: Wireless router (Беспроводной маршрутизатор) **EPOS**** **AAA-S**: AAA policy server (Сервер политики AAA) **DS**: Digital signage (Цифровая система оповещения) **NP**: Network printer (Сетевой принтер) **CNTRLER**: Controller (Контроллер)
DDP Ver	Версия протокола DDP.

В примере ниже показано, как отобразить подробную информацию о соседних устройствах DDP.

```
Switch#show ddp neighbors detail
Total Entries: 2

Interface: eth1/0/8
MAC Address: 28-3B-82-7F-5A-08
IP Address: 10.90.90.90
 Prefix Length: 24
 Model Name: DGS-3130-54TS
 DDP Version: 5
 Role: Client
 System Name: Switch-East1
 Product Category: Switch
 Firmware Version: 1.10.B024
 Hardware Version: A1
 Serial Number: DDLN7160002

Interface: eth1/0/10
MAC Address: 28-3B-82-AA-BB-CC
IP Address: 3FFE:22:33:44::55
 Prefix Length: 64
 Model Name: DGS-3130-54PS
 DDP Version: 5
 Role: Client
 System Name: Switch-East2
 Product Category: Switch
 Firmware Version: 1.10.T032
 Hardware Version: A1
 Serial Number: SG16114000021

Switch#
```

Отображаемые параметры

Interface	Интерфейс, на котором получена и изучена запись.
MAC Address	MAC-адрес устройства.
IP Address	IPv4/IPv6-адрес устройства.
Prefix Length	Длина префикса устройства.
Model Name	Модель устройства.
System Name	Имя системы.
Product Category	Идентификация типа продукта, выполняется в сообщении DDP.
Firmware Version	Версия программного обеспечения устройства.
Hardware Version	Аппаратная версия устройства.
DDP Version	Версия протокола DDP.
Role	Назначение устройства (сервер или клиент).

Serial Number	Серийный номер устройства.

31. Команды Domain Name System (DNS)

31.1 clear host

Данная команда используется для удаления динамически изученных записей узла в режиме Privileged User Mode.

clear host {all | *HOST-NAME***}**

Параметры

all	Укажите, чтобы удалить все записи узла.
HOST-NAME	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#
```

31.2 ip domain lookup

Данная команда используется для включения DNS, что позволяет использовать функцию Domain Name Resolution. Для отключения данной функции воспользуйтесь формой **no** этой команды.

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)#
```

31.3 ip host

Данная команда используется для настройки статической записи привязки для имени узла, а также IP-адреса в таблице узлов. Для удаления статической записи узла воспользуйтесь формой **no** данной команды.

ip host *HOST-NAME* **{***IP-ADDRESS* **|** *IPV6-ADDRESS***}**
no ip host *HOST-NAME* **{***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

Параметры

HOST-NAME	Укажите имя узла устройства.
IP-ADDRESS	Укажите IPv4-адрес устройства.
IPV6-ADDRESS	Укажите IPv6-адрес устройства.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Имя узла, указанное в этой команде, должно быть подходящим. Чтобы удалить статическую запись узла, используйте форму **no** данной команды.

Пример

В данном примере показано, как настроить запись привязки имени узла «www.abc.com» и IP-адреса 192.168.5.243.

```
Switch#configure terminal
Switch(config)#ip host www.abc.com 192.168.5.243
Switch(config)#
```

31.4 ip name-server

Данная команда используется для настройки IP-адреса Domain Name Server. Для удаления сконфигурированного DNS-сервера воспользуйтесь формой **no** этой команды.

ip name-server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [{***IP-ADDRESS2* **|** *IPV6-ADDRESS2***}]**

no ip name-server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [{***IP-ADDRESS2* **|** *IPV6-ADDRESS2***}]**

Параметры

IP-ADDRESS	Укажите IPv4-адрес Domain Name Server.
IPV6-ADDRESS	Укажите IPv6-адрес Domain Name Server.
IP-ADDRESS2	Укажите несколько IP-адресов, разделяя их при помощи пробелов. Можно указать не более 2 серверов.
IPV6-ADDRESS2	Укажите несколько IPv6-адресов, разделяя их при помощи пробелов. Можно указать не более 2 серверов.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте 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 серверы Name Server уже сконфигурировны, то серверы, сконфигурированные позже, будут добавлены в список серверов. Можно сконфигурировать до 4 серверов Name Server.

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)#
```

31.5 ip name-server timeout

Данная команда используется для конфигурации значения тайм-аута для Name Server. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

ip name-server timeout *SECONDS*

no ip name-server timeout

Параметры

SECONDS	Укажите максимальное время ожидания ответа от указанного Name Server. 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)#
```

31.6 show hosts

Данная команда используется для отображения настроек DNS.

show hosts

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о настройках DNS.

Пример

В данном примере показано, как отобразить информацию о настройках DNS.

```
Switch#show hosts

 Number of Static Entries:   1
 Number of Dynamic Entries:  0

 Host Name:          www.abc.com
 IP Address:         192.168.5.243
 TTL:                forever


Switch#
```

Отображаемые параметры

TTL	Значение TTL (Time-To-Leave) отображается, если запись является динамической. Если запись – статическая, отображается ключевое слово «forever».

31.7 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.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить DNS.

Пример

В данном примере показано, как отобразить настройки DNS, если получены записи Dynamic Name Server от DHCP-сервера.

```
Switch#show ip name-server

 Static name server:
 192.168.5.134
 5001:5::2

 Dynamic name server:
 1.1.1.1
 1.1.1.2

Switch#
```

В примере ниже показано, как отобразить настройки DNS, если не получена запись Dynamic Name Server от DHCP-сервера.

```
Switch#show ip name-server

 Static name server:
 192.168.5.134
 5001:5::2

 Dynamic name server:

Switch#
```

32. Команды DoS Prevention

32.1 dos-prevention

Данная команда используется для включения и настройки механизма предотвращения атак DoS (DoS Prevention). Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

dos-prevention *DOS-ATTACK-TYPE*

no dos-prevention *DOS-ATTACK-TYPE*

Параметры

DOS-ATTACK-TYPE	Укажите строку, идентифицирующую тип DoS, который необходимо настроить.

По умолчанию

По умолчанию все поддерживаемые типы DoS отключены.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для включения и настройки механизма предотвращения DoS-атак определенного типа или всех поддерживаемых типов. Механизмы предотвращения атак DoS (сопоставление и принятие мер) являются функциями аппаратного обеспечения.

При включенном предотвращении атак DoS коммутатор сохранит событие (лог) в журнале, если был получен хотя бы один «атакующий» пакет.

Команда **no dos-prevention** с ключевым словом **all** используется для отключения механизма предотвращения атак DoS для всех поддерживаемых типов. Все настройки будут возвращены к значениям по умолчанию для определенных типов атак.

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

- **Blat:** данный тип атаки включает в себя отправку устройству пакетов с портом источника TCP/UDP, равным порту назначения. Это может послужить причиной того, что устройство будет отвечать самому себе.
- **Land:** атака LAND включает в себя отправку устройству IP-пакетов с адресом источника и назначения, равным адресу устройства. Это может послужить причиной того, что устройство будет непрерывно отвечать самому себе.
- **TCP-NULL-scan:** сканирование порта с использованием определенных пакетов, содержащих последовательность чисел от 0 и не содержащих флаги.
- **TCP-SYN-fin:** сканирование порта с использованием определенных пакетов, содержащих флаги SYN и FIN.
- **TCP-SYN-SRCport-less-1024:** сканирование порта с использованием определенных пакетов, содержащих порт источника 0-1023 и флаг SYN.

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



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)#
```

32.2 show dos-prevention

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

show dos-prevention [*DOS-ATTACK-TYPE***]**

Параметры

DOS-ATTACK-TYPE	(Опционально.) Укажите тип DoS, который необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

```
Switch#show dos-prevention

DoS Prevention Information
DoS Type                    State
--------------------------- --------
Land Attack                 Enabled
Blat Attack                 Enabled
TCP Null                    Disabled
TCP Xmas                    Disabled
TCP SYN-FIN                 Disabled
TCP SYN SrcPort Less 1024   Disabled
Ping of Death Attack        Disabled
TCP Tiny Fragment Attack    Disabled

Switch#
```

В данном примере показано, как отобразить информацию о настройках предотвращения атак DoS для типа атаки Land.

```
Switch#show dos-prevention land

DoS Type : Land Attack
State    : Enabled

Switch#
```

32.3 snmp-server enable traps dos-prevention

Данная команда используется для отправки SNMP-уведомлений о DoS-атаках. Для отключения отправки SNMP-уведомлений воспользуйтесь формой **no** этой команды.

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

При включенной функции предотвращения атак DoS коммутатор будет записывать событие в журнал каждые пять минут, если какой-либо атакующий пакет будет принят за этот промежуток времени. Используйте данную команду, чтобы включить или отключить отправку уведомлений SNMP для таких событий.

Пример

В данном примере показано, как включить отправку trap-сообщений для атак DoS.

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

33. Команды Dynamic ARP Inspection

33.1 arp access-list

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

arp access-list *NAME*

no arp access-list *NAME*

Параметры

NAME	Укажите имя списка доступа ARP, который необходимо настроить. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Имя должно быть уникальным среди всех списков доступа. Имя чувствительно к регистру. В конце списка доступа указан запрет в доступе всем, кого нет в списке разрешений.

Пример

В данном примере показано, как настроить список доступа ARP с двумя разрешающими записями.

```
Switch#configure terminal
Switch(config)#arp access-list 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)#
```

33.2 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#
```

33.3 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, чтобы удалить данные статистики Dynamic ARP Inspection для всех VLAN.
vlan *VLAN-ID*	Укажите VLAN или диапазон 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

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#
```

33.4 ip arp inspection filter vlan

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

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

Параметры

ARP-ACL-NAME	Укажите имя списка управления доступом. Максимальное количество символов – 32.
vlan *VLAN-ID*	Укажите VLAN, сопоставленную со списком доступа ARP.
,	(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.
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 применяется 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 привязок DHCP Snooping. Проверка будет производиться, если данная команда сконфигурирована.

Списки управления доступом ARP (ARP ACL) имеют более высокий приоритет над таблицей привязок 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)#
```

33.5 ip arp inspection limit

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

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

По умолчанию

Для недоверенных интерфейсов DAI ограничение скорости составляет 15 пакетов в секунду с интервалом 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 eth1/0/10
Switch(config-if)#ip arp inspection limit rate 30 burst interval 5
Switch(config-if)#
```

33.6 ip arp inspection log-buffer

Данная команда используется для настройки параметра буфера журнала ARP Inspection. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip arp inspection log-buffer entries *NUMBER*

no ip arp inspection log-buffer entries

Параметры

NUMBER	Укажите количество записей в буфере. Максимальное значение – 1024.

По умолчанию

Значение по умолчанию – 32.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для настройки максимального количества записей в буфере журнала. Буфер журнала ARP Inspection хранит информацию об ARP-пакетах. Первый пакет, прошедший 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)#
```

33.7 ip arp inspection trust

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

ip arp inspection trust
no ip arp inspection trust

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если интерфейс находится в состоянии trust (доверенный), ARP-пакеты, поступающие на интерфейс, не будут проверяться. Если интерфейс находится в состоянии untrusted (недоверенный), ARP-пакеты, поступающие на порт и принадлежащие VLAN, в которой включена проверка, будут проверяться.

Пример

В данном примере показано, как настроить состояние Trust (доверенный) для интерфейса Ethernet 1/0/3 для DAI.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ip arp inspection trust
Switch(config-if)#
```

33.8 ip arp inspection validate

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

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 заголовке ARP.
dst-mac	(Опционально.) Укажите для проверки пакетов ARP-ответов, а также согласованности MAC-адреса источника в заголовке Ethernet с MAC-адресом источника в заголовке ARP.
ip	(Опционально.) Укажите для проверки содержимого ARP на наличие недопустимых и непредвиденных IP-адресов. Укажите для проверки допустимости IP-адреса в заголовке ARP. Проверяются IP-адреса источника во всех ARP-запросах и ответах, и IP-адрес назначения в ARP-ответе. Пакеты, отправляемые на IP-адреса 0.0.0.0, 255.255.255.255 и все IP-адреса многоадресной рассылки отбрасываются. IP-адреса источника проверяются во всех ARP-запросах и ответах, а IP-адреса назначения проверяются только в ARP-ответах.

По умолчанию

По умолчанию данная 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 параметры не указаны, все опции включены или выключены.

Пример

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

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

33.9 ip arp inspection vlan

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

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

Параметры

VLAN-ID	Укажите VLAN, для которой необходимо включить или отключить функцию ARP Inspection.
,	(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

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 или таблицей привязок 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)#
```

33.10 ip arp inspection vlan logging

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

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.) 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.
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

Данная команда используется для управления типом пакетов, которые будут логироваться.

Пример

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

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

33.11 permit | deny (arp access-list)

Данная команда применяется для создания разрешающей или запрещающей ARP-записи. Для удаления записи воспользуйтесь формой **no** этой команды.

{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)#
```

33.12 show ip arp inspection

Данная команда используется для отображения статуса DAI для указанного диапазона VLAN.

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

Параметры

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

vlan *VLAN-ID*	(Опционально.) Укажите VLAN или группу 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.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

В данном примере показано, как 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 котором 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 привязок 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 котором 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 основе совпадения 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 основе таблицы привязок DHCP. **None**: пакеты, отброшенные или разрешенные таблицей привязок DHCP, не логируются. **Permit**: логирование происходит, если пакеты разрешены таблицей привязок DHCP. **Deny**: логирование происходит, если пакеты отброшены таблицей привязок DHCP. **All**: пакеты, отброшенные или разрешенные таблицей привязок DHCP, логируются.

Пример

В данном примере показано, как включить отображение состояния для интерфейса Ethernet 1/0/10.

```
Switch#show ip arp inspection interfaces eth1/0/10

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.

33.13 show ip arp inspection log

Данная команда используется для отображения буфера лога (журнала) ARP Inspection.

show ip arp inspection log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения содержимого буфера лога (журнала) ARP Inspection.

Пример

В данном примере показано, как включить отображение буфера лога (журнала) ARP Inspection.

```
Switch#show ip arp inspection log
Total log buffer size: 64

Interface       VLAN Sender IP       Sender MAC        Occurrence
--------------- ---- --------------- ----------------- ------------------------
eth1/0/1        100  10.20.1.1       00-20-30-40-50-60 1 (2013-12-28 23:08:66)
eth1/0/2        100  10.5.10.16      55-66-20-30-40-50 2 (2013-12-02 00:11:54)
eth1/0/3        100  10.58.2.30      10-22-33-44-50-60 1 (2013-12-30 12:01:38)

Total Entries: 3

Switch#
```

Отображаемые параметры

Interface	Имя интерфейса, на котором производится логирование.
VLAN	VLAN, на которой производится логирование.
Sender IP	IP-адрес источника у логируемого ARP.
Sender MAC	MAC-адрес источника у логируемого ARP.
Occurence	Счетчик общего числа логирования записей, а также времени последнего логирования.

34. Команды Error Recovery

34.1 errdisable recovery

Данная команда используется для включения функции Error Recovery (автоматическое восстановление порта при возникновении ошибок), а также для настройки Recovery Interval (время восстановления). Используйте форму **no**, чтобы отключить опцию Auto-Recovery или вернуться к настройкам по умолчанию.

errdisable recovery cause {all | psecure-violation | storm-control | bpdu-protect | arp-rate | dhcp-rate | loopback-detect | l2pt-guard} [interval *SECONDS***]**

no errdisable recovery cause {all | psecure-violation | storm-control | bpdu-protect | arp-rate | dhcp-rate | loopback-detect | l2pt-guard} [interval *SECONDS***]**

Параметры

all	Укажите, чтобы включить опцию Auto-Recovery для всех ситуаций.
psecure-violation	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной Port Security Violation.
storm-control	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной Storm Control.
bpdu-protect	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной BPDU Protection.
arp-rate	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной ARP Rate Limiting.
dhcp-rate	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной DHCP Rate Limiting.
loopback-detect	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной Loop Detection.
l2pt-guard	Укажите, чтобы включить опцию Auto-Recovery при ошибке на порту, вызванной L2PT guard.
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 такими событиями, как 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)#
```

34.2 show errdisable recovery

Данная команда используется для отображения настроек Recovery Timer (таймер восстановления).

show errdisable recovery

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки Recovery Timer.

Пример

В данном примере показано, как отобразить настройки Recovery Timer.

```
Switch#show errdisable recovery

ErrDisable Cause                    State         Interval
----------------------------------  ------------  -------------
Port Security                       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

Interfaces that will be recovered at the next timeout:

Interface    Errdisable Cause                     Time left(sec)
---------    ----------------------------------   --------------
eth1/0/7     BPDU Attack Protection               infinite

Switch#
```

34.3 snmp-server enable traps errdisable

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

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 trap-сообщений 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 trap-сообщений в минуту, при этом настройки отправки уведомлений об ошибке на порту останутся прежними.

Пример

В данном примере показано, как включить отправку SNMP-уведомлений об ошибке на порту.

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

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

DESCRIPTION	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. Для удаления физического кольца G.8032 воспользуйтесь формой **no** этой команды.

ethernet ring g8032 *RING-NAME*

no ethernet ring g8032 *RING-NAME*

Параметры

RING-NAME	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. Для удаления профиля G.8032 воспользуйтесь формой **no** этой команды.

ethernet ring g8032 profile *PROFILE-NAME*
no ethernet ring g8032 profile *PROFILE-NAME*

Параметры

PROFILE-NAME	Укажите имя профиля G.8032. Максимально допустимое количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы создать или изменить профиль G.8032 и войти в режим G.8032 Profile Configuration Mode.

Пример

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

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 profile campus
Switch(config-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. Для отключения передачи уведомлений об изменении топологии воспользуйтесь формой **no** этой команды.

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. Для удаления настроек воспользуйтесь формой **no** этой команды.

r-aps channel-vlan *VLAN-ID*

no r-aps channel-vlan

Параметры

VLAN-ID	Укажите ID R-APS VLAN для экземпляра ERPS. 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 eth1/0/1
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#r-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. Для удаления заданных VLAN ID воспользуйтесь формой **no** этой команды.

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

Параметры

VLAN-ID	Укажите VLAN ID защищенных VLAN экземпляра ERPS. Доступный диапазон значений: от 1 до 4094.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

ERPS Instance Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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 eth1/0/1
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. Для удаления экземпляра ERPS воспользуйтесь формой **no** этой команды.

instance *INSTANCE-ID*
no instance *INSTANCE-ID*

Параметры

INSTANCE-ID	Укажите идентификатор экземпляра ERPS в диапазоне от 1 до 32.

По умолчанию

Нет.

Режим ввода команды

ERPS Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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 eth1/0/1
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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

level *MEL-VALUE*

no level

Параметры

MEL-VALUE	Укажите значение MEL кольца экземпляра ERPS в диапазоне от 0 до 7.

По умолчанию

Значение по умолчанию – 1.

Режим ввода команды

ERPS Instance Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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 eth1/0/1
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 (sub-ring default instance) для экземпляра физического кольца по умолчанию (physical ring default instance). Для удаления экземпляра подкольца по умолчанию воспользуйтесь формой **no** этой команды.

sub-ring *SUB-RING-NAME*
no sub-ring *SUB-RING-NAME*

Параметры

SUB-RING-NAME	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 связанный 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. Для удаления экземпляра подкольца для экземпляра физического кольца воспользуйтесь формой **no** этой команды.

sub-ring instance *INSTANCE-ID*
no sub-ring instance *INSTANCE-ID*

Параметры

INSTANCE-ID	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. Для удаления привязки воспользуйтесь формой **no** этой команды.

profile *PROFILE-NAME*
no profile *PROFILE-NAME*

Параметры

PROFILE-NAME	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 eth1/0/1
Switch(config-erps-ring)#port1 interface eth1/0/2
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 eth1/0/3
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. Для удаления заданных настроек воспользуйтесь формой **no** этой команды.

port0 interface *INTERFACE-ID*
no port0

Параметры

INTERFACE-ID	Укажите interface ID порта кольца. Доступны физические порты и

	port-channel.

По умолчанию

Нет.

Режим ввода команды

ERPS Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить первый порт физического кольца.

Пример

В данном примере показано, как настроить интерфейс 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 eth1/0/1
Switch(config-erps-ring)#
```

35.13 port1

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

port1 {interface *INTERFACE-ID* **| none}**

no port1

Параметры

INTERFACE-ID	Укажите второй порт кольца. Доступны физические порты и port-channel.
none	Укажите, чтобы настроить связанный узел в качестве 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. Для удаления настройки RPL воспользуйтесь формой **no** этой команды.

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 eth1/0/1
Switch(config-erps-ring)#port1 interface eth1/0/2
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

RING-NAME	(Опционально.) Укажите, чтобы отобразить информацию о физическом кольце ERPS.
PROFILE-NAME	(Опционально.) Укажите, чтобы отобразить информацию о профиле ERPS.
INSTANCE-ID	(Опционально.) Укажите, чтобы отобразить информацию об экземпляре ERPS.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об ERPS.

Пример

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

```
Switch#show ethernet ring g8032 status

 ERPS Version: G.8032v2
 ----------------------------
 Ethernet Ring ring1
 Admin Port0: eth1/0/1
 Admin Port1: eth1/0/2
 Ring Type: Major ring
 Ring ID: 1
 ----------------------------
 Instance  : 1
 Instance Status: Idle
 R-APS Channel : 2,Protected VLANs:3
 Port0: eth1/0/1, Blocking
 Port1: eth1/0/2, 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: eth1/0/1
Admin Port1: eth1/0/2
Ring Type: Major ring
Ring ID: 1
----------------------------
Instance  : 1
Instance Status: Idle
R-APS Channel : 2,Protected VLANs:3
Port0: eth1/0/1, Blocking
Port1: eth1/0/2, 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                            InstID  Status      Port-State
-----                            ----    -----       -------
ring1                            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                            InstID  Status      Port-State
-----                            ----    -----       -------
ring1                            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	TC распространяются / не распространяются в кольце.
Revertive / Non-revertive	Реверсивный/нереверсивный режим работы колец.
Instance Status	Текущий статус узла кольца экземпляра ERPS (Deactivated / Init / Idle / Protection / force / manual / pending).
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. Для отключения экземпляра ERPS воспользуйтесь формой **no** этой команды.

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, чтобы настроить таймеры для профиля ERPS. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

timer {guard *MILLI-SECONDS* **| hold-off** *SECONDS* **| wtr** *MINUTES***}**
no timer [guard | hold-off | wtr]

Параметры

guard *MILLI-SECONDS*	Укажите значение Guard Timer в диапазоне от 10 до 2000 миллисекунд. Указанное значение должно быть кратным 10.
hold-off *SECONDS*	Укажите значение Hold-Off Timer в диапазоне от 0 до 10 секунд.
wtr *MINUTES*	Укажите значение WTR Timer в диапазоне от 1 до 12 минут.

По умолчанию

Значение Guard Timer по умолчанию – 500 миллисекунд.

Значение Hold-Off Timer по умолчанию – 0.

Значение WTR Timer по умолчанию – 5 минут.

Режим ввода команды

G.8032 Profile Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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. Для удаления настроек воспользуйтесь формой **no** этой команды.

ring_id *RING_ID*

no ring_id

Параметры

RING-ID	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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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)#
```

35.24 erps version

Данная команда используется для настройки версии ERPS. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

erps version {G.8032v1 | G.8032v2}
no erps version

Параметры

G.8032v1	Укажите, чтобы использовать версию ERPS G.8032v1.
G.8032v2	Укажите, чтобы использовать версию ERPS G.8032v2.

По умолчанию

Версия по умолчанию – G.8032v2.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

G.8032v2 поддерживает следующие расширенные функции:

- Несколько экземпляров (multi-instance) в физическом кольце.
- Операции переключения: manual, force и clear.
- Настройки отправки адреса назначения (destination) R-APS PDU с ID физического кольца.

Изменение версии ERPS перед указанием G.8032v1 для устройства с G.8032v2 приведет к перезапуску действующего протокола.

Если кольцевые узлы Ethernet используют ITU-T G.8032v1 и ITU-T G.8032v2, настройки устройства с G.8032v2 должны быть следующими:

- ID физических колец по умолчанию – 1.
- R-APS VID экземпляров подкольца и основного кольца связанного узла должны отличаться.
- Операции manual и force недоступны.
- Количество экземпляров физического кольца – 1.

Пример

В данном примере показано, как установить версию ERPS.

```
Switch#configure terminal
Switch(config)#erps version G.8032v1
Switch(config)#
```

36. Команды File System

36.1 cd

Данная команда используется для смены текущего каталога.

cd [*DIRECTORY-URL***]**

Параметры

DIRECTORY-URL	(Опционально.) Укажите путь к каталогу. Если путь не указан, будет отображен текущий каталог.

По умолчанию

По умолчанию текущим каталогом является корневой каталог в файловой системе внутренней памяти.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если путь не указан, текущий каталог не будет сменен.

Пример

В данном примере показано, как сменить текущий каталог на каталог «d» в файловой системе.

```
Switch#dir

Directory of /c:
1   d--             0 Jan 01 2019 03:12:49  d
2   -rw      14993776 Jan 01 2019 00:18:42  runtime.had
3   -rw      14991008 Jan 01 2019 00:26:02  Run_1_00_015.had
4   -rw          1802 Jan 01 2019 00:02:18  config.cfg
5   -rw      14887648 Jan 01 2019 04:56:22  Run-1.00.022.had
6   d--             0 Jan 01 2019 00:00:10  system

62283264 bytes total (16477184 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

FILE-URL	Укажите имя файла, который необходимо удалить.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Файл программного обеспечения или файл конфигурации, указанный в качестве загрузочного файла, удалить невозможно.

Пример

В данном примере показано, как удалить файл «test.txt» из файловой системы внутренней памяти.

```
Switch#delete c:/test.txt

Delete test.txt? (y/n) [n] y
File is deleted

Switch#
```

36.3 dir

Данная команда используется для отображения информации о файле или списке файлов в указанном пути.

dir [*URL***]**

Параметры

URL	(Опционально.) Укажите имя файла или каталога, который необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если путь не указан, будет использован текущий каталог. По умолчанию текущий каталог расположен в корне файловой системы внутренней памяти. Накопитель установлен в файловой системе и отображается пользователю в качестве подкаталога корневого каталога.

Используйте команду **dir** для корневого каталога, чтобы отобразить поддерживаемые файловые системы. Используйте команду **show storage media**, чтобы отобразить накопитель, привязанный к файловой системе.

Пример

В данном примере показано, как отобразить корневой каталог автономного коммутатора.

```
Switch#dir /

Directory of /
1   d--              0 Jan 01 2019 00:00:10   c:

0 bytes total (0 bytes free)

Switch#
```

36.4 mkdir

Данная команда используется для создания каталога в текущем каталоге.

mkdir *DIRECTORY-NAME*

Параметры

DIRECTORY-NAME	Укажите имя каталога.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы создать каталог в текущем каталоге.

Пример

В данном примере показано, как создать каталог «newdir» в текущем каталоге.

```
Switch#mkdir newdir
Switch#
```

36.5 more

Данная команда используется для отображения содержимого файла.

more *FILE-URL*

Параметры

FILE-URL	Укажите путь к файлу, который необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы отобразить содержимое файла в файловой системе. Обычно команда применяется для отображения текстовых файлов. Нестандартные печатные символы будут отображены как нечитаемые знаки или пробелы.

Пример

В данном примере показано, как отобразить содержимое файла «config.cfg».

```
Switch#more config.cfg


!----------------------------------------------------------------------------
!                  DGS-1520-28MP Gigabit Ethernet Smart Managed Switch
!                                Configuration
!
!                            Firmware: Build 1.00.022
!           Copyright(C) 2020 D-Link Corporation. All rights reserved.
!----------------------------------------------------------------------------

# AAA START
# AAA END
!
# COMMAND LEVEL START
# COMMAND LEVEL END
# LEVEL START
# LEVEL END
# ACCOUNT START
# ACCOUNT END
!
ip http server
ip http service-port 80
ip http timeout-policy idle 180
no ip http secure-server
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

36.6 rename

Данная команда используется для переименования файла.

rename *FILE-URL1 FILE-URL2*

Параметры

FILE-URL1	Укажите путь к файлу, который необходимо переименовать.
FILE-URL2	Укажите путь к переименованному файлу.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Переименованный файл может располагаться в том же или другом каталоге.

Пример

В данном примере показано, как изменить имя файла с «doc.1» на «test.txt».

```
Switch#rename /c:/doc.1 /c:/test.txt

Rename file doc.1 to text.txt? (y/n) [n] y

Switch#
```

36.7 rmdir

Данная команда используется для удаления каталога из файловой системы.

rmdir *DIRECTORY-NAME*

Параметры

DIRECTORY-NAME	Укажите имя каталога, который необходимо удалить.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы удалить каталог из текущего каталога.

Пример

В данном примере показано, как удалить каталог «newdir» из текущего каталога.

```
Switch#rmdir newdir

Remove directory newdir? (y/n) [n] y
The directory is removed

Switch#
```

36.8 show storage media-info

Данная команда используется для отображения информации о накопителе.

show storage media-info [unit *UNIT-ID***]**

Параметры

unit *UNIT-ID*	(Опционально.) Укажите Unit ID устройства в стеке.

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. Если параметр не указан, будут отображены все устройства.

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       59 MB     FFS

Switch#
```

Отображаемые параметры

Media-Type	**Flash:** отображает внутреннюю память коммутатора.

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

mac-address-table aging-time *SECONDS*

no mac-address-table aging-time

Параметры

SECONDS	Укажите время устаревания в диапазоне от 0 или 10 до 1000000 секунд. Укажите 0, чтобы отключить функцию устаревания MAC-адресов в таблице.

По умолчанию

Значение по умолчанию – 300 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Укажите время устаревания «0», чтобы отключить функцию устаревания MAC-адресов в таблице.

Пример

В данном примере показано, как указать значение времени устаревания 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. Для отключения функции воспользуйтесь формой **no** этой команды.

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, чтобы включить изучение MAC-адресов на физическом порту или VLAN. Для отключения данной функции воспользуйтесь формой **no** этой команды.

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	(Опционально.) Укажите интерфейс физического порта, который необходимо сконфигурировать.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.

-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить/отключить изучение MAC-адресов на физическом порту 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 IMPB, 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 eth1/0/5
Switch(config)#
```

37.5 mac-address-table notification change

Данная команда используется для включения/настройки функции уведомлений о MAC-адресах. Для отключения функции или возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 trap-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 trap-сообщении содержать VLAN ID.
with-vlanid	Укажите для включения VLAN ID в информацию о trap-сообщении.
without-vlanid	Укажите для исключения VLAN ID из информации о trap-сообщении.

По умолчанию

Уведомления о MAC-адресах отключены.

Интервал отправки trap-сообщений по умолчанию – 1 секунда.

Количество записей в таблице истории уведомлений по умолчанию – 1.

Тип trap-сообщения 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 trap-сообщения. 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. Для удаления записи из таблицы воспользуйтесь формой **no** этой команды.

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. Диапазон 01-80-C2-XX-XX-XX зарезервирован для MAC-адресов. Для групповых IPv4 MAC-адресов предназначен диапазон 01-00-5E-XX-XX-XX. Для групповых IPv6 MAC-адресов предназначен диапазон 33-33-XX-XX-XX.
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 eth1/0/1
Switch(config)#
```

37.7 multicast filtering-mode

Данная команда используется, чтобы настроить способ обработки групповых пакетов на интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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

no multicast filtering-mode

Параметры

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

По умолчанию

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

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данный режим фильтрации применим только к групповым пакетам, предназначенным для адресов, незарезервированных для групповых адресов.

Пример

В данном примере показано, как установить режим фильтрации групповых пакетов на VLAN 100, чтобы отфильтровать незарегистрированные адреса.

```
Switch#configure terminal
Switch(config)#vlan 100
Switch(config-vlan)#multicast filtering-mode filter-unregistered
Switch(config-vlan)#
```

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.

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.

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

VLAN-ID	(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.
INTERFACE-ID	(Опционально.) Укажите интерфейс, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если не указаны дополнительные параметры, будут отображены все физические порты.

Пример

В данном примере показано, как отобразить статус изучения MAC-адресов на всех физических портах от 1 до 10.

```
Switch#show mac-address-table learning interface eth1/0/1-10

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 *INTERFACE-ID*	(Опционально.) Укажите интерфейс, который необходимо отобразить.
history	(Опционально.) Укажите, чтобы отобразить историю уведомлений об изменении MAC-адреса.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить режим фильтрации при обработке групповых пакетов, полученных на интерфейсе.

Пример

В данном примере показано, как отобразить настройки режима фильтрации групповых пакетов для всех VLAN.

```
Switch#show multicast filtering-mode

Interface                        Layer 2 Multicast Filtering Mode
-------------------------------- --------------------------------
default                          forward-unregistered

Total Entries: 1

Switch#
```

37.13 snmp-server enable traps mac-notification change

Данная команда используется для включения отправки SNMP trap об уведомлениях MAC. Для отключения функции воспользуйтесь формой **no** этой команды.

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/отключить отправку SNMP trap об уведомлениях MAC.

Пример

В данном примере показано, как включить отправку SNMP trap об уведомлениях MAC.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps mac-notification change
Switch(config)#
```

37.14 snmp trap mac-notification change

Данная команда используется для включения уведомлений об изменении MAC-адреса на указанном интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 trap-сообщений 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 eth1/0/2
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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
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 *INTERFACE-ID*	Укажите интерфейсы, которые необходимо сконфигурировать.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы обнулить счетчики GVRP.

Пример

В данном примере показано, как удалить статистику для всех интерфейсов.

```
Switch#clear gvrp statistics all
Switch#
```

39.2 gvrp global

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

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. Для отключения функции воспользуйтесь формой **no** этой команды.

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 применима исключительно для настройки интерфейсов физического порта 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 интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
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. Для отключения функции воспользуйтесь формой **no** этой команды.

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

no gvrp advertise

Параметры

all	Укажите, чтобы включить анонсирование для всех VLAN на интерфейсе.
add	(Опционально.) Укажите одну или несколько VLAN, которые необходимо добавить в список анонсирования.
remove	(Опционально.) Укажите одну или несколько VLAN, которые необходимо удалить из списка анонсирования.
VLAN-ID	Укажите VLAN ID, который необходимо добавить в список анонсирования или удалить из данного списка. Если не указан параметр **add** или **remove**, список указанных VLAN заменит текущий список анонсирования. Доступный диапазон значений: от 1 до 4094.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию анонсирование VLAN отключено.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel в режимах hybrid и trunk. Используйте команду **gvrp advertise**, чтобы включить функцию анонсирования GVRP для указанных VLAN на указанном интерфейсе. Предварительно необходимо включить GVRP.

Пример

В данном примере показано, как включить функцию анонсирования для VLAN 1000 на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#gvrp advertise 1000
Switch(config-if)#
```

39.5 gvrp vlan create

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

gvrp vlan create
no gvrp vlan create

Параметры

Нет.

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если данная функция включена и на порту обнаружено новое членство VLAN, но при этом данной VLAN не существует, VLAN будет создана автоматически. В противном случае изученная VLAN не будет создана.

Пример

В данном примере показано, как включить создание Dynamic VLAN, зарегистрированных с помощью GVRP-протокола.

```
Switch#configure terminal
Switch(config)#gvrp vlan create
Switch(config)#
```

39.6 gvrp forbidden

Данная команда используется для указания порта, которому запрещено быть членом обозначенной VLAN. Чтобы удалить статус запрещенного члена всех VLAN для порта, воспользуйтесь формой **no** этой команды.

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

no gvrp forbidden

Параметры

all	Укажите, чтобы запретить на интерфейсе все VLAN, кроме VLAN 1.
add	(Опционально.) Укажите одну или несколько VLAN, которые необходимо добавить в список запрещенных VLAN.
remove	(Опционально.) Укажите одну или несколько VLAN, которые необходимо удалить из списка запрещенных VLAN.
VLAN-ID	Укажите список запрещенных VLAN. Если не указан параметр **add** или **remove**, список данных VLAN заменит текущий список запрещенных VLAN. Доступный диапазон значений: от 2 до 4094.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию ни одна из VLAN не запрещена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel в режимах hybrid и trunk. Порт, указанный в качестве запрещенного порта VLAN, не может стать членом VLAN при помощи GVRP. VLAN, обозначенная при помощи данной команды, может не существовать.

Команда влияет только на работу GVRP, при этом необходимо предварительно включить GVRP.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве запрещенного порта для VLAN 1000 при помощи GVRP.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#gvrp forbidden 1000
Switch(config-if)#
```

39.7 gvrp timer

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

gvrp timer [join *TIMER-VALUE***] [leave** *TIMER-VALUE***] [leave-all** *TIMER-VALUE***]**
no gvrp timer [join] [leave] [leave-all]

Параметры

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

По умолчанию

Join: 20.

Leave: 60.

Leave-all: 1000.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить значение таймера GVRP на порту.

Пример

В данном примере показано, как настроить значение таймера для выхода из всех групп на интерфейсе Ethernet 1/0/1. Установленное значение – 500 сотых долей секунды.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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.
INTERFACE-ID	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки GVRP. Если не указан ни один из параметров, будут отображены глобальные настройки GVRP.

Пример

В данном примере показано, как отобразить глобальные настройки GVRP.

```
Switch#show gvrp configuration

Global GVRP State      : Enabled
Dynamic VLAN Creation : Disabled
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 eth1/0/5-6

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 *INTERFACE-ID*	Укажите интерфейсы, которые необходимо сконфигурировать.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

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 eth1/0/5-6

 Interface      JoinEmpty  JoinIn     LeaveEmpty LeaveIn   LeaveAll   Empty
 ------------------------------------------------------------------------------
 eth1/0/5    RX 0          0          0          0         0          0
             TX 4294967296 4294967296 4294967296 42949672964294967296 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, чтобы включить изучение пакетов Gratuitous ARP в таблице ARP-кэша. Для отключения ARP control воспользуйтесь формой no этой команды.

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, чтобы включить передачу пакетов Gratuitous ARP Request. Для отключения передачи воспользуйтесь формой **no** этой команды.

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 интерфейсе. Для отключения функции воспользуйтесь формой **no** этой команды.

arp gratuitous-send interval *SECONDS*

no arp gratuitous-send interval

Параметры

SECONDS	Укажите временной интервал для отправки сообщений с Gratuitous ARP Request. Доступный диапазон значений: от 0 до 3600. Если указан 0, данная опция отключена.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если интерфейс коммутатора используется в качестве шлюза для конечных устройств и у данных устройств наблюдается поведение ложного шлюза, администратор может настроить регулярную отправку сообщений с Gratuitous ARP Request на данном интерфейсе для уведомления о том, что коммутатор является подлинным шлюзом.

Пример

В данном примере показано, как включить отправку сообщений Gratuitous ARP.

```
Switch#configure terminal
Switch(config)#ip gratuitous-arps
Switch(config)#interface vlan100
Switch(config-if)#arp gratuitous-send interval 1
Switch(config-if)#
```

40.4 snmp-server enable traps gratuitous-arp

Данная команда используется, чтобы включить отправку SNMP-уведомлений об обнаружении дублированного IP-адреса Gratuitous ARP. Для отключения функции воспользуйтесь формой **no** этой команды.

snmp-server enable traps gratuitous-arp

no snmp-server enable traps gratuitous-arp

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для включения/отключения отправки SNMP-уведомлений об обнаружении дублированного IP-адреса Gratuitous ARP.

Пример

В данном примере показано, как включить отправку SNMP-уведомлений об обнаружении дублированного IP-адреса Gratuitous ARP.

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

41. Команды управления интерфейсом

41.1 clear counters

Данная команда используется для сброса всех счетчиков указанных интерфейсов.

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

Параметры

all	Укажите, если необходимо сбросить счетчики для всех интерфейсов.
interface *INTERFACE-ID*	Укажите один или несколько интерфейсов, для которых необходимо обнулить счетчики. Параметр применим для физических портов, port-channel или интерфейсов VLAN 2-го уровня.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду, чтобы сбросить счетчики для одного или нескольких указанных интерфейсов / для всех интерфейсов.

Пример

В данном примере показано, как сбросить счетчики для интерфейса Ethernet 1/0/1.

```
Switch#clear counters interface eth1/0/1
Switch#
```

41.2 description

Данная команда используется для добавления описания на интерфейс. Для удаления описания воспользуйтесь формой **no** этой команды.

description *STRING*
no description

Параметры

STRING	Описание интерфейса. Максимально допустимое количество символов – 64.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

```
Switch#configure terminal
Switch(config)#interface eth1/0/10
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. Для удаления интерфейса воспользуйтесь формой **no** этой команды.

interface *INTERFACE-ID*
no interface *INTERFACE-ID*

Параметры

INTERFACE-ID	Укажите ID интерфейса (Interface ID). В качестве ID интерфейса указывается тип и номер интерфейса без пробелов между ними.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для входа в режим Interface Configuration Mode для определенного интерфейса. ID интерфейса состоит из типа интерфейса и номера интерфейса без пробелов между ними.

Для обозначения интерфейсов используются следующие ключевые слова:

- **Ethernet** – физический Ethernet-порт коммутатора;
- **L2vlan** – интерфейс VLAN уровня 2 на основе IEEE 802.1Q;
- **Loopback** – программный интерфейс, который всегда находится в рабочем состоянии;
- **mgmt** – интерфейс Ethernet, используемый для управления портом out-of-band **(только для DGS-1520-28 and DGS-1520-52)**;
- **Null** – интерфейс null;
- **Port-channel** – агрегированный интерфейс port-channel;
- **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 создается автоматически, когда для настройки интерфейса физического порта используется команда **channel-group**. Интерфейс port-channel будет удален автоматически, если интерфейс физического порта для команды **channel-group** не будет настроен. Используйте команду **no interface Port-channel**, чтобы удалить port-channel.

Для интефейса null поддерживается интерфейс null0, который не может быть удален.

Для интерфейсов loopback или tunnel команда **interface** используется для создания нового интерфейса или изменения настроек существующего. При использовании формы **no** команда удалит интерфейс.

Режим интерфейса **l2vlan** используется только для добавления описания к существующим L2VLAN. Команда **interface l2vlan** не создает новые интерфейсы, а форма **no** данной команды не удаляет существующие интерфейсы.

Пример

В данном примере показано, как войти в режим Interface Configuration Mode для интерфейса Ethernet 1/0/5.

```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#
```

В данном примере показано, как войти в режим Interface Configuration Mode для VLAN 100.

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

В данном примере показано, как войти в режим Interface Configuration Mode для port-channel 3.

```
Switch#configure terminal
Switch(config)#interface port-channel3
Switch(config-if)#
```

В данном примере показано, как добавить интерфейс 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 позволяет войти в режим Interface Range Configuration Mode для нескольких интерфейсов.

interface range *INTERFACE-ID* **[, | -]**

Параметры

INTERFACE-ID	Укажите ID интерфейса. В качестве ID интерфейса указывается тип и номер интерфейса без пробелов между ними.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда используется для входа в режим Interface Range Configuration Mode для указанного диапазона интерфейсов. Команды, введенные в режиме Interface Range Configuration Mode, применяются ко всем интерфейсам указанного диапазона.

Пример

В данном примере показано, как войти в режим Interface Range Configuration Mode для диапазона интерфейсов от Ethernet 1/0/1 до 1/0/5, а также для интерфейса Ethernet 1/0/8.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-5,1/0/8
Switch(config-if-range)#
```

41.5 show counters

Данная команда используется для отображения информации об интерфейсе.

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

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите необходимый интерфейс (физический порт, port-channel или VLAN 2-го уровня). Если интерфейс не указан, будут отображаться счетчики для всех интерфейсов.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется, чтобы отобразить статистику счетчиков для интерфейса.

Статистическая информация о скорости port-channel представляет собой сумму всех скоростей физических интерфейсов портов для данного port-channel. Например, если 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 и 100, то скорость ошибок CRC данного port-channel будет 600 пакетов в секунду.

Следующие пункты предоставляют подробную информацию об отображении параметров данной команды:

- **max-rcv-frame-size:** максимальный размер Ethernet-кадра, определенный в командах **Jumbo Frame.** Диапазон значений: от 64 до 12288 байт.

Пример

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

```
Switch#show counters interface eth1/0/1

eth1/0/1 counters
rxHCTotalPkts                    : 45340
txHCTotalPkts                    : 11516
rxHCUnicastPkts                  : 18220
txHCUnicastPkts                  : 11516
rxHCMulticastPkts                : 24994
txHCMulticastPkts                : 0
rxHCBroadcastPkts                : 2126
txHCBroadcastPkts                : 0
rxHCOctets                       : 5876961
txHCOctets                       : 5111397
rxHCPkt64Octets                  : 31884
rxHCPkt65to127Octets             : 5800
rxHCPkt128to255Octets            : 1005
rxHCPkt256to511Octets            : 3208
rxHCPkt512to1023Octets           : 3443
rxHCPkt1024to1518Octets          : 0
rxHCPkt1519to1522Octets          : 0
rxHCPkt1519to2047Octets          : 0
rxHCPkt2048to4095Octets          : 0
rxHCPkt4096to9216Octets          : 0
rxHCPkt9217to16383Octets         : 0
txHCPkt64Octets                  : 183
txHCPkt65to127Octets             : 5054
txHCPkt128to255Octets            : 1082
txHCPkt256to511Octets            : 2481
txHCPkt512to1023Octets           : 560
txHCPkt1024to1518Octets          : 2156
txHCPkt1519to1522Octets          : 0
txHCPkt1519to2047Octets          : 0
txHCPkt2048to4095Octets          : 0
txHCPkt4096to9216Octets          : 0
txHCPkt9217to16383Octets         : 0

rxCRCAlignErrors                 : 0
rxUndersizedPkts                 : 0
rxOversizedPkts                  : 0
rxFragmentPkts                   : 0
```

```
rxJabbers                          : 0
rxSymbolErrors                     : 0
rxBufferFullDropPkts               : 0
rxACLDropPkts                      : 0
rxMulticastDropPkts                : 0
rxVLANIngressCheckDropPkts         : 0
rxIpv6DropPkts                     : 0
rxSTPDropPkts                      : 0
rxStormAndTableDropPkts            : 0
rxMTUDropPkts                      : 0

txCollisions                       : 0
ifInErrors                         : 0
ifOutErrors                        : 0
ifInDiscards                       : 24616
ifOutDiscards                      : 0
ifInUnknownProtos                  : 0
txDelayExceededDiscards            : 0
txCRC                              : 0
txSTPDropPkts                      : 0
txHOLDropPkts                      : 0

dot3StatsAlignmentErrors           : 0
dot3StatsFCSErrors                 : 0
dot3StatsSingleColFrames           : 0
dot3StatsMultiColFrames            : 0
dot3StatsSQETestErrors             : 0
dot3StatsDeferredTransmissions     : 0
dot3StatsLateCollisions            : 0
dot3StatsExcessiveCollisions       : 0
dot3StatsInternalMacTransmitErrors : 0
dot3StatsCarrierSenseErrors        : 0
dot3StatsFrameTooLongs             : 0
dot3StatsInternalMacReceiveErrors  : 0

linkChange                         : 1


Switch#
```

Отображаемые параметры

rxHCTotalPkts	Счетчик принятых пакетов. Увеличивается с каждым принятым пакетом (включая поврежденные пакеты, все одноадресные, широковещательные и многоадресные пакеты, а также пакеты управления MAC).
txHCTotalPkts	Счетчик переданных пакетов. Увеличивается с каждым переданным пакетом (включая поврежденные пакеты, все одноадресные, широковещательные и многоадресные пакеты, а также пакеты управления MAC).

rxHCUnicastPkts	Счетчик принятых пакетов одноадресной рассылки. Увеличивается с каждым успешно принятым пакетом одноадресной рассылки.
txHCUnicastPkts	Счетчик переданных пакетов одноадресной рассылки. Увеличивается с каждым успешно переданным пакетом одноадресной рассылки.
rxHCMulticastPkts	Счетчик принятых пакетов многоадресной рассылки. Увеличивается с каждым успешно принятым пакетом многоадресной рассылки (за исключением пакетов управления MAC).
txHCMulticastPkts	Счетчик переданных пакетов многоадресной рассылки. Увеличивается с каждым успешно переданным пакетом многоадресной рассылки (за исключением пакетов управления MAC).
rxHCBroadcastPkts	Счетчик принятых пакетов широковещательной рассылки. Увеличивается с каждым успешно принятым пакетом широковещательной рассылки.
txHCBroadcastPkts	Счетчик переданных пакетов широковещательной рассылки. Увеличивается с каждым успешно переданным пакетом широковещательной рассылки.
rxHCOctets	Счетчик принятых байтов. Увеличивается с подсчетом байтов принятых пакетов, включая поврежденные пакеты (за исключением битов кадров, но включая байты FCS). **Примечание**: для усеченного пакета счетчик учитывает только размер max-rcv-frame.
txHCOctets	Счетчик переданных байтов. Увеличивается с подсчетом байтов переданных пакетов (за исключением битов кадров, но включая байты FCS).
rxHCPkt64Octets	Счетчик принятых 64-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) до 64 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt65to127Octets	Счетчик принятых 65 – 127-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 65 до 127 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt128to255Octets	Счетчик принятых 128 – 255-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 128 до 255 байт включительно (за исключением битов кадров, но включая байты FCS).

rxHCPkt256to511Octets	Счетчик принятых 256 – 511-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 256 до 511 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt512to1023Octets	Счетчик принятых 512 – 1023-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 512 до 1023 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt1024to1518Octets	Счетчик принятых 1024 – 1518-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 1024 до 1518 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt1519to1522Octets	Счетчик принятых допустимых 1519 – 1522-байтовых кадров VLAN. Увеличивается с каждым допустимым принятым кадром VLAN (исключая FCS, Symbol, ошибка Truncated), от 1519 до 1522 байт включительно (за исключением битов кадров, но включая байты FCS). Подсчитываются как одиночные, так и дважды тегированные кадры.
rxHCPkt1519to2047Octets	Счетчик принятых 1519 – 2047-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 1519 до 2047 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt2048to4095Octets	Счетчик принятых 2048 – 4095-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 2048 до 4095 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt4096to9216Octets	Счетчик принятых 4096 – 9216-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type), от 4096 до 9216 байт включительно (за исключением битов кадров, но включая байты FCS).
rxHCPkt9217to16383Octets	Счетчик принятых 9217 – 16383-байтовых кадров. Увеличивается с каждым допустимым или поврежденным принятым кадром (включая FCS, Symbol, ошибка Len/Type) от 9217 до 16383 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt64Octets	Счетчик переданных 64-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) до 64 байт включительно (за исключением битов кадров, но включая байты FCS).

txHCPkt65to127Octets	Счетчик переданных 65 – 127-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 65 до 127 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt128to255Octets	Счетчик переданных 128 – 255-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 128 до 255 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt256to511Octets	Счетчик переданных 256 – 511-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 256 до 511 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt512to1023Octets	Счетчик переданных 512 – 1023-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 512 до 1023 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt1024to1518Octets	Счетчик переданных 1024 – 1518-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 1024 до 1518 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt1519to1522Octets	Счетчик переданных допустимых 1519 – 1522-байтовых кадров VLAN. Увеличивается с каждым допустимым кадром VLAN (исключая FCS и ошибки TX) от 1519 до 1522 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt1519to2047Octets	Счетчик переданных 1519 – 2047-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type), от 1519 до 2047 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt2048to4095Octets	Счетчик переданных 2048 – 4095-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 2048 до 4095 байт включительно (за исключением битов кадров, но включая байты FCS).

txHCPkt4096to9216Octets	Счетчик переданных 4096 – 9216-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 4096 до 9216 байт включительно (за исключением битов кадров, но включая байты FCS).
txHCPkt9217to16383Octets	Счетчик переданных 9217 – 16383-байтовых кадров. Увеличивается с каждым допустимым или поврежденным переданным кадром (включая FCS, Symbol, ошибка Len/Type) от 9217 до 16383 байт включительно (за исключением битов кадров, но включая байты FCS).
rxCRCAlignErrors	Счетчик принятых кадров с ошибкой выравнивания. Увеличивается с каждым принятым пакетом от 64 до max-rcv-frame-size (или max-rcv-frame-size+4 для тегированных кадров) октетов в длину (за исключением битов кадров и включая октеты FCS), но содержащим либо поврежденный FCS с целым числом октетов (ошибка FCS), либо поврежденный FCS с нецелым числом октетов (Ошибка выравнивания).
rxUndersizedPkts	Счетчик принятых кадров неполного размера. Увеличивается с каждым принятым пакетом меньше 64 байт в длину (за исключением битов кадров и включая октеты FCS), но в остальном сформированным верно (содержащим допустимый FCS).
rxOversizedPkts	Счетчик принятых кадров слишком большого размера. Увеличивается с каждым принятым пакетом более 1518 байт в длину (за исключением битов кадров и включая октеты FCS), но в остальном сформированным верно (содержащим допустимый FCS). **Примечание:** Подсчет кадров слишком большого размера зависит от ASIC.
rxFragmentPkts	Счетчик принятых фрагментов. Увеличивается с каждым принятым пакетом меньше 64 байт в длину (за исключением битов кадров и включая октеты FCS), но содержащим либо поврежденный FCS с целым числом октетов (ошибка FCS), либо поврежденный FCS с нецелым числом октетов (Ошибка выравнивания).
rxJabbers	Счетчик принятых кадров Jabber. Увеличивается с каждым принятым пакетом более 1518 байт в длину (за исключением битов кадров и включая октеты FCS), но содержащим либо поврежденный FCS с целым числом октетов (ошибка FCS), либо поврежденный FCS с нецелым числом октетов (Ошибка выравнивания). **Примечание:** Подсчет кадров rxJabbers зависит от ASIC.
rxSymbolErrors	Счетчик принятых кадров с ошибкой кода. Увеличивается с каждым принятым кадром, содержащим недопустимый символ данных, но допустимый носитель.

rxBufferFullDropPkts	Счетчик принятых проигнорированных пакетов. Увеличивается с каждым пакетом, проигнорированным по причине заполненного входного буфера или обратного давления (back pressure).
rxACLDropPkts	Счетчик принятых пакетов ACL Drop. Возрастает с каждым пакетом, отброшенным по правилам ACL.
rxMulticastDropPkts	Счетчик принятых пакетов Multicast Drop. Возрастает с каждым отброшенным пакетом multicast (L2+L3).
rxVLANIngressCheckDropPkts	Счетчик принятых пакетов VLAN Drop. Возрастает с каждым пакетом, отброшенным при проверке по VLAN на входе (VLAN ingress).
rxIpv6DropPkts	Счетчик принятых пакетов IPv6 L3 Drop. Возрастает с каждым пакетом, отправленным на интерфейс L3 и проигнорированным по следующим причинам: буфер RX превышает установленное ограничение или GBP заполнен.
rxSTPDropPkts	Счетчик принятых пакетов STP Drop. Возрастает с каждым пакетом, отброшенным по причине того, что статус Spanning Tree State входного порта не находится в состоянии перенаправления.
rxStormAndTableDropPkts	Счетчик принятых пакетов Policy Discard. Возрастает с каждым пакетом, отброшенным благодаря политике получения: действие storm control, действие FDB и т.д.
rxMTUDropPkts	Счетчик принятых кадров MTU Check Error. Возрастает с принятым каждым кадром, размер которого превышает max-rcv-frame-size и который содержит корректный или некорректный FCS. **Примечание**: с тегированием Single VLAN усечение выполняется при max-rcv-frame-size +4; с тегированием double VLAN усечение происходит при max-rcv-frame-size +8.
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 дальшейшую передачу протоколу на уровень выше. Счетчик представляет собой сумму dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsFrameTooLongs, dot3StatsInternalMacReceiveErrors, dot3StatsSymbolErrors, undersize, fragment, oversize, and jabber error.
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 дальшейшем 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.
ifInUnknownProtos	Счетчик полученных, но отброшенных пакетов с неизвестным или не поддерживаемым протоколом. Возрастает с каждым принятым пакетом, который был отброшен из-за неизвестного или не поддерживаемого протокола.
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.
txSTPDropPkts	Счетчик переданных пакетов STP Drop. Возрастает с каждым пакетом, отброшенным по причине того, что статус Spanning Tree State выходного порта не находится в состоянии перенаправления.
txHOLDropPkts	Счетчик переданных пакетов HOL Drop. Возрастает с каждым пакетом, отброшенным из-за блокировки Head Of Line.
dot3StatsAlignmentErrors	Счетчик принятых кадров Alignment Error. Возрастает с каждым принятым кадром с нецелым числом октетов в длину и не прошедшим проверку FCS.
dot3StatsFCSErrors	Счетчик принятых кадров FCS Error. Возрастает с каждым принятым кадром с целым числом октетов в длину, но 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 во время передачи.
dot3StatsMultiColFrames	Счетчик переданных кадров многочисленных коллизий. Доступен только в режиме 10/100. Возрастает с каждым успешно переданным кадром, испытавшим больше одной коллизии во время передачи.

dot3StatsSQETestErrors	Счетчик SQET Test Error. Возрастает с каждым сообщением SQE TEST ERROR, сгенерированным подуровнем PLS для отдельного интерфейса. Сообщение SQE TEST ERROR указано в разделе 7.2.2.2.4 ANSI/IEEE 802.3-1985 и его генерирование описано в разделе 7.2.4.6 того же документа. **Примечание**: Данный счетчик не увеличивается при скоростях свыше 10 Мб/с или в режиме полного дуплекса.
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. Увеличивается с каждым переданным кадром с поздней коллизией во время попытки передачи.
dot3StatsExcessiveCollisions	Счетчик переданных кадров с избытком коллизий. Доступен только в режиме 10/100. Увеличивается с каждым кадром, передача которого не состоялась из-за избытка коллизий.
dot3StatsInternalMacTransmitErrors	Счетчик переданных кадров с внутренней ошибкой MAC. Увеличивается 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.
dot3StatsCarrierSenseErrors	Счетчик False Carrier. Возрастает каждый раз, когда условие контроля несущей потеряно или никогда не подтверждалось при попытке передачи кадра.
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 ни одним из следующих счетчиков: dot3StatsLateCollisions, dot3StatsExcessiveCollisions и dot3StatsCarrierSenseErrors.
dot3StatsFrameTooLongs	Счетчик принятых кадров слишком большой длины. Возрастает с каждым принятым кадром, превышающим размер max-rcv-frame-size.
dot3StatsInternalMacReceiveErrors	Счетчик Internal MAC Error. Возрастает с каждым кадром, не принятым из-за получения ошибки внутренним подуровнем MAC. Кадр подсчитывается только в том случае, если он не учтен соответствующим экземпляром любого из параметров dot3StatsFrameTooLongs, dot3StatsAlignmentErrors или dot3StatsFCSErrors.

41.6 show interfaces

Данная команда используется для отображения информации об интерфейсе.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если интерфейс не указан, будут отображены данные для всех интерфейсов.

Пример

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

```
Switch#show interfaces vlan 1

vlan1 is enabled, Link status is up
  Interface type: VLAN
  Interface description:
  MAC address: 80-26-89-15-28-00



Switch#
```

В данном примере показано, как включить отображение информации об интерфейсе loopback для интерфейса loopback 1.

```
Switch#show interfaces loopback 1

loopback1 is enabled, Link status is up
  Interface type: Loopback
  Interface description: Loopback 1 for MIS



Total Entries: 1

Switch#
```

В данном примере показано, как включить отображение информации об интерфейсе NULL для интерфейса null0.

```
Switch#show interfaces null 0

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 eth1/0/1

eth1/0/1 is enabled link status is up
  Interface type: 1000BASE-T
  Interface description:
  MAC Address: 80-26-89-15-28-01
  Auto-duplex, auto-speed, auto-mdix
  Send flow-control: off, receive flow-control: off
  Send flow-control oper: off, receive flow-control oper: off
  Full-duplex, 100Mb/s
  Maximum transmit unit: 1536 bytes
  RX rate: 0 bytes/sec, TX rate: 0 bytes/sec
  RX bytes: 31953789, TX bytes: 2114661
  RX rate: 0 packets/sec, TX rate: 0 packets/sec
  RX packets: 29103, TX packets: 15446
  RX multicast: 1830, RX broadcast: 2981
  RX CRC error: 0, RX undersize: 0
  RX oversize: 0, RX fragment: 0
  RX jabber: 0, RX dropped Pkts: 0
  RX MTU exceeded: 0
  TX CRC error: 0, TX excessive deferral: 0
  TX single collision: 0, TX excessive collision: 0
  TX late collision: 0, TX collision: 0


Switch#
```

В данном примере показано, как включить отображение информации об интерфейсе для порта управления (management port 0) **(только для DGS-1520-28 and DGS-1520-52)**.

```
Switch#show interfaces mgmt 0

mgmt_ipif 0 is enabled, Link status is up
  Interface type: Management port
  Interface description:

Switch#
```

41.7 show interfaces counters

Данная команда используется для отображения счетчиков на определенных интерфейсах.

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

show interfaces [*INTERFACE-ID* **[, | -]] counters history {15_minute [slot** *INDEX***] | 1_day [slot** *INDEX***]}**

Параметры

INTERFACE-ID	(Опционально.) Укажите идентификатор (ID) интерфейса для отображения. Если интерфейс не указан, будут отображаться счетчики для всех интерфейсов. Разрешены только физический порт, port-channel и L2VLAN.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
errors	(Опционально.) Укажите для отображения счетчика ошибок. Если параметр не указан, отображаются счетчики общей статистики. Разрешены только физический порт и port-channel.
INTERFACE-ID	(Опционально.) Укажите идентификатор (ID) интерфейса для отображения. Если интерфейс не указан, будут отображаться счетчики для всех интерфейсов. Разрешены только физические порты.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
history	Укажите для отображения истории счетчиков.

15_minute	(Опционально.) Укажите для отображения истории статистики за 15 минут.
slot *INDEX*	(Опционально.) Укажите номер слота. Слот 1 отображает историю последней статистики. Если номер слота не указан, отображается история со всех слотов. Диапазон значений: от 1 до 5.
1_day	(Опционально.) Укажите для отображения истории статистики за сутки.
slot *INDEX*	(Опционально.) Укажите номер слота. Слот 1 отображает историю последней статистики. Если номер слота не указан, отображается история со всех слотов. Диапазон значений: от 1 до 2.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения общих счетчиков, счетчиков ошибок или архивной информации для указанного интерфейса или для всех интерфейсов.

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.

Существует два типа статистики: за 15 минут и за сутки. В первом случае (15 минут) слот 1 позволяет отобразить статистику за прошедшие 15 минут, а слот 2 – статистику для интервала, который начался 30 минут назад и завершился 15 минут назад, и т.д. Во втором случае (сутки) слот 1 позволяет отобразить статистику за прошедшие 24 часа, а слот 2 – статистику для интервала, который начался 48 часов назад и закончился 24 часа назад.

Пример

В данном примере показано, как включить отображение счетчиков принятых пакетов (RX) для интерфейсов Ethernet 1/0/1-2.

```
Switch#show interfaces eth1/0/1-2 counters

Port          InOctets /              InMcastPkts /
              InUcastPkts             InBcastPkts
------------- ----------------------- -----------------------
eth1/0/1      12414924                4786
              54604                   12638
eth1/0/2      0                       0
              0                       0

Port          OutOctets /             OutMcastPkts /
              OutUcastPkts            OutBcastPkts
------------- ----------------------- -----------------------
eth1/0/1      14009021                249
              40466                   282
eth1/0/2      0                       0
              0                       0

Total Entries:2


Switch#
```

В примере ниже показано, как включить отображение счетчиков ошибок на портах коммутатора.

```
Switch#show interfaces eth1/0/1,1/0/3 counters errors

Port          Align-Err /             Fcs-Err /
              Rcv-Err /               Undersize /
              Xmit-Err                OutDiscard
------------- ----------------------- -----------------------
eth1/0/1      0                       0
              0                       0
              0                       0
eth1/0/3      0                       0
              0                       0
              0                       0

Port          Single-Col /            Excess-Col /
              Multi-Col /             Carri-Sen /
              Late-Col                Runts
------------- ----------------------- -----------------------
eth1/0/1      0                       0
              0                       0
              0                       0
```

```
eth1/0/3        0                       0
                0                       0
                0                       0

Port            Giants /                DeferredTx /
                Symbol-Err /            IntMacTx /
                SQETest-Err             IntMacRx
-------------- ----------------------- -----------------------
eth1/0/1        0                       0
                0                       0
                0                       0
eth1/0/3        0                       0
                0                       0
                0                       0

Total Entries:2


Switch#
```

Отображаемые параметры

Align-Err	Относится к строке «dot3StatsAlignmentErrors» в разделе «Отображаемые параметры» команды **show counters**.
Fcs-Err	Относится к строке «dot3StatsFCSErrors» в разделе «Отображаемые параметры» команды **show counters**.
Rcv-Err	Относится к строке «ifInErrors» в разделе «Отображаемые параметры» команды **show counters**.
UnderSize	Относится к строке «rxUndersizedPkts» в разделе «Отображаемые параметры» команды **show counters**.
Xmit-Err	Относится к строке «ifOutErrors» в разделе «Отображаемые параметры» команды **show counters**.
OutDiscard	Относится к строке «ifOutDiscards» в разделе «Отображаемые параметры» команды **show counters.**
Single-Col	Относится к строке «dot3StatsSingleColFrames» в разделе «Отображаемые параметры» команды **show counters.**
Multi-Col	Относится к строке «dot3StatsMultiColFrames» в разделе «Отображаемые параметры» команды **show counters.**
Late-Col	Относится к строке «dot3StatsLateCollisions» в разделе «Отображаемые параметры» команды **show counters.**
Excess-Col	Относится к строке «dot3StatsExcessiveCollisions» в разделе «Отображаемые параметры» команды **show counters.**

Carri-Sen	Относится к строке «dot3StatsCarrierSenseErrors» в разделе «Отображаемые параметры» команды **show counters**.
Runts	Увеличивается с каждым пакетом размером менее 64 байт.
Giants	Возрастает с каждым пакетом, размер которого более 1518 байтов в длину.
Symbol-Err	Относится к строке «rxSymbolErrors» в разделе «Отображаемые параметры» команды **show counters**.
SQETst-Err	Относится к строке «dot3StatsSQETestErrors» в разделе «Отображаемые параметры» команды **show counters**.
DeferredTx	Относится к строке «txDelayExceededDiscards» в разделе «Отображаемые параметры» команды **show counters.**
IntMacTx	Относится к строке «dot3StatsInternalMacTransmitErrors» в разделе «Отображаемые параметры» команды **show counters.**
InMacRx	Относится к строке «dot3StatsInternalMacReceiveErrors» в разделе «Отображаемые параметры» команды **show counters**.

В данном примере показано, как отобразить статистику за 15 минут на интерфейсе Ethernet 1/0/1.

```
Switch#show interfaces eth1/0/1 counters history 15_minute slot 1

eth1/0/1  15-Minute Slot 1 :
Starttime : 1  Jan 2019  01:44:38
Endtime   : 1  Jan 2019  01:29:38
rxHCTotalPkts                    : 3974
txHCTotalPkts                    : 3317
rxHCUnicastPkts                  : 3292
txHCUnicastPkts                  : 3303
rxHCMulticastPkts                : 280
txHCMulticastPkts                : 0
rxHCBroadcastPkts                : 402
txHCBroadcastPkts                : 14
rxHCOctets                       : 1617308
txHCOctets                       : 869791
rxHCPkt64Octets                  : 514
rxHCPkt65to127Octets             : 123
rxHCPkt128to255Octets            : 1213
rxHCPkt256to511Octets            : 1069
rxHCPkt512to1023Octets           : 670
rxHCPkt1024to1518Octets          : 385
rxHCPkt1519to1522Octets          : 0
rxHCPkt1519to2047Octets          : 0
rxHCPkt2048to4095Octets          : 0
rxHCPkt4096to9216Octets          : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

41.8 show interfaces status

Данная команда используется для отображения статуса подключения портов коммутатора.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Команда используется для просмотра состояния подключения портов коммутатора. Если параметр не указан, отображается статус подключения для всех портов коммутатора.

Пример

В данном примере показано, как отобразить статус 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      connected     1            a-full  a-100          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     not-connected 1            auto    auto           2500BASE-T
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

41.9 show interfaces utilization

Данная команда используется для отображения информации о загрузке указанных портов коммутатора.

show interfaces [*INTERFACE-ID* **[, | -]] utilization [history {15_minute [slot** *INDEX***] | 1_day [slot** *INDEX***]}]**

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса. Если параметр не указан, будет отображаться информация о загрузке всех физических портов коммутатора. Разрешены физические порты и port-channel.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
utilization	Укажите для отображения информации о загрузке.
history	(Опционально.) Укажите для отображения архивной информации о загрузке портов. Разрешены только физические порты.

15_minute	(Опционально.) Укажите для отображения архивной статистики за 15 минут.
slot *INDEX*	(Опционально.) Укажите номер слота. Слот 1 отображает последнюю архивную информацию. Если номер слота не указан, отображается архивная информация для всех слотов. Доступно значение от 1 до 5.
1_day	(Опционально.) Укажите для отображения архивной статистики за сутки.
slot *INDEX*	(Опционально.) Укажите номер слота. Слот 1 отображает последнюю архивную информацию. Если номер слота не указан, отображается архивная информация для всех слотов. Доступно значение от 1 до 2.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда позволяет пользователю просмотреть информацию о загрузке всех или указанных интерфейсов, а также 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.

Существует два типа статистики: за 15 минут и за сутки. В первом случае (15 минут) слот 1 позволяет отобразить статистику за прошедшие 15 минут, а слот 2 – статистику для интервала, который начался 30 минут назад и завершился 15 минут назад, и т.д. Во втором случае (сутки) слот 1 позволяет отобразить статистику за прошедшие 24 часа, а слот 2 – статистику для интервала, который начался 48 часов назад и закончился 24 часа назад.

Пример

В данном примере показано, как отобразить информацию о загрузке всех 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
```

В примере ниже показано, как отобразить архивную информацию о загрузке интерфейса Ethernet 1/0/1 за 15 минут.

```
Switch#show interfaces eth1/0/1 utilization history 15_minute


eth1/0/1  Utilization:
9  Apr 2018  14:56:13 - 9  Apr 2018  14:41:13  : 0   %
9  Apr 2018  14:41:13 - 9  Apr 2018  14:26:13  : 0   %
9  Apr 2018  14:26:13 - 9  Apr 2018  14:11:13  : 0   %
9  Apr 2018  14:11:13 - 9  Apr 2018  13:56:13  : 0   %
9  Apr 2018  13:56:13 - 9  Apr 2018  13:41:13  : 0   %

Switch#
```

41.10 show interfaces gbic

Данная команда используется для отображения информации о состоянии GBIC.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса. Если параметр не указан, будет отображена информация о состоянии GBIC для всех интерфейсов GBIC.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
gbic	Отображение информации о состоянии GBIC.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о состоянии GBIC.

Пример

В данном примере показано, как отобразить информацию о состоянии GBIC.

```
Switch#show interfaces eth1/0/1 gbic

eth1/0/1
 Interface Type: 1000BASE-T


Switch#
```

41.11 show interfaces auto-negotiation

Данная команда используется для отображения подробной информации об автосогласовании на физических портах.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса. Если параметр не указан, будет отображена информация обо всех физических портах.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
auto-negotiation	Укажите, чтобы отобразить подробную информацию об автосогласовании.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения подробной информации об автосогласовании.

Пример

В данном примере показано, как отобразить информацию об автосогласовании.

```
Switch#show interfaces eth1/0/1 auto-negotiation

eth1/0/1
 Auto Negotiation: Enabled

 Remote Signaling: Detected
 Configure Status: Complete
 Capability Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
 Capability Advertised Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
 Capability Received Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full
 RemoteFaultAdvertised: Disabled
 RemoteFaultReceived: NoError


Switch#
```

41.12 show interfaces description

Данная команда используется для отображения описания и состояния интерфейсов.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса. Если параметр не указан, будет отображена информация обо всех интерфейсах.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
description	Укажите для отображения описания и состояния интерфейсов.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта, port-channel, L2VLAN и VLAN.

Команда используется для отображения описания и состояния интерфейсов.

Пример

В данном примере показано, как отобразить описание и состояние 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. Для включения интерфейса воспользуйтесь формой **no** этой команды.

shutdown
no shutdown

Параметры

Нет.

По умолчанию

Опция по умолчанию – **no shutdown**.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта, loopback, VLAN и MGMT, а также для портов-участников port-channel.

Команда отключает порт. В отключенном состоянии порт не будет принимать и 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 интерфейс Ethernet 1/0/1.

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

41.14 max-rcv-frame-size

Данная команда используется для настройки максимального размера кадра Ethernet. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

max-rcv-frame-size *BYTES*

no max-rcv-frame-size

Параметры

BYTES	Укажите максимально допустимый размер кадра Ethernet. Диапазон значений: от 64 до 12288 байт.

По умолчанию

По умолчанию используется значение 1536 байт.

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.

Кадры слишком большого размера будут отброшены и проверки будут выполняться на входных портах. Используйте данную команду для передачи кадров большого размера или jumbo-фреймов через коммутатор для оптимизации производительности сервер-сервер.

Пример

В данном примере показано, как настроить максимальный размер полученного кадра со значением 6000 на интерфейсе Ethernet 1/0/3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#max-rcv-frame-size 6000
Switch(config-if)#
```

42. Команды Internet Group Management Protocol (IGMP)

42.1 clear ip igmp groups

Данная команда используется для удаления из буфера IGMP информации об участниках динамических групп, полученной из ответных сообщений.

clear ip igmp groups {all | *IP-ADDRESS* **| interface** *INTERFACE-ID***}**

Параметры

all	Укажите, чтобы удалить записи всех групп.
IP-ADDRESS	Укажите, чтобы удалить запись определенной группы.
Interface *INTERFACE-ID*	Укажите, чтобы удалить записи групп, изученных на интерфейсе.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Буфер IGMP содержит список, включающий динамические многоадресные группы, в которые вступают узлы из данной подсети. Используйте данную команду, чтобы удалить информацию о динамических группах. Чтобы удалить все записи о динамических группах из буфера IGMP, используйте команду **clear ip igmp groups all**.

Пример

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

```
Switch#clear ip igmp groups all
Switch#
```

В данном примере показано, как удалить из кэша IGMP записи для многоадресной группы 224.0.255.1.

```
Switch#clear ip igmp groups 224.0.255.1
Switch#
```

В данном примере показано, как удалить из кэша IGMP записи для определенного интерфейса.

```
Switch#clear ip igmp groups interface vlan1
Switch#
```

42.2 ip igmp enable

Данная команда используется для включения протокола IGMP. Для отключения протокола IGMP воспользуйтесь формой **no** этой команды.

ip igmp enable
no ip igmp 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 действует только при настроенном на интерфейсе IP-адресе.

Пример

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

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip igmp enable
Switch(config-if)#
```

42.3 ip igmp ignore-subscriber-ip-check

Данная команда используется для отключения проверки IP-адреса источника подписчика при получении сообщений IGMP report или leave. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp ignore-subscriber-ip-check
no ip igmp ignore-subscriber-ip-check

Параметры

Нет.

По умолчанию

По умолчанию коммутатор будет проверять IP-адрес источника подписчика.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

По умолчанию будет проверено, находится ли IP-адрес источника полученных на интерфейсе сообщений IGMP report или leave в той же сети, что и интерфейс. Если они не находятся в одной подсети, информация из сообщения не будет рассматриваться протоколом IGMP.

Используйте команду **ip igmp ignore-subscriber-ip-check**, чтобы отключить проверку IP-адреса источника. Если проверка отключена, протоколом IGMP будут обрабатываться сообщения report и leave с любым IP-адресом источника.

Пример

В данном примере показано, как отключить проверку IP-адреса источника подписчика на VLAN 1.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip igmp ignore-subscriber-ip-check
Switch(config-if)#
```

42.4 ip igmp last-member-query-interval

Данная команда используется для настройки интервала между сообщениями IGMP group-specific query (с указанием группы) или group-source-specific query (с указанием источника группы) / channel-source-specific query (с указанием источника канала). Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp last-member-query-interval *SECONDS*
no ip igmp last-member-query-interval

Параметры

SECONDS	Укажите интервал между сообщениями IGMP group-specific query. Доступный диапазон значений: от 1 до 25 секунд.

По умолчанию

Значение по умолчанию – 1 секунда.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Когда маршрутизатор принимает сообщение leave, означающее, что узел собирается покинуть группу или канал, он отправляет запрос (group specific query или group-source specific query) на интерфейс получателя. В этом сообщении будет объявлен и передан получателю интервал запросов для последнего участника (IGMP last-member query interval). Эта команда задает период, по истечении которого маршрутизатор будет отправлять следующий запрос group-specific query или group-source specific query, если нет сообщений о принадлежности получателя к определенной группе или определенному каналу. Маршрутизатор повторит запрос для последнего участника несколько раз в соответствии со счетчиком last member query count. Если после этого нет сообщений report, интерфейс будет удален из соответствующей группы или канала.

Пример

В данном примере показано, как включить IGMP и настроить значение IGMP last member query interval на VLAN 1000. Указанный интервал – 2 секунды.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ip igmp enable
Switch(config-if)#ip igmp last-member-query-interval 2
Switch(config-if)#
```

42.5 ip igmp query-interval

Данная команда используется для настройки интервала между общими запросами IGMP, отправляемыми маршрутизатором. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp query-interval *SECONDS*

no ip igmp query-interval

Параметры

SECONDS	Укажите, чтобы настроить интервал между общими запросами IGMP, которые отправляет 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

Команда применяется для конфигурирования интервала запросов принадлежности к группам IGMP (query). IGMP Querier отправляет запросы с интервалом, заданным командой **ip igmp query-interval**, чтобы обнаружить на интерфейсе получателей, желающих присоединиться к многоадресным группам. Узлы отвечают на запросы сообщениями IGMP report, чтобы указать многоадресную группу, к которой они собираются присоединиться.

Пример

В данном примере показано, как включить IGMP и настроить интервал IGMP query на VLAN 1000. Указанный интервал – 300 секунд.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ip igmp enable
Switch(config-if)#ip igmp query-interval 300
Switch(config-if)#
```

42.6 ip igmp query-max-response-time

Данная команда используется для конфигурирования максимального времени ответа, анонсируемого в сообщениях IGMP query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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

no ip igmp query-max-response-time

Параметры

INTERFACE-ID	Укажите, чтобы сконфигурировать максимальное время ответа, анонсируемое в запросах IGMP 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

Используйте данную команду, чтобы сконфигурировать интервал, в течение которого участник группы может ответить на запрос до того, как членство будет удалено маршрутизатором. Время членства в группе вычисляется следующим образом: (query interval x robustness) + maximum response time.

Пример

В данном примере показано, как сконфигурировать максимальное время ответа, анонсируемое в запросах IGMP query, на VLAN 1000. Указанное значение – 10 секунд.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ip igmp query-max-response-time 10
Switch(config-if)#
```

42.7 ip igmp robustness-variable

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

ip igmp robustness-variable *VALUE*
no ip igmp robustness-variable

Параметры

VALUE	Укажите значение robustness variable.

По умолчанию

Значение по умолчанию – 2.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Robustness variable обеспечивает точную настройку с учетом ожидаемой потери пакетов на интерфейсе. Значение robustness variable используется для вычисления следующих интервалов сообщений IGMP:

- **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 (с указанием группы), отправленных маршрутизатором до того, как он предполагает, что в группе нет локальных участников. Robustness variable является значением по умолчанию данного счетчика.

Пример

В данном примере показано, как сконфигурировать robustness variable на интерфейсе VLAN 1000. Указанное значение – 3.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ip igmp robustness-variable 3
Switch(config-if)#
```

42.8 ip igmp static-group

Данная команда используется для создания статического членства для группы или канала на интерфейсе. Для удаления членства воспользуйтесь формой **no** этой команды.

ip igmp static-group *GROUP-ADDRESS*
no ip igmp static-group *GROUP-ADDRESS*

Параметры

GROUP-ADDRESS	Укажите групповой IP-адрес.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы создать статическую группу IGMP, если подключенный узел не поддерживает протокол IGMP. При настройке в кэш IGMP добавляется запись группы.

Пример

В данном примере показано, как сконфигурировать запись статической группы IGMP на VLAN 1000.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ip igmp static-group 238.1.1.2
Switch(config-if)#
```

42.9 ip igmp version

Данная команда используется для изменения версии IGMP на указанном интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp version *NUMBER*
no ip igmp version

Параметры

NUMBER	Укажите версию IGMP. **1:** укажите, чтобы запустить на коммутаторе IGMP версии 1. **2:** укажите, чтобы запустить на коммутаторе IGMP версии 2. **3:** укажите, чтобы запустить на коммутаторе IGMP версии 3.

По умолчанию

По умолчанию используется IGMP версии 3.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Разные версии IGMP поддерживают разные функции для маршрутизации многоадресных данных. Некоторые команды работают только на IGMPv2 и IGMPv3. Например, при переключении на версию 1, настройки, выполненные командой **ip igmp query-max-response-time**, работать не будут.

Пример

В данном примере показано, как включить IGMP и сконфигурировать версию 3.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ip igmp enable
Switch(config-if)#ip igmp version 3
Switch(config-if)#
```

42.10 show ip igmp groups

Данная команда используется для отображения информации о группах IGMP на интерфейсе.

show ip igmp groups [*IP-ADDRESS* **| interface** *INTERFACE-ID***] [{detail | static}]**

Параметры

IP-ADDRESS	(Опционально.) Укажите IP-адрес группы для отображения. Если IP-адрес не указан, будет отображена информация обо всех группах IGMP.
interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс, который необходимо отобразить. Если интерфейс не указан, будет отображена информация о группах IGMP для всех интерфейсов с включенным IGMP.
detail	(Опционально.) Укажите, чтобы отобразить подробную информацию.
static	(Опционально.) Укажите, чтобы отобразить статические группы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Выберите определенную группу или интерфейс для отображения информации IGMP.

Пример

В данном примере показано, как отобразить информацию о группах IGMP для интерфейса VLAN 1000.

```
Switch#show ip igmp groups interface vlan1000

Interface       Group Address   Uptime          Expire          Last Reporter
-----------------------------------------------------------------------------
vlan1000         224.0.1.149    0DT00H00M09S  0DT00H04M15S   10.10.0.91

Total Entries: 1

Switch#
```

В данном примере показано, как отобразить подробную информацию IGMP для группы 224.1.1.1.

```
Switch#show ip igmp groups 224.1.1.1 detail

Interface      : vlan1000
Group          : 224.1.1.1
Uptime         : 0DT00H00M42S
Expires        : Stopped
Group mode     : Include
Last reporter  : 192.168.50.111

Group source list:
      Source Address    v3 Exp
    ----------------- ----------
      192.168.55.55     0DT00H03M38S
      192.168.10.55     0DT00H03M38S

    Total Source Entries: 2

Interface      : vlan2000
Group          : 224.1.1.1
Uptime         : 0DT00H00M42S
Expires        : 0DT00H03M38S
Group mode     : Exclude
Last reporter : 192.168.51.111
Source list is empty

Total Entries: 2

Switch#
```

Отображаемые параметры

Uptime	Время, прошедшее с момента создания записи, в формате [n]DT[n]H[n]M[n]S.
Expires	Время, по истечении которого запись будет удалена при отсутствии обновлений, в формате [n]DT[n]H[n]M[n]S. Состояние stopped указывает, что истечение срока записи не определяется данным таймером. Если маршрутизатор работает в режиме Include для группы, срок записи всей группы истекает по истечении срока записи последнего источника (если до этого режим не будет изменен на Exclude).
Group mode	**Include** или **Exclude**: режим группы основывается на типе сообщений membership report, принимаемых на интерфейсе для группы.
Last reporter	Последний узел, который сообщает, что является участником данной группы.

42.11 show ip igmp interface

Данная команда используется для отображения конфигурации IGMP на интерфейсе.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейс. Если интерфейс не указан, будет отображена информация IGMP для всех интерфейсов с включенным IGMP. Можно указать только интерфейсы VLAN.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить конфигурацию IGMP на интерфейсах.

Пример

В данном примере показано, как отобразить конфигурацию IGMP для интерфейса VLAN1.

```
Switch#show ip igmp interface vlan1

VLAN 1
  Version                      : 3
  IP Address/Netmask           : 172.18.67.139/21
  IGMP State                   : Enabled
  Querier                      : 172.18.67.139
  Query Interval               : 125 seconds
  Query Maximum Response Time  : 10 seconds
  Robustness Variable          : 2
  Last Member Query Interval   : 1 seconds
  Subscriber Source IP Check   : Enabled

Total Entries: 1

Switch#
```

Отображаемые параметры

Version	Версия протокола IGMP на интерфейсе.
Querier	IP-адрес Querier на интерфейсе LAN.

Subscriber Source IP Check	Укажите, чтобы определить, будет ли игнорироваться проверка IP-адреса источника во входящих IGMP-пакетах от подписчика. **Enabled** указывает, что проверка IP-адреса источника не будет игнорирована. **Disabled** указывает, что проверка IP-адреса источника будет игнорирована.

43. Команды Internet Group Management Protocol (IGMP) Proxy

43.1 ip igmp proxy

Данная команда используется для включения функции IGMP Proxy. Для отключения функции IGMP Proxy воспользуйтесь формой **no** этой команды.

ip igmp proxy
no ip igmp proxy

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Функция IGMP Proxy действует только в простой древовидной топологии. Убедитесь в отсутствии других многоадресных маршрутизаторов за исключением proxy-устройств в простой древовидной топологии. При получении пакетов report IGMP с downstream-интерфейса функция IGMP Proxy выполнит обновление базы данных участия, которая создается объединением всех подписок на любом downstream-интерфейсе. Если база данных изменена, proxy-устройство отправит незапрашиваемые отчеты или покинет upstream-интерфейс. При запросе proxy-устройство также может отправить отчеты об участии с upstream-интерфейса.

Пример

В данном примере показано, как включить функцию IGMP Proxy на устройстве.

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

43.2 ip igmp proxy upstream

Данная команда используется для настройки интерфейса как «upstream» в IGMP Proxy. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ip igmp proxy upstream
no ip igmp proxy upstream

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

На устройстве IGMP Proxy может существовать только один upstream-интерфейс.

Пример

В данном примере показано, как настроить интерфейс VLAN 3 в качестве интерфейса proxy upstream.

```
Switch#configure terminal
Switch(config)#interface vlan 3
Switch(config-if)#ip igmp proxy upstream
Switch(config-if)#
```

43.3 ip igmp proxy downstream

Данная команда используется для настройки интерфейса как «downstream» в IGMP Proxy. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ip igmp proxy downstream
no ip igmp proxy downstream

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

На устройстве IGMP Proxy можно настроить несколько downstream-интерфейсов.

Пример

В данном примере показано, как настроить интерфейс VLAN 4 в качестве интерфейса proxy downstream.

```
Switch#configure terminal
Switch(config)#interface vlan4
Switch(config-if)#ip igmp proxy downstream
Switch(config-if)#
```

43.4 ip igmp proxy designated-forwarding

Данная команда используется для включения назначенного перенаправления на downstream-интерфейсе IGMP Proxy, который не является Querier. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ip igmp proxy designated-forwarding
no ip igmp proxy designated-forwarding

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Во избежание локальных петель и избыточного трафика для каналов, которые несколько серверов пересылки IGMP считают downstream-каналами, функция IGMP Proxy использует механизм IGMP Querier election, чтобы выбрать один сервер пересылки в сети LAN. Данная команда применяется, чтобы сделать устройство, не являющееся Querier, сервером пересылки. Используйте конфигурацию в соответствующей топологии. Некорректное применение может привести к возникновению локальных петель или избыточного трафика. Команда не будет действовать, если интерфейс не настроен как downstream или установлен как upstream-интерфейс.

Пример

В данном примере показано, как включить назначенное перенаправление на downstream-интерфейсе VLAN 4.

```
Switch#configure terminal
Switch(config)#interface vlan4
Switch(config-if)#ip igmp proxy designated-forwarding
Switch(config-if)#
```

43.5 show ip igmp proxy

Данная команда используется для отображения настроек IGMP Proxy.

show ip igmp proxy

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки интерфейсов upstream и downstream.

Пример

В данном примере показано, как отобразить настройки IGMP Proxy на устройстве.

```
Switch#show ip igmp proxy

IGMP Proxy Global State:    Enabled
Upstream Interface:          vlan14
Downstream Interface:
vlan11, vlan12(DF), vlan13(DF)

Switch#
```

43.6 show ip igmp proxy group

Данная команда используется для отображения multicast-групп, изученных функцией IGMP Proxy.

show ip igmp proxy group [*GROUP-ADDRESS***]**

Параметры

GROUP-ADDRESS	Укажите групповой IPv4-адрес.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду без указания адреса конкретной группы, чтобы отобразить информацию обо всех группах.

Пример

В данном примере показано, как отобразить информацию о группах, изученных функцией IGMP Proxy.

```
Switch#show ip igmp proxy group

224.2.2.2, Exclude
Source list: 1.2.2.3, 1.3.3.8

227.3.1.5 , Include
Source list: 3.2.3.9

Total entries: 2

Switch#
```

43.7 show ip igmp proxy forwarding

Данная команда используется для отображения записей перенаправления multicast, созданных функцией IGMP Proxy.

show ip igmp proxy forwarding [*GROUP-ADDRESS***]**

Параметры

GROUP-ADDRESS	Укажите групповой IPv4-адрес.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду без указания адреса конкретной группы, чтобы отобразить всю информацию о перенаправлении.

Пример

В данном примере показано, как отобразить информацию о перенаправлении, созданную функцией IGMP Proxy.

```
Switch#show ip igmp proxy forwarding

237.1.1.0, 100.52.1.10, vlan52
outgoing interface:
vlan20, vlan30

237.1.1.1, 100.52.1.10, vlan52
outgoing interface:
vlan20

Total Entries: 2

Switch#
```

44. Команды Internet Group Management Protocol (IGMP) Snooping

44.1 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#
```

44.2 ip igmp snooping

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

ip igmp snooping

no ip igmp snooping

Параметры

Нет.

По умолчанию

По умолчанию функция IGMP Snooping отключена на всех интерфейсах VLAN.

По умолчанию функция IGMP Snooping отключена глобально.

Режим ввода команды

VLAN Configuration Mode.

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для работы VLAN с IGMP Snooping необходимо включить данную функцию и в режиме Global Configuration Mode, и в режиме VLAN Configuration Mode. IGMP Snooping и MLD Snooping могут быть включены одновременно в одной и той же VLAN.

Пример

В данном примере показано, как включить 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)#
```

44.3 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. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ip igmp snooping access-group *ACCESS-LIST-NAME* **[vlan** *VLAN-ID***]**
no ip igmp snooping access-group [vlan *VLAN-ID***]**

Параметры

ACCESS-LIST-NAME	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 *VLAN-ID*	(Опционально.) Укажите VLAN уровня 2 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 данную команду, 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 исключительно 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 eth1/0/1
Switch(config-if)#ip igmp snooping access-group igmp_filter
Switch(config-if)#
```

44.4 ip igmp snooping accounting

Данная команда используется для включения IGMP Accounting при подключении получателя к IGMP-группе. Для отключения данной функции воспользуйтесь формой **no** этой команды.

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 eth1/0/1
Switch(config-if)#ip igmp snooping accounting
Switch(config-if)#
```

44.5 ip igmp snooping authentication

Данная команда используется, чтобы включить функцию аутентификации для сообщений IGMP join. Для отключения данной функции воспользуйтесь формой **no** этой команды.

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 eth1/0/1
Switch(config-if)#ip igmp snooping authentication
Switch(config-if)#
```

44.6 ip igmp snooping fast-leave

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

ip igmp snooping fast-leave
no ip igmp snooping fast-leave

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, 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). Если данная функция включена, коммутатор не будет генерировать сообщения specific query. Если данная функция выключена, коммутатор будет генерировать сообщения specific query.

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)#
```

44.7 ip igmp snooping ignore-topology-change-notification

Данная команда используется для игнорирования изменений STP и отказа от отправки на интерфейс STP-запроса. Для отключения игнорирования изменений STP и отправки STP-запросов на интерфейс воспользуйтесь формой **no** этой команды.

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

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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 времени сетевой сходимости. 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)#
```

44.8 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). Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp snooping last-member-query-interval *SECONDS*

no ip igmp snooping last-member-query-interval

Параметры

SECONDS	Укажите максимальный интервал между сообщениями group-specific query, включая отправленные в ответ на сообщения leave group. Доступный диапазон значений: от 1 до 25.

По умолчанию

Значение по умолчанию – 1 секунда.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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 требуется коммутатору, чтобы обнаружить выход последнего участника из 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)#
```

44.9 ip igmp snooping limit

Данная команда позволяет установить ограничение по количеству записей кэша IGMP, которые можно создать. Для удаления ограничения воспользуйтесь формой **no** этой команды.

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

NUMBER	Укажите максимальное количество записей кэша IGMP, которое можно создать. Доступный диапазон значений: от 1 до 512.
exceed-action	(Опционально.) Укажите, чтобы применить действие к изученным группам при превышении ограничения.
drop	(Опционально.) Укажите, чтобы отбросить новую группу.
replace	(Опционально.) Укажите, чтобы заменить старую группу новой.
except *ACCESS-LIST-NAME*	(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 источника 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 *VLAN-ID*	(Опционально.) Укажите VLAN уровня 2, чтобы включить фильтрацию пакетов, прибывающих на данную VLAN.

По умолчанию

По умолчанию ограничений нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel. 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 ограничением настройки от ACL, к которому может подключиться интерфейс Ethernet 1/0/4 с VLAN ID 1000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/4
Switch(config-if)#ip igmp snooping limit 80 except igmp_filter vlan 1000
Switch(config-if)#
```

В данном примере показано, как сбросить настройки по ограничению количества групп IGMP Snooping, к которым может подключиться интерфейс port-channel 4 с VLAN ID 1000, до настроек по умолчанию.

```
Switch#configure terminal
Switch(config)#interface port-channel 4
Switch(config-if)#no ip igmp snooping limit vlan 1000
Switch(config-if)#
```

44.10 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. Для удаления интерфейса/интерфейсов из списка router-портов или списка запрещенных router-портов воспользуйтесь формой **no** этой команды.

ip igmp snooping mrouter {interface *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -]}**

no ip igmp snooping mrouter {interface *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -]}**

Параметры

interface	Укажите статический multicast router-порт.
forbidden interface	Укажите порт, который не может быть multicast router-портом.
INTERFACE-ID	Укажите интерфейс или список интерфейсов. В качестве интерфейса может быть использован физический порт или port-channel.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию multicast router-порты IGMP Snooping отсутствуют.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Multicast router-портом можно назначить физический порт или port-channel. Указанный multicast router-порт должен являться портом-участником сконфигурированной VLAN. Multicast router-порт может быть изучен динамически или сконфигурирован статически. При помощи динамического изучения устройство IGMP Snooping будет изучать пакеты IGMP, PIM или DVMRP, чтобы идентифицировать multicast router-порт.

Пример

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

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping mrouter interface eth1/0/4
Switch(config-vlan)#
```

44.11 ip igmp snooping proxy-reporting

Данная команда используется для включения функции Proxy Reporting. Для отключения данной функции воспользуйтесь формой **no** этой команды.

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 – 0.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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-vlan)#ip igmp snooping proxy-reporting source 1.2.2.2
Switch(config-vlan)#
```

44.12 ip igmp snooping querier

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

ip igmp snooping querier
no ip igmp snooping querier

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если система может 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)#
```

44.13 ip igmp snooping query-interval

Данная команда используется для настройки интервала между сообщениями IGMP general query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp snooping query-interval *SECONDS*

no ip igmp snooping query-interval

Параметры

SECONDS	Укажите интервал между сообщениями IGMP General Query для обозначенного маршрутизатора. Доступный диапазон значений: от 1 до 31744.

По умолчанию

Значение по умолчанию – 125 секунд.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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)#
```

44.14 ip igmp snooping query-max-response-time

Данная команда используется, чтобы настроить максимальное значение времени ожидания, анонсированное в сообщениях IGMP snooping query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp snooping query-max-response-time *SECONDS*
no ip igmp snooping query-max-response-time

Параметры

SECONDS	Укажите максимальное значение времени ожидания, анонсированное в сообщениях IGMP snooping query. Доступный диапазон значений: от 1 до 25 секунд.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить период времени, в течение которого участник группы может ответить на сообщение IGMP query, прежде чем его принадлежность будет удалена 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)#
```

44.15 ip igmp snooping query-version

Данная команда используется для настройки версии пакетов general query, отправляемых IGMP Snooping Querier. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp snooping query-version *NUMBER*
no ip igmp snooping query-version

Параметры

NUMBER	Укажите версию пакета IGMP general query, отправленного IGMP Snooping Querier. Диапазон значений: от 1 до 3.

По умолчанию

Значение по умолчанию – 3.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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)#
```

44.16 ip igmp snooping rate-limit

Данная команда используется, чтобы установить ограничение скорости передачи входящих управляющих IGMP-пакетов. Для отключения ограничения воспользуйтесь формой **no** этой команды.

ip igmp snooping rate-limit *NUMBER*

no ip igmp snooping rate-limit

Параметры

NUMBER	Укажите пропускную способность (количество пакетов в секунду) для управляющих IGMP-пакетов, обработка которых возможна на определенном интерфейсе. Диапазон значений: от 1 до 1000.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

В режиме Interface Configuration Mode данная команда применима исключительно для настройки интерфейсов 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 установить ограничение 30 пакетов в секунду на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip igmp snooping rate-limit 30
Switch(config-if)#
```

В примере ниже показано, как установить ограничение 30 пакетов в секунду на интерфейсе VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping rate-limit 30
Switch(config-vlan)#
```

44.17 ip igmp snooping report-suppression

Данная команда используется для включения функции Report Suppression. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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)#
```

44.18 ip igmp snooping robustness-variable

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

ip igmp snooping robustness-variable *VALUE*

no ip igmp snooping robustness-variable

Параметры

VALUE	Укажите значение robustness variable в диапазоне от 1 до 7.

По умолчанию

Значение по умолчанию – 2.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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 query (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)#
```

44.19 ip igmp snooping static-group

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

ip igmp snooping static-group *GROUP-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**
no ip igmp snooping static-group *GROUP-ADDRESS* **[interface** *INTERFACE-ID* **[, | -]]**

Параметры

GROUP-ADDRESS	Укажите IP-адрес многоадресной группы.
interface *INTERFACE-ID*	Укажите интерфейс или список интерфейсов. Доступны физические порты или port-channel.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения 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 настроена.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, 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 eth1/0/5
Switch(config-vlan)#
```

44.20 ip igmp snooping suppression-time

Данная команда используется, чтобы настроить время подавления (suppression) дублированных сообщений IGMP report или IGMP leave. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip igmp snooping suppression-time *SECONDS*

no ip igmp snooping suppression-time

Параметры

SECONDS	Укажите время подавления дублированных сообщений IGMP report. Доступный диапазон значений: от 1 до 300.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Функция Report Suppression подавляет дублированные пакеты IGMP report или IGMP leave, полученные в течение указанного времени. Чем меньше значение времени подавления, тем чаще будут отправляться дублированные IGMP-пакеты.

Пример

В данном примере показано, как настроить время подавления 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)#
```

44.21 ip igmp snooping minimum-version

Данная команда используется для настройки минимальной версии IGMP-узлов, разрешенной на интерфейсе. Для удаления ограничения воспользуйтесь формой **no** этой команды.

ip igmp snooping minimum-version *NUMBER*
no ip igmp snooping minimum-version

Параметры

NUMBER	**2:** укажите, чтобы отфильтровать сообщения IGMPv1.
	3: укажите, чтобы отфильтровать сообщения IGMPv1 и IGMPv2.

По умолчанию

По умолчанию ограничения минимальной версии отсутствуют.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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)#
```

44.22 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.

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#
```

44.23 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 *INTERFACE-ID*	(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.

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#
```

44.24 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 для отображения. Если VLAN не указана, будет отображена информация о группе IGMP Snooping для всех VLAN с включенной функцией IGMP Snooping.
,	(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.
IP-ADDRESS	(Опционально.) Укажите IP-адрес группы для отображения. Если IP-адрес не указан, будет отображена информация обо всех группах IGMP.
detail	(Опционально.) Укажите для отображения подробной информации о группе IGMP.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о группе 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

vlan1, 230.1.1.1
Learned on port: 1/0/3,1/0/5

Switch#
```

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

```
Switch#show ip igmp snooping groups detail

Total Group Entries : 1
Total Source Entries: 2

vlan1, 230.1.1.1
Learned on port: 1/0/3,1/0/5
  1/0/3
    version: v2, filter mode: Exclude, uptime: 0DT00H00M05S, expires: 0DT00H04M16S
  1/0/5
    version: v3, filter mode: Include, uptime: 0DT00H00M07S, expires: 0DT00H00M00S
      source 192.168.1.1, uptime: 0DT00H00M07S, expires: 0DT00H04M13S

Switch#
```

44.25 show ip igmp snooping filter

Данная команда используется, чтобы отобразить информацию о конфигурации IGMP Snooping Filter для всех интерфейсов или для указанного интерфейса.

show ip igmp snooping filter [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(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.

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
    vlan1:
      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
    vlan1:
      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 eth1/0/2


eth1/0/2
    Rate limit: 10pps
    Access group: Not Configured
    Groups/Channel Limit: Not Configured
    vlan1:
      Access group: Not Configured
      Groups/Channel Limit: 100 (Exception List: ExtendACL, exceed-action: drop)

Switch#
```

44.26 show ip igmp snooping mrouter

Данная команда используется для отображения информации о многоадресном маршрутизаторе IGMP Snooping, который был автоматически изучен и настроен вручную на коммутаторе.

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 одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить 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#
```

44.27 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.

INTERFACE-ID	(Опционально.) Укажите интерфейс, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
vlan	Укажите, чтобы отобразить счетчики статистики VLAN.
VLAN-ID	(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.

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#
```

44.28 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

GROUP-ADDRESS	(Опционально.) Укажите IP-адрес группы, которую необходимо отобразить.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN ID, который необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статически настроенные группы IGMP Snooping на коммутаторе. Если дополнительные параметры не выбраны, будет отображена вся информация.

Пример

В данном примере показано, как отобразить статически настроенные группы IGMP Snooping.

```
Switch#show ip igmp snooping static-group

VLAN ID  Group address    Interface
-------  ---------------  ------------------------
1        230.1.1.1        1/0/1-1/0/2

Total Entries: 1

Switch#
```

45. Команды IP Multicast (IPMC)

45.1 clear ip multicast-statistics

Данная команда используется, чтобы обнулить счетчики статистики пакетов протокола многоадресной рассылки.

clear ip multicast-statistics [igmp] [pim] [dvmrp]

Параметры

igmp	(Опционально.) Укажите, чтобы обнулить счетчик IGMP-пакетов.
pim	(Опционально.) Укажите, чтобы обнулить счетчик PIM-пакетов.
dvmrp	(Опционально.) Укажите, чтобы обнулить счетчик DVMRP-пакетов.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы обнулить счетчик статистики пакетов протокола многоадресной рассылки на коммутаторе. Если не указаны дополнительные параметры, будут обнулены все счетчики статистики пакетов протокола многоадресной рассылки IP.

Пример

В данном примере показано, как обнулить счетчик статистики пакетов протокола многоадресной рассылки.

```
Switch#clear ip multicast-statistics
Switch#
```

45.2 ip multicast table-lookup-mode

Данная команда позволяет настроить режим поиска (lookup mode) перенаправления многоадресной рассылки IP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip multicast table-lookup-mode {ip | mac}
no ip multicast table-lookup-mode

Параметры

ip	Укажите для поиска перенаправления многоадресной рассылки на основе IP-адресов.
mac	Укажите для поиска перенаправления многоадресной рассылки на основе MAC-адресов.

По умолчанию

По умолчанию используется поиск (lookup mode) на основе IP-адресов.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить режим поиска (lookup mode) перенаправления многоадресной рассылки IP.

Пример

В данном примере показано, как настроить режим поиска перенаправления многоадресной рассылки IP на основе MAC.

```
Switch#configure terminal
Switch(config)#ip multicast table-lookup-mode mac
Switch(config)#
```

45.3 ip multicast-routing

Данная команда используется для включения функции IP Multicast Routing. Для отключения IP Multicast Routing воспользуйтесь формой **no** этой команды.

ip multicast-routing
no ip multicast-routing

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если функция IP Multicast Routing выключена, система остановит пакеты multicast routing, даже если протокол Multicast Routing включен.

Пример

В данном примере показано, как включить функцию IP Multicast Routing.

```
Switch#configure terminal
Switch(config)#ip multicast-routing
Switch(config)#
```

45.4 ip multicast boundary

Данная команда используется, чтобы избежать утечки ограниченного трафика multicast через граничные интерфейсы в частном домене. Для удаления границы воспользуйтесь формой **no** этой команды.

ip multicast boundary *ACCESS-LIST* **[in | out]**

no ip multicast boundary *ACCESS-LIST* **[in | out]**

Параметры

ACCESS-LIST	Укажите стандартный список доступа IP, включающий список разрешенных записей *,G или S,G / запрещенных записей *,G или S,G.
in	(Опционально.) Укажите для фильтрации трафика multicast, полученного на интерфейсе на основе указанного списка доступа. Выполняется фильтрация multicast-трафика для определенной группы или групп из указанного источника.
out	(Опционально.) Укажите для фильтрации сообщений о присоединении к PIM или IGMP, полученных на интерфейсе. Данная фильтрация предотвращает превращение интерфейса в исходящий интерфейс для запрещенных записей *,G или S,G.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима, если включен PIM, при этом для каждого направления можно указать только один список доступа. Если не указаны дополнительные параметры, фильтрация по списку доступа применяется как для входящего, так и для исходящего направления.

Пример

В данном примере показано, как настроить VLAN1 в качестве граничного интерфейса для фильтрации трафика на основе списка доступа, StandIPACL.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip multicast boundary StandIPACL
Switch(config-if)#
```

45.5 ip mroute

Данная команда используется для создания статического multicast-маршрута (mroute). Для удаления маршрута воспользуйтесь формой **no** этой команды.

ip mroute *SOURCE-ADDRESS MASK* **{***RPF-ADDRESS* **| null}**
no ip mroute {*SOURCE-ADDRESS MASK* **| all}**

Параметры

SOURCE-ADDRESS	Укажите сетевой адрес multicast-источника.
MASK	Укажите сетевую маску для multicast-источника.
RPF-ADDRESS	Укажите IP-адрес соседнего устройства RPF для достижения сети.
null	Укажите, чтобы проверка RPF никогда не выполнялась для multicast-трафика, отправленного из данной сети источника.
all	Укажите, чтобы удалить все статические IP multicast-маршруты.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

У PIM-протокола нет собственной таблицы маршрутизации, но он использует таблицу индивидуальной маршрутизации, чтобы определить интерфейс перенаправления обратного пути для установки соединения с сетью. Используйте данную команду для настройки статического multicast-маршрута, чтобы указать адрес RPF для сети. Если указан параметр **null**, проверка RPF не будет выполняться для сети источника, указанной командой. Если для маршрута указан адрес RPF, будет выполнен поиск в таблице маршрутизации для преобразования RPF-интерфейса.

Пример

В данном примере показано, как настроить источник данных multicast с сетевым номером 192.168.6.0/24 для доступности с соседнего маршрутизатора 10.1.1.1.

```
Switch#configure terminal
Switch(config)#ip mroute 192.168.6.0 255.255.255.0 10.1.1.1
Switch(config)#
```

В примере ниже показано, как настроить источник данных multicast с сетевым номером 192.168.8.0/24 для отбрасывания.

```
Switch#configure terminal
Switch(config)#ip mroute 192.168.8.0 255.255.255.0 null
Switch(config)#
```

В данном примере показано, как удалить предварительно настроенную запись IP mroute 192.168.8.0/24.

```
Switch#configure terminal
Switch(config)#no ip mroute 192.168.8.0 255.255.255.0
Switch(config)#
```

45.6 cpu-filter l3-control-pkt

Данная команда используется для отбрасывания пакетов управления уровня 3 (Layer 3 control packets), отправленных на ЦПУ с указанных портов. Используйте форму **no**, чтобы остановить отбрасывание пакетов управления уровня 3, отправленных на ЦПУ.

cpu-filter l3-control-pkt type [*PACKET-TYPE***]**

no cpu-filter l3-control-pkt type [*PACKET-TYPE***]**

Параметры

PACKET-TYPE	(Опционально.) Укажите тип управляющего пакета 3 уровня (Layer 3 control packets), который необходимо настроить. Ниже указаны типы поддерживаемых пакетов управления уровня 3: • **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 уровня 3 (Layer 3 control packets), отправленные на ЦПУ с указанных портов.

Пример

В данном примере показано, как отбросить DVMRP-пакеты, отправленные на ЦПУ.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#cpu-filter l3-control-pkt type dvmrp
Switch(config-if)#
```

45.7 show cpu-filter l3-control-pkt

Данная команда используется для отображения статуса фильтрации ЦПУ управляющих пакетов уровня 3 (Layer 3 control packets).

show cpu-filter l3-control-pkt [interface *INTERFACE-ID***]**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейс. Разрешены только интерфейсы физического порта и port-channel. Если интерфейс не указан, будет отображен статус фильтрации ЦПУ управляющих пакетов уровня 3 (Layer 3 control packets) для всех интерфейсов.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения статуса фильтрации ЦПУ управляющих пакетов уровня 3 (Layer 3 control packets).

Пример

В данном примере показано, как отобразить статус фильтрации ЦПУ управляющих пакетов уровня 3.

```
Switch#show cpu-filter l3-control-pkt


eth1/0/2
    Filter packet: DVMRP

Switch#
```

45.8 show ip multicast

Данная команда используется для отображения информации multicast системы или любого IP-интерфейса.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите имя интерфейса, для которого необходимо отобразить информацию об IP multicast.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения информации об интерфейсе IP multicast. Если параметр **interface** не указан, будет отображен общий статус IP multicast routing. Если параметр **interface** указан, но нет параметра *INTERFACE-ID*, будет отображена информация по всем интерфейсам.

Пример

В данном примере показано, как отобразить общий статус IP multicast routing и режим поиска (lookup mode) перенаправления IP multicasting.

```
Switch#show ip multicast

IP multicast-routing global state: Enabled
Table lookup mode: IP

Switch#
```

В данном примере показано, как отобразить информацию об интерфейсе IP multicast.

```
Switch#show ip multicast interface

vlan2
  Internet address is 192.168.2.109/24
  Multicast routing: enabled, PIM Sparse mode
  Multicast boundary: not set

vlan3
  Internet address is 192.168.3.109/24
  Multicast routing: enabled, PIM Sparse mode
  Multicast boundary: not set

vlan4
  Internet address is 192.168.4.109/24
  Multicast routing: enabled, PIM Sparse mode
  Multicast boundary: not set


Total Entries: 3

Switch#
```

45.9 show ip mroute

Данная команда используется, чтобы отобразить содержимое таблицы IP multicast routing.

show ip mroute [{[*GROUP-ADDRESS*** [***SOURCE-ADDRESS***] | dense | sparse | dvmrp] | summary | static}]**

Параметры

GROUP-ADDRESS	(Опционально.) Укажите IP-адрес группы.
SOURCE-ADDRESS	Укажите IP-адрес multicast-источника.
summary	(Опционально.) Укажите, чтобы отобразить краткую однострочную информацию для каждой записи в таблице IP multicast routing.
sparse	(Опционально.) Укажите, чтобы отобразить только маршруты PIM-SM.
dense	(Опционально.) Укажите, чтобы отобразить только маршруты PIM-DM.
dvmrp	(Опционально.) Укажите, чтобы отобразить только маршруты DVMRP.
static	(Опционально.) Укажите для отображения только статических multicast-маршрутов.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить содержимое таблицы IP multicast. Таймер безотказной работы «Uptime» содержит время создания записи. Таймер истечения срока действия «Expire» – это таймер активности потока данных групповой рассылки. Значение таймера истечения срока действия основано на PIM Sparse или Dense Mode. Если данные multicast продолжают поступать на устройство, таймер будет обновлен. Если указан сетевой адрес, коммутатор отображает записи с адресами источника, которые соответствуют указанному адресу.

Пример

В данном примере показано, как отобразить краткую информацию о multicast-маршруте.

```
Switch#show ip mroute summary

IP Multicast Routing Table: 2 entries
Flags: D - PIM-DM, S - PIM-SM, V - DVMRP
Timers: Uptime/Expires

(10.10.1.52, 224.0.1.3), vlan1, 0DT00H01M32S/0DT00H03M20S, Flags: D
(20.1.1.1, 228.10.2.1), vlan10, 0DT00H05M10S/0DT00H03M11S, Flags: S

Switch#
```

В данном примере показано, как отобразить записи multicast-маршрутов.

```
Switch#show ip mroute

IP Multicast Routing Table
Flags: D - PIM-DM, S - PIM-SM, V - DVMRP, s - SSM Group, F - Register flag
       P - Pruned, R - (S, G) RPT-bit set, T - SPT-bit set
Outgoing interface flags: W - Assert winner
 Timers: Uptime/Expires

(10.10.1.52, 224.0.1.3), 0DT05H29M15S/0DT00H02M59S, flags: ST
    Incoming interface: vlan1, RPF neighbor: 10.3.4.5
    Outgoing interface list:
      vlan121, Forwarding 0DT00H01M23S/0DT00H03M34S
      vlan125, Forwarding 0DT00H01M23S/null

(20.1.1.1, 228.0.0.20), 0DT05H29M15S/0DT00H02M59S  flags: D
    Incoming interface: vlan10, RPF neighbor: 10.3.4.5
    Outgoing interface list: NULL

Total Entries: 2

Switch#
```

В данном примере показано, как отобразить запись multicast-маршрута в режиме sparse.

```
Switch#show ip mroute sparse

(10.10.1.52, 224.0.1.3), 0DT05H29M15S/0DT00H02M59S, flags: ST
    Incoming interface: vlan1, RPF neighbor: 10.3.4.5
    Outgoing interface list:
      vlan126, Forwarding 0DT00H00M03S/0DT00H04M07S
      vlan127, Forwarding 0DT00H00M03S/0DT00H04M11S

Total Entries: 1

Switch#
```

В данном примере показано, как отобразить статический настроенный multicast-маршрут.

```
Switch#show ip mroute static

Mroute: 192.168.6.0/24, RPF neighbor: 10.1.1.1
Mroute: 192.168.8.0/24, RPF neighbor: NULL

 Total Entries   : 2

Switch#
```

45.10 show ip mroute forwarding-cache

Данная команда позволяет отобразить содержимое базы данных кэша перенаправления IP multicast routing.

show ip mroute forwarding-cache [group-addr *GROUP-ADDRESS* **[source-addr** *SOURCE-ADDRESS***]]**

Параметры

group-addr *GROUP-ADDRESS*	(Опционально.) Укажите IP-адрес группы.
source-addr *SOURCE-ADDRESS*	(Опционально.) Укажите IP-адрес multicast-источника.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда позволяет отобразить содержимое кэша перенаправления IP multicast. Кэш перенаправления IP multicast представляет собой сводную таблицу на основе таблицы маршрутизации IP multicast, таблицы участников группы IGMP snooping и multicast router-портов.

Пример

В данном примере показано, как отобразить содержимое кэша перенаправления IP multicast routing.

```
Switch#show ip mroute forwarding-cache

(10.1.1.1, 239.0.0.0) VLAN0060
  Outgoing interface list: 1/0/1, port-channel2

(*,225.0.0.0) VLAN0070
Outgoing interface list: 1/0/1-1/0/2

(10.1.1.1, 239.0.0.1) VLAN0060
  Outgoing interface list: 1/0/1, 2/0/2

Total entries: 3

Switch#
```

45.11 show ip rpf

Данная команда используется, чтобы проверить информацию об RPF (Reverse Path Forwarding) для указанного адреса unicast-узла.

show ip rpf *IP-ADDRESS*

Параметры

IP-ADDRESS	Укажите IP-адрес, которй необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить, как IP multicast routing выполняет RPF. Так как маршрутизатор может найти информацию об RPF в нескольких таблицах маршрутизации (например, таблице unicast routing или таблице статических multicast-маршрутов), при помощи команды **show ip rpf** можно отобразить источник, из которого получена информация.

Пример

В данном примере показано, как отобразить информацию об RPF для unicast-узла с IP-адресом 20.1.1.3.

```
Switch#show ip rpf 20.1.1.3

RPF information for 20.1.1.3
RPF interface: vlan11
RPF type: unicast
Metric: 10

Switch#
```

В данном примере показано, как отобразить информацию об RPF для unicast-узла с IP-адресом 1.3.3.3.

```
Switch#show ip rpf 1.3.3.3

RPF information for 1.3.3.3
RPF neighbor: 2.1.5.1
RPF type: static

Switch#
```

В данном примере показано, как отобразить информацию об RPF для unicast-узла с IP-адресом 3.2.2.2.

```
Switch#show ip rpf 3.2.2.2

RPF information for 3.2.2.2
RPF interface: NULL
RPF type: static

Switch#
```

Отображаемые параметры

RPF neighbor	IP-адрес upstream-маршрутизатора для источника. Если нет соседнего устройства, данное поле является опциональным.
RPF type	**unicast** – информация об RPF, полученная из таблицы unicast routing. **static** – информация об RPF, полученная из статического multicast-маршрута.
Metric	Указывает метрику unicast routing. Если метрики не существует, поле является опциональным.

45.12 show ip multicast-statistics

Данная команда позволяет отобразить счетчики статистики полученных и отправленных multicast-пакетов.

show ip multicast-statistics [igmp] [pim] [dvmrp] [interface [*INTERFACE-ID*]]

Параметры

INTERFACE-ID	(Опционально.) Укажите имя интерфейса, для которого необходимо отобразить счетчик статистики IP multicast.
igmp	(Опционально.) Укажите, чтобы отобразить счетчик полученных и отправленных IGMP-пакетов.
pim	(Опционально.) Укажите, чтобы отобразить счетчик полученных и отправленных PIM-пакетов.
dvmrp	(Опционально.) Укажите, чтобы отобразить счетчик полученных и отправленных DVMRP-пакетов.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения счетчиков полученных и отправленных пакетов протокола многоадресной рассылки на коммутаторе в соответствии с типом сообщения.

Пример

В данном примере показано, как отобразить счетчик пакетов протокола многоадресной рассылки на коммутаторе.

```
Switch#show ip multicast-statistics

IGMP Packets Counter
                          Received          Sent
    IGMP Query v1/v2/v3     0/0/0           0/0/0
    IGMP Report v1/v2/v3    0/0/0           0/0/0
    IGMP Leave                0               0
    Unknown IGMP              0               0

PIM Packets Counter
                        Received      Sent
    PIM Hello             0               0
    PIM Register          0               0
    PIM Register-Stop     0               0
    PIM Join/Prune        0               0
    PIM Bootstrap         0               0
    PIM Assert            0               0
    PIM Graft             0               0
    PIM Graft-Ack         0               0
    PIM C-RP-Adv          0               0
    PIM State Refresh     0               0
    Unknown PIM           0               0

DVMRP Packets Counter
                        Received      Sent
    DVMRP Probe           0               0
    DVMRP Report          0               0
    DVMRP Prune           0               0
    DVMRP Graft           0               0
    DVMRP Graft-Ack       0               0
    Unknown DVMRP         0               0

Switch#
```

46. Команды IP Multicast Version 6 (IPMCv6)

46.1 ipv6 multicast-routing

Данная команда используется для включения функции IPv6 Multicast Routing. Для отключения IPv6 Multicast Routing воспользуйтесь формой **no** этой команды.

ipv6 multicast-routing
no ipv6 multicast-routing

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если функция IPv6 Multicast Routing выключена, система остановит пакеты multicast routing, даже если протокол Multicast Routing включен.

Пример

В данном примере показано, как включить функцию IPv6 Multicast Routing.

```
Switch#configure terminal
Switch(Config)#ipv6 multicast-routing
Switch(Config)#
```

46.2 show ipv6 multicast

Данная команда используется, чтобы отобразить основную информацию multicast для IPv6-интерфейса.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите имя интерфейса, для которого необходимо отобразить информацию об IPv6 multicast. Если не указан interface ID, будут отображены все интерфейсы. Если не указан параметр **interface**, будет отображен статус IPv6 multicast routing.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить основную информацию multicast для IPv6-интерфейса или статус IPv6 multicast routing. Если interface ID не указан, будет отображена информация для всех IPv6-интерфейсов.

Пример

В данном примере показано, как отобразить статус IPv6 multicast routing.

```
Switch#show ipv6 multicast

IPv6 multicast-routing global state: Enabled

Switch#
```

В данном примере показано, как отобразить информацию об интерфейсе IPv6 multicast.

```
Switch#show ipv6 multicast interface

Interface     Owner Module
------------  ---------------
vlan100       PIM-SM
vlan200       PIM-SM

Total Entries: 2

Switch#
```

Отображение параметров

Interface	Имя интерфейса.

Owner Module	Указывает, включен ли модуль на интерфейсе. **PIM-SM**: на интерфейсе включен режим PIM Sparse Mode. **PIM-DM**: на интерфейсе включен режим PIM Dense Mode.

46.3 show ipv6 mroute

Данная команда используется, чтобы отобразить содержимое таблицы IPv6 dynamic multicast routing.

show ipv6 mroute [*GROUP-ADDRESS* **[***SOURCE-ADDRESS***] | dense | sparse | summary]**

Параметры

GROUP-ADDRESS	(Опционально.) Укажите IPv6-адрес группы.
SOURCE-ADDRESS	(Опционально.) Укажите IPv6-адрес multicast-источника.
dense	(Опционально.) Укажите, чтобы отобразить только маршруты PIM-DM.
sparse	(Опционально.) Укажите, чтобы отобразить только маршруты PIM-SM.
summary	(Опционально.) Укажите, чтобы отобразить краткую однострочную информацию для каждой записи в таблице IPv6 multicast routing.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить содержимое таблицы IPv6 multicast. Таймер безотказной работы «Uptime» содержит время создания записи. Таймер истечения срока действия «Expire» – это таймер активности потока данных групповой рассылки. Если данные multicast продолжают поступать на устройство, таймер будет обновлен. Если указан сетевой адрес, коммутатор отображает записи с адресами источника, которые соответствуют указанному адресу. Если не указаны дополнительные параметры, будут отображены все динамические multicast-маршруты.

Пример

В данном примере показано, как отобразить краткую информацию о multicast-маршруте.

```
Switch#show ipv6 mroute summary

IPv6 Multicast Routing Table: 3 entries
Flags: S - Sparse, D - Dense, s - SSM Group
Timers: Uptime/Expires

(2000::1010:134, FF07::1), vlan1, 0DT00H01M32S/0DT00H03M20S, Flags: S
(2000::2001:101, FF06::100), vlan10, 0DT00H05M10S/0DT00H03M11S, Flags: S
(2000::5001:101, FF1E::100), vlan100, 0DT00H04M10S/0DT00H04M11S, Flags: D

Switch#
```

В данном примере показано, как отобразить записи multicast-маршрутов.

```
Switch#show ipv6 mroute

IPv6 Multicast Routing Table - 3 entries
Flags: S - Sparse, D - Dense, s - SSM Group
Timers: Uptime/Expires

(2000::1010:134, FF07::1), 0DT05H29M15S/0DT00H02M59S, Flags: S
    Incoming interface: vlan1
    RPF nbr: 2000::103:405
    Outgoing interface list:
      vlan2
      vlan3

(2000::2001:101, FF06::20), 0DT05H29M15S/0DT00H02M59S  Flags: S
    Incoming interface: vlan10
    RPF nbr: 2000::1003:405
    Outgoing interface list:
      vlan20

(2000::5001:101, FF1E::100), 0DT00H04M10S/0DT00H04M11S, Flags: D
    Incoming interface: vlan100
    RPF nbr: -
    Outgoing interface list:
      vlan200

Switch#
```

Отображаемые параметры

Flags	Предоставление информации о записи. S – Sparse. Запись функционирует в режиме Sparse. D – Dense. Запись функционирует в режиме Dense. s – SSM Group. Запись представляет собой группу SSM.

Timers: Uptime/Expires	Таймер «Uptime» указывает период (в днях, часах, минутах, секундах) существования записи в таблице IPv6 multicast routing. Информация выводится для интерфейса. Таймер «Expires» указывает период (в днях, часах, минутах, секундах), по истечении которого запись будет удалена из таблицы IPv6 multicast routing. Информация выводится для интерфейса.
Incoming interface	Интерфейс для multicast-пакета от источника. Если пакет не получен на интерфейсе, он будет отброшен.
RPF nbr	IPv6-адрес upstream маршрутизатора для RP или источника.
Outgoing interface	Интерфейс, через который будут перенаправлены пакеты. Для записей (S,G) список не будет включать интерфейсы, полученные от записи (*,G).

46.4 show ipv6 mroute forwarding-cache

Данная команда позволяет отобразить содержимое базы данных кэша перенаправления IPv6 multicast routing.

show ipv6 mroute forwarding-cache [group-addr *GROUP-ADDRESS* **[source-addr** *SOURCE-ADDRESS***]]**

Параметры

group-addr *GROUP-ADDRESS*	(Опционально.) Укажите IPv6-адрес группы.
source-addr *SOURCE-ADDRESS*	Укажите IPv6-адрес multicast-источника.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить содержимое кэша перенаправления IPv6 multicast. Кэш перенаправления IPv6 multicast представляет собой сводную таблицу на основе таблицы маршрутизации IPv6 multicast, таблицы участников группы MLD Snooping и multicast router-портов.

Пример

В данном примере показано, как отобразить содержимое кэша перенаправления IPv6 multicast routing.

```
Switch#show ipv6 mroute forwarding-cache

(2000:60:1:1::10, FF0E::1:1:1) VLAN0060
  Outgoing interface list: 1/0/1, port-channel2

(2000:60:1:1::10, FF0E::1:1:2) VLAN0060
  Outgoing interface list: 1/0/1, 2/0/2

Total entries: 2

Switch#
```

46.5 show ipv6 rpf

Данная команда используется, чтобы проверить информацию об RPF (Reverse Path Forwarding) для указанного адреса unicast-узла.

show ipv6 rpf *IPV6-ADDRESS*

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес, который необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить, как IPv6 multicast routing выполняет RPF. Так как маршрутизатор может найти информацию об RPF в нескольких таблицах маршрутизации (например, таблице unicast routing или таблице статических multicast-маршрутов), при помощи команды **show ipv6 rpf** можно отобразить источник, из которого получена информация.

Пример

В данном примере показано, как отобразить информацию об RPF для unicast-узла с IPv6-адресом 2001::1:1:3.

```
Switch#show ipv6 rpf 2001::1:1:3

RPF information for 2001::1:1:3
RPF interface: vlan11
RPF neighbor: FE80::40:1:3
RPF route/mask: 2001::/64
RPF type: unicast
Metric: 2

Switch#
```

Отображаемые параметры

RPF neighbor	IPv6-адрес upstream-маршрутизатора для RP или источника. Если нет соседнего устройства, данное поле является опциональным.
RPF type	**unicast** – информация об RPF, полученная из таблицы unicast routing.
Metric	Указывает метрику unicast routing. Если метрики не существует, поле является опциональным.

47. Команды IP Source Guard

47.1 ip verify source vlan dhcp-snooping

Данная команда используется для включения на порту функции защиты IP-адреса – IP Source Guard. Для отключения IP Source Guard воспользуйтесь формой **no** этой команды.

ip verify source vlan dhcp-snooping [ip-mac]

no ip verify source vlan dhcp-snooping [ip-mac]

Параметры

ip-mac	(Опционально.) Укажите для проверки IP- и MAC-адреса получаемых IP-пакетов.

По умолчанию

По умолчанию 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 команду для включения IP Source Guard на необходимом порту.

При включении на порту IP Source Guard IP-пакеты, приходящие на порт, будут проверяться списком управления доступом (ACL). Порт ACL – аппаратный механизм, записи которого могут быть настроены вручную либо получены с помощью таблицы DHCP. Пакет, не прошедший проверку, будет отброшен.

Если для VLAN включена функция IP Source Guard, IP-пакеты, приходящие на указанный порт, будут проверяться. Это поможет узлам, принадлежащим группе IP Inspection, перемещаться между указанными портами домена VLAN.

Существует два типа проверки:

- Если **ip-mac** не указан, проверка основана только на IP-адресе источника и VLAN.
- Если **ip-mac** указан, проверка основана на MAC-адресе источника, VLAN и IP-адресе источника.

Пример

В данном примере показано, как включить IP Source Guard для интерфейса Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip verify source vlan dhcp-snooping
Switch(config-if)#
```

47.2 ip source binding

Данная команда используется для создания статической записи для IP Source Guard. Для удаления статической записи привязки воспользуйтесь формой **no** этой команды.

ip source binding *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**
no ip source binding *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

Параметры

MAC-ADDRESS	Укажите MAC-адрес для привязки IP-to-MAC.
vlan *VLAN-ID*	Укажите VLAN, которой принадлежит проверенный узел.
IP-ADRESS	Укажите IP-адрес для привязки IP-to-MAC.
interface *INTERFACE-ID*	Укажите порт, к которому подключен проверенный узел.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

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** данной команды статическая привязка будет удалена. Указанные параметры команды должны в точности совпадать с настроенными параметрами для удаления.

Если MAC-адрес и VLAN настраиваемой привязки уже есть, существующая привязка будет обновлена. Интерфейсом, указанным для команды, может быть физический порт или port-channel.

Пример

В данном примере показано, как настроить привязку IP Source Guard с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 на интерфейсе Ethernet 1/0/10.

```
Switch#configure terminal
Switch(config)#ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10
Switch(config)#
```

В данном примере показано, как удалить привязку IP Source Guard с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 на интерфейсе Ethernet 1/0/10.

```
Switch#configure terminal
Switch(config)#no ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10
Switch(config)#
```

47.3 show ip source binding

Данная команда используется для отображения привязки IP Source Guard.

show ip source binding [*IP-ADDRESS***] [***MAC-ADDRESS***] [dhcp-snooping | static] [vlan** *VLAN-ID***]**

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

Параметры

IP-ADDRESS	(Опционально.) Укажите для отображения привязки IP Source Guard на основе IP-адреса.
MAC-ADDRESS	(Опционально.) Укажите для отображения привязки IP Source Guard на основе MAC-адреса.
dhcp-snooping	(Опционально.) Укажите для отображения привязки IP Source, изученной при помощи DHCP Snooping.
static	(Опционально.) Укажите для отображения привязки IP Source Guard, настроенной вручную.
vlan *VLAN-ID*	(Опционально.) Укажите для отображения привязки IP Source Guard на основе VLAN.
interface *INTERFACE-ID*	(Опционально.) Укажите для отображения привязки IP Source Guard на основе порта.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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 отобразить все записи привязки привязки IP Source Guard.

```
Switch#show ip source binding

MAC Address       IP Address      Lease(sec)  Type         VLAN Interface
----------------- --------------- ---------- ------------- ---- ---------
00-01-01-01-01-01 10.1.1.10        infinite  static        100  eth1/0/3
00-01-01-01-01-10 10.1.1.11          3120    dhcp-snooping 100  eth1/0/3

Total Entries: 2

Switch#
```

В данном примере показано, как настроить отображение привязки IP Source Guard для IP-адреса 10.1.1.10.

```
Switch#show ip source binding 10.1.1.10

MAC Address       IP Address      Lease(sec)  Type         VLAN   Interface
----------------- --------------- ---------- ------------- ----- ----------
00-01-01-01-01-01 10.1.1.10        infinite  static        100    eth1/0/3

Total Entries: 1

Switch#
```

В данном примере показано, как настроить отображение привязки IP Source Guard на основе IP-адреса 10.1.1.11 и MAC-адреса 00-01-01-01-01-10 на VLAN 100 для интерфейса Ethernet 1/0/3, а также задать изучение DHCP Snooping.

```
Switch#show ip source binding 10.1.1.10 00-01-01-01-01-10 dhcp-snooping vlan 100 interface
eth1/0/3

MAC Address       IP Address      Lease(sec)  Type          VLAN   Interface
----------------- --------------- ---------- ------------- ----- -----------
00-01-01-01-01-10 10.1.1.11          3564    dhcp-snooping 100    eth1/0/3

Total Entries: 1

Switch#
```

Отображаемые параметры

MAC Address	MAC-адрес клиента.
IP Address	IP-адрес клиента, назначенный DHCP-сервером или настроенный пользователем.
Lease (sec)	Время аренды IP-адреса.
Type	Тип привязки. Статическая привязка настраивается вручную. Динамическая привязка изучается с помощью DHCP Snooping.
VLAN	Номер VLAN, где находится интерфейс клиента.
Interface	Интерфейс, подключаемый к узлу DHCP-клиента.

47.4 show ip verify source

Данная команда используется для отображения записи списка управления доступом (ACL) аппаратного порта на определенном интерфейсе.

show ip verify source [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите порт или диапазон портов для настройки.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения записей в аппаратной таблице ACL.

Пример

В данном примере показано, как отобразить запись, если на VLAN 100 – VLAN 110 включен DHCP Snooping, на интерфейсе активирован режим IP Source Filter Mode, настроенный как IP, а текущая привязка произведена на основе IP-адреса 10.1.1.1 на VLAN 100.

```
Switch#show ip verify source interface eth1/0/3

Interface       Filter-type Filter-mode IP address      MAC address       VLAN
---------       ----------- ----------- --------------- ----------------- ----
eth1/0/3        ip          active      10.1.1.1        -                 100
eth1/0/3        ip          active      deny-all        -                 101-120

Total Entries: 2

Switch#
```

В данном примере показано, как отобразить запись, если интерфейс в режиме IP Source Filter Mode настроен как IP MAC, и существует привязка IP-адреса 10.1.1.10 к MAC-адресу 00-01-01-01-01-01 в VLAN 100, а также IP-адреса 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.

48. Команды IP Utility

48.1 ping

Данная команда используется для диагностики базового сетевого соединения.

ping {[ip] *IP-ADDRESS* **| [ipv6]** *IPV6-ADDRESS* **|** *HOST-NAME***} [count** *TIMES***] [timeout** *SECONDS***]**

[source {*IP-ADDRESS* **|** *IPV6-ADDRESS***}]**

Параметры

ip	(Опционально.) Укажите, чтобы использовать IPv4-адрес.
IP-ADDRESS	Укажите IPv4-адрес узла назначения (destination).
ipv6	(Опционально.) Укажите, чтобы использовать IPv6-адрес.
IPV6-ADDRESS	Укажите IPv6-адрес системы, который необходимо обнаружить. Если это адрес link-local или multicast, название IP-интерфейса необходимо указать в следующем формате: *IPV6-ADDRESS %INTERFACE-ID*.
HOST-NAME	Укажите имя узла системы для обнаружения.
count *TIMES*	(Опционально.) Укажите, чтобы завершить процесс после отправки указанного количества пакетов echo request.
timeout *SECONDS*	(Опционально.) Укажите время ожидания ответа в секундах.
source {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**	(Опционально.) Укажите IP-адрес источника (source), используемый для пакетов команды **ping**. Указанный IP-адрес должен быть одним из IP-адресов, сконфигурированных для коммутатора. У IP-адреса назначения и IP-адреса источника должен быть один тип – IPv4 или IPv6.

По умолчанию

Параметр **count** отключен. Проверка 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. Чтобы прервать ping принудительно, используйте сочетание клавиш CTRL+C. Максимальное количество активных сессий ping – 5.

Пример

В данном примере показано, как проверить 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 проверить 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#
```

48.2 ping access-class

Данная команда используется для указания списка доступа, который ограничит доступ для ping. Для удаления проверки при помощи списка доступа воспользуйтесь формой **no** этой команды.

ping access-class *IP-ACL*

no ping access-class *IP-ACL*

Параметры

IP-ACL	Укажите стандартный список доступа IP. Поле адреса источника (source) разрешающей или запрещающей записи определяет, действителен узел, или нет.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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 доступ для ping. Проверять коммутатор разрешено только узлу 10.1.1.1.

```
Switch#configure terminal
Switch(config)#ip access-list ping-filter
Switch(config-ip-acl)#permit 10.1.1.1 0.0.0.0
Switch(config-ip-acl)#exit
Switch(config)#ping access-class ping-filter
Switch(config)#
```

48.3 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***} [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 датаграмм, 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-датаграмм. Максимальный доступный диапазон значений: от 1 до 255.

port *DEST-PORT*	(Опционально.) Укажите количество базовых UDP-портов назначения, используемых в исходящих датаграммах. Значение увеличивается при отправке каждой датаграммы. 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

Значение **probe** (количество запросов для каждого TTL) – 1.
Значение **timeout** – 5 секунд.
Максимальное значение TTL – 30.
Номер UDP-порта назначения – 33434.

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. Максимальное количество активных сессий traceroute – 3.

Данная команда использует поле TTL в IP-заголовке, чтобы маршрутизаторы и серверы могли генерировать определенные ответные сообщения (return messages). **Traceroute** запускается при отправке UDP-датаграммы на узел назначения с полем TTL 1. Если маршрутизатор обнаруживает значение TTL 1 или 0, датаграмма будет отброшена, а отправителю будет выслано ответное сообщение об истечении времени ответа (ICMP time exceeded). **Traceroute** определяет адрес первого узла при проверке поля адреса источника (source) сообщения ICMP time exceeded.

Чтобы идентифицировать следующий узел, **traceroute** снова отправляет UDP-пакет, но в этот раз значение TTL равно 2. Первый маршрутизатор уменьшает поле TTL на 1 и отправляет датаграмму на следующий маршрутизатор. Обнаружив TTL со значением 1, второй маршрутизатор отбрасывает датаграмму и отправляет на источник сообщение time exceeded. Этот процесс продолжается до тех пор, пока значение TTL не увеличится настолько, чтобы датаграмма могла достичь узла назначения (или до тех пор, пока не будет достигнуто максимальное значение TTL).

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

Пример

В данном примере показано, как выполнить трассировку маршрута к узлу 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 max-ttl 2

  *      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

Trace complete.


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#
```

48.4 ip helper-address

Данная команда используется, чтобы добавить адрес назначения для передачи пакетов UDP broadcast. Для удаления адреса назначения передачи воспользуйтесь формой **no** этой команды.

ip helper-address *IP-ADDRESS*
no ip helper-address [*IP-ADDRESS***]**

Параметры

IP-ADDRESS	Укажите IP-адрес назначения для передачи пакетов UDP broadcast.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для конфигурирования интерфейса VLAN. Используйте данную команду, чтобы контролировать передачу пакетов UDP broadcast. Команда действует только в том случае, если полученному интерфейсу присвоен IP-адрес.

Система передает только те пакеты, которые соответствуют следующим требованиям:

- MAC-адрес назначения (destination) должен быть широковещательным адресом.
- IP-адрес назначения должен быть широковещательным адресом.
- Тип пакетов – IPv4 UDP.
- Значение IP TTL должно быть больше или равно 2.

Пример

В данном примере показано, как сконфигурировать адрес IP Helper для VLAN 100. Указанный адрес – 172.50.71.123.

```
Switch#configure terminal
Switch(config)#interface vlan 100
Switch(config-if)#ip helper-address 172.50.71.123
Switch(config-if)#
```

48.5 ip forward-protocol

Данная команда используется для включения передачи пакетов UDP определенного типа службы. Для отключения передачи пакетов UDP определенного типа службы воспользуйтесь формой **no** этой команды.

ip forward-protocol udp [*PORT***]**

no ip forward-protocol udp [*PORT***]**

Параметры

PORT	(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 **no** данной команды сконфигурирована без указания номера порта, будут применены порты по умолчанию. Порт 67 и порт 68 BOOTP UDP указать нельзя, так как пакеты передаются при помощи DHCP Relay. Ниже перечислены порты по умолчанию:

- Порт 69 Trivial File Transfer Protocol (TFTP).
- Порт 53 Domain Naming System (DNS).
- Порт 37 Time Service.
- Порт 137 NetBIOS Name Server.
- Порт 138 NetBIOS Datagram Server.
- Порт 49 TACACS service.
- Порт 42 IEN-116 Name Service.

Пример

В 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)#
```

48.6 show ip helper-address

Данная команда используется для отображения таблицы адресов UDP Helper.

show ip helper-address [*INTERFACE-ID***]**

Параметры

INTERFACE-ID	(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.

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
----------  ---------------
vlan100     172.50.71.123

Switch#
```

48.7 show ip forward-protocol udp

Данная команда используется для отображения информации обо всех указанных UDP-портах.

show ip forward-protocol udp

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию обо всех указанных UDP-портах.

Пример

В данном примере показано, как отобразить информацию обо всех указанных UDP-портах.

```
Switch#show ip forward-protocol udp

Application                 UDP Port
--------------------        ---------------
Time Service                37
IEN-116 Name Service        42
TACACS                      49
TFTP                        69
NetBIOS-NS                  137
NetBIOS-DS                  138

Switch#
```

49. Команды IP-MAC-Port Binding (IMPB)

49.1 clear ip ip-mac-port-binding violation

Данная команда используется для удаления заблокированных записей IP-MAC-Port Binding (IMPB).

clear ip ip-mac-port-binding violation {all | interface *INTERFACE-ID* **|** *MAC-ADDRESS***}**

Параметры

all	Укажите для удаления всех неразрешенных записей.
interface *INTERFACE-ID*	Укажите для удаления неразрешенных записей, созданных определенным интерфейсом.
MAC-ADDRESS	Укажите для удаления неразрешенных записей с определенным MAC-адресом.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда используется для удаления неразрешенных записей IMPB из базы данных фильтрации.

Пример

В данном примере показано, как удалить заблокированную запись на интерфейсе Ethernet 1/0/4.

```
Switch#clear ip ip-mac-port-binding violation interface eth1/0/4
Switch#
```

49.2 ip ip-mac-port-binding

Данная команда используется для включения управления доступом IMPB для интерфейсов порта. Для отключения функции управления доступом IMPB воспользуйтесь формой **no** этой команды.

ip ip-mac-port-binding [*MODE***]**
no ip ip-mac-port-binding

Параметры

MODE	Укажите режим управления доступом IMPB. **strict-mode:** укажите для включения 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 интерфейсе Ethernet 1/0/10.

```
Switch#configure terminal
Switch(config)#interface eth1/0/10
Switch(config-if)#ip ip-mac-port-binding strict
Switch(config-if)#
```

49.3 show ip ip-mac-port-binding

Данная команда используется для отображения настроек IMPB или записей, заблокированных с помощью управления доступом IMPB.

show ip ip-mac-port-binding [interface *INTERFACE-ID* **[, | -]] [violation]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите для отображения определенного интерфейса.
,	(Опционально.) 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.
violation	(Опционально.) Укажите для отображения заблокированной записи.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте команду **show ip ip-mac-port-binding** для отображения настроек IMPB. Используйте команду **show ip ip-mac-port-binding violation** для отображения записей, заблокированных из-за нарушения проверки IMPB.

Пример

В данном примере показано, как включить отображение всех заблокированных записей управления доступом IMPB.

```
Switch#show ip ip-mac-port-binding violation

Port       VLAN      MAC Address
------- --------- -------------------
eth1/0/3      1       01-00-0c-cc-cc-cc
eth1/0/3      1       01-80-c2-00-00-00
eth1/0/4      1       01-00-0c-cc-cc-cd
eth1/0/4      1       01-80-c2-00-00-01

Total Entries: 4

Switch#
```

В данном примере показано, как включить отображение настроек IMPB для всех портов.

```
Switch#show ip ip-mac-port-binding

Port           Mode
---------- ------------
eth1/0/1       Strict
eth1/0/2       Strict
eth1/0/3       Loose
eth1/0/4       Loose

Total Entries: 4

Switch#
```

49.4 snmp-server enable traps ip-mac-port-binding

Данная команда используется, чтобы включить уведомления SNMP для привязки IP-MAC-Port Binding. Для отключения уведомлений SNMP воспользуйтесь формой **no** этой команды.

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 trap-сообщения при нарушениях безопасности, если будет получен некорректный пакет. Используйте эту команду для включения или отключения отправки SNMP-уведомлений для таких событий.

Пример

В данном примере показано, как включить отправку trap-сообщений для IP-MAC-Port Binding.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps ip-mac-port-binding
Switch(config)#
```

50. Команды IPv6 Snooping

50.1 ipv6 snooping policy

Данная команда используется для создания или изменения политики IPv6 Snooping. Команда позволяет войти в режим IPv6 Snooping Configuration Mode. Для удаления политики IPv6 Snooping воспользуйтесь формой **no** этой команды.

ipv6 snooping policy *POLICY-NAME*
no ipv6 snooping policy *POLICY-NAME*

Параметры

POLICY-NAME	Укажите имя политики IPv6 Snooping.

По умолчанию

По умолчанию ни одной политики IPv6 Snooping не создано.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для создания политики IPv6 Snooping 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)#
```

50.2 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 | dhcp-pd-ext}
no protocol {dhcp | ndp | dhcp-pd | dhcp-pd-ext}

Параметры

dhcp	Укажите для отслеживания адресов DHCPv6-пакетов.
ndp	Укажите для отслеживания адресов NDP-пакетов.
dhcp-pd	Укажите для отслеживания префикса IPv6 в пакетах DHCPv6 PD.
dhcp-pd-ext	Укажите для отслеживания префикса IPv6 в пакетах DHCPv6 PD. Отслеживание в PD-пакетах осуществляется в режиме extension mode.

По умолчанию

По умолчанию все протоколы отключены.

Режим ввода команды

IPv6 Snooping Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Функция Neighbor Discovery (ND) Snooping используется для IPv6-адресов, настроенных вручную или созданных с помощью механизма автоконфигурации Stateless Autoconfiguration. Перед назначением IPv6-адреса узел должен сначала выполнить обнаружение Duplicate Address Detection (DAD), позволяющее определить дублирование адресов узлов локальной сети. ND Snooping обнаруживает сообщения DAD, включающие DAD Neighbor Solicitation (NS) и DAD Neighbor Advertisement (NA), для построения таблицы привязок. NDP-пакет (NS и NA) также используется, чтобы определить, доступен ли узел по-прежнему и можно ли удалить привязку.

DHCPv6 Snooping анализирует DHCPv6-пакеты, отправляемые между DHCPv6-клиентом и сервером во время процедуры назначения адреса. Когда DHCPv6-клиент успешно получает действительный IPv6-адрес, DHCPv6 Snooping создает свою таблицу привязок.

DHCP-PD Snooping анализирует пакеты DHCPv6 Prefix Delegation (PD) между Delegating Router (назначенным IPv6-префиксом) и соответствующим Requesting Router для настройки привязки префикса.

Ниже описаны режимы, которые поддерживаются PD Snooping.

Standard Mode (стандартный режим): DHCPv6-пакеты Request/Confirm (с Reply) запускают PD Snooping, чтобы создать новую запись привязки. DHCPv6-пакеты Renew (с Reply) запускают PD Snooping, чтобы указать для существующей записи привязки новое время аренды.

Extension Mode (расширенный режим): DHCPv6-пакеты Request/Confirm Renew/Rebind (с Reply) запускают PD Snooping, чтобы создать новую запись привязки. DHCPv6-пакеты Renew (с Reply) запускают PD Snooping, чтобы указать для существующей записи привязки новое время аренды.

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)#
```

50.3 data-glean

Данная команда используется для включения функции Data Glean. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

data-glean
no data-glean

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

IPv6 Snooping Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если коммутатор теряет корректный адрес некоторых устройств в таблице привязок, трафик этих устройств отклоняется при помощи IPv6 Source Guard. Функция Data Glean позволяет коммутатору восстановить потерянные IPv6-адреса с помощью IPv6 Duplicate Address Detection (DAD).

Пример

В данном примере показано, как включить функцию Data Glean.

```
Switch#configure terminal
Switch(config)#ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#data-glean
Switch(config-ipv6-snooping)#
```

50.4 limit address-count

Данная команда используется для ограничения максимального количества привязок IPv6 Snooping. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

limit address-count *MAXIMUM*
no limit address-count

Параметры

MAXIMUM	Укажите максимальное количество привязок IPv6 Snooping. Диапазон значений: от 0 до 511.

По умолчанию

По умолчанию ограничений нет.

Режим ввода команды

IPv6 Snooping Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для ограничения количества привязок IPv6 Snooping, для которых применяется политика IPv6 Sooping. Команда помогает ограничить размер таблицы привязок.

Пример

В данном примере показано, как задать максимальное число записей IPv6 Snooping. Указанное значение – 25.

```
Switch#configure terminal
Switch(config)#ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#limit address-count 25
Switch(config-ipv6-snooping)#
```

50.5 ipv6 snooping attach-policy

Данная команда используется для применения политики IPv6 Snooping к указанной VLAN. Для удаления привязки воспользуйтесь формой **no** этой команды.

ipv6 snooping policy attach-policy *POLICY-NAME*
no ipv6 snooping policy attach-policy

Параметры

POLICY-NAME	Укажите имя политики IPv6 Snooping.

По умолчанию

По умолчанию политика IPv6 Snooping не применяется.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

После создания политики IPv6 Snooping Policy используйте данную команду для применения политики к определенной VLAN.

Пример

В данном примере показано, как включить IPv6 Snooping в VLAN 200.

```
Switch#configure terminal
Switch(config)#vlan 200
Switch(config-vlan)#ipv6 snooping attach-policy policy1
Switch(config-vlan)#
```

50.6 ipv6 snooping station-move deny

Данная команда используется, чтобы запретить функцию Station Move для привязки IPv6 Snooping. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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)#
```

50.7 ipv6 neighbor binding max-entries

Данная команда используется для настройки максимального количества записей IPv6 Snooping. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 neighbor binding max-entries {dhcp | ndp | dhcp-pd} *NUMBER*
no ipv6 neighbor binding max-entries {dhcp | ndp | dhcp-pd}

Параметры

dhcp	Укажите максимальное количество записей DHCPv6 Snooping.
ndp	Укажите максимальное количество записей ND Snooping.
dhcp-pd	Укажите максимальное количество записей DHCPv6 PD Snooping.
NUMBER	Укажите максимальное количество записей. Диапазон значений: от 0 до 511. Укажите 0, чтобы отключить изучение на указанном порту.

По умолчанию

Значение по умолчанию – 511.

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 настроить максимальное количество записей IPv6 Snooping. Каждый протокол snooping можно настроить отдельно.

Пример

В данном примере показано, как настроить максимальное количество записей DHCPv6 Snooping на интерфейсе Ethernet 1/0/1. Указанное значение – 10.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#ipv6 neighbor binding max-entries dhcp 10
Switch(config-if)#
```

50.8 clear ipv6 snooping entries

Данная команда используется для удаления записей IPv6 Snooping на указанном интерфейсе.

clear ipv6 snooping entries {dhcp | ndp | dhcp-pd} interface *INTERFACE-ID* **[, | -]**

Параметры

dhcp	Укажите, чтобы удалить записи DHCPv6 Snooping.
ndp	Укажите, чтобы удалить записи ND Snooping.
dhcp-pd	Укажите, чтобы удалить записи DHCPv6 PD Snooping.
interface *INTERFACE-ID*	Укажите interface ID.
,	(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

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы удалить записи IPv6 Snooping на указанном интерфейсе.

Пример

В данном примере показано, как удалить записи IPv6 Snooping на интерфейсе Ethernet 1/0/1.

```
Switch#clear ipv6 snooping entries ndp interface eth1/0/1
Switch#
```

50.9 show ipv6 snooping policy

Данная команда используется для просмотра информации о DHCPv6 Guard.

show ipv6 snooping policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики DHCPv6 Guard, которую необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для просмотра информации о DHCPv6 Guard. Если параметр не указан, будет отображаться 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
    Data Glean: Enabled
    Limit Address Count: 25
    Target VLAN: 200

Switch#
```

Отображаемые параметры

Protocol	Протокол, используемый для Snooping.
Data Glean	Состояние функции Data Glean.
Limit Address Count	Максимально допустимое число записей для данной политики IPv6 Snooping.
Target VLAN	Имя списка VLAN.

51. Команды IPv6 Source Guard

51.1 ipv6 source binding vlan

Данная команда используется для добавления статической записи в таблицу привязок. Для удаления статической привязки воспользуйтесь формой **no** этой команды.

ipv6 source binding *MAC-ADDRESS* **vlan** *VLAN-ID IPV6-ADDRESS* **interface** *INTERFACE-ID*
no ipv6 source binding *MAC-ADDRESS* **vlan** *VLAN-ID IPV6-ADDRESS* **interface** *INTERFACE-ID*

Параметры

MAC-ADDRESS	Укажите MAC-адрес привязки, созданной вручную.
VLAN-ID	Укажите VLAN привязки, созданной вручную.
IPV6-ADDRESS	Укажите IPv6-адрес привязки, созданной вручную.
INTERFACE-ID	Укажите номер интерфейса привязки, созданной вручную.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для добавления статической записи в таблицу привязок вручную. При конфигурации данной команды нет необходимости в существующей указанной VLAN. Если указанный интерфейс позднее будет удален, конфигурация данной команды также будет удалена.

Пример

В данном примере показано, как настроить привязку IPv6 Source Guard с IPv6-адресом 2000::1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 на интерфейсе Ethernet 1/0/10.

```
Switch#configure terminal
Switch(config)#ipv6 source binding 00-01-02-03-04-05 vlan 2 2000::1 interface eth1/0/1
Switch(config)#
```

51.2 ipv6 source-guard policy

Данная команда используется для создания политики IPv6 Source Guard. Команда позволяет войти в режим IPv6 Source-Guard Policy Configuration Mode. Для удаления политики Pv6 Source Guard воспользуйтесь формой **no** этой команды.

ipv6 source-guard policy *POLICY-NAME*
no ipv6 source-guard policy *POLICY-NAME*

Параметры

POLICY-NAME	Укажите имя политики IPv6 Source Guard.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для создания/удаления политики IPv6 Source Guard. Команда позволяет войти в режим IPv6 Source-Guard Policy Configuration Mode.

Пример

В данном примере показано, как создать политику IPv6 Source Guard.

```
Switch#configure terminal
Switch(config)#ipv6 source-guard policy policy1
Switch(config-source-guard)#
```

51.3 deny global-autoconfig

Данная команда используется для запрета трафика от автоматически сконфигурированных глобальных адресов. Для отключения функции воспользуйтесь формой **no** этой команды.

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. Рекомендуется к применению, если 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)#
```

51.4 permit link-local

Данная команда используется для аппаратного разрешения трафика данных, отправленных с адреса Link-Local. Для отключения данной функции воспользуйтесь формой **no** этой команды.

permit link-local
no permit link-local

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Source-guard Policy Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для аппаратного разрешения трафика данных, отправленных с адреса Link-Local.

Пример

В данном примере показано, как разрешить весь трафик данных, отправленных с адреса Link-Local.

```
Switch#configure terminal
Switch(config)#ipv6 source-guard policy policy1
Switch(config-source-guard)#permit link-local
Switch(config-source-guard)#
```

51.5 validate address

Данная команда используется, чтобы включить IPv6 Source Guard для выполнения проверки адреса. Для отключения функции проверки адреса воспользуйтесь формой **no** этой команды.

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

Используйте данную команду, чтобы включить функцию 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)#
```

51.6 validate prefix

Данная команда используется, чтобы включить функцию IPv6 Source Guard для выполнения операции защиты IPv6 Prefix-Guard. Для отключения функции воспользуйтесь формой **no** этой команды.

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

Используйте данную команду, чтобы включить функцию 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)#
```

51.7 ipv6 source-guard attach-policy

Данная команда используется для применения IPv6 Source Guard на интерфейсе. Чтобы отменить применение IPv6 Source Guard на интерфейсе, воспользуйтесь формой **no** этой команды.

ipv6 source-guard attach-policy [*POLICY-NAME***]**
no ipv6 source-guard attach-policy

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики Source Guard.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Если команда применена к порту, будет выполнена проверка привязки адреса для полученного IPv6-пакета, кроме ND, RA, RS и DHCP-сообщений. Пакет будет разрешен, если он соответствует любой записи в таблице привязок адресов. Таблица привязок включает в себя динамическую таблицу (созданную с помощью команд IPv6 Snooping) и статическую таблицу (созданную с помощью команды **ipv6 source binding vlan**).

Если команда применяется к VLAN, она позволяет узлам, принадлежащим группе IP Inspection, перемещаться в указанном домене VLAN между портами.

Если имя политики не указано, используемая по умолчанию политика Source Guard разрешит пакеты, отправленные с автоматически сконфигурированного адреса, и запретит пакеты, отправленные с адреса Link-Local.

Пример

В данном примере показано, как применить политику IPv6 Source Guard «pol1» на интерфейсе Ethernet 1/0/3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 source-guard attach-policy pol1
Switch(config-if)#
```

51.8 show ipv6 source-guard policy

Данная команда используется для просмотра настроек политики IPv6 Source Guard.

show ipv6 source-guard policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики Source Guard.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для просмотра настроек политики IPv6 Source Guard. Если имя политики не указано, отображаться будет информация для всех политик IPv6 Source Guard.

Пример

В данном примере показано, как включить отображение настроек для политики IPv6 Source Guard.

```
Switch#show ipv6 source-guard policy

Policy policy1 configuration:
    Target: eth1/0/3

Switch#
```

51.9 show ipv6 neighbor binding

Данная команда используется для просмотра таблицы привязок IPv6.

show ipv6 neighbor binding [vlan *VLAN-ID***] [interface** *INTERFACE-ID***] [ipv6** *IPV6-ADDRESS***] [mac** *MAC-ADDRESS***]**

Параметры

vlan *VLAN-ID*	(Опционально.) Укажите для отображения привязок, соответствующих указанной VLAN.
interface *INTERFACE-ID*	(Опционально.) Укажите для отображения привязок, соответствующих указанному номеру интерфейса.
ipv6 *IPV6-ADDRESS*	(Опционально.) Укажите для отображения привязок, соответствующих указанному IPv6-адресу.
mac *MAC-ADDRESS*	(Опционально.) Укажите для отображения привязок, соответствующих указанному MAC-адресу.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда используется для просмотра таблицы привязок.

Пример

В данном примере показано, как включить отображение указанных записей из таблицы привязок.

```
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   AABB.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                 AABB.CC01.F500 eth1/0/5        100  3181
D 2001:100::2                 AABB.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.

52. Команды Layer 2 Protocol Tunnel (L2PT)

52.1 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 *INTERFACE-ID*	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. Команда применима исключительно для интерфейсов физических портов и port-channel.

Пример

В данном примере показано, как обнулить счетчики L2PT для всех портов L2PT.

```
Switch#clear l2protocol-tunnel counters all
Switch#
```

52.2 l2protocol-tunnel

Данная команда используется, чтобы включить туннелирование для указанных протоколов. Для отключения данной функции воспользуйтесь формой **no** этой команды.

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 декапсулирует 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 eth1/0/1
Switch(config-if)#l2protocol-tunnel stp

 WARNING: STP doesn't run when l2 protocol tunnel is enabled for the port.
Switch(config-if)#
```

52.3 l2protocol-tunnel cos

Данная команда используется, чтобы указать значение CoS для L2PT. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

l2protocol-tunnel cos *COS-VALUE*
no l2protocol-tunnel cos

Параметры

COS-VALUE	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)#
```

52.4 l2protocol-tunnel drop-threshold

Данная команда используется, чтобы указать пороговое количество пакетов L2-протокола, полученных на порту. Пакеты, полученные после превышения заданного значения, будут отброшены. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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.
PPS	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 eth1/0/1
Switch(config-if)#l2protocol-tunnel drop-threshold stp 2000
Switch(config-if)#
```

52.5 l2protocol-tunnel global drop-threshold

Данная команда используется для указания максимального количества пакетов L2-протокола, которое может быть обработано системой за 1 секунду. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

l2protocol-tunnel global drop-threshold *PPS*
no l2protocol-tunnel global drop-threshold

Параметры

PPS	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)#
```

52.6 l2protocol-tunnel shutdown-threshold

Данная команда используется, чтобы указать пороговое количество пакетов L2-протокола, полученных на порту. Пакеты, полученные после превышения заданного значения, будут отброшены. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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.
PPS	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 eth1/0/1
Switch(config-if)#l2protocol-tunnel shutdown-threshold stp 200
Switch(config-if)#
```

52.7 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 *INTERFACE-ID*	(Опционально.) Укажите интерфейс, который необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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            :7
Drop Threshold for Encapsulated Packets :5000

Protocol             Drop Counter
-----------------    ------------
gvrp                 0
stp                  0
01-00-0c-cc-cc-cc    0
01-00-0c-cc-cc-cd    0

Port       Protocol     Shutdown  Drop      Encap      Decap      Drop
                        Threshold Threshold Counter    Counter    Counter
---------- ------------ --------- --------- ---------- ---------- ----------
eth1/0/1   stp          3200      2000      0          0          0

Switch#
```

В данном примере показано, как отобразить протоколы, туннелированные на интерфейсе Ethernet 1/0/1.

```
Switch#show l2protocol-tunnel interface eth1/0/1

Port       Protocol     Shutdown  Drop      Encap      Decap      Drop
                        Threshold Threshold Counter    Counter    Counter
---------- ------------ --------- --------- ---------- ---------- ----------
eth1/0/1   stp          3200      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.
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.

53. Команды Link Aggregation Control Protocol (LACP)

53.1 channel-group

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

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

no channel-group

Параметры

CHANNEL-NO	Укажите channel-group ID. Доступный диапазон значений: от 1 до 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 eth1/0/4-5
Switch(config-if)#channel-group 3 mode active
Switch(config-if)#
```

53.2 lacp port-priority

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

lacp port-priority *PRIORITY*
no lacp port-priority

Параметры

PRIORITY	Укажите приоритет порта в диапазоне от 1 до 65535.

По умолчанию

Приоритет порта по умолчанию – 32768.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Приоритет порта LACP определяет, какие порты могут подключиться к port-channel и на каких портах включен режим Standalone Mode. Чем ниже значение, тем выше приоритет. Если у двух и более портов совпадает приоритет, то приоритет будет определяться номером порта.

Пример

В данном примере показано, как сконфигурировать приоритет порта на интерфейсах от Ethernet 1/0/4 до Ethernet 1/0/5. Указанное значение – 20000.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/4-5
Switch(config-if)#lacp port-priority 20000
Switch(config-if)#
```

53.3 lacp timeout

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

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 Timeout.
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 Timeout.

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 eth1/0/1
Switch(config-if)#lacp timeout long
Switch(config-if)#
```

53.4 lacp system-priority

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

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)#
```

53.5 port-channel load-balance

Данная команда используется для настройки алгоритма Load Balancing (балансировка нагрузки), используемого коммутатором для распределения пакетов на порты одного канала. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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.

Если сконфигурировать хэш-параметр load-balance так, чтобы использовать IP-адрес (**src-ip**, **dst-ip** и **src-dst-ip**) или MAC-адрес (**src-mac**, **dst-mac** и **src-dst-mac**) для Load Balancing на канале LAG (Link Aggregation Group), Load Balancing будет рассчитан в соответствии с различными типами пакетов.

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)#
```

53.6 show channel-group

Данная команда используется для отображения информации о channel-group.

show channel-group [channel [*CHANNEL-NO*] {detail | neighbor} | load-balance | sys-id]

Параметры

channel	(Опционально.) Укажите, чтобы отобразить информацию для указанных port-channel.
CHANNEL-NO	(Опционально.) Укажите channel-group ID.
detail	(Опционально) Укажите, чтобы отобразить подробную информацию о channel-group.
neighbor	(Опционально.) Укажите, чтобы отобразить информацию о соседнем устройстве.
load-balance	(Опционально.) Укажите, чтобы отобразить информацию о балансировке нагрузки.
sys-id	(Опционально.) Укажите, чтобы отобразить system identifier, используемый LACP.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если номер port-channel не указан, будут отображены все port-channel. Если в команде **show channel-group** не указаны параметры **channel**, **load-balance** и **sys-id**, будет отображена только краткая информация о channel-group.

Пример

В данном примере показано, как отобразить подробную информацию обо всех port-channel.

```
Switch#show channel-group channel detail

Flag:
  S - Port is requesting Slow LACPDUs   F - Port is requesting fast LACPDU
  A - Port is in active mode            P - Port is in passive mode
LACP state:
  bndl:     Port is attached to an aggregator and bundled with other ports.
  hot-sby:  Port is in a hot-standby state.
  indep:    Port is in an independent state(not bundled but able to switch data
            traffic)
  down:     Port is down.

Channel Group 3
  Member Ports: 2, Maxports = 12, Protocol: LACP
  Description:
                       LACP          Port        Port
  Port          Flags  State         Priority    Number
  ------------------------------------------------
  eth1/0/4      FA     down          20000       0
  eth1/0/5      FA     down          20000       0

Switch#
```

В данном примере показано, как отобразить информацию о соседнем устройстве для port-channel 3.

```
Switch#show channel-group channel 3 neighbor

Flag:
  S - Port is requesting Slow LACPDUs   F - Port is requesting fast LACPDU
  A - Port is in active mode            P - Port is in passive mode

Channel Group 3
                Partner                   Partner    Partner    Partner
  Port          System ID                 PortNo     Flags      Port_Pri
  ------------------------------------------------------------------------
  eth1/0/21     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 enhanced MPLS label
System-ID: 32768,F0-7D-68-30-36-00

Group          Protocol
-----------------------
3              LACP

Switch#
```

54. Команды Link Layer Discovery Protocol (LLDP)

54.1 clear lldp counters

Данная команда используется для удаления статистики LLDP.

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

Параметры

all	(Опционально.) Укажите, чтобы обнулить счетчик LLDP для всех интерфейсов и статистики Global LLDP.
interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс, на котором необходимо обнулить счетчик LLDP. Доступны только физические интерфейсы.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, указав параметр **interface**, чтобы сбросить счетчик статистики LLDP на выбранном интерфейсе/интерфейсах. Используйте команду **clear lldp counters**, указав параметр **all**, чтобы удалить статистику LLDP и Global LLDP на всех интерфейсах. Если не указаны дополнительные параметры, будут обнулены только счетчики Global LLDP.

Пример

В данном примере показано, как удалить всю статистику LLDP.

```
Switch#clear lldp counters all
Switch#
```

54.2 clear lldp table

Данная команда используется для удаления всей информации об LLDP, полученной от соседних устройств.

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

Параметры

all	Укажите, чтобы удалить информацию об LLDP, полученную от соседних устройств, для всех интерфейсов.
INTERFACE-ID	Укажите interface ID. Доступны только физические интерфейсы.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если в команде указан параметр **interface**, будет удалена информация, полученная от соседних устройств, на указанных интерфейсах. Используйте команду, указав параметр **all**, чтобы удалить всю информацию, полученную от соседних устройств.

Пример

В данном примере показано, как удалить всю информацию, полученную от соседних устройств, на всех интерфейсах.

```
Switch#clear lldp table all
Switch#
```

54.3 lldp dot1-tlv-select

Данная команда используется для указания дополнительных настроек TLV (type-length-value) в указанном в пределах IEEE 802.1 наборе TLV, которые будут переданы и инкапсулированы в LLDPDU, а затем отправлены на соседние устройства. Для отключения передачи TLV используйте форму **no**.

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.
VLAN-ID	Укажите VLAN ID в PPVID TLV. Доступный диапазон значений: от 1 до 4094. Если VLAN ID не указан, все сконфигурированные PPVID VLAN будут удалены, PPVID TLV отправлен не будет.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
vlan-name	Укажите VLAN Name TLV, который необходимо отправить. VLAN Name TLV – это дополнительный TLV, который позволяет IEEE 802 LAN station, совместимой с IEEE 802.1Q, анонсировать присвоенное имя любой VLAN, с которой она сконфигурирована.
VLAN-ID	(Опционально.) Укажите VLAN ID в VLAN Name TLV. Доступный диапазон значений: от 1 до 4094. Если VLAN ID не указан, все сконфигурированные VLAN для VLAN Name TLV будут удалены, VLAN Name TLV отправлен не будет.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
protocol-identity	Укажите Protocol Identity TLV, который необходимо отправить. Protocol Identity TLV – это дополнительный TLV, который позволяет IEEE 802 LAN station анонсировать определенные протоколы, доступные через порт.

PROTOCOL-NAME	(Опционально.) Укажите имя протокола. Ниже перечислены допустимые для *PROTOCOL-NAME* строки: **eapol** - Extensible Authentication Protocol (EAP) over LAN **lacp** - Link Aggregation Control Protocol **gvrp** - GARP VLAN Registration Protocol **stp** - Spanning Tree Protocol

По умолчанию

По умолчанию указанные в пределах IEEE 802.1 TLV не заданы.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. Если включено анонсирование дополнительных TLV, они будут инкапсулированы в LLDPDU и отправлены на другие устройства.

Тип Protocol Identity TLV определяет, анонсировать ли соответствующий экземпляр Protocol Identity локальной системы на порту. Protocol Identity TLV позволяет устройствам анонсировать протоколы, которые важны для работы сети. Например, такие протоколы как Spanning Tree Protocol, Link Aggregation Control Protocol и другие протоколы, установленные vendor-ом, отвечают за поддержку топологии и подключения к сети. Если работают обе функции протокола и на порту включено анонсирование Protocol Identity, Protocol Identity TLV будет анонсирован.

PPVID TLV будет отправлен на VLAN только при условии, что сконфигурированный VLAN ID соответствует настройкам Protocol VLAN на данном интерфейсе, а данная VLAN существует. VLAN будет анонсирована в VLAN Name TLV только при условии, что интерфейс является портом-членом сконфигурированного VLAN ID.

Пример

В данном примере показано, как включить анонсирование Port VLAN ID TLV.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp dot1-tlv-select port-vlan
Switch(config-if)#
```

В 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 eth1/0/1
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 eth1/0/1
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 eth1/0/1
Switch(config-if)#lldp dot1-tlv-select protocol-identify lacp
Switch(config-if)#
```

54.4 lldp dot3-tlv-select

Данная команда используется для указания дополнительных настроек TLV в указанном в пределах IEEE 802.3 наборе TLV, которые будут инкапсулированы в LLDPDU, а затем отправлены на соседние устройства. Для отключения передачи TLV воспользуйтесь формой **no** этой команды.

lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | power | max-frame-size]

no lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | power | max-frame-size]

Параметры

mac-phy-cfg	(Опционально.) Укажите MAC/PHY Configuration/Status TLV, который необходимо отправить. MAC/PHY Configuration/Status TLV – это дополнительный TLV, который определяет (1) режим дуплекса и максимальную скорость передачи узла EEE 802.3 LAN в бит/сек, а также (2) текущий режим дуплекса и настройки скорости передачи узла IEEE 802.3 LAN в бит/сек.
link-aggregation	(Опционально.) Укажите Link Aggregation TLV, который необходимо отправить. Link Aggregation TLV содержит информацию о том, можно ли агрегировать группу, агрегируется ли группа в данный момент, а также информацию об агрегированном port channel ID. Если порт не агрегирован, значение port channel ID – 0.
power	Укажите мощность, которую следует отправлять с помощью MDI TLV. Три реализации PMD IEEE 802.3 (10Base-T, 100Base-TX и 1000Base-T) позволяют подавать питание через соединение для подключенных неэлектрифицированных систем. TLV Power Via MDI позволяет управлению сетью анонсировать и получать информацию о возможности подачи питания с помощью MDI при отправке IEEE 802.3 LAN station

max-frame-size	(Опционально.) Укажите Maximum Frame Size TLV, который необходимо отправить. Maximum Frame Size TLV указывает максимальный размер кадра для используемого MAC и PHY.

По умолчанию

По умолчанию указанный в пределах IEEE 802.3 TLV не выбран.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. 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 eth1/0/1
Switch(config-if)#lldp dot3-tlv-select mac-phy-cfg
Switch(config-if)#
```

54.5 lldp fast-count

Данная команда используется для настройки количества отправляемых пакетов Fast Start (LLDP MED Fast Start Repeat Count Option) на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lldp fast-count *VALUE*

no lldp fast-count

Параметры

VALUE	Укажите количество отправляемых пакетов Fast Start. Доступный диапазон значений: от 1 до 10.

По умолчанию

Значение по умолчанию – 4.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При обнаружении LLDP MED Capabilities TLV будет запущена процедура Fast Start. Используйте данную команду, чтобы настроить количество отправляемых пакетов Fast Start, которое соответствует количеству передач LLDP-сообщений за один полный интервал Fast Start.

Пример

В данном примере показано, как сконфигурировать количество отправляемых пакетов Fast Start.

```
Switch#configure terminal
Switch(config)#lldp fast-count 10
Switch(config)#
```

54.6 lldp hold-multiplier

Данная команда используется для того, чтобы настроить множитель удержания для обновлений LLDP на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lldp hold-multiplier *VALUE*
no hold-multiplier

Параметры

VALUE	Укажите множитель для интервала передачи LLDPDU, с помощью которого будет вычислено значение TTL для LLDPDU. Доступный диапазон значений: от 2 до 10.

По умолчанию

Значение по умолчанию – 4.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данный параметр – это множитель для интервала передачи LLDPDU, с помощью которого будет вычислено значение TTL в LLDPDU. Время жизни определяется при помощи множителя удержания, умноженного на интервал TX. Если TTL для определенного анонса на соседнем коммутаторе истек, анонсированная информация будет удалена из MIB соседнего устройства.

Пример

В данном примере показано, как указать значение 3 для множителя удержания LLDP.

```
Switch#configure terminal
Switch(config)#lldp hold-multiplier 3
Switch(config)#
```

54.7 lldp management-address

Данная команда используется для настройки адреса управления (Management Address), который будет анонсирован на физическом интерфейсе. Для удаления заданных настроек воспользуйтесь формой **no** этой команды.

lldp management-address [*IP-ADDRESS* **|** *IPV6-ADDRESS***]**
no lldp management-address [*IP-ADDRESS* **|** *IPV6-ADDRESS***]**

Параметры

IP-ADDRESS	(Опционально.) Укажите IPv4-адрес, передаваемый в Management Address TLV.
IPV6-ADDRESS	(Опционально.) Укажите IPv6-адрес, передаваемый в Management Address TLV.

По умолчанию

По умолчанию адрес управления LLDP не настроен (Management Address TLV не отправляется).

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. 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 1/0/1-1/0/3.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-3
Switch(config-if-range)#lldp management-address 10.1.1.1
Switch(config-if-range)#
```

В данном примере показано, как настроить адрес управления IPv6 на интерфейсах Ethernet 1/0/4-1/0/6.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/4-6
Switch(config-if-range)#lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

В данном примере показано, как удалить адрес управления IPv4 из интерфейсов Ethernet 1/0/1-Ethernet 1/0/3.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-3
Switch(config-if-range)#no lldp management-address 10.1.1.1
Switch(config-if-range)#
```

В данном примере показано, как удалить адрес управления IPv6 из интерфейсов Ethernet 1/0/4-Ethernet 1/0/6.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/4-6
Switch(config-if-range)#no lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

В данном примере показано, как удалить все адреса управления IPv4/IPv6 из интерфейса Ethernet 1/0/5. В этом случае с Ethernet 1/0/5 Management Address TLV отправлен не будет.

```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#no lldp management-address
Switch(config-if)#
```

54.8 lldp med-tlv-select

Данная команда используется для указания дополнительного LLDP-MED TLV, который будет передан, инкапсулипрован в LLDPDU и отправлен на соседние устройства. Для отключения передачи TLV воспользуйтесь формой **no** этой команды.

lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]

no lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]

Параметры

capabilities	(Опционально.) Укажите, чтобы передать LLDP-MED Capabilities TLV.
inventory-management	(Опционально.) Укажите, чтобы передать LLDP-MED Inventory Management TLV.
network-policy	(Опционально.) Укажите, чтобы передать LLDP-MED Network Policy TLV.
power-management	(Опционально.) Укажите, чтобы передать LLDP-MED Extended Power Via MDI TLV, локальное устройство – PSE или PD.

По умолчанию

LLDP-MED TLV по умолчанию не выбран.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта. Команда применяется для включения/отключения передачи LLDP-MED TLV. Если параметры не указаны, будут настроены все дополнительные 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 eth1/0/1
Switch(config-if)#lldp med-tlv-select capabilities
Switch(config-if)#
```

54.9 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 eth1/0/1
Switch(config-if)#lldp receive
Switch(config-if)#
```

54.10 lldp reinit

Данная команда используется для настройки минимального интервала перед повторной инициализацией на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lldp reinit *SECONDS*
no lldp reinit

Параметры

SECONDS	Укажите время задержки инициализации LLDP на интерфейсе. Доступный диапазон значений: от 1 до 10 секунд.

По умолчанию

Значение по умолчанию – 2 секунды.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При перезапуске физического интерфейса LLDP будет выдержан заданный интервал времени между последней командой disable и повторной инициализацией.

Пример

В данном примере показано, как сконфигурировать интервал перед повторной инициализацией. Указанное значение – 5 секунд.

```
Switch#configure terminal
Switch(config)#lldp reinit 5
Switch(config)#
```

54.11 lldp run

Данная команда используется для глобального включения функции LLDP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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)#
```

54.12 lldp forward

Данная команда используется для включения состояния LLDP Forwarding. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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)#
```

54.13 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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 eth1/0/1
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 eth1/0/1
Switch(config-if)#lldp tlv-select system-name
Switch(config-if)#
```

54.14 lldp transmit

Данная команда используется для включения анонсирования/передачи LLDP. Для отключения передачи LLDP воспользуйтесь формой **no** этой команды.

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

Данная команда применима исключительно для настройки интерфейсов физического порта. 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 eth1/0/1
Switch(config-if)#lldp transmit
Switch(config-if)#
```

54.15 lldp tx-delay

Данная команда используется для настройки таймера Transmission Delay, определяющего минимальный интервал между отправкой LLDP-сообщений на основе постоянно изменяющегося содержания MIB. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lldp tx-delay *SECONDS*
no lldp tx-delay

Параметры

SECONDS	Укажите время задержки для отправки последовательных LLDPDU на интерфейсе. Доступный диапазон значений: от 1 до 8192 секунд, при этом указанное значение не должно превышать одну четвертую значения таймера Transmission Interval.

По умолчанию

Значение по умолчанию – 2 секунды.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Значение LLDP Transmission Interval должно быть больше или равно значению таймера Transmission Delay, умноженному на четыре.

Пример

В данном примере показано, как указать значение таймера Transmission Delay. Заданное значение – 8 секунд.

```
Switch#configure terminal
Switch(config)#lldp tx-delay 8
Switch(config)#
```

54.16 lldp tx-interval

Данная команда используется для настройки интервала LLDPDU Transmission. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

lldp tx-interval *SECONDS*

no lldp tx-interval

Параметры

SECONDS	Укажите интервал между отправкой последовательных анонсов LLDPD на каждом физическом интерфейсе. Доступный диапазон значений: от 5 до 32768 секунд.

По умолчанию

Значение по умолчанию – 30 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данный интервал определяет скорость передачи LLDP-пакетов.

Пример

В данном примере показано, как сконфигурировать отправку обновлений LLDP через каждые 50 секунд.

```
Switch#configure terminal
Switch(config)#lldp tx-interval 50
Switch(config)#
```

54.17 snmp-server enable traps lldp

Данная команда используется для включения отправки LLDP Trap и LLDP-MED Trap. Для отключения данной функции воспользуйтесь формой **no** этой команды.

snmp-server enable traps lldp [med]

no snmp-server enable traps lldp [med]

Параметры

med	(Опционально.) Укажите, чтобы включить отправку LLDP-MED Trap.

По умолчанию

По умолчанию отправка LLDP Trap и LLDP-MED Trap отключены.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду **snmp-server enable traps lldp**, чтобы включить отправку LLDP-уведомлений.

Используйте команду **ssnmp-server enable traps lldp med**, чтобы включить отправку LLDP-MED-уведомлений.

Пример

В данном примере показано, как включить отправку LLDP-MED Trap.

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

54.18 lldp notification enable

Данная команда используется для включения отправки уведомлений LLDP и LLDP-MED на интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 eth1/0/1
Switch(config-if)#lldp med notification enable
Switch(config-if)#
```

54.19 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 eth1/0/1
Switch(config-if)#lldp subtype port-id mac-address
Switch(config-if)#
```

54.20 show lldp

Данная команда используется для отображения общих настроек функции LLDP на коммутаторе.

show lldp

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить общие настройки функции LLDP на коммутаторе.

Пример

В данном примере показано, как отобразить общие настройки функции LLDP на коммутаторе.

```
Switch#show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address
    Chassis ID                : 80-26-89-15-28-00
    System Name               : Switch
    System Description        : Gigabit Ethernet Smart Managed Switch
    System Capabilities Supported: Repeater, Bridge
    System Capabilities Enabled  : Repeater, Bridge

LLDP-MED System Information:
    Device Class              : Network Connectivity Device
    Hardware Revision         : A1
    Firmware Revision         : 1.00.010
    Software Revision         : 1.00.022
    Serial Number             : DGS1520-28MPA
    Manufacturer Name         : D-Link Corporation
    Model Name                : DGS-1520-28MP
    Asset ID                  :
    PoE Device Type           : PSE Device
    PoE PSE Power Source      : Primary

LLDP Configurations
    LLDP State                : Disabled
    LLDP Forward State        : Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

54.21 show lldp interface

Данная команда используется для того, чтобы отобразить настройки функции LLDP на физическом интерфейсе.

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

Параметры

INTERFACE-ID	Укажите interface ID, который необходимо отобразить. Доступны только физические интерфейсы.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о функции LLDP для каждого физического интерфейса.

Пример

В данном примере показано, как отобразить настройки функции LLDP для интерфейса Ethernet 1/0/1.

```
Switch#show lldp interface eth1/0/1

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID                                                 :eth1/0/1
Admin Status                                            :TX and RX
Notification                                            :Disabled
Basic Management TLVs:
    Port Description                                    :Disabled
    System Name                                         :Disabled
    System Description                                  :Disabled
    System Capabilities                                 :Disabled
    Enabled Management Address:
        (None)
IEEE 802.1 Organizationally Specific TLVs:

    Port VLAN ID                                        :Disabled
    Enabled Port_and_Protocol_VLAN_ID
        (None)
    Enabled VLAN Name
        (None)
    Enabled Protocol_Identity
        (None)
IEEE 802.3 Organizationally Specific TLVs:

    MAC/PHY Configuration/Status                        :Disabled
    Power Via MDI                                       :Disabled
    Link Aggregation                                    :Disabled
    Maximum Frame Size                                  :Disabled

LLDP-MED Organizationally Specific TLVs:

    LLDP-MED Capabilities TLV                           :Disabled
    LLDP-MED Network Policy TLV                         :Disabled
    LLDP-MED Extended Power Via MDI PSE TLV             :Disabled
    LLDP-MED Inventory TLV                              :Disabled



Switch#
```

Отображаемые параметры

Enabled Management Address	Отображает включенные IPv4/IPv6-адреса. «(None)» означает, что пользователь не сконфигурировал адрес управления (Management Address) при помощи команды **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)».

54.22 show lldp local interface

Данная команда используется для отображения информации о физическом интерфейсе, которая будет отправлена на соседние устройства в LLDP TLV.

show lldp local interface *INTERFACE-ID* **[, | -] [brief | detail]**

Параметры

INTERFACE-ID	Укажите interface ID. Доступны только физические интерфейсы.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
brief	(Опционально.) Укажите, чтобы отобразить информацию в сокращенном формате.
detail	(Опционально.) Укажите, чтобы отобразить информацию в подробном формате. Если не указан ни параметр **brief**, ни параметр **detail**, информация будет отображена в стандартном формате.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить текущую анонсируемую локальную информацию в исходящих LLDP-объявлениях для каждого физического интерфейса.

Пример

В данном примере показано, как отобразить локальную информацию для интерфейса физического порта Ethernet 1/0/1 в подробном формате.

```
SSwitch#show lldp local interface eth1/0/1 detail

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DGS-1520-28MP HW
                                           A1 firmware 1.00.022 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                              : 1.3.6.1.4.1.171.10.171.2.1

    Address 2 :
        Subtype                          : IPv4
        Address                          : 10.90.90.90
        IF Type                          : IfIndex
        OID                              : 1.3.6.1.4.1.171.10.171.2.1

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 eth1/0/1

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DGS-1520-28MP HW
                                           A1 firmware 1.00.022 Port 1 on Unit
                                           1
Port PVID                                : 1
Management Address Count                 : 2
PPVID Entries Count                      : 0
VLAN Name Entries Count                  : 1
Protocol Identity Entries Count          : 0
MAC/PHY Configuration/Status             : (See Detail)
Power Via MDI                            : (See Detail)
Link Aggregation                         : (See Detail)
Maximum Frame Size                       : 1536
LLDP-MED capabilities                    : (See Detail)
Network Policy                           : (See Detail)
Extended power via MDI                   : (See Detail)


Switch#
```

В данном примере показано, как отобразить локальную информацию для интерфейса физического порта Ethernet 1/0/1 в сокращенном формате.

```
Switch#show lldp local interface eth1/0/1 brief

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DGS-1520-28MP HW
                                           A1 firmware 1.00.022 Port 1 on Unit
                                           1


Switch#
```

54.23 show lldp management-address

Данная команда используется для отображения информации об адресе управления (Management Address).

show lldp management-address [*IP-ADDRESS* **|** *IPV6-ADDRESS***]**

Параметры

IP-ADDRESS	(Опционально.) Укажите, чтобы отобразить информацию об LLDP Management для указанного IPv4-адреса.

IPV6-ADDRESS	(Опционально.) Укажите, чтобы отобразить информацию об LLDP Management для указанного IPv6-адреса.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об адресе управления.

Пример

В данном примере показано, как отобразить всю информацию об адресе управления.

```
Switch#show lldp management-address

Address 1 : (default)
-----------------------------------------------
    Subtype                          : IPv4
    Address                          : 10.90.90.90
    IF Type                          : IfIndex
    OID                              : 1.3.6.1.4.1.171.10.171.2.1
    Advertising Ports                : -

Address 2 :
-----------------------------------------------
    Subtype                          : IPv4
    Address                          : 10.90.90.90
    IF Type                          : IfIndex
    OID                              : 1.3.6.1.4.1.171.10.171.2.1
    Advertising Ports                : -

Total Entries : 2


Switch#
```

54.24 show lldp neighbors interface

Данная команда используется для отображения актуальной информации, полученной от соседнего устройства на указанном физическом интерфейсе.

show lldp neighbors interface *INTERFACE-ID* **[, | -] [brief | detail]**

Параметры

INTERFACE-ID	Укажите interface ID. Доступны только физические интерфейсы.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
brief	(Опционально.) Укажите, чтобы отобразить информацию в сокращенном формате.
detail	(Опционально.) Укажите, чтобы отобразить информацию в подробном формате. Если не указан ни параметр **brief**, ни параметр **detail**, информация будет отображена в стандартном формате.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию, полученную от соседних устройств.

Пример

В данном примере показано, как отобразить информацию о соседних устройствах, изученную LLDP на интерфейсе Ethernet 1/0/1, в подробном формате.

```
Switch#show lldp neighbors interface eth1/0/1 detail

Port ID: eth1/0/1
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                          : MAC Address
    Chassis ID                                  : 80-26-89-15-28-A0
    Port ID Subtype                             : Local
    Port ID                                     : eth1/0/1
    Port Description                            :
    System Name                                 :
    System Description                          :
    System Capabilities                         :
    Management Address Count                    : 0
        (None)

    Port PVID                                   : 0
    PPVID Entries Count                         : 0
        (None)

    VLAN Name Entries Count                     : 0
        (None)

    Protocol ID Entries Count                   : 0
        (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 Enabled:
            Capabilities                    : Not Support
            Network Policy                  : Not Support
            Location Identification         : Not Support
            Extended Power Via MDI          : Not Support
            Inventory                       : Not Support

    Inventory Management:
        None


Switch#
```

В примере ниже показано, как отобразить информацию о соседних устройствах, изученную LLDP на интерфейсе Ethernet 1/0/1, в стандартном формате.

```
Switch#show lldp neighbors interface eth1/0/1

Port ID: eth1/0/1
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                      : MAC Address
    Chassis ID                              : 80-26-89-15-28-A0
    Port ID Subtype                         : Local
    Port ID                                 : eth1/0/1
    Port Description                        :
    System Name                             :
    System Description                      :
    System Capabilities                     :
    Management Address Count                : 0
    Port PVID                               : 0
    PPVID Entries Count                     : 0
    VLAN Name Entries Count                 : 0
    Protocol ID Entries Count               : 0
    MAC/PHY Configuration/Status            : (None)
    Power Via MDI                           : (None)
    Link Aggregation                        : (None)
    Maximum Frame Size                      : 0
    LLDP-MED capabilities                   : (See Detail)
    Extended power via MDI                  : (See Detail)
    Network policy                          : (See Detail)
    Inventory Management                    : (See Detail)
    Unknown TLVs Count                      : 0


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 neighbors interface eth1/0/1-2 brief

Port ID: eth1/0/1
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                      : MAC Address
    Chassis ID                              : 80-26-89-15-28-A0
    Port ID Subtype                         : Local
    Port ID                                 : eth1/0/1
    Port Description                        :

Port ID: eth1/0/2
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                      : MAC Address
    Chassis ID                              : 80-26-89-A5-43-D0
    Port ID Subtype                         : Local
    Port ID                                 : eth1/0/22
    Port Description                        :


Switch#
```

54.25 show lldp traffic

Данная команда используется для отображения глобальной информации о трафике LLDP.

show lldp traffic

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об обнаружении соседних устройств на коммутаторе.

Пример

В данном примере показано, как отобразить глобальную информацию о трафике LLDP.

```
Switch#show lldp traffic

Last Change Time  : 0D4H31M5S
Total Inserts     : 5
Total Deletes     : 0
Total Drops       : 0
Total Ageouts     : 1

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.

54.26 show lldp traffic interface

Данная команда используется для отображения информации о трафике LLDP на указанном физическом интерфейсе.

show lldp traffic interface *INTERFACE-ID* **[, | -]**

Параметры

INTERFACE-ID	Укажите interface ID. Доступны только физические интерфейсы.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить трафик LLDP на каждом физическом интерфейсе.

Пример

В данном примере показано, как отобразить статистику для порта 1.

```
Switch#show lldp traffic interface eth1/0/1

Port ID : eth1/0/1
-----------------------------------------------
    Total Transmits     : 55
    Total Discards      : 0
    Total Errors        : 0
    Total Receives      : 38
    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.

55. Команды Loopback Detection (LBD)

55.1 loopback-detection (Global)

Данная команда используется, чтобы включить функцию LBD (Loopback Detection) глобально. Для глобального отключения данной функции воспользуйтесь формой **no** этой команды.

loopback-detection [mode {port-based | vlan-based}]

no loopback-detection [mode]

Параметры

mode	(Опционально.) Укажите режим обнаружения.
port-based	(Опционально.) Укажите режим обнаружения петли port-based (на порту).
vlan-based	(Опционально.) 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)#
```

55.2 loopback-detection (Interface)

Данная команда используется для включения функции LBD на интерфейсе. Для отключения данной функции на интерфейсе воспользуйтесь формой **no** этой команды.

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

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

Используйте данную команду, чтобы включить/отключить функцию LBD на интерфейсе.

Пример

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

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

55.3 loopback-detection interval

Данная команда используется для конфигурирования временного интервала. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

loopback-detection interval *SECONDS*
no loopback-detection interval

Параметры

SECONDS	Укажите интервал передачи пакетов LBD. Доступный диапазон значений: от 1 до 32767 секунд.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы сконфигурировать интервал передачи пакетов LBD, отправляемых для обнаружения петли.

Пример

В данном примере показано, как сконфигурировать интервал 20 секунд.

```
Switch#configure terminal
Switch(config)#loopback-detection interval 20
Switch(config)#
```

55.4 loopback-detection vlan

Данная команда используется для того, чтобы включить функцию LBD на VLAN. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

loopback-detection vlan *VLAN-LIST*
no loopback-detection vlan *VLAN-LIST*

Параметры

VLAN-LIST	Укажите идентификационный номер / номера / диапазон номеров VLAN. Диапазоны разделяются при помощи дефисов. Значения разделяются при помощи запятых. Пробелы до и после дефиса/запятой недопустимы.

По умолчанию

По умолчанию данная опция включена для всех VLAN.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы сконфигурировать список VLAN, на которых включена функция LBD. Настройки команды будут применены, если на порту сконфигурирован режим обнаружения петли VLAN-based.

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)#
```

55.5 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.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки и статус функции LBD.

Пример

В данном примере показано, как отобразить текущие настройки и статус функции LBD.

```
Switch#show loopback-detection

 Loop Detection       : Enabled
 Detection Mode       : 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 eth1/0/1

 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.

55.6 loopback-detection action

Данная команда используется для настройки режима LBD. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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)#
```

55.7 snmp-server enable traps loopback-detection

Данная команда используется для включения отправки SNMP-уведомлений для LBD. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 или отключить отправку SNMP-уведомлений для LBD.

Пример

В данном примере показано, как включить отправку SNMP-уведомлений для LBD.

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

55.8 loopback-detection address-type

Данная команда используется для того, чтобы настроить тип адреса назначения (destination) пакетов LBD. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

loopback-detection address-type {multicast | broadcast}

no loopback-detection address-type

Параметры

multicast	Укажите, чтобы отсылать только групповые пакеты LBD. Адрес назначения – CF-00-00-00-00-00.
broadcast	Укажите, чтобы отсылать только широковещательные пакеты LBD. Адрес назначения – FF-FF-FF-FF-FF-FF.

По умолчанию

Параметр по умолчанию – **multicast**.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить тип адреса назначения пакетов LBD.

Пример

В данном примере показано, как настроить тип адреса назначения пакетов LBD. Указанный тип – broadcast.

```
Switch#configure terminal
Switch(config)#loopback-detection address-type broadcast
Switch(config)#
```

56. Команды Loopback Test

56.1 loopback

Данная команда используется для настройки режима Loopback на интерфейсах физических портов, а также для запуска тестирования. Для удаления настроек и остановки тестирования воспользуйтесь формой **no** этой команды.

loopback {internal | external} {mac | phy [copper | fiber]}

no loopback

Параметры

internal	Укажите, чтобы выбрать режим Internal Loopback. Для MAC или PHY установлен режим Internal Loopback. В этом режиме ЦПУ начинает непрерывно отправлять пакеты на порт. Все пакеты, отправленные ЦПУ, будут закольцованы и ЦПУ выполнит проверку полученных пакетов, чтобы определить, корректен ли путь пакета между ЦПУ и MAC/PHY.
external	Укажите, чтобы выбрать режим External Loopback. Для MAC или PHY установлен режим External Loopback (Line Loopback). Пакеты, отправленные генератором внешнего трафика, будут закольцованы на уровне MAC или PHY и отправлены назад генератору. Далее генератор внешнего трафика может выполнить проверку полученных пакетов, чтобы определить, корректен ли путь пакета между MAC/PHY и генератором.
mac	Укажите, чтобы выполнить закольцовывание на уровне MAC.
phy	Укажите, чтобы выполнить закольцовывание на физическом уровне (PHY).
copper	(Опционально.) Укажите для тестирования medium to copper.
fiber	(Опционально.) Укажите для тестирования medium to fiber.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применима исключительно для настройки интерфейсов физического порта.

Пример

В данном примере показано, как запустить тест Loopback на интерфейсе Ethernet 1/0/1 в режиме Internal PHY Copper.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#loopback internal phy copper

Success

Switch(config-if)#
```

56.2 show loopback result

Данная команда позволяет отобразить результаты теста Loopback для всех или для указанного физического порта.

show loopback result [interface *INTERFACE-ID* **[- | ,]]**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейс физического порта, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить результаты теста Loopback для указанного физического порта / для всех физических портов.

Пример

В данном примере показано, как отобразить результаты теста Loopback на интерфейсе Ethernet 1/0/1.

```
Switch#show loopback result interface eth1/0/1

Port       Loopback     64B          512B         1024B        1536B
           Mode         Tx    Rx     Tx    Rx     Tx    Rx     Tx    Rx
---------  -----------  ----- -----  ----- -----  ----- -----  ----- -----
eth1/0/1   Int. copper  9     9      9     9      9     9      9     9

Loopback Test Result : Success

Switch#
```

57. Команды аутентификации MAC

57.1 mac-auth system-auth-control

Данная команда используется для глобального включения MAC-аутентификации. Для отключения глобальной MAC-аутентификации воспользуйтесь формой **no** этой команды.

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. 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)#
```

57.2 mac-auth enable

Данная команда используется для включения MAC-аутентификации на указанном интерфейсе. Для отключения MAC-аутентификации воспользуйтесь формой **no** этой команды.

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

Данная команда применима исключительно для настройки интерфейсов физического порта. Она может использоваться для включения MAC-аутентификации на указанном интерфейсе.

Также у MAC-аутентификации есть 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 интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mac-auth enable
Switch(config-if)#
```

57.3 mac-auth password

Данная команда используется, чтобы настроить пароль для локальной и RADIUS-аутентификации. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

mac-auth password [0 | 7] *STRING*
no mac-auth password

Параметры

0	(Опционально.) Пароль в обычном текстовом виде. Если не указан ни 0, ни 7, по умолчанию пароль будет в обычном текстовом виде.
7	(Опционально.) Зашифрованный пароль. Если не указан ни 0, ни 7, по умолчанию пароль будет в обычном текстовом виде.

password *STRING*	Укажите, чтобы задать пароль для аутентификации на основе MAC-адреса. Если пароль указан в обычном текстовом виде, длина строки не может превышать 16 символов. Если пароль указан в зашифрованном виде, длина строки не может превышать 44 символа.

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)#
```

57.4 mac-auth username

Данная команда используется, чтобы настроить имя пользователя для локальной и RADIUS-аутентификации. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

mac-auth username *STRING*
no mac-auth username

Параметры

STRING	Укажите, чтобы задать имя пользователя для MAC-аутентификации. Длина строки не может превышать 16 символов.

По умолчанию

По умолчанию именем пользователя является MAC-адрес клиента.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда позволяет настроить имя 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 аутентификации на основе MAC-адреса.

```
Switch#configure terminal
Switch(config)#mac-auth username user1
Switch(config)#
```

57.5 snmp-server enable traps mac-auth

Данная команда позволяет включить отправку SNMP-уведомлений для MAC-аутентификации. Для отключения SNMP-уведомлений воспользуйтесь формой **no** этой команды.

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 отправку trap-сообщений для MAC-аутентификации.

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

58. Команды Mirror

58.1 monitor session destination interface

Данная команда используется, чтобы настроить интерфейс назначения (destination) для сессии мониторинга, позволяя отслеживать пакеты на портах источника (source) через порт назначения. Для удаления интерфейса назначения сессии воспользуйтесь формой **no** этой команды.

monitor session *SESSION-NUMBER* **destination interface** *INTERFACE-ID*
no monitor session *SESSION-NUMBER* **destination interface** *INTERFACE-ID*

Параметры

SESSION-NUMBER	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
INTERFACE-ID	Укажите интерфейс назначения для сессии мониторинга.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте 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 eth1/0/1
Switch(config)#monitor session 1 source interface eth1/0/2-4
Switch(config)#
```

58.2 monitor session destination remote vlan

Данная команда используется для настройки RSPAN VLAN и порта назначения (destination) для сессии источника (source) RSPAN. Для удаления настроек RSPAN VLAN воспользуйтесь формой **no** этой команды.

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

SESSION-NUMBER	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
VLAN-ID	Укажите RSPAN VLAN, используемую для туннелирования отслеживаемых пакетов на удаленный сайт. Доступный диапазон значений: от 2 до 4094.
interface *INTERFACE-ID*	Укажите интерфейс, с помощью которого необходимо передать отслеживаемые пакеты на удаленный сайт.
access-list *ACCESS-LIST-NAME*	(Опционально.) Укажите поток, используемый для замены RSPAN VLAN потока. Поток будет сконфигурирован, даже если список доступа не существует.
replace vlan *VLAN-ID*	(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 eth1/0/2-4
Switch(config)#monitor session 2 destination remote vlan 100 interface eth1/0/6
Switch(config)#
```

58.3 monitor session source interface

Данная команда используется, чтобы сконфигурировать порт источника (source) сессии мониторинга. Для удаления порта источника из сессии мониторинга воспользуйтесь формой **no** этой команды.

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

SESSION-NUMBER	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
interface *INTERFACE-ID*	Укажите интерфейс источника для сессии мониторинга.

,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
both	(Опционально.) Укажите, чтобы отслеживать пакеты, переданные и полученные портом.
rx	(Опционально.) Укажите, чтобы отслеживать пакеты, полученные портом.
tx	(Опционально.) Укажите, чтобы отслеживать пакеты, переданные портом.
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 eth1/0/1
Switch(config)#monitor session 1 source interface ethe1/0/2-4
Switch(config)#
```

58.4 monitor session source acl

Данная команда используется, чтобы сконфигурировать список доступа для мониторинга на основе потока. Для удаления списка доступа для мониторинга на основе потока воспользуйтесь формой **no** этой команды.

monitor session *SESSION-NUMBER* **source acl** *ACCESS-LIST-NAME*

no monitor session *SESSION-NUMBER* **source acl** *ACCESS-LIST-NAME*

Параметры

SESSION-NUMBER	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
ACCESS-LIST-NAME	Укажите зеркалирование на основе потока. 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 команды

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 eth1/0/1
Switch(config)#monitor session 2 source acl MAC-Monitored-flow
Switch(config)#
```

58.5 monitor session source remote vlan

Данная команда используется, чтобы настроить RSPAN VLAN для сессии назначения (destination) RSPAN. Для удаления заданных настроек воспользуйтесь формой **no** этой команды.

monitor session *SESSION-NUMBER* **source remote vlan** *VLAN-ID*

no monitor session *SESSION-NUMBER* **source remote vlan**

Параметры

SESSION-NUMBER	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
VLAN-ID	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 1/0/5 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 eth1/0/5
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 100
Switch(config-if)#exit
Switch(config)#interface eth1/0/4
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 eth1/0/4
Switch(config)#
```

58.6 monitor session source vlan

Данная команда используется, чтобы настроить VLAN для мониторинга на основе VLAN. Для удаления VLAN из мониторинга на основе VLAN воспользуйтесь формой **no** этой команды.

monitor session *SESSION-NUMBER* **source vlan** *VLAN-ID* **[, | -] rx**
no monitor session *SESSION-NUMBER* **source vlan** *VLAN-ID* **[, | -]**

Параметры

SESSION-NUMBER	Укажите номер сессии мониторинга. Доступный диапазон значений: от 1 до 4.
VLAN-ID	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 eth1/0/1
Switch(config)#monitor session 2 source vlan 2-4 rx
Switch(config)#
```

58.7 remote-span

Данная команда используется для указания VLAN в качестве RSPAN VLAN. Для возврата к non-RSPAN VLAN воспользуйтесь формой **no** этой команды.

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 eth1/0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 100
Switch(config-if)#exit
Switch(config)#interface eth1/0/5
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)#
```

58.8 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)#
```

58.9 show monitor session

Данная команда используется для отображения указанной сессии / всех сессий мониторинга.

show monitor session [*SESSION-NUMBER* **| remote | local]**

Параметры

SESSION-NUMBER	(Опционально.) Укажите номер сессии, которую необходимо отобразить.
local	(Опционально.) Укажите, чтобы отобразить локальную сессию.
remote	(Опционально.) Укажите, чтобы отобразить удаленную сессию RSPAN.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду без указания номера сессии, чтобы отобразить все сессии мониторинга.

Пример

В данном примере показано, как отобразить сессию мониторинга порта с номером 1.

```
Switch#show monitor session

 Session 1
    Session Type: local session
    Destination Port: Ethernet1/0/1
    Source Ports:
        Both:
            Ethernet1/0/2
            Ethernet1/0/3
            Ethernet1/0/4

 Total Entries: 1

Switch#
```

59. Команды Multicast Listener Discovery (MLD)

59.1 ipv6 mld enable

Данная команда используется, чтобы включить состояние MLD-протокола. Для отключения состояния MLD-протокола воспользуйтесь формой **no** этой команды.

ipv6 mld enable
no ipv6 mld 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 действует только в случае, если на интерфейсе настроен IPv6-адрес.

Пример

В данном примере показано, как включить MLD на VLAN 1.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 mld enable
Switch(config-if)#
```

59.2 ipv6 mld last-listener-query-count

Данная команда используется, чтобы установить количество запросов принадлежности к указанной группе (group-specific queries) или запросов с указанием источника и группы (group-and-source-specific queries), отправленных прежде, чем маршрутизатор обнаружит отсутствие локальных участников группы. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld last-listener-query-count *VALUE*
no ipv6 mld last-listener-query-count

Параметры

VALUE	Укажите количество last member query. Доступный диапазон значений: от 1 до 7.

По умолчанию

Значение по умолчанию – 2.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Пользователь может применять данную команду, чтобы указать количество запросов принадлежности к указанной группе или запросов с указанием группы и источника, отправленных прежде, чем маршрутизатор обнаружит отсутствие локальных участников группы. Если в течение определенного времени маршрутизатор не получает сообщения report от узлов, то отправка трафика multicast-группы на интерфейс будет прекращена.

Пример

В данном примере показано, как указать количество MLD last listener query на VLAN 1000. Указанное значение – 5.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ipv6 mld last-listener-query-count 5
Switch(config-if)#
```

59.3 ipv6 mld last-listener-query-interval

Данная команда используется, чтобы настроить на интерфейсе интервал MLD last listener query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld last-listener-query-interval *SECONDS*
no ipv6 mld last-listener-query-interval

Параметры

SECONDS	Укажите интервал между запросами принадлежности к указанной группе или запросами с указанием группы и источника. Доступный диапазон значений: от 1 до 25 секунд.

По умолчанию

Значение по умолчанию – 1 секунда.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если MLD Querier получает сообщение о выходе из группы или канала, он отправляет запрос принадлежности к указанной группе или с указанием группы и источника. После того как MLD Querier получает пакет от интерфейса, запускается таймер выхода. Если таймер истек, а интерфейс так и не получил сообщение report, то членство интерфейса будет удалено из группы или канала, из которого необходимо выйти. Значение таймера выхода рассчитывается следующим образом: (last listener query interval) x (last listener query count).

Пример

В данном примере показано, как настроить интервал между last listener query на VLAN 1000. Указанное значение – 2 секунды.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ipv6 mld last-listener-query-interval 2
Switch(config-if)#
```

59.4 ipv6 mld query-interval

Данная команда позволяет указать интервал между сообщениями с общим запросом MLD, отправляемыми маршрутизатором. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld query-interval *SECONDS*
no ipv6 mld query-interval

Параметры

query-interval *SECONDS*	Укажите частоту, с которой указанный маршрутизатор будет отправлять сообщения с общим запросом MLD. 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 применима исключительно для настройки интерфейсов VLAN. Команду можно использовать для изменения интервала запроса MLD (MLD query interval) на интерфейсе.

MLD Querier отправит общий запрос с интервалом, указанным командой query interval. При получении общего запроса слушателю MLD необходимо ответить на сообщение report, чтобы заявить о своей заинтересованности в определенной multicast-группе.

Пример

В данном примере показано, как указать интервал MLD query на VLAN 1000. Указанное значение – 150 секунд.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ipv6 mld query-interval 150
Switch(config-if)#
```

59.5 ipv6 mld query-max-response-time

Данная команда используется, чтобы настроить максимальное время ответа, объявляемое в запросах MLD. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld query-max-response-time *SECONDS*
no ipv6 mld query-max-response-time

Параметры

SECONDS	Укажите максимальное время ответа, объявляемое в запросах MLD. 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

Используйте данную команду, чтобы указать период времени, в течение которого участник группы может ответить на сообщение запроса MLD, прежде чем его членство будет удалено маршрутизатором.

Пример

В данном примере показано, как настроить максимальное время ответа на запрос MLD для VLAN 1000. Указанное значение – 10 секунд.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ipv6 mld query-max-response-time 10
Switch(config-if)#
```

59.6 ipv6 mld robustness-variable

Данная команда используется для настройки robustness variable (переменной надежности), применяемой в MLD. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld robustness-variable *VALUE*

no ipv6 mld robustness-variable

Параметры

VALUE	Укажите значение переменной надежности 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

Переменная надежности обеспечивает точную настройку в соответствии с ожидаемой потерей пакетов на интерфейсе. Значение переменной надежности используется для расчета следующих интервалов между сообщениями 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).

Пользователи могут увеличить данное значение, если ожидается, что подсеть будет не нагружена.

Пример

В данном примере показано, как указать значение 3 для переменной надежности MLD (MLD robustness variable) на VLAN 1000.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ipv6 mld robustness-variable 3
Switch(config-if)#
```

59.7 ipv6 mld version

Данная команда позволяет изменить версию MLD на указанном интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld version *NUMBER*

no ipv6 mld version

Параметры

NUMBER	Укажите версию MLD: **1:** укажите, чтобы использовать на коммутаторе версию 1 MLD. **2:** укажите, чтобы использовать на коммутаторе версию 2 MLD.

По умолчанию

Версия MLD по умолчанию – 2.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

С помощью данной команды пользователь может изменить версию запроса MLD на интерфейсе.

Пример

В данном примере показано, как указать версию 1 MLD.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ipv6 mld version 1
Switch(config-if)#
```

59.8 ipv6 mld static-group

Данная команда используется, чтобы создать статическое членство на интерфейсе. Для удаления членства воспользуйтесь формой **no** этой команды.

ipv6 mld static-group *GROUP-ADDRESS*
no ipv6 mld static-group *GROUP-ADDRESS*

Параметры

GROUP-ADDRESS	Укажите IPv6-адрес multicast-группы.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы создать статическую группу MLD, если подключенный узел не поддерживает MLD-протокол.

Пример

В данном примере показано, как создать статическую группу MLD на VLAN 1000.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ipv6 mld static-group FF1E::1
Switch(config-if)#
```

59.9 show ipv6 mld groups

Данная команда используется, чтобы отобразить информацию о группе MLD на интерфейсе.

show ipv6 mld groups [*GROUP-ADDRESS* **| interface** *INTERFACE-ID***] [{detail | static}]**

Параметры

GROUP-ADDRESS	(Опционально.) Укажите IPv6-адрес группы, который необходимо отобразить. Если IPv6-адрес не указан, будет отображена информация обо всех группах MLD.
interface *INTERFACE-ID*	(Опционально.) Укажите интерфейс, который необходимо отобразить. Если интерфейс не указан, будет отображена информация о группе MLD для всех интерфейсов.
detail	(Опционально.) Укажите, чтобы отобразить подробную информацию о группе.
static	(Опционально.) Укажите, чтобы отобразить информацию о статической группе.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда позволяет отобразить информацию о multicast-группе для указанной группы или интерфейса.

Пример

В данном примере показано, как отобразить информацию о группе MLD на интерфейсе VLAN 1.

```
Switch#show ipv6 mld groups interface vlan1

Group Address                    Interface  Uptime       Expire
-------------------------------------------------------------------
FF12::1:FF00:65                  vlan1      0DT00H05M26S 0DT00H01M12S
FF12::1:FF23:86CC                vlan1      0DT00H03M26S 0DT00H01M55S
FF12::4:FF00:1                   vlan1      0DT00H04M12S Stopped
Total Entries: 3

Switch#
```

В данном примере показано, как отобразить подробную информацию о группе MLD ff12::1:ff23:86cc.

```
Switch#show ipv6 mld groups ff12::1:ff23:86cc detail

Interface     : vlan1
Group         : FF12::1:FF23:86CC
Uptime        : 0DT00H00M42S
Expires       : Stopped
Group mode    : Include
Last reporter : FE80::202:B3FF:FEF0:79D8

Group source list:
       Source Address               Uptime        Expire
       ------------------------------------------------
       2004:4::6                    0DT00H00M42S  0DT00H03M38S

       Total Source Entries: 1

Total Entries: 1

Switch#
```

В данном примере показано, как отобразить информацию о статической группе MLD.

```
Switch#show ipv6 mld groups static

Interface        Multicast Group
------------     ---------------
vlan1000         FF1E::1

Total Entries: 1

Switch#
```

Отображение параметров

Uptime	Время, прошедшее с момента создания записи, в следующем формате: [n]DT[n]H[n]M[n]S.
Expires	Время, по истечении которого запись будет удалена (если она не обновлялась), в следующем формате: [n]DT[n]H[n]M[n]S. **Stopped:** указывает, что тайм-аут данной записи не определен таймером истечения срока записи. Если маршрутизатор функционирует в режиме Include mode для группы, то срок действия записи группы будет завершен по истечении времени последней записи источника (только если режим не был изменен на Exclude mode перед истечением записи). **Static:** указывает, что запись создана вручную и тайм-аут для данной записи не указан таймером.
Group mode	Include или Exclude: режим группы зависит от типа отчетов о членстве, полученных на интерфейсе для группы.

Last reporter	Последний узел, сообщивший о принадлежности к многоадресной группе.

59.10 show ipv6 mld interface

Данная команда используется для отображения информации об MLD на коммутаторе.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите interface ID. Если интерфейс не указан, будет отображена информация об MLD для всех интерфейсов.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об MLD на всех интерфейсах.

Пример

В данном примере показано, как отобразить информацию об MLD на VLAN 1000.

```
Switch#show ipv6 mld interface vlan1000

VLAN 1000
Version                         : 2
IPv6 Address/Netmask            : FE80::260:3EFF:FE86:5649/128
MLD State                       : Enabled
Querier                          : FE80::233:1265:3322:6387
Query Interval                  : 125 seconds
Query Maximum Response Time     : 10 seconds
Robustness Variable             : 3
Last Listener Query Count       : 2
Last Listener Query Interval    : 1 seconds

Total Entries: 1

Switch#
```

Отображение параметров

Version	Версия MLD-проктокола, действующая на коммутаторе.
Querier	IP-адрес Querier на интерфейсе LAN.

60. Команды Multicast Listener Discovery (MLD) Proxy

60.1 ipv6 mld proxy

Данная команда используется для включения функции MLD Proxy. Для отключения функции MLD Proxy воспользуйтесь формой **no** этой команды.

ipv6 mld proxy
no ipv6 mld proxy

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Функция MLD Proxy работает в топологии простого дерева. Убедитесь, что в топологии нет других multicast-маршрутизаторов (за исключением proxy).

При получении пакета MLD-report с downstream-интерфейса функция MLD Proxy обновит базу данных участников, которая создается за счет объединения всех подписок на любом downstream-интерфейсе. При изменении базы данных прокси-устройство отправит незатребованные сообщения report или leave от upstream-интерфейса. Если требуется, с upstream-интерфейса также могут быть отправлены сообщения о членстве (membership reports).

Пример

В данном примере показано, как включить функцию MLD Proxy на устройстве.

```
Switch#configure terminal
Switch(config)#ipv6 mld proxy
Switch(config)#
```

60.2 ipv6 mld proxy upstream

Данная команда используется для настройки интерфейса в качестве интерфейса upstream в MLD Proxy. Для отключения функции Proxy на интерфейсе воспользуйтесь формой **no** этой команды.

ipv6 mld proxy upstream
no ipv6 mld proxy upstream

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для корректного функционирования команды необходимо предварительно сконфигурировать IPv6-адрес интерфейса. На устройстве MLD Proxy может существовать только один upstream-интерфейс. На каждом upstream-интерфейсе действует часть MLD-протокола (RFC2710, RFC3810).

Пример

В данном примере показано, как настроить VLAN 3 как действующий proxy upstream-интерфейс.

```
Switch#configure terminal
Switch(config)#interface vlan3
Switch(config-if)#ipv6 mld proxy upstream
Switch(config-if)#
```

60.3 ipv6 mld proxy downstream

Данная команда используется для настройки интерфейса в качестве интерфейса downstream в MLD Proxy. Для отключения функции Proxy на интерфейсе воспользуйтесь формой **no** этой команды.

ipv6 mld proxy downstream
no ipv6 mld proxy downstream

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для корректного функционирования команды необходимо предварительно сконфигурировать IPv6-адрес интерфейса. На устройстве MLD Proxy можно настроить несколько downstream-интерфейсов. На каждом downstream-интерфейсе действует часть MLD-протокола.

Пример

В данном примере показано, как настроить VLAN 4 как действующий proxy downstream-интерфейс.

```
Switch#configure terminal
Switch(config)#interface vlan4
Switch(config-if)#ipv6 mld proxy downstream
Switch(config-if)#
```

60.4 ipv6 mld proxy designated-forwarding

Данная команда используется для включения перенаправления на downstream-интерфейсе MLD Proxy, который не является Querier. Для отключения данной опции воспользуйтесь формой **no** этой команды.

ipv6 mld proxy designated-forwarding
no ipv6 mld proxy designated-forwarding

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для корректного функционирования команды необходимо предварительно сконфигурировать IPv6-адрес интерфейса, а также назначить интерфейс в качестве интерфейса downstream.

Во избежание локальных петель и избыточного трафика для каналов, которые несколько серверов пересылки IGMP считают downstream-каналами, функция MLD proxy использует механизм MLD Querier election, чтобы выбрать один сервер пересылки в сети LAN. Данная команда позволяет администраторам сделать устройство, не являющееся MLD querier, сервером пересылки. Используйте

конфигурацию в соответствующей топологии. Некорректное применение может привести к возникновению локальных петель или избыточного трафика.

Пример

В данном примере показано, как включить заданное перенаправление на downstream-интерфейсе VLAN 4.

```
Switch#configure terminal
Switch(config)#interface vlan4
Switch(config-if)#ipv6 mld proxy designated-forwarding
Switch(config-if)#
```

60.5 show ipv6 mld proxy

Данная команда используется для отображения настроек MLD Proxy.

show ipv6 mld proxy

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки интерфейсов upstream и downstream.

Пример

В данном примере показано, как отобразить настройки MLD Proxy на коммутаторе.

```
Switch#show ipv6 mld proxy

MLD Proxy Global State:    Enabled
Upstream Interface:        vlan14
Downstream Interface:
vlan11, vlan12(DF), vlan13(DF)

Switch#
```

60.6 show ipv6 mld proxy group

Данная команда используется для отображения multicast-групп, изученных функцией MLD Proxy.

show ipv6 mld proxy group [*GROUP-ADDRESS***]**

Параметры

GROUP-ADDRESS	Укажите групповой IPv6-адрес.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить multicast-группы, изученные при помощи функции MLD Proxy. Если не указаны дополнительные параметры, будет отображена информация обо всех группах.

Пример

В данном примере показано, как отобразить группы, изученные при помощи функции MLD Proxy.

```
Switch#show ipv6 mld proxy group

FF1E::330E:32, Exclude
Source list: 2000::2, 2000::3

FF1E::EC20:1, Include
Source list: 100::1

Total Entries: 2

Switch#
```

В данном примере показано, как отобразить подробную информацию для группы FF1E::330E:32.

```
Switch#show ipv6 mld proxy group FF1E::330E:32

FF1E::330E:32, Include
Source list: 100::1

Total Entries: 1

Switch#
```

60.7 show ipv6 mld proxy forwarding

Данная команда используется для отображения записей группового перенаправления, созданных функцией MLD Proxy.

show ipv6 mld proxy forwarding [*GROUP-ADDRESS***]**

Параметры

GROUP-ADDRESS	Укажите групповой IPv6-адрес.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду без указания адреса конкретной группы, чтобы отобразить всю информацию о перенаправлении MLD Proxy.

Пример

В данном примере показано, как отобразить информацию о перенаправлении, созданном при помощи функции MLD Proxy.

```
Switch#show ipv6 mld proxy forwarding

FF1E::330E:32, 2000::2, vlan52
outgoing interface:
vlan20, vlan30

FF1E::EC20:1, 100::1, vlan52
outgoing interface:
vlan20

Total Entries: 2

Switch#
```

В данном примере показано, как отобразить подробную информацию о группе FF1E::330E:32.

```
Switch#show ipv6 mld proxy forwarding FF1E::330E:32

FF1E::330E:32, 2000::2, vlan52
outgoing interface:
vlan20, vlan30

Total Entries: 1

Switch#
```

61. Команды Multicast Listener Discovery (MLD) Snooping

61.1 clear ipv6 mld snooping statistics

Данная команда используется для обнуления счетчиков статистики MLD Snooping на коммутаторе.

clear ipv6 mld snooping statistics {all | vlan *VLAN-ID* **| interface** *INTERFACE-ID***}**

Параметры

all	Укажите, чтобы удалить статистику IPv6 MLD Snooping для всех VLAN и портов.
vlan *VLAN-ID*	Укажите VLAN, для которой необходимо удалить статистику IPv6 MLD Snooping.
interface *INTERFACE-ID*	Укажите интерфейс, для которого необходимо удалить статистику IPv6 MLD Snooping.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы обнулить счетчики статистики MLD Snooping на коммутаторе.

Пример

В данном примере показано, как удалить всю статистику MLD Snooping.

```
Switch#clear ipv6 mld snooping statistics all
Switch#
```

61.2 ipv6 mld snooping

Данная команда используется для включения MLD Snooping. Для отключения функции MLD Snooping воспользуйтесь формой **no** этой команды.

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

Global Configuration Mode.

VLAN 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 VLAN. Настройки IGMP Snooping и MLD Snooping являются независимыми, поэтому их можно включать одновременно на одной и той же VLAN.

Пример

В примере ниже показано, как включить MLD Snooping на VLAN, доступных для данной функции.

```
Switch#configure terminal
Switch(config)#ipv6 mld snooping
Switch(config)#
```

В следующем 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)#
```

61.3 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. Для отключения данной функции воспользуйтесь формой **no** этой команды.

ipv6 mld snooping access-group *IPV6-ACCESS-LIST-NAME* **[vlan** *VLAN-ID***]**
no ipv6 mld snooping access-group [vlan *VLAN-ID***]**

Параметры

IPV6-ACCESS-LIST-NAME	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 *VLAN-ID*	(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 multicast-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 применима исключительно для настройки интерфейсов физического порта и 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 eth1/0/1
Switch(config-if)#ipv6 mld snooping access-group mld_filter
Switch(config-if)#
```

61.4 ipv6 mld snooping fast-leave

Данная команда используется для включения функции MLD Snooping Fast Leave на интерфейсе. Для отключения данной опции воспользуйтесь формой **no** этой команды.

ipv6 mld snooping fast-leave
no ipv6 mld snooping fast-leave

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, 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)#
```

61.5 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. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld snooping last-listener-query-interval *SECONDS*
no ipv6 mld snooping last-listener-query-interval

Параметры

SECONDS	Укажите максимальный интервал между сообщениями group-specific query. В том числе учитываются сообщения, отправленные в ответ на сообщения leave-group. Диапазон значений: от 1 до 25.

По умолчанию

Значение по умолчанию – 1 секунда.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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)#
```

61.6 ipv6 mld snooping limit

Данная команда используется для указания максимального количества многоадресных групп или каналов MLD Snooping, на которые может подписаться интерфейс уровня 2. Для удаления ограничения воспользуйтесь формой **no** этой команды.

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. Диапазон значений: от 1 до 256.
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 *IPv6-ACCESS-LIST-NAME*	(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 *VLAN-ID*	(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 применима исключительно для настройки интерфейсов физического порта 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 eth1/0/4
Switch(config-if)#ipv6 mld snooping limit 80 except mld_filter vlan 1000
Switch(config-if)#
```

В примере ниже 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)#
```

61.7 ipv6 mld snooping mrouter

Данная команда используется для того, чтобы настроить указанный интерфейс в качестве IPv6 multicast router-порта или порта, которому запрещено подключаться к многоадресному маршрутизатору (forbidden), на интерфейсе VLAN. Для удаления интерфейса из списка multicast

router-портов или портов, которым запрещено подключаться к многоадресному маршрутизатору (forbidden), воспользуйтесь формой **no** этой команды.

ipv6 mld snooping mrouter {interface *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -] | learn pimv6}**

no ipv6 mld snooping mrouter {interface *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -] | learn pimv6}**

Параметры

interface	Укажите диапазон интерфейсов, подключенных к многоадресным маршрутизаторам.
forbidden interface	Укажите диапазон интерфейсов, не подключенных к многоадресным маршрутизаторам.
INTERFACE-ID	Укажите интерфейс или список интерфейсов. Доступны физические интерфейсы или port-channel.
,	(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.
learn pimv6	Укажите, чтобы включить динамическое изучение на портах, подключенных к многоадресному маршрутизатору.

По умолчанию

IPv6 multicast router-порт не настроен.

Автоматическое изучение включено.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

В качестве multicast router-порта можно использовать физический порт или port-channel. Указанный порт должен являться member-портом сконфигурированной VLAN. Нельзя указать member-порт port-channel.

Multicast router-порт 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 multicast router-порта с включенной функцией MLD Snooping, а интерфейс Ethernet 1/0/2 в качестве порта, которому запрещено подключаться к многоадресному маршрутизатору (forbidden) MLD Snooping, на VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping mrouter interface eth1/0/1
Switch(config-vlan)#ipv6 mld snooping mrouter forbidden interface eth1/0/2
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)#
```

61.8 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. Воспользуйтесь формой **no** этой команды, 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 функция отключена.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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)#
```

61.9 ipv6 mld snooping proxy-reporting

Данная команда используется для включения функции Proxy Reporting. Для отключения данной функции воспользуйтесь формой **no** этой команды.

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 функция отключена.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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)#
```

61.10 ipv6 mld snooping querier

Данная команда используется для включения MLD Snooping Querier на коммутаторе. Для отключения MLD Snooping Querier воспользуйтесь формой **no** этой команды.

ipv6 mld snooping querier
no ipv6 mld snooping querier

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если система может 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)#
```

61.11 ipv6 mld snooping query-interval

Данная команда используется для того, чтобы задать интервал отправки сообщений MLD general query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld snooping query-interval *SECONDS*

no ipv6 mld snooping query-interval

Параметры

SECONDS	Укажите интервал между сообщениями MLD general query, которые отправляет указанный маршрутизатор. Диапазон значений: от 1 до 31744.

По умолчанию

Значение по умолчанию – 125 секунд.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Query interval – 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)#
```

61.12 ipv6 mld snooping query-max-response-time

Данная команда используется для настройки максимального времени ответа, анонсированного в запросах MLD snooping query. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld snooping query-max-response-time *SECONDS*
no ipv6 mld snooping query-max-response-time

Параметры

SECONDS	Укажите максимальное время ответа, анонсированное в сообщениях MLD snooping query. Диапазон значений: от 1 до 25 секунд.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применяется для настройки периода времени, в течение которого участник группы может ответить на сообщение MLD query. После истечения данного периода его принадлежность к группе будет удалена.

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)#
```

61.13 ipv6 mld snooping query-version

Данная команда используется для того, чтобы настроить версию пакетов general query, отправленного MLD Snooping Querier. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld snooping query-version *NUMBER*
no ipv6 mld snooping query-version

Параметры

NUMBER	Укажите версию пакета MLD general query, отправленного MLD Snooping Querier (1 или 2).

По умолчанию

Версия по умолчанию – 2.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить версию пакета MLD general query, отправленного MLD Snooping Querier.

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)#
```

61.14 ipv6 mld snooping rate-limit

Данная команда используется для настройки максимального количества входящих пакетов управления MLD в секунду. Для отключения данного ограничения воспользуйтесь формой **no** этой команды.

ipv6 mld snooping rate-limit *NUMBER*
no ipv6 mld snooping rate-limit

Параметры

NUMBER	Укажите максимальное количество пакетов управления MLD, обрабатываемых коммутатором на указанном интерфейсе в секунду. Диапазон значений: от 1 до 1000.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

В режиме Interface Configuration Mode данная команда применима исключительно для настройки интерфейсов физического порта и port-channel.

Используйте данную команду, чтобы указать максимальное количество пакетов ingress MLD control в секунду.

Пример

В данном примере показано, как указать максимальное количество пакетов на интерфейсе Ethernet 1/0/1 в секунду. Указанное значение – 30 пакетов.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ipv6 mld snooping rate-limit 30
Switch(config-if)#
```

В примере ниже 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)#
```

61.15 ipv6 mld snooping report-suppression

Данная команда используется для включения функции MLD Report Suppression на VLAN. Для отключения MLD Report Suppression на VLAN воспользуйтесь формой **no** этой команды.

ipv6 mld snooping report-suppression
no ipv6 mld snooping report-suppression

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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)#
```

61.16 ipv6 mld snooping robustness-variable

Данная команда используется для настройки значения robustness variable для MLD Snooping. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld snooping robustness-variable *VALUE*
no ipv6 mld snooping robustness-variable

Параметры

VALUE	Укажите значение robustness variable в диапазоне от 1 до 7.

По умолчанию

Значение по умолчанию – 2.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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)#
```

61.17 ipv6 mld snooping static-group

Данная команда используется для настройки статической группы MLD Snooping. Для удаления статической группы воспользуйтесь формой **no** этой команды.

ipv6 mld snooping static-group *IPV6-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**
no ipv6 mld snooping static-group *IPV6-ADDRESS* **[interface** *INTERFACE-ID* **[, | -]]**

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес многоадресной группы.
interface *INTERFACE-ID*	Укажите интерфейс, который необходимо использовать.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию статическая группа не сконфигурирована.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду на интерфейсе VLAN, чтобы добавить статические записи о принадлежности к группе и/или записи источника (source).

Используйте данную команду, 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 eth1/0/5
Switch(config-vlan)#
```

61.18 ipv6 mld snooping suppression-time

Данная команда используется для настройки времени блокирования дублированных сообщений MLD report или MLD leave. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld snooping suppression-time *SECONDS*

no ipv6 mld snooping suppression-time

Параметры

SECONDS	Укажите, чтобы настроить время блокирования дублированных сообщений MLD report. Диапазон значений: от 1 до 300.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Функция Report Suppression будет блокировать дублированные пакеты MLD report или MLD leave, полученные в течение времени блокирования. Чем меньше время блокирования, тем чаще будут отправляться дублированнные пакеты MLD.

Пример

В данном примере показано, как настроить время блокирования на VLAN 1000. Указанное значение – 125.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping suppression-time 125
Switch(config-vlan)#
```

61.19 ipv6 mld snooping minimum-version

Данная команда используется для настройки минимальной версии MLD, разрешенной на интерфейсе. Для удаления заданного ограничения воспользуйтесь формой **no** этой команды.

ipv6 mld snooping minimum-version 2
no ipv6 mld snooping minimum-version

Параметры

Нет.

По умолчанию

По умолчанию ограничение не установлено.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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)#
```

61.20 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 для отображения.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если параметры не указаны, 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              : v1
    Fast leave                   : Disabled (host-based)
    Report suppression           : Disabled
    Suppression time             : 10 seconds
    Proxy reporting              : Disabled (Source ::)
    Mrouter port learning        : Enabled
    Querier state                : Disabled
    Query version                : v2
    Query interval               : 125 seconds
    Max response time            : 10 seconds
    Robustness value             : 2
    Last listener query interval : 1 seconds
    Rate limit                   : 0
    Ignore topology change       : Disabled

Total Entries: 1

Switch#
```

61.21 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 *INTERFACE-ID*	(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.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об ограничениях и группе доступа MLD Snooping. Если параметры не указаны, 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
    vlan1:
      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
    vlan1:
      Access group: mld_filter
      Groups/Channel Limit: Not Configured
    vlan2:
      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#
```

61.22 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

IPV6-ADDRESS	(Опционально.) Укажите IP-адрес группы. Если IPv6-адрес не указан, будет отображена информация обо всех группах MLD Snooping.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN ID для отображения. 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.

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

vlan1, FF1E::1
Learned on port: 1/0/3

Switch#
```

61.23 show ipv6 mld snooping mrouter

Данная команда используется для отображения информации 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 для отображения. 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.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить интерфейсы динамически изученного или настроенного вручную многоадресного маршрутизатора.

Пример

В данном примере показано, как отобразить информацию о многоадресном маршрутизаторе MLD Snooping.

```
Switch#show ipv6 mld snooping mrouter

VLAN    Ports
-----   ----------------------------
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#
```

61.24 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

GROUP-ADDRESS	(Опционально.) Укажите IPv6-адрес группы для отображения.

vlan *VLAN-ID*	(Опционально.) Укажите VLAN ID для отображения.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения статически сконфигурированных групп MLD Snooping на коммутаторе. Если параметры не указаны, 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#
```

61.25 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.
INTERFACE-ID	(Опционально.) Укажите интерфейсы для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

vlan	Укажите, чтобы отобразить счетчики статистики для VLAN.
VLAN-ID	(Опционально.) Укажите VLAN ID для отображения.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статистику MLD Snooping.

Пример

В данном примере показано, как отобразить статистику MLD Snooping для интерфейсов Ethernet 1/0/4, 1/0/7 и 1/0/9.

```
Switch#show ipv6 mld snooping statistics interface eth1/0/4,1/0/7,1/0/9

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 eth1/0/9
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0


Total Entries: 3

Switch#
```

В данном примере показано, как отобразить статистику MLD Snooping для VLAN 20.

```
Switch#show ipv6 mld snooping 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#
```

62. Команды Multicast Source Discovery Protocol (MSDP)

62.1 ip msdp

Данная команда используется для включения функции MSDP. Для отключения этой функции воспользуйтесь формой **no** этой команды.

ip msdp
no ip msdp

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 функции MSDP.

Пример

В данном примере показано, как включить функцию MSDP.

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

62.2 ip msdp connect-retry-interval

Данная команда позволяет указать интервал между попытками повторной установки одноранговой сессии после сброса одноранговой сессии MSDP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip msdp connect-retry-interval *SECONDS*
no ip msdp connect-retry-interval

Параметры

SECONDS	Укажите интервал между попытками повторного подключения (в секундах). Диапазон значений: от 1 до 65535.

По умолчанию

Значение по умолчанию – 30 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Увеличенный интервал между попытками повторного подключения задерживает время между попытками повторной установки одноранговой сессии. Для максимальной эффективности укажите значение в диапазоне от 1 до 60 секунд.

Пример

В примере показано, как указать интервал между повторными подключениями со значением 50 секунд.

```
Switch#configure terminal
Switch(config)#ip msdp connect-retry-interval 50
Switch(config)#
```

62.3 ip msdp sa-originating-filter

Данная команда используется, чтобы настроить фильтр создания сообщений SA. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip msdp sa-originating-filter [list *ACCESS-LIST-NAME***]**

no ip msdp sa-originating-filter

Параметры

list *ACCESS-LIST-NAME*	(Опционально.) Укажите имя стандартного списка доступа IP, определяющего пары (S, G).

По умолчанию

По умолчанию фильтр создания сообщений SA не настроен.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Точка встречи (Rendezvous Point, RP) настраивается, чтобы включить MSDP и создать сообщения SA для всех локальных источников, зарегистрированных в RP. Если не применены дополнительные параметры, то сообщения SA, создаваемые RP, будут отклонены для всех локальных источников.

Если команда **ip msdp sa-originating-filter** настроена со списком, RP будет создавать сообщения SA для локальных источников, отправляя их только группам, которые соответствуют парам (S, G), определенным в стандартном списке доступа IP.

Пример

В данном примере показано, как настроить фильтр создания сообщений SA.

```
Switch#configure terminal
Switch(config)#ip msdp sa-originating-filter list source1
Switch(config)#
```

62.4 ip msdp sa-cache-time

Данная команда используется, чтобы указать срок хранения записей кэша SA. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip msdp sa-cache-time *SECONDS*

no ip msdp sa-cache-time

Параметры

SECONDS	Укажите срок хранения записей кэша SA. Диапазон значений: от 65 до 65535 секунд.

По умолчанию

Значение по умолчанию – 145 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Интервал между создаваемыми сообщениями – 60 секунд. Данный интервал нельзя изменить, но можно настроить срок хранения записей кэша SA с учетом возможной потери ожидаемого пакета в сети.

Пример

В данном примере показано, как настроить срок хранения записей кэша SA.

```
Switch#configure terminal
Switch(config)#ip msdp sa-cache-time 210
Switch(config)#
```

62.5 ip msdp peer

Данная команда используется для создания MSDP-узла. Для удаления MSDP-узла воспользуйтесь формой **no** этой команды.

ip msdp peer *PEER-ADDRESS* **connect-interface** *INTERFACE-ID*

no ip msdp peer *PEER-ADDRESS*

Параметры

PEER-ADDRESS	Укажите IP-адрес MSDP-узла.
connect-interface *INTERFACE-ID*	Укажите локальный интерфейс, используемый как IP-адрес источника для TCP-соединений.

По умолчанию

По умолчанию нет настроенного MSDP-узла.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

MSDP-узел указывается IP-адресом.

Пример

В данном примере показано, как создать MSDP-узел на интерфейсе VLAN 1.

```
Switch#configure terminal
Switch(config)#ip msdp peer 10.1.1.1 connect-interface vlan1
Switch(config)#
```

62.6 ip msdp peer description

Данная команда позволяет указать описание для MSDP-узла, чтобы упростить идентификацию. Для удаления описания воспользуйтесь формой **no** этой команды.

ip msdp peer description *PEER-ADDRESS STRING*
no ip msdp peer description *PEER-ADDRESS*

Параметры

PEER-ADDRESS	Укажите IP-адрес MSDP-узла.
STRING	Укажите описание для MSDP-узла.

По умолчанию

По умолчанию нет описания для MSDP-узла.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Описание должно быть указано для существующего MSDP-узла.

Пример

В данном примере показано, как указать описание для узла 10.1.1.1.

```
Switch#configure terminal
Switch(config)#ip msdp peer description 10.1.1.1 router a
Switch(config)#
```

62.7 ip msdp peer shutdown

Данная команда используется для закрытия TCP-соединения между двумя узлами. Чтобы настроить состояние no shutdown для MSDP-узла, воспользуйтесь формой **no** этой команды.

ip msdp peer shutdown *PEER-ADDRESS*
no ip msdp peer shutdown *PEER-ADDRESS*

Параметры

PEER-ADDRESS	Укажите IP-адрес MSDP-узла.

По умолчанию

По умолчанию MSDP-узел находится в состоянии **no shutdown**.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

На существующем MSDP-узле должно быть настроено состояние shutdown. Если MSDP-узел находится в состоянии shutdown, то TCP-соединение между двумя узлами не будет установлено. Если MSDP-узел находится в состоянии no shutdown, будет предпринята попытка повторной установки TCP-соединения между двумя узлами.

Пример

В данном примере показано, как настроить состояние shutdown на узле 10.1.1.1.

```
Switch#configure terminal
Switch(config)#ip msdp peer shutdown 10.1.1.1
Switch(config)#
```

62.8 ip msdp peer password

Данная команда позволяет включить шифрование пароля MD5 для TCP-соединений между двумя узлами. Для отключения шифрование пароля MD5 воспользуйтесь формой **no** этой команды.

ip msdp peer password *PEER-ADDRESS PASSWORD*
no ip msdp peer password *PEER-ADDRESS*

Параметры

PEER-ADDRESS	Укажите IP-адрес MSDP-узла.
PASSWORD	Укажите пароль MD5.

По умолчанию

По умолчанию шифрование пароля MD5 выключено.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Аутентификация MD5 должна быть настроена с одинаковыми паролями на обоих MSDP-узлах. В противном случае невозможно установить соединение между узлами.

Пример

В данном примере показано, как включить шифрование MD5 для MSDP-узла 10.1.1.1.

```
Switch#configure terminal
Switch(config)#ip msdp peer password 10.1.1.1 testmd5
Switch(config)#
```

62.9 ip msdp peer keep-alive

Данная команда позволяет указать интервал между сообщениями keep-alive, отправляемыми MSDP-узлом. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip msdp peer keep-alive *PEER-ADDRESS* **{***SECONDS* **| infinity}**
no ip msdp peer keep-alive *PEER-ADDRESS*

Параметры

PEER-ADDRESS	Укажите IP-адрес MSDP-узла.
SECONDS	Укажите интервал keep-alive для MSDP-узла. Диапазон значений: от 1 до 21845 секунд.
infinity	Укажите, чтобы никогда не отправлять сообщения keep-alive с MSDP-узла.

По умолчанию

Интервал keep-alive по умолчанию – 60 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Значение интервала keep-alive должно быть меньше времени ожидания, указанного на удаленном устройстве MSDP, с которым установлено TCP-соединение. В противном случае перед получением сообщения MSDP keep-alive TCP-соединение с удаленным устройством MSDP может быть прервано.

Пример

В данном примере показано, как указать интервал keep-alive. Указанное значение – 50 секунд.

```
Switch#configure terminal
Switch(config)#ip msdp peer keep-alive 10.1.1.1 50
Switch(config)#
```

62.10 ip msdp peer hold-time

Данная команда позволяет указать время ожидания сообщений keep-alive от других узлов, по истечении которого MSDP-узел считает их недоступными. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip msdp peer hold-time *PEER-ADDRESS* **{***SECONDS* **| infinity}**

no ip msdp peer hold-time *PEER-ADDRESS*

Параметры

PEER-ADDRESS	Укажите IP-адрес MSDP-узла.
SECONDS	Укажите время ожидания для MSDP-узла. Диапазон значений: от 3 до 65535 секунд.
infinity	Укажите, чтобы соединение между двумя узлами никогда не прерывалось.

По умолчанию

Время ожидания по умолчанию – 75 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Значение времени ожидания должно быть больше значения времени keep-alive, указанного на удаленном устройстве MSDP, с которым установлено TCP-соединение. В противном случае перед получением сообщения MSDP keep-alive соединение MSDP TCP может быть прервано.

Пример

В данном примере показано, как указать время ожидания. Настроенное значение – 60 секунд.

```
Switch#configure terminal
Switch(config)#ip msdp peer hold-time 10.1.1.1 60
Switch(config)#
```

62.11 ip msdp peer sa-filter-in

Данная команда используется для контроля сообщений SA, принимаемых от узла. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip msdp peer sa-filter-in *PEER-ADDRESS* **[list** *ACCESS-LIST-NAME***]**
no ip msdp peer sa-filter-in *PEER-ADDRESS*

Параметры

PEER-ADDRESS	Укажите IP-адрес MSDP-узла.
list *ACCESS-LIST-NAME*	(Опционально.) Укажите имя стандартного списка доступа IP, определяющего пары (S, G).

По умолчанию

По умолчанию фильтрация входящих сообщений SA не настроена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Маршрутизатор будет получать все сообщения SA от указанного узла. Если команда **ip msdp sa-filter-in** настроена без какого-либо списка доступа, все сообщения SA, отправленные с указанного узла на маршрутизатор, будут проигнорированы. Если команда **ip msdp sa-filter-in** настроена со списком, маршрутизатор будет получать только входящие сообщения SA от узла, который соответствует парам (S, G), определенным в стандартном списке доступа IP.

Пример

В данном примере показано, как настроить фильтрацию входящих сообщений SA.

```
Switch#configure terminal
Switch(config)#ip msdp peer sa-filter-in 10.1.1.1 list msdp_in
Switch(config)#
```

62.12 ip msdp peer sa-filter-out

Данная команда используется для контроля сообщений SA, перенаправленных на узел. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip msdp peer sa-filter-out *PEER-ADDRESS* **[list** *ACCESS-LIST-NAME***]**
no ip msdp peer sa-filter-out *PEER-ADDRESS*

Параметры

PEER-ADDRESS	Укажите IP-адрес MSDP-узла.
list *ACCESS-LIST-NAME*	(Опционально.) Укажите имя стандартного списка доступа IP, определяющего пары (S, G).

По умолчанию

По умолчанию фильтрация исходящих сообщений SA не настроена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Маршрутизатор перенаправляет все сообщения SA на указанный MSDP-узел. Если команда **ip msdp sa-filter-out** применяется без какого-либо списка доступа, маршрутизатор прекратит отправку сообщений SA на указанный узел. Если команда **ip msdp sa-filter-out** настроена со списком, маршрутизатор перенаправляет на указанный узел только те сообщения SA, которые соответствуют парам (S, G), определенным в стандартном списке доступа IP.

Пример

В данном примере показано, как настроить фильтрацию исходящих сообщений SA.

```
Switch#configure terminal
Switch(config)#ip msdp peer sa-filter-out 10.1.1.1 list msdp_out
Switch(config)#
```

62.13 ip msdp peer sa-filter-request

Данная команда используется для контроля сообщений SA request, которые маршрутизатор получает от определенного узла. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip msdp peer sa-filter-request *PEER-ADDRESS* **[list** *ACCESS-LIST-NAME***]**

no ip msdp peer sa-filter-request *PEER-ADDRESS*

Параметры

PEER-ADDRESS	Укажите IP-адрес MSDP-узла.
list *ACCESS-LIST-NAME*	(Опционально.) Укажите имя стандартного списка доступа IP, определяющего группу.

По умолчанию

По умолчанию фильтрация сообщений SA request не настроена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Маршрутизатор будет обрабатывать все сообщения SA request от определенного узла. Если команда **ip msdp sa-filter-request** настроена без какого-либо списка доступа, маршрутизатор прекратит обработку всех сообщений SA request от определенного узла. Если команда **ip msdp sa-filter-request** настроена со списком, маршрутизатор обрабатывает только сообщения SA request в группах request, указанных в стандартном списке доступа IP, от определенного узла.

Пример

В примере показано, как настроить фильтрацию сообщений SA request.

```
Switch#configure terminal
Switch(config)#ip msdp peer sa-filter-request 10.1.1.1
Switch(config)#
```

62.14 ip msdp peer minimum-ttl

Данная команда позволяет указать минимальное TTL-значение для сообщений SA с инкапсулированными данными, отправленных на указанный MSDP-узел. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip msdp peer minimum-ttl *PEER-ADDRESS TTL*
no ip msdp peer minimum-ttl *PEER-ADDRESS*

Параметры

PEER-ADDRESS	Укажите IP-адрес MSDP-узла.
TTL	Укажите минимальное TTL-значение для сообщений SA с инкапсулированными данными, отправленных на указанные MSDP-узлы. Диапазон значений: от 0 до 255.

По умолчанию

Значение по умолчанию – 0.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если сообщение SA отправлено с MSDP-узла, то TTL-значение снижается. Если TTL-значение меньше минимального TTL-значения MSDP-узла, на который должно быть отправлено сообщение SA, то отправки не будет.

Пример

В данном примере показано, как настроить минимальное TTL-значение.

```
Switch#configure terminal
Switch(config)#ip msdp peer minimum-ttl 10.1.1.1 100
Switch(config)#
```

62.15 ip msdp peer sa-cache-maximum

Данная команда используется для указания максимального количества записей кэша SA, изучаемых с узла. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip msdp peer sa-cache-maximum *PEER-ADDRESS* **{***COUNT* **| none}**
no ip msdp peer sa-cache-maximum *PEER-ADDRESS*

Параметры

PEER-ADDRESS	Укажите IP-адрес MSDP-узла.
COUNT	Укажите минимальное количество записей кэша SA, изучаемых с узла. Диапазон значений: от 0 до 256.
none	Укажите, чтобы количество записей кэша SA не было ограничено.

По умолчанию

По умолчанию максимальное количество записей кэша SA не ограничено (параметр **none**).

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если для максимального количества записей кэша SA установлено значение 0, коммутатор не сможет изучать записи кэша SA с узла. При достижении максимального количества записей кэша SA старые записи будут удаляться до тех пор, пока число записей не станет равным указанному максимальному количеству.

Пример

В данном примере показано, как указать максимальное количество записей кэша SA. Настроенное значение – 10.

```
Switch#configure terminal
Switch(config)#ip msdp peer sa-cache-maximum 10.1.1.1 10
Switch(config)#
```

62.16 ip msdp static-rpf

Данная команда используется для настройки MSDP-узла по умолчанию, от которого будут приниматься все сообщения MSDP. Чтобы удалить настройки RPF, воспользуйтесь формой **no** этой команды.

ip msdp static-rpf *PEER-ADDRESS* **[rp-list** *ACCESS-LIST-NAME***]**
no ip msdp static-rpf *PEER-ADDRESS*

Параметры

PEER-ADDRESS	Укажите IP-адрес MSDP-узла.
rp-list *ACCESS-LIST-NAME*	(Опционально.) Укажите имя стандартного списка доступа IP, определяющего список префиксов RP.

По умолчанию

По умолчанию статический узел RPF не указан.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Перед настройкой статического узла RPF сначала необходимо добавить MSDP-узел с помощью команды **ip msdp peer**. Если указан список префиксов RP, узлом будет статический узел RPF, который будет использоваться только для RP из списка префиксов. Если указаны несколько статических узлов RPF без списка префиксов RP, то только подключенный узел с наименьшим адресом будет активным статическим узлом RPF. Если MSDP-узел настраивался несколько раз как статический узел RPF,

действует только последняя запись настройки. При наличии только одного MSDP-узла данный узел будет действовать как статический узел RPF.

Пример

В данном примере показано, как настроить MSDP-узел 10.1.1.1 в качестве статического узла RPF.

```
Switch#configure terminal
Switch(config)#ip msdp static-rpf 10.1.1.1 rp-list rplist1
Switch(config)#
```

62.17 ip msdp mesh-group

Данная команда используется для добавления MSDP-узла в указанную группу Mesh. Чтобы удалить MSDP-узел из группы Mesh, воспользуйтесь формой **no** этой команды.

ip msdp mesh-group *PEER-ADDRESS MESH-NAME*
no ip msdp mesh-group *PEER-ADDRESS*

Параметры

PEER-ADDRESS	Укажите IP-адрес MSDP-узла.
MESH-NAME	Укажите имя группы Mesh.

По умолчанию

По умолчанию группа Mesh не указана.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Перед добавлением в группу Mesh MSDP-узел сначала должен быть добавлен с помощью команды **ip msdp peer**. Если MSDP-узел был добавлен в несколько групп Mesh, будет действовать только последняя запись конфигурации.

Пример

В данном примере показано, как добавить MSDP-узел 10.1.1.1 в группу Mesh под именем «mesh1».

```
Switch#configure terminal
Switch(config)#ip msdp mesh-group 10.1.1.1 mesh1
Switch(config)#
```

62.18 clear ip msdp peer

Данная команда используется для удаления TCP-соединения с указанным MSDP-узлом.

clear ip msdp peer [*PEER-ADDRESS***]**

Параметры

PEER-ADDRESS	(Опционально.) Укажите IP-адрес MSDP-узла.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда также применяется для сброса счетчиков статистики MSDP. Если адрес MSDP-узла не указан, TCP-соединения будут удалены со всеми MSDP-узлами.

Пример

В данном примере показано, как удалить TCP-соединение с MSDP-узлом 10.1.1.1.

```
Switch#clear ip msdp peer 10.1.1.1
Switch#
```

62.19 clear ip msdp statistics

Данная команда используется для сброса счетчиков статистики указанного MSDP-узла.

clear ip msdp statistics [*PEER-ADDRESS***]**

Параметры

PEER-ADDRESS	(Опционально.) Укажите IP-адрес MSDP-узла.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если адрес MSDP-узла не указан, будут сброшены счетчики статистики всех MSDP-узлов.

Пример

В данном примере показано, как сбросить счетчик статистики MSDP-узла 10.1.1.1.

```
Switch#clear ip msdp statistics 10.1.1.1
Switch#
```

62.20 clear ip msdp sa-cache

Данная команда используется для очистки записей кэша Source-Active (SA).

clear ip msdp sa-cache [*GROUP-ADDRESS***]**

Параметры

GROUP-ADDRESS	(Опционально.) Укажите адрес группы записи кэша SA (SA cache).

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если адрес группы не указан, будут очищены все записи кэша SA.

Пример

В данном примере показано, как очистить все записи кэша SA.

```
Switch#clear ip msdp sa-cache
Switch#
```

62.21 show ip msdp

Данная команда используется для отображения глобальных настроек MSDP.

show ip msdp

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения глобальных настроек MSDP.

Пример

В данном примере показано, как отобразить глобальные настройки MSDP.

```
Switch#show ip msdp

MSDP global state: Enabled
Connect retry interval: 30
SA cache expiry time: 210
SA originating filter: Configured, List: source1

Switch#
```

62.22 show ip msdp peer

Данная команда используется для отображения информации об MSDP-узле.

show ip msdp peer [*PEER-ADDRESS***]**

Параметры

PEER-ADDRESS	(Опционально.) Укажите IP-адрес MSDP-узла.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации об MSDP-узле. Если указан IP-адрес узла, будет отображена подробная информация об узле. Когда IP-адрес не указан, отображается краткая информация обо всех MSDP-узлах.

Пример

В данном примере показано, как отобразить краткую информацию обо всех MSDP-узлах.

```
Switch#show ip msdp peer

MSDP Peer Information:
Configured    Shutdown    Down    Connect    Listen    Up
3               0             2       0           0          1

Peer's Address      State      SA Count      Up/Down Time
10.1.1.1             Up          4              0DT03H04M11S
10.2.1.3             Down        0              -
10.2.1.3             Down        0              -

Switch#
```

В примере ниже показано, как отобразить подробную информацию об MSDP-узле 10.1.1.1.

```
Switch#show ip msdp peer 10.1.1.1

MSDP Peer Information:
MSDP peer 10.1.1.1
Description:
Mesh Group:
Static RPF: Not configured
Information About Connection Status:
   State: Up
   Password:
   Up/Down time:  0DT03H04M41S
   Connection interface: vlan1(10.1.1.3)
   Keep-alive/Hold-time interval: 60/75
   Remote/Local port: 1024/639
   The total number of times this peer transfer into Up state: 1
Information About SA messages filter:
  Incoming filter: Not configured
  Outgoing filter: Configured, List: msdp_out
  Request filter: Configured, List: -
Minimum TTL for data-encapsulated SA message: 100
```

```
The number of SAs learned from this peer: 4
The maximum number of SAs can be learned from this peer: 20
Counters of MSDP Messages:
   Count of RPF check failure: 0
   Incoming/Outgoing control messages: 20/20
   Incoming/Outgoing SA messages: 10/10
   Incoming/Outgoing SA requests: 0/0
   Incoming/Outgoing SA responses: 0/0
   Incoming/Outgoing data packets: 0/0

Switch#
```

Отображаемые параметры

MSDP Peer	Адрес удаленного MSDP-узла.
Description	Описание MSDP-узла, используемое для упрощения идентификации.
Mesh Group	Имя группы Mesh, которой принадлежит данный MSDP-узел.
Static RPF	Настройка static RPF на данном MSDP-узле.
State	Состояние TCP-соединения с данным MSDP-узлом. В RFC3618 статусы «DISABLED» и «INACTIVE» отображаются как «Down», а статус «ESTABLISHED» – как «Up».
Password	Шифрование пароля MD5 для TCP-соединения с данным MSDP-узлом.
Up/Down Time	Системное время перехода MSDP-узла в состояние / из состояния «Up». При загрузке MSDP-маршрутизатора устанавливается значение «0».
Connection interface: **vlan1(10.1.1.3)**	Локальный IP-адрес и IP-интерфейс, используемые для TCP-соединения с MSDP-узлом.
Keep-alive/Hold-time interval	Интервалы keep alive и hold time. Интервал keep alive – это интервал времени между сообщениями keep alive, отправляемыми MSDP-узлом. Интервал hold time – это интервал ожидания сообщений keep alive от других узлов, по истечении которого MSDP-узел считает их недоступными.
Remote/Local port	Удаленный порт и локальный порт для TCP-соединения между MSDP-узлами.
The total times of this peer transfer into Up state	Общее количество переходов MSDP в состояние «Up».

Incoming filter	Фильтр входящих сообщений SA, настроенный на данном узле MSDP.
Outgoing filter	Фильтр исходящий сообщений SA, настроенный на данном узле MSDP.
Request filter	Фильтр сообщений SA request, настроенный на данном узле MSDP.
Minimum TTL for data-encapsulated SA message	Минимальное значение TTL инкапсулированного пакета, которое требуется, прежде чем пакет может быть перенаправлен на данный узел.
The number of SAs learned from this peer	Количество сообщений SA, изученных с данного узла.
The maximum number of SAs can be learned from this peer	Максимальное количество сообщений SA, которые могут быть изучены с данного узла.
Count of RPF check failure	Количество сообщений SA, полученных с данного узла и не прошедших проверку Peer-RPF.
Incoming/Outgoing control messages	Количество сообщений MSDP, полученных от данного узла (за исключением инкапсулированных пакетов данных) и переданных на этот узел.
Incoming/Outgoing SA messages	Количество сообщений MSDP SA, полученных от данного узла и переданных на него.
Incoming/Outgoing SA requests	Количество сообщений MSDP SA request, полученных от данного узла и переданных на него.
Incoming/Outgoing SA responses	Количество сообщений MSDP SA response, полученных от данного узла и переданных на него.

62.23 show ip msdp sa-cache

Данная команда используется для отображения информации о кэше SA.

show ip msdp sa-cache [group *GROUP-ADDRESS***] [source** *SOURCE-ADDRESS***] [rp** *RP-ADDRESS***]**

Параметры

group *GROUP-ADDRESS*	(Опционально.) Укажите для отображения кэша SA по адресу группы.
source *SOURCE-ADDRESS*	(Опционально.) Укажите для отображения кэша SA по адресу источника.
rp *RP-ADDRESS*	(Опционально.) Укажите для отображения кэша SA по RP-адресу.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о кэше SA.

Пример

В данном примере показано, как отобразить информацию о кэше SA.

```
Switch#show ip msdp sa-cache

MSDP Source-Active Cache Information:

Group Address Source Address RP Address     Learned Peer  Up/Expire Time
230.1.1.0     192.168.120.1  192.168.122.1  10.1.1.1      0DT00H05M03S/0DT00H02M01S
230.1.1.1     192.168.120.1  192.168.122.1  10.1.1.1      0DT00H05M03S/0DT00H02M01S
230.1.1.2     192.168.120.1  192.168.122.1  10.1.1.1      0DT00H05M04S/0DT00H02M00S
230.1.1.3     192.168.120.1  192.168.122.1  10.1.1.1      0DT00H05M04S/0DT00H02M00S

Total Entries: 4

Switch#
```

62.24 show ip msdp static-rpf

Данная команда используется для отображения настроек статического узла RPF.

show ip msdp static-rpf [*PEER-ADDRESS***]**

Параметры

PEER-ADDRESS	(Опционально.) Укажите IP-адрес MSDP-узла.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения настроек статического узла RPF.

Пример

В данном примере показано, как отобразить настройки статического узла RPF.

```
Switch#show ip msdp static-rpf

MSDP Static RPF Peer Information:

Peer's Address   RP List
10.1.1.1         rplist1
10.1.2.1         msdp_rp
10.1.3.2         -

Total Entries: 3

Switch#
```

62.25 show ip msdp mesh-group

Данная команда используется для отображения настроек MSDP группы Mesh.

show ip msdp mesh-group [*PEER-ADDRESS***]**

Параметры

PEER-ADDRESS	(Опционально.) Укажите IP-адрес MSDP-узла.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения настроек MSDP группы Mesh.

Пример

В данном примере показано, как отобразить настройки MSDP группы Mesh.

```
Switch#show ip msdp mesh-group

MSDP Mesh Group Information:

Peer's Address   Group Name
10.1.1.1         group1
10.1.2.1         group1
10.1.3.2         group1

Total Entries: 3

Switch#
```

63. Команды Multicast VLAN

63.1 mvlan enable

Данная команда используется для включения функции Multicast VLAN и настройки некоторых ее параметров. Воспользуйтесь формой **no** этой команды, чтобы отключить функцию или 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)#
```

63.2 mvlan

Данная команда используется для настройки характеристик функции Multicast VLAN. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

mvlan {forward-unmatched | ignore-vlan}

no mvlan {forward-unmatched | ignore-vlan}

Параметры

forward-unmatched	Укажите, чтобы полученные пакеты управления IGMP/MLD 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 пакеты управления IGMP/MLD. Если данная функция включена, коммутатор проигнорирует VLAN полученных пакетов управления IGMP/MLD 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 примере ниже показано, как включить параметр **forward-unmatched** и не учитывать настройки VLAN.

```
Switch#configure terminal
Switch(config)#mvlan forward-unmatched
Switch(config)#mvlan ignore-vlan
Switch(config)#
```

63.3 mvlan vlan

Данная команда используется для создания Multicast VLAN. Для удаления Multicast VLAN воспользуйтесь формой **no** этой команды.

mvlan vlan *VLAN-ID*
no mvlan vlan *VLAN-ID*

Параметры

VLAN-ID	Укажите Multicast VLAN. 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)#
```

63.4 member

Данная команда используется для настройки интерфейсов в качестве портов source (источник) или receiver (получатель) для Multicast VLAN. Для удаления портов source и receiver воспользуйтесь формой **no** этой команды.

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 receiver не является member-портом 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 receiver (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 receiver для нескольких VLAN одновременно.

Ниже перечислены некоторые ограничения при настройке порта source или receiver для Multicast VLAN:

- Порт не может быть портом source и receiver одновременно в одной Multicast VLAN.
- Порты source в одной Multicast VLAN должны быть все либо с тегом, либо все без тега.
- Тегированные порты receiver не должны совпадать с нетегированными портами receiver в одной Multicast VLAN.
- Порты source в одной Multicast VLAN не должны совпадать с портами receiver 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 интерфейсы Ethernet от 1/0/1 до 1/0/4 в качестве тегированных портов receiver в Multicast VLAN 100.

```
Switch#configure terminal
Switch(config)#mvlan vlan 100
Switch(config-mvlan)#member receiver tagged eth1/0/1-4
Switch(config-mvlan)#
```

63.5 name

Данная команда используется для указания имени Multicast VLAN. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

name *VLAN-NAME*

no name

Параметры

VLAN-NAME	Укажите имя VLAN. Максимальное 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 применяется для указания имени Multicast VLAN.

Пример

В данном примере показано, как настроить имя для Multicast VLAN 100. Указанное имя – ip-tv.

```
Switch#configure terminal
Switch(config)#mvlan vlan 100
Switch(config-mvlan)#name ip-tv
Switch(config-mvlan)#
```

63.6 replace-priority

Данная команда используется для замены приоритета трафика, перенаправленного в Multicast VLAN. Чтобы отменить замену приоритета, воспользуйтесь формой **no** этой команды.

replace-priority {ipv4 *PRIORITY* **| ipv6** *PRIORITY***}**
no replace-priority {ipv4 | ipv6}

Параметры

ipv4 *PRIORITY*	Укажите, чтобы изменить приоритет многоадресных пакетов IPv4, перенаправленных в Multicast VLAN.
ipv6 *PRIORITY*	Укажите, чтобы изменить приоритет многоадресных пакетов IPv6, перенаправленных в Multicast VLAN.

По умолчанию

Нет.

Режим ввода команды

Multicast VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При использовании команды приоритет пакетов данных многоадресной рассылки, перенаправленных

в Multicast VLAN, будет перемаркирован коммутатором на значение, настроенное в данной команде. В противном случае в качестве приоритета используется значение исходного пакета.

Пример

В данном примере показано, как изменить приоритет пакетов IPv4 на значение 4.

```
Switch#configure terminal
Switch(config)#mvlan vlan 100
Switch(config-mvlan)#replace-priority ipv4 4
Switch(config-mvlan)#
```

63.7 replace-source-ip

Данная команда используется для изменения IP-адреса источника в IGMP/MLD-пакетах report, отправленных на порты uplink. Чтобы отменить замену IP-адреса источника, воспользуйтесь формой **no** этой команды.

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 пакетах управления IGMP report на портах uplink.
ipv6 *IPV6-ADDRESS*	Укажите IP-адрес источника, который необходимо использовать для замены в пакетах управления MLD 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 применяется для передачи информации о подключениях к порту source во избежание отбрасывания пакетов управления (control) маршрутизатором uplink во время проверок IP Spoofing.

Для замены 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)#
```

63.8 mvlan group-profile

Данная команда используется, чтобы создать профиль группы для функции Multicast VLAN. Для удаления одного или всех профилей группы воспользуйтесь формой **no** этой команды.

mvlan group-profile *PROFILE-NAME*
no mvlan group-profile {*PROFILE-NAME* **| all}**

Параметры

PROFILE-NAME	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 применяется 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)#
```

63.9 access-group

Данная команда используется для привязки профиля группы доступа к Multicast VLAN. Для удаления привязки воспользуйтесь формой **no** этой команды.

access-group *PROFILE-NAME*
no access-group *PROFILE-NAME*

Параметры

PROFILE-NAME	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)#
```

63.10 range

Данная команда используется, чтобы настроить диапазон многоадресных адресов для профиля Multicast VLAN. Для удаления диапазона воспользуйтесь формой **no** этой команды.

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

IPV4-ADDRESS-START	Укажите начальный многоадресный IPv4-адрес в диапазоне.
IPV4-ADDRESS-END	Укажите конечный многоадресный IPv4-адрес в диапазоне.
IPV6-ADDRESS-START	Укажите начальный многоадресный IPv6-адрес в диапазоне.
IPV6-ADDRESS-END	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)#
```

63.11 show mvlan group-profile

Данная команда используется для отображения настроек профиля группы многоадресной рассылки.

show mvlan group-profile [*PROFILE-NAME***]**

Параметры

PROFILE-NAME	(Опционально.) Укажите имя профиля.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

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#
```

63.12 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.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду без указания VLAN ID, чтобы отобразить информацию обо 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#
```

63.13 show mvlan

Данная команда используется для отображения настроек Multicast VLAN.

show mvlan [*VLAN-ID***]**

Параметры

VLAN-ID	(Опционально.) Укажите VLAN ID.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если параметры не указаны, будут отображены настройки и информация обо всех Multicast VLAN.

Пример

В данном примере показано, как отобразить настройки и информацию обо 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 пакетов управления IGMP 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 пакетах управления IGMP/MLD перед их отправкой в Multicast VLAN.

64. Команды Multiple Spanning Tree Protocol (MSTP)

64.1 instance

Данная команда используется для сопоставления VLAN с экземпляром MST (Multiple Spanning Tree). Для удаления указанного экземпляра MST воспользуйтесь командой **no instance** *INSTANCE-ID*. Для возврата VLAN к экземпляру по умолчанию (CIST) воспользуйтесь командой **no instance** *INSTANCE-ID* **vlans** *VLAND-ID* **[, | -]**.

instance *INSTANCE-ID* **vlans** *VLAN-ID* **[, | -]**
no instance *INSTANCE-ID* **[vlans** *VLAN-ID* **[, | -]]**

Параметры

INSTANCE-ID	Укажите идентификатор экземпляра MSTP, сопоставляемый с указанными VLAN. Диапазон значений: от 1 до 64.
VLAN-ID	Укажите VLAN ID для настройки.
,	(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 сопоставляются с CIST (экземпляр 0).

Режим ввода команды

MST Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для сопоставления VLAN с экземпляром MST. Если экземпляр не существует, то при сопоставлении VLAN с экземпляром MST он будет создан автоматически.

Пример

В примере показано, как сопоставить VLAN с экземпляром MST.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance 2 vlans 1-100
Switch(config-mst)#
```

64.2 name

Данная команда используется для настройки имени региона MST (MST region). Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

name *NAME*
no name

Параметры

NAME	Укажите имя региона MST. Максимальное 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

Данная команда применяется для настройки имени региона MST. При наличии более одного коммутатора с одним и тем же сопоставлением VLAN и номером версии настройки, но с различными именами региона, считается, что данные коммутаторы находятся в разных регионах MST.

Пример

В примере показано, как настроить имя региона MST – «MSTP».

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#name MSTP
Switch(config-mst)#
```

64.3 revision

Данная команда используется, чтобы указать номер ревизии для конфигурации MST. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

revision *REVISION*
no revision

Параметры

REVISION	Укажите другую ревизию, если используется одно и то же имя. 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

Данная команда применяется, чтобы указать номер ревизии для конфигурации MST. При наличии более одного коммутатора с одинаковыми настройками, но с различными ревизиями, считается, что данные коммутаторы находятся в разных регионах MST.

Пример

В данном примере показано, как указать ревизию «2» для конфигурации MST.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#revision 2
Switch(config-mst)#
```

64.4 show spanning-tree mst

Данная команда используется для отображения информации об экземплярах и MST.

show spanning-tree mst [configuration [digest]]

show spanning-tree mst [instance *INSTANCE-ID* **[, | -]] [interface** *INTERFACE-ID* **[, | -]] [detail]**

Параметры

configuration	(Опционально.) Укажите для отображения текущей конфигурации MST оборудования.
digest	(Опционально.) Укажите для отображения MD5 digest, включенного в идентификатор настройки текущего MST (MSTCI).
instance *INSTANCE-ID*	(Опционально.) Укажите номер экземпляра для отображения.

,	(Опционально.) Используется для перечисления нескольких экземпляров или отделения одного диапазона экземпляров от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона экземпляров. Пробелы до и после дефиса недопустимы.
interface *INTERFACE-ID*	(Опционально.) Укажите ID интерфейса для отображения.
,	(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.
detail	(Опционально.) Укажите для отображения подробной информации об MST.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации об MST.

Пример

В данном примере показано, как отобразить информацию о настройках spanning tree на интерфейсе Ethernet 1/0/1.

```
Switch#show spanning-tree mst configuration

 Name      : F0:7D:68:34:00:10
 Revision  : 0,Instances configured: 1
 Instance    Vlans
 -------     ------------------------------------------------------------
      0      1-4094

Switch#
```

64.5 spanning-tree mst

Данная команда позволяет настроить стоимость пути и приоритет порта для экземпляра MST. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

spanning-tree mst *INSTANCE-ID* **{cost** *COST* **| port-priority** *PRIORITY***}**
no spanning-tree mst *INSTANCE-ID* **{cost | port-priority}**

Параметры

INSTANCE-ID	Укажите идентификатор экземпляра MSTP. Диапазон значений: от 0 до 64. Экземпляр 0 – это экземпляр по умолчанию, CIST.
cost *COST*	Укажите стоимость пути экземпляра. Диапазон значений: от 1 до 200000000.
port-priority *PRIORITY*	Укажите приоритет порта экземпляра. Диапазон значений: от 0 до 240 с шагом 16.

По умолчанию

Стоимость указывается на основе скорости порта. Чем выше скорость, тем меньше стоимость пути. MST всегда использует стоимость «длинного» пути (long path cost).

Приоритет порта – 128.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физических портов.

Пример

В данном примере показано, как настроить стоимость пути интерфейса.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

В примере ниже показано, как настроить приоритет порта.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#spanning-tree mst 0 port-priority 64
Switch(config-if)#
```

64.6 spanning-tree mst configuration

Данная команда используется для входа в режим MST Configuration Mode и настройки региона MSTP (MSTP region). Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

spanning-tree mst configuration

no spanning-tree mst configuration

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для входа в режим MST Configuration Mode.

Пример

В данном примере показано, как войти в режим MST Configuration Mode.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#
```

64.7 spanning-tree mst max-hops

Данная команда используется, чтобы указать максимальное число переходов для служебных пакетов MSTP. Для возврата к настройками по умолчанию воспользуйтесь формой **no** этой команды.

spanning-tree mst max-hops *HOP-COUNT*

no spanning-tree mst max-hops

Параметры

HOP-COUNT	Укажите максимальное число переходов для служебных пакетов MSTP. Диапазон значений: от 1 до 40.

По умолчанию

Максимальное число переходов по умолчанию – 20.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применяется, чтобы указать максимальное число переходов для служебных пакетов MSTP.

Пример

В данном примере показано, как указать максимальное число переходов для служебных пакетов MSTP.

```
Switch#configure terminal
Switch(config)#spanning-tree mst max-hops 19
Switch(config)#
```

64.8 spanning-tree mst hello-time

Данная команда используется, чтобы указать интервал отправки hello-сообщений, используемых в версии MSTP для определенного порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

spanning-tree mst hello-time *SECONDS*
no spanning-tree mst hello-time

Параметры

SECONDS	Укажите интервал отправки одного BPDU на указанном порту. Диапазон значений: от 1 до 2 секунд.

По умолчанию

По умолчанию интервал отправки hello-сообщений – 2 секунды.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применяется, чтобы указать интервал отправки hello-сообщений, используемых в версии MSTP для определенного порта. Данная команда действует только в режиме MSTP.

Пример

В данном примере показано, как указать интервал отправки hello-сообщений, используемых в версии MSTP, на интерфейсе Ethernet 1/0/1.

```
Switch(config)#interface eth1/0/1
Switch(config-if)#spanning-tree mst hello-time 1
Switch(config-if)#
```

64.9 spanning-tree priority

Данная команда позволяет указать значение приоритета моста для выбранного экземпляра MSTP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

spanning-tree mst *INSTANCE-ID* **priority** *PRIORITY*
no spanning-tree mst *INSTANCE-ID* **priority**

Параметры

INSTANCE-ID	Укажите идентификатор экземпляра MSTP. Экземпляр 0 − это экземпляр по умолчанию, CIST.
PRIORITY	Указывает, что приоритет моста и MAC-адрес моста вместе образуют Spanning-Tree Bridge-ID, который является важным фактором в топологии Spanning-Tree. Диапазон значений: от 0 до 61440.

По умолчанию

Значение по умолчанию – 32768.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Приоритет имеет то же значение, что и приоритет моста в справочнике команд STP, но можно указать другое значение приоритета для разных экземпляров MSTP.

Пример

В данном примере показано, как указать приоритет моста для экземпляра MSTP 2.

```
Switch#configure terminal
Switch(config)#spanning-tree mst 2 priority 0
Switch(config)#
```

65. Команды Neighbor Discovery (ND) Inspection

65.1 ipv6 nd inspection policy

Данная команда используется для создания политики ND Inspection Policy и для входа в режим ND Inspection Policy Configuration Mode. Чтобы удалить политику ND Inspection Policy, воспользуйтесь формой **no** этой команды.

ipv6 nd inspection policy *POLICY-NAME*
no ipv6 nd inspection policy *POLICY-NAME*

Параметры

POLICY-NAME	Укажите имя политики ND Inspection Policy.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы создать политику ND Inspection Policy и войти в режим ND Inspection Policy Configuration Mode. ND Inspection предназначена для проверки сообщений Neighbor Solicitation (NS) и Neighbor Advertisement (NA).

Пример

В данном примере показано, как создать политику ND под именем «policy1».

```
Switch#configure terminal
Switch(config)#ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#
```

65.2 validate source-mac

Данная команда используется для проверки MAC-адреса на соответствие адресу Link Layer для ND-сообщений. Чтобы отменить проверку, воспользуйтесь формой **no** этой команды.

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 на коммутаторе будет получено 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)#
```

65.3 device-role

Данная команда используется для указания роли подключенного устройства. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

device-role {host | router}
no device-role

Параметры

host	Укажите, чтобы настроить устройство в качестве узла.
router	Укажите, чтобы настроить устройство в качестве маршрутизатора.

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)#
```

65.4 mode

Данная команда используется для настройки режима ND Inspection. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

mode {precise | fuzzy}
no mode

Параметры

precise	Укажите, чтобы использовать режим precise.
fuzzy	Укажите, чтобы использовать режим fuzzy.

По умолчанию

Режим по умолчанию – precise.

Режим ввода команды

ND Inspection Policy Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы указать режим ND Inspection. Если выбран режим **precise**, ND Inspection будет проверять, соответствует ли адрес назначения в пакетах DANA/NA адресу источника. Если выбран режим **fuzzy**, ND Inspection будет проверять, существуют ли адрес назначения и адрес источника в таблице привязок.

Пример

В данном примере показано, как создать политику ND под именем «policy1» и выбрать режим **fuzzy**.

```
Switch#configure terminal
Switch(config)#ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#mode fuzzy
Switch(config-nd-inspection)#
```

65.5 ipv6 nd inspection attach-policy

Данная команда используется для применения политики ND Inspection Policy на определенном интерфейсе. Чтобы удалить политику ND Inspection Policy, воспользуйтесь формой **no** этой команды.

ipv6 nd inspection attach-policy [*POLICY-NAME***]**
no ipv6 nd inspection attach-policy

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики ND Inspection Policy.

По умолчанию

По умолчанию политика ND Inspection Policy не применена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов 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 eth1/0/3
Switch(config-if)#ipv6 nd inspection attach-policy policy1
Switch(config-if)#
```

65.6 show ipv6 nd inspection policy

Данная команда используется для отображения информации о политике ND Inspection Policy.

show ipv6 nd inspection policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики ND Inspection Policy.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если имя политики указано, отображаться будет информация только для указанной политики. Если имя политики не указано, отображаться будет информация для всех политик.

Пример

В данном примере показано, как отобразить конфигурацию политики под именем «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#
```

66. Команды Network Access Authentication

66.1 authentication guest-vlan

Данная команда используется для настройки Guest VLAN. Чтобы удалить Guest VLAN, воспользуйтесь формой **no** этой команды.

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. Если один узел проходит аутентификацию, порт останется в Guest VLAN, а PVID порта не будет изменен.

Если Guest VLAN отключена, порт выйдет из Guest VLAN и вернется к 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 eth1/0/1
Switch(config-if)#authentication guest-vlan 5
Switch(config-if)#
```

66.2 authentication host-mode

Данная команда используется для указания режима аутентификации. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

authentication host-mode {multi-host | multi-auth [vlan *VLAN-ID* **[, | -]]}**

no authentication host-mode [multi-auth vlan *VLAN-ID* **[, | -]]**

Параметры

multi-host	Укажите порт для работы в режиме multi-host. Выполняется только одна аутентификация, и все хосты, подключенные к порту, будут разрешены.
multi-auth	Укажите порт для работы в режиме multi-auth. Каждый узел будет проходить аутентификацию индивидуально.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN аутентификации. Это может быть полезно, если различные VLAN на коммутаторе имеют различные требования к аутентификации. При использовании формы **no** все VLAN будут удалены, если не указаны конкретные. Это значит, что не важно, из какой VLAN клиент, клиент будет аутентифицирован, если MAC-адрес клиента (независимо от VLAN) не аутентифицирован. После аутентификации клиенту не нужно будет проходить повторную аутентификацию из других VLAN. Данная опция полезна для управления аутентификацией per-VLAN для портов trunk. Если режим аутентификации порта меняется на multi-host, предыдущие VLAN аутентификации на этом порту будут удалены.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одной 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 блокироваться на период молчания (quiet period). Порт восстановит обработку пакетов EAPOL после периода молчания.

Если порт работает в режиме **multi-auth**, каждый узел должен проходить аутентификацию индивидуально для доступа к порту. Узел представлен своим MAC-адресом. Доступ есть только у авторизованных узлов.

Пример

В данном примере показано, как назначить режим multi-host для интерфейса Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication host-mode multi-host
Switch(config-if)#
```

66.3 authentication periodic

Данная команда используется для включения периодического повторения аутентификации для порта. Для отключения периодического повторения аутентификации воспользуйтесь формой **no** этой команды.

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 интерфейса Ethernet 1/0/1.

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

66.4 authentication timer inactivity

Данная команда используется для настройки таймера бездействия, по истечении которого неактивная сессия будет завершена. Для отключения таймера бездействия воспользуйтесь формой **no** этой команды.

authentication timer inactivity {*SECONDS***}**

no authentication timer inactivity

Параметры

SECONDS	Укажите время, после которого неактивная сессия будет завершена. 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. Значение таймера бездействия (inactivity timer) должно быть меньше, чем значение таймера, настроенного с помощью команды **authentication timer reauthentication**.

Пример

В данном примере показано, как настроить значение таймера бездействия для интерфейса Ethernet 1/0/1. Указанное значение – 240.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication timer inactivity 240
Switch(config-if)#
```

66.5 authentication timer reauthentication

Данная команда используется для настройки таймера, по истечении которого будет необходимо пройти повторную аутентификацию. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

authentication timer reauthentication {*SECONDS***}**

no authentication timer reauthentication

Параметры

SECONDS	Укажите время, по истечении которого будет необходимо пройти повторную аутентификацию. Диапазон значений: от 1 до 65535.

По умолчанию

Значение по умолчанию – 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**, чтобы определить, будет ли производиться повторная аутентификация.

Пример

В данном примере показано, как настроить значение таймера повторной аутентификации для интерфейса Ethernet 1/0/1. Указанное значение – 200.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication timer reauthentication 200
Switch(config-if)#
```

66.6 authentication timer restart

Данная команда используется для настройки таймера, по истечении которого станет возможна повторная аутентификация после последней неудачной попытки. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

authentication timer restart *SECONDS*

no authentication timer restart

Параметры

SECONDS	Укажите время, по истечении которого станет возможна повторная аутентификация. Диапазон значений: от 1 до 65535.

По умолчанию

Значение по умолчанию – 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, пока не истечет таймер.

Пример

В данном примере показано, как настроить значение таймера повторной аутентификации для интерфейса Ethernet 1/0/1. Указанное значение – 20.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication timer restart 20
Switch(config-if)#
```

66.7 authentication username

Данная команда используется для создания пользователя в локальной базе данных аутентификации. Чтобы удалить пользователя из локальной базе данных аутентификации, воспользуйтесь формой **no** этой команды.

authentication username *NAME* **password [0 | 7]** *PASSWORD* **[vlan** *VLAN-ID***]**

no authentication username *NAME* **[vlan]**

Параметры

NAME	Укажите имя пользователя. Максимальное количество символов – 32.
0	(Опционально.) Пароль в обычном текстовом виде. Если не указан ни 0, ни 7, по умолчанию паролем будет обычный текст.
7	(Опционально.) Зашифрованный пароль. Если не указан ни 0, ни 7, по умолчанию паролем будет обычный текст.
password *PASSWORD*	Укажите, чтобы задать пароль для MAC-аутентификации. Если указан пароль в обычном текстовом виде, длина строки не может превышать 32 символа.
vlan *VLAN-ID*	(Опционально.) Укажите, чтобы назначить VLAN.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы настроить локальную базу 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)#
```

66.8 clear authentication sessions

Данная команда используется для удаления сессий аутентификации.

clear authentication sessions {mac | wac | dot1x | all | interface *INTERFACE-ID* **[mac | wac | dot1x] |**
mac-address *MAC-ADDRESS***}**

Параметры

mac	Укажите для удаления всех MAC-сессий.
wac	Укажите для удаления всех WAC-сессий.
dot1x	Укажите для удаления всех сессий dot1x.
all	Укажите для удаления всех сессий.
interface *INTERFACE-ID*	Укажите для удаления сессий порта.
mac-address *MAC-ADDRESS*	Укажите для удаления 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 интерфейсе Ethernet 1/0/1.

```
Switch#clear authentication sessions interface eth1/0/1
Switch#
```

66.9 authentication username mac-format

Данная команда используется для настройки формата MAC-адреса, который будет использоваться при аутентификации через RADIUS-сервер в качестве имени пользователя. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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: AA-BB-CC-DD-EE-FF
colon	Укажите, чтобы использовать «:» в качестве разделителя: AA:BB:CC:DD:EE:FF
dot	Укажите, чтобы использовать «.» в качестве разделителя: AA.BB.CC.DD.EE.FF
none	Укажите, чтобы не использовать разделитель: AABBCCDDEEFF
number	Укажите количество знаков разделения: **1:** один разделитель: AABBCC.DDEEFF **2:** два разделителя: AABB.CCDD.EEFF **5:** пять разделителей: AA.BB.CC.DD.EE.FF Если выбран параметр none, знаки разделения 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)#
```

66.10 authentication compauth mode

Данная команда используется для указания режима Compound Authentication Mode. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 интерфейса Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication compauth mode mac-wac
Switch(config-if)#
```

66.11 authentication max users

Данная команда используется для настройки максимального количества аутентифицированных пользователей для всей системы или для порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

authentication max users *NUMBER*
no authentication max users

Параметры

NUMBER	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

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 следующие ограничения:

- 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)#
```

66.12 authentication mac-move deny

Данная команда используется для запрета MAC move на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

authentication mac-move deny
no authentication mac-move deny

Параметры

Нет.

По умолчанию

По умолчанию данная опция разрешена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда разрешает/запрещает аутентифицированным узлам перемещаться по различным портам коммутатора. Команда позволяет настроить управление таким образом, чтобы только узлу, аутентифицированному на порту в режиме **multi-auth**, было разрешено перемещаться к другому порту.

Если узлу разрешено перемещаться, может возникнуть две ситуации. Он может быть либо повторно аутентифицирован, либо он напрямую переместится на новый порт без повторной аутентификации на основе следующего правила. Если новый порт имеет ту же настройку аутентификации, что и оригинальный (исходный) порт, повторная аутентификация не требуется. Узел наследует те же атрибуты авторизации для нового порта. Аутентифицированный узел может перемещаться от порта 1 к порту 2 с теми же атрибутами авторизации без необходимости повторной аутентификации. Если у нового порта настройки аутентификации отличны от оригинального порта, то будет необходима повторная аутентификация. Аутентифицированный узел на порту 1 может переместиться и быть повторно аутентифицированным на порту 2. Если на новом порту не включен метод аутентификации, то узел напрямую может переместиться на него. Сессия с оригинальным портом будет удалена. Аутентифицированный узел можно переместить с порта 1 на порт 2.

Если функция MAC move отключена и аутентифицированный узел перемещается на другой порт, это расценивается как нарушение правила.

Пример

В данном примере показано, как включить MAC move на коммутаторе.

```
Switch#configure terminal
Switch(config)#authentication mac-move deny
Switch(config)#
```

66.13 authorization disable

Данная команда используется для отключения приема авторизованной конфигурации. Чтобы включить принятие авторизованной конфигурации, воспользуйтесь формой **no** этой команды.

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)#
```

66.14 show authentication sessions

Данная команда используется для просмотра информации об аутентификации.

show authentication sessions [mac | wac | dot1x | interface *INTERFACE-ID* **[, | -] [mac | wac | dot1x] |**

mac-address *MAC-ADDRESS***]**

Параметры

mac	(Опционально.) Укажите для отображения всех MAC-сессий.
wac	(Опционально.) Укажите для отображения всех WAC-сессий.
dot1x	(Опционально.) Укажите для отображения всех сессий dot1x.
interface *INTERFACE-ID*	(Опционально.) Укажите порт для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
mac-address *MAC-ADDRESS*	(Опционально.) Укажите для отображения определенного пользователя.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

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 интерфейсе Ethernet 1/0/1.

```
Switch#show authentication sessions interface eth1/0/1

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 помощью данного метода **Success** – узел прошел аутентификацию с помощью данного метода аутентификации **Selected** – результат аутентификации данного метода, берется и анализируется системой для узла. **Failure** – узел не прошел аутентификацию с помощью данного метода **No Information** – информация об аутентификации недоступна.
Aging Time/Block Time	**Aging Time** – время старения, период времени, во время которого аутентифицированный узел будет сохраняться в аутентифицированном состоянии. По истечении данного времени узел будет возвращен в не аутентифицированное состояние. **Blocked Time** – если узел не смог пройти аутентификацию, следующая попытка не начнется, пока не истечет время блокировки, если только пользователь не очистит состояние ввода entry state вручную.
Idle Time	Оставшееся время сессии аутентификации, которое будет завершено, если сессия неактивна в течение настроенного периода времени. Доступно только для сессий WEB.

802.1X Authenticator State	Состояние аутентификатора PAE 802.1X: возможны следующие значения: **INITIALIZE** – аутентификатор в процессе инициализации и ожидает запросов на аутентификацию. **DISCONNECTED** – инициализация завершена, но ни одно запрашивающее устройство не подключено к порту. **CONNECTING** – коммутатор обнаружил, что запрашивающее устройство подключается к порту. PAE произведет попытку установить подключение с запрашивающим устройством. **AUTHENTICATING** – запрашивающее устройство проходит аутентификацию. **AUTHENTICATED** – аутентификатор успешно аутентифицировал запрашивающее устройство. **ABORTING** – процедура аутентификации преждевременно отменена из-за запроса на повторную авторизацию, кадра EAPOL-Start, EAPOL-Logoff или тайм-айта аутентификации. **HELD** – коммутатор игнорирует или отбрасывает все EAPOL-пакеты для защиты от атак. В данное состояние можно перейти из состояния AUTHENTICATING после ошибки аутентификации. **FORCE_AUTH** – запрашивающее устройство всегда авторизовано **FORCE_UNAUTH** – запрашивающее устройство всегда не авторизовано.
802.1X Backend State	Состояние Backend PAE 802.1X. Возможны следующие значения: **REQUEST** – коммутатор получил пакет EAP-запроса от сервера аутентификации, и отправил пакет запрашивающему устройству в качестве EAPOL-инкапсулированного кадра. **RESPONSE** – коммутатор получил EAPOL-инкапсулированный пакет EAP-ответа от запрашивающего устройства и отправил EAP-пакет серверу аутентификации. **SUCCESS** – сервер аутентификации подтвердил, что запрашивающее устройство является допустимым клиентом. Backend уведомит аутентификатор PAE и запрашивающее устройство. **FAIL** – сервер аутентификации подтвердил, что запрашивающее устройство является недопустимым клиентом. Backend уведомит конечный автомат аутентификатор PAE и запрашивающее устройство. **TIMEOUT** – на сервере аутентификации или запрашивающем устройстве есть тайм-аут. **IDLE** – коммутатор ожидает начала новой сессии аутентификации. **INITIALIZE** – аутентификатор производит инициализацию.

67. Команды Network Load Balancing (NLB)



Примечание: когда функция NLB включена, порты-участники группы агрегирования (Link Aggregation) не могут существовать на различных коммутаторах в физическом стеке.

67.1 nlb unicast-fdb

Данная команда используется для добавления одноадресной (unicast) NLB-записи в таблицу MAC-адресов (FDB). Чтобы удалить одноадресную NLB-запись из таблицы MAC-адресов (FDB) или удалить интерфейсы из NLB-записи, воспользуйтесь формой **no** этой команды.

nlb unicast-fdb *MAC-ADDR* **interface** *INTERFACE-ID* **[, | -]**
no nlb unicast-fdb *MAC-ADDR* **[interface** *INTERFACE-ID* **[, | -]]**

Параметры

MAC-ADDR	Укажите MAC-адрес 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 *INTERFACE-ID*	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 (unicast) MAC-адрес.
- **Multicast Mode**: клиент для доступа к серверу в качестве MAC-адреса назначения использует групповой (multicast) MAC-адрес.

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 eth1/0/1-5
Switch(config)#
```

67.2 nlb multicast-fdb

Данная команда используется для добавления NLB-записи в таблицу групповых адресов. Чтобы удалить NLB-запись из таблицы групповых адресов или удалить интерфейсы из записи NLB multicast, воспользуйтесь формой **no** этой команды.

nlb multicast-fdb *MAC-ADDR* **vlan** *VLAN-ID* **interface** *INTERFACE-ID* **[, | -]**
no nlb multicast-fdb *MAC-ADDR* **vlan** *VLAN-ID* **[interface** *INTERFACE-ID* **[, | -]]**

Параметры

MAC-ADDR	Укажите групповой MAC-адрес записи. Полученный пакет, MAC-адрес назначения которого соответствует указанному MAC-адресу, будет перенаправлен на указанные интерфейсы.
vlan *VLAN-ID*	Укажите VLAN ID записи. Диапазон значений: от 1 до 4094.
interface *INTERFACE-ID*	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. NLB-запись 01:00:5E:xx:xx:xx (MAC-адрес, привязанный к многоадресной рассылке IPv4) имеет более высокий приоритет.

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 eth1/0/1-5
Switch(config)#
```

67.3 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.

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#
```

68. Команды Network Protocol Port Protection

68.1 network-protocol-port protect

Данная команда используется, чтобы включить функцию защиты порта сетевого протокола. Для отключения функции воспользуйтесь формой **no** этой команды.

network-protocol-port protect {tcp | udp}

no network-protocol-port protect {tcp | udp}

Параметры

tcp	Укажите для защиты TCP-порта.
udp	Укажите для защиты UDP-порта.

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применяется, чтобы включить или отключить функцию защиты порта сетевого протокола.

Пример

В данном примере показано, как включить защиту TCP-порта.

```
Switch#configure terminal
Switch(config)#network-protocol-port protect tcp
Switch(config)#
```

68.2 show network-protocol-port protect

Данная команда используется для отображения информации о защите порта сетевого протокола.

show network-protocol-port protect

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда применяется для отображения информации о защите порта сетевого протокола.

Пример

В данном примере показано, как отобразить информацию о защите порта сетевого протокола.

```
Switch#show network-protocol-port protect

    TCP Port protect state: Enabled
    UDP Port protect state: Enabled

Switch#
```

69. Команды Network Time Protocol (NTP)

69.1 ntp access-group

Данная команда используется для управления службами NTP на коммутаторе. Чтобы отменить управление доступом служб NTP, воспользуйтесь формой **no** этой команды.

ntp access-group {default | *IP-ADDRESS* [*IP-MASK*] | *IPV6-ADDRESS* | *IPV6-ADDRESS* /*IPREFIX-LENGTH*} [ignore] [nomodify] [noquery] [nopeer] [noserve] [notrust] [version]

no ntp access-group {default | *IP-ADDRESS* [*IP-MASK*] | *IPV6-ADDRESS* | *IPV6-ADDRESS* /*IPREFIX-LENGTH*}

Параметры

default	Укажите, чтобы использовать IPv4-адрес (0.0.0.0/0.0.0.0) или IPv6-адрес (::/::) address по умолчанию. У IP-адреса по умолчанию всегда самый низкий приоритет в списке.
IP-ADDRESS	Укажите IP-адрес узла или сети.
IP-MASK	(Опционально.) Укажите маску IP-адреса.
IPV6-ADDRESS	Укажите IPv6-адрес узла или сети.
IPV6-ADDRESS /PREFIX-LENGTH	(Опционально.) Укажите длину префикса IPv6.
ignore	(Опционально.) Укажите, чтобы запретить доступ всем пакетам, включая NTP Control Queries.
nomodify	(Опционально.) Укажите, чтобы запретить доступ NTP Control Queries, которые пытаются изменить состояние сервера.
noquery	(Опционально.) Укажите, чтобы запретить доступ всем NTP Control Queries.
nopeer	(Опционально.) Укажите, чтобы запретить доступ пакетам, которые могут быть ассоциированы без аутентификации. Пакеты могут быть: broadcast, symmetric-active и manycast. Обратите внимание, что данный параметр применяется только к пакетам, которые могут быть ассоциированы.
noserve	(Опционально.) Укажите, чтобы запретить доступ всем пакетам, кроме NTP Control Queries.

notrust	(Опционально.) Укажите, чтобы запретить доступ пакетам, которые не прошли криптографическую аутентификацию. Если команда **ntp authenticate** включена, аутентификация проводится для всех пакетов, которые могут запустить ассоциацию. Если команда **ntp authenticate** отключена, но не присутствует параметр **notrust**, ассоциация может быть запущена независимо от того, аутентифицирован пакет или нет. Если команда **ntp authenticate** отключена, но параметр **notrust** указан, аутентификация требуется только для указанного диапазона адресов/масок.
version	(Опционально.) Укажите, чтобы запретить доступ пакетам, не соответствующим текущей NTP-версии.

По умолчанию

Для записи по умолчанию применены параметры **noquery** и **nomodify**, чтобы защититься от DoS-атак в службе NTP, указанной в «NTP.Monlist.Command.DoS».

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/соответствий. 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 128.175.0.0 255.255.0.0
Switch(config)#ntp access-group 128.4.1.0 255.255.255.0 notrust
Switch(config)#ntp access-group 192.43.244.18
Switch(config)#
```

69.2 ntp authenticate

Данная команда используется для включения NTP-аутентификации. Чтобы отключить NTP-аутентификацию, воспользуйтесь формой **no** этой команды.

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)#
```

69.3 ntp authentication-key

Данная команда используется для включения NTP-аутентификации. Чтобы отключить NTP-аутентификацию, воспользуйтесь формой **no** этой команды.

ntp authentication-key *KEY-ID* **md5** *VALUE*
no ntp authentication-key *KEY-ID*

Параметры

KEY-ID	Укажите ID NTP-ключа. Диапазон значений: от 1 до 255.
md5	Укажите тип MD5 для ключа аутентификации.
VALUE	Укажите ключевую строку. Максимальное 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. Чтобы удалить ключ, воспользуйтесь формой no этой команды.

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)#
```

69.4 ntp control-key

Данная команда используется для указания ID ключа для контрольных NTP-сообщений. Чтобы удалить ключ, воспользуйтесь формой **no** этой команды.

ntp control-key *KEY-ID*

no ntp control-key

Параметры

KEY-ID	Укажите ID NTP-ключа. 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)#
```

69.5 ntp disable

Данная команда используется для отключения отправки NTP-пакетов на интерфейсе. Чтобы включить отправку NTP-пакетов на интерфейсе, воспользуйтесь формой **no** этой команды.

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 vlan1
Switch(config-if)#ntp disable
Switch(config-if)#
```

69.6 ntp master

Данная команда используется для настройки RTC в качестве основных NTP-часов, в случае если внешний NTP недоступен. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ntp master *STRATUM*

no ntp master

Параметры

STRATUM	Укажите часовой слой NTP. 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. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

Пример

В данном примере показано, как настроить маршрутизатор в качестве основных часов NTP.

```
Switch#configure terminal
Switch(config)#ntp master 10
Switch(config)#
```

69.7 ntp max-associations

Данная команда используется для настройки максимального количества NTP-узлов и клиентов на коммутаторе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ntp max-associations *NUMBER*

no ntp max-associations

Параметры

NUMBER	Укажите количество NTP-ассоциаций. 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)#
```

69.8 ntp peer

Данная команда используется для включения NTP-аутентификации. Чтобы отключить NTP-аутентификацию, воспользуйтесь формой **no** этой команды.

ntp peer {*IP-ADDRESS* **|** *IPv6-ADDRESS***} [version** *NUMBER***] [key** *KEY-ID***] [prefer] [min-poll** *INTERVAL***] [max-poll** *INTERVAL***]**

no ntp peer {*IP-ADDRESS* **|** *IPv6-ADDRESS***}**

Параметры

IP-ADDRESS	Укажите IPv4-адрес узла.
IPv6-ADDRESS	Укажите IPv6-адрес узла.
version	(Опционально.) Укажите номер NTP-версии.
NUMBER	(Опционально.) Введите номер NTP-версии. Диапазон значений: от 1 до 4. Значение по умолчанию – 4.
key	(Опционально.) Укажите ключ аутенификации.
KEY-ID	(Опционально.) Укажите ID ключа аутентификации. Диапазон значений: от 1 до 255.
prefer	(Опционально.) Укажите предпочтительный для синхронизации узел.

min-poll	(Опционально.) Укажите минимальный интервал опроса для NTP-сообщений. Интервал опроса рассчитывается как 2 в степени указанного значения. Например, если указано значение 6, то минимальный интервал опроса будет составлять 64 секунды (2^6=64).
INTERVAL	(Опционально.) Укажите значение минимального интервала опроса. Значение по умолчанию – 6.
max-poll	(Опционально.) Укажите максимальный интервал опроса для NTP-сообщений. Интервал опроса рассчитывается как 2 в степени указанного значения. Например, если указано значение 6, то максимальный интервал опроса будет составлять 64 секунды (2^6=64).
INTERVAL	(Опционально.) Укажите значение максимального интервала опроса. Значение по умолчанию – 10.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Настройки NTP системного времени коммутатора могут быть синхронизированы с узлом.

Пример

В данном примере показано, как настроить IP-адрес 192.168.22.33 для NTP-узла с использованием NTP-версии 3.

```
Switch#configure terminal
Switch(config)#ntp peer 192.168.22.33 version 3
Switch(config)#
```

69.9 ntp request-key

Данная команда используется для указания ID ключа для NTP-пакетов Mode 7, используемых утилитой *ntpdc*. Чтобы удалить ключ, воспользуйтесь формой **no** этой команды.

ntp request-key *KEY-ID*

no ntp request-key

Параметры

KEY-ID	Укажите ID NTP-ключа. Диапазон значений: от 1 до 255.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Утилита ntpdc использует проприетарный протокол (Proprietary Protocol), указанный для реализации NTP.

Пример

В данном примере показано, как указать ключ NTP request.

```
Switch#configure terminal
Switch(config)#ntp request-key 45
Switch(config)#
```

69.10 ntp server

Данная команда используется для синхронизации времени коммутатора с NTP-сервером. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ntp server {*IP-ADDRESS* **|** *IPv6-ADDRESS***} [version** *NUMBER***] [key** *KEY-ID***] [prefer] [min-poll** *INTERVAL***] [max-poll** *INTERVAL***]**

no ntp server {*IP-ADDRESS* **|** *IPv6-ADDRESS***}**

Параметры

IP-ADDRESS	Укажите IPv4-адрес NTP-сервера.
IPv6-ADDRESS	Укажите IPv6-адрес NTP-сервера.
version	(Опционально.) Укажите номер NTP-версии.
NUMBER	(Опционально.) Укажите номер NTP-версии. Диапазон значений: от 1 до 4. Значение по умолчанию – 4.
key	(Опционально.) Укажите ключ аутенификации.

KEY-ID	(Опционально.) Укажите ID ключа аутентификации. Диапазон значений: от 1 до 255.
prefer	(Опционально.) Укажите предпочтительный для синхронизации узел.
min-poll	(Опционально.) Укажите минимальный интервал опроса для NTP-сообщений. Интервал опроса рассчитывается как 2 в степени указанного значения. Например, если указано значение 6, то минимальный интервал опроса будет составлять 64 секунды (2^6=64).
INTERVAL	(Опционально.) Укажите значение минимального интервала опроса. Значение по умолчанию – 6.
max-poll	(Опционально.) Укажите максимальный интервал опроса для NTP-сообщений. Интервал опроса рассчитывается как 2 в степени указанного значения. Например, если указано значение 6, то максимальный интервал опроса будет составлять 64 секунды (2^6=64).
INTERVAL	(Опционально.) Укажите значение максимального интервала опроса. Значение по умолчанию – 10.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для синхронизации времени коммутатора с NTP-сервером.

Пример

В данном примере показано, как настроить IP-адрес 192.168.10.33 для NTP-сервера с использованием NTP-версии 2.

```
Switch#configure terminal
Switch(config)#ntp server 192.168.10.33 version 2
Switch(config)#
```

69.11 ntp trusted-key

Данная команда используется для указания доверенного ключа узла, который будет аутентифицирован NTP-системой. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ntp trusted-key *KEY-ID*
no ntp trusted-key *KEY-ID*

Параметры

KEY-ID	Укажите ID NTP-ключа. 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. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

Пример

В данном примере показано, как настроить доверенный NTP-ключ.

```
Switch#configure terminal
Switch(config)#ntp trusted-key 45
Switch(config)#
```

69.12 ntp update-calendar

Данная команда используется для периодической синхронизации аппаратных часов со временем, полученным по NTP. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

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. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

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)#
```

69.13 service ntp

Данная команда используется для включения NTP. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

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)#
```

69.14 show ntp associations

Данная команда используется для отображения статуса NTP-ассоциаций.

show ntp associations [detail]

Параметры

detail	(Опционально.) Укажите для отображения подробной информации по каждой NTP-ассоциации.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения статуса NTP-ассоциаций.

Пример

В данном примере показано, как отобразить NTP-ассоциации.

```
Switch#show ntp associations

     Remote           Local      St Poll Reach  Delay   Offset    Disp
==============================================================================
=192.168.10.33   0.0.0.0        16  128    0 0.00000  0.000000 3.99217
+192.168.22.33   0.0.0.0        16  128    0 0.00000  0.000000 3.99217
+ Symmetric active, - Symmetric passive, = Client, * System Peer

Switch#
```

Отображаемые параметры

Leading Characters	Ниже перечислены возможные первые символы в строке, 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 примере ниже 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. 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.

69.15 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.

70. Команды Open Shortest Path First Version 2 (OSPFv2)

70.1 area default-cost

Данная команда используется для указания стоимости, ассоциированной с маршрутом по умолчанию 3-го типа (type-3 default route), который будет автоматически добавлен в тупиковую зону (Stub Area) или зону NSSA (Not-So-Stubby Area). Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

area *AREA-ID* **default-cost** *COST*
no area *AREA-ID* **default-cost**

Параметры

AREA-ID	Укажите ID зоны в виде десятичного значения или IP-адреса.
COST	Укажите стоимость маршрута по умолчанию. Диапазон значений: 24-битное число от 0 до 65535.

По умолчанию

Значение по умолчанию – 1.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется на пограничном маршрутизаторе Area Border Router (ABR), который подключен к тупиковой зоне (Stub Area) или зоне NSSA, для указания стоимости, ассоциированной с маршрутом по умолчанию 3-го типа (type-3 default route), генерируемым в данную зону.

Пример

В данном примере показано, как назначить стоимость по умолчанию для тупиковой зоны (Stub Area) 10.0.0.0. Указанное значение – 20.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#area 10.0.0.0 default-cost 20
Switch(config-router)#
```

70.2 area nssa

Данная команда используется для назначения зоны в качестве зоны NSSA. Чтобы удалить настройки, ассоциированные с назначенной зоной NSSA, воспользуйтесь формой **no** этой команды.

area *AREA-ID* **nssa [no-summary]**
no area *AREA-ID* **nssa [no-summary]**

Параметры

AREA-ID	Укажите ID зоны, которую необходимо назначить как зону NSSA.
no-summary	(Опционально.) Укажите, чтобы данная функция запускалась, только когда маршрутизатор является ABR.

По умолчанию

По умолчанию зона NSSA настроена.

По умолчанию параметр no-summary не используется, а сумарный маршрут (summary route) будет анонсирован в зону NSSA.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При вводе команды **no area** *AREA-ID* **nssa** будут удалены все настройки, ассоциированные с назначенной зоной NSSA.

В тупиковой зоне (Stub Area) OSPF отсутствуют внешние маршруты (external route), поэтому перераспределение маршрутов из другого протокола в тупиковую зону (Stub Area) невозможно.

В NSSA разрешено анонсирование внешних маршрутов в зону LSA типа 7. Эти маршруты впоследствии попадают в другие зоны. Однако внешние маршруты из других зон все равно не могут быть добавлены в NSSA.

Используйте команду **area nssa**, чтобы упростить управление при подключении центрального маршрутизатора через OSPF к удаленному маршрутизатору, который использует другой протокол маршрутизации. Для охвата удаленного подключения, определяющего зону между центральным маршрутизатором и удаленным маршрутизатором, таким как NSSA, необходимо расширение OSPF.

Если в зоне NSSA сгенерировано несколько маршрутов по умолчанию, действует следующее правило приоритета: intra-route > inter-route > external route.

Пример

В данном примере показано, как настроить зону NSSA.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#area 1 nssa
Switch(config-router)#
```

70.3 area range

Данная команда используется для суммирования маршрутов OSPF на маршрутизаторе Area Border Router. Чтобы удалить суммирование маршрутов, воспользуйтесь формой **no** этой команды.

area *AREA-ID* **range** *NETWORK-PREFIX NETWORK-MASK* **[advertise | no-advertise]**
no area *AREA-ID* **range** *NETWORK-PREFIX NETWORK-MASK*

Параметры

AREA-ID	Укажите ID зоны, из которой необходимо суммировать маршруты.
NETWORK-PREFIX	Укажите префикс сети суммарного (summary) маршрута.
NETWORK-MASK	Укажите маску сети суммарного (summary) маршрута.
advertise	(Опционально.) Укажите, чтобы анонсировать summary LSA типа 3 для заданного диапазона адресов.
not-advertise	(Опционально.) Укажите, чтобы отключить анонсирование summary LSA типа 3. Маршруты, входящие в состав объединенного, по-прежнему скрыты за ним.

По умолчанию

По умолчанию функция отключена.

По умолчанию используется параметр **advertise**.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда может применяться к одной зоне несколько раз. Используйте команду на ABR, чтобы суммировать внутризоновые маршруты (intra-area route). Команда также позволяет указать суммированные маршруты в магистральной зоне (Area 0) или немагистральной зоне (Non-Zero Area). Команду можно применять к нескольким зонам. Таким образом, OSPF может суммировать адреса из нескольких диапазонов адресов.

Пример

В данном примере показано, как настроить один суммарный (summary) маршрут, который будет анонсирован ABR в другие зоны для всех подсетей в сети 192.168.0.0.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#area 1 range 192.168.0.0 255.255.0.0
Switch(config-router)#
```

70.4 area stub

Данная команда используется для указания зоны в качестве тупиковой (Stub Area). Чтобы удалить настройки, ассоциированные с назначенной тупиковой зоной (Stub Area), воспользуйтесь формой **no** этой команды.

area *AREA-ID* **stub [no-summary]**

no area *AREA-ID* **stub [no-summary]**

Параметры

AREA-ID	Укажите ID зоны, которую необходимо назначить в качестве тупиковой (Stub Area).
no-summary	(Опционально.) Укажите, чтобы назначить тупиковую зону в качестве полностью тупиковой (Total Stub Area).

По умолчанию

По умолчанию зона является нормальной (Normal Area).

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При вводе команды **no area** *AREA-ID* **stub** будут удалены все настройки, ассоциированные с назначенной тупиковой зоной (Stub Area). Используйте данную команду на всех маршрутизаторах в тупиковой зоне (Stub Area).

Укажите параметр **no-summary**, чтобы назначить тупиковую зону (Stub Area) в качестве полностью тупиковой (Total Stub Area). Маршрутизаторам в данной зоне не требуется изучение межзональных маршрутов (inter-area route), за исключением маршрута по умолчанию 3-го типа (type-3 default route).

Пример

В данном примере показано, как настроить зону 3 в качестве тупиковой (Stub Area).

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#area 3 stub
Switch(config-router)#
```

70.5 area virtual-link

Данная команда используется для настройки виртуального канала (virtual link) через немагистральную зону (Non-Backbone Area), которая физически отделена от магистральной зоны (Backbone Area). Чтобы удалить виртуальный канал или вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

area *AREA-ID* **virtual-link** *ROUTER-ID* **[authentication [message-digest | null]] [hello-interval** *SECONDS*] **[dead-interval** *SECONDS*] **[authentication-key** *PASSWORD* **| message-digest-key** *KEY-ID* **md5** *KEY*]

no area *AREA-ID* **virtual-link** *ROUTER-ID* **[authentication] [hello-interval] [dead-interval] [message-digest-key** *KEY-ID*]

Параметры

AREA-ID	Укажите ID зоны, в которой необходимо настроить виртуальный канал. ID задается в виде десятичного значения или IPv4-адреса.
ROUTER-ID	Укажите ID соседнего маршрутизатора виртуального канала.
authentication	(Опционально.) Укажите тип аутентификации. Если тип аутентификации для виртуального канала не настроен, для данной зоны будет использован тип аутентификации по паролю.
message-digest	(Опционально.) Укажите тип аутентификации Message Digest (дайджест сообщений) для виртуального канала.
null	(Опционально.) Укажите, чтобы не использовать аутентификацию.
hello-interval *SECONDS*	(Опционально.) Укажите интервал между пакетами hello, которые маршрутизатор отправляет по виртуальному каналу. Диапазон значений: от 1 до 65535 секунд. Если не указано, значение по умолчанию составляет 10 секунд.
dead-interval *SECONDS*	(Опционально.) Укажите интервал, по истечении которого соседнее устройство будет считаться недоступным, если не было получено ни одного пакета hello. Диапазон значений: от 1 до 65535 секунд. Если не указано, значение по умолчанию составляет 40 секунд.
authentication-key *PASSWORD*	(Опционально.) Укажите пароль для аутентификации. Максимальное количество байтов – 8.
message-digest-key *KEY-ID* **md5** *KEY*	(Опционально.) Укажите ключ MD для аутентификации MD5 Message Digest. Максимальное количество байтов – 16.

По умолчанию

По умолчанию ни одного виртуального канала OSPF не настроено.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если немагистральная зона физически не подключена к магистральной зоне, необходимо настроить подключение типа «точка-точка». Маршрутизатор будет отправлять OSPF-сообщения соседнему маршрутизатору в качестве одноадресных (unicast) IP-пакетов.

Пример

В данном примере показано, как настроить виртуальный канал с интервалом hello в 5 секунд и интервалом dead в 10 секунд.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#area 1 virtual-link 10.10.11.50 hello-interval 5 dead-interval 10
Switch(config-router)#
```

В примере ниже показано, как настроить параметры для виртуального канала в зоне 1 и ID удаленного устройства (Remote ID). Указанное значение Remote ID – 192.168.255.1. Настроенным ключом является аутентификация по простому паролю – yourpass.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#area 1 virtual-link 192.168.255.1 authentication
Switch(config-router)#area 1 virtual-link 192.168.255.1 authentication-key yourpass
Switch(config-router)#
```

70.6 clear ip ospf

Данная команда используется для перезапуска процесса IPv4 OSPF.

clear ip ospf process

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При удалении процесса OSPF база данных маршрутизации OSPF очищается, а процесс будет перезапущен.

Пример

В данном примере показано, как удалить процесс OSPF.

```
Switch#clear ip ospf process
Switch#
```

70.7 compatible rfc3509

Данная команда используется для настройки режима работы OSPF маршрутизатора Area Border Router (ABR). Настроенный режим работы определен в RFC 3509. Чтобы отключить данную опцию, воспользуйтесь формой **no** этой команды.

compatible rfc3509

no compatible rfc3509

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Несмотря на то что при настройке ABR в OSPF маршрутизатору с несколькими привязанными к нему зонами не требуется магистральное соединение, необходимо обеспечить успешную маршрутизацию к межзональным (inter-area) и внешним (external) сетям назначениям (destination). Если данное требование не выполняется, весь трафик, предназначенный для зон, которые не присоединены к ABR или находятся за пределами домена OSPF, отбрасывается. Для разрешения данной ситуации существует альтернативная реализация (RFC 3509).

Пример

В данном примере показано, как включить альтернативную реализацию OSPF для ABR.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#compatible rfc3509
Switch(config-router)#
```

70.8 compatible rfc1583

Данная команда используется для настройки совместимости с RFC 1583 в RFC 2328. Для отключения данной опции воспользуйтесь формой **no** этой команды.

compatible rfc1583
no compatible rfc1583

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

В RFC 2328 существует метод сопоставления приоритетов для внешних (external) маршрутов AS. Для обратной совместимости необходимо включить опцию RFC 1583 Compatibility (совместимость с RFC 1583).

Пример

В данном примере показано, как настроить совместимость с RFC 1583 в RFC 2328.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#compatible rfc1583
Switch(config-router)#
```

70.9 default-information originate

Данная команда используется для анонсирования маршрута по умолчанию в домене маршрутизации OSPF. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

default-information originate [always] [metric *METRIC-VALUE***]**
no default-information originate [always] [metric]

Параметры

always	(Опционально.) Укажите, чтобы маршрут по умолчанию генерировался всегда, независимо от того, существует ли данный маршрут в таблице маршрутизации.
metric *METRIC-VALUE*	(Опционально.) Укажите стоимость, ассоциированную с генерированным маршрутом по умолчанию. Если параметр не указан, значение метрики по умолчанию равно 1. Диапазон значений: от 1 до 65535.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду на ASBR, чтобы настроить процесс маршрутизации для анонсирования маршрута по умолчанию (network 0.0.0.0) в домене маршрутизации. Если указан параметр **always**, маршрут по умолчанию генерируется всегда. Если параметр **always** не указан, маршрут по умолчанию генерируется, только когда он существует в таблице маршрутизации.

Пример

В данном примере показано, как анонсировать маршрут по умолчанию, который может отсутствовать в системе.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#default-information originate always
Switch(config-router)#
```

70.10 default-metric

Данная команда используется, чтобы настроить значение метрики по умолчанию для протокола маршрутизации. Для удаления настроек метрики по умолчанию воспользуйтесь формой **no** этой команды.

default-metric *METRIC-VALUE*
no default-metric

Параметры

metric *METRIC-VALUE*	(Опционально.) Укажите значение метрики по умолчанию для перераспределяемых маршрутов. Диапазон значений: от 1 до 16777214.

По умолчанию

Значение по умолчанию – 20.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда **default-metric** применяется вместе с командой **redistribute**, чтобы настроить значение метрики по умолчанию текущего протокола маршрутизации для перераспределяемых маршрутов, метрика которых не указана.

Пример

В данном примере показано, как настроить перераспределение маршрутов, полученных из RIP, в домен OSPF на маршрутизаторе. Настроенное значение метрики OSPF при анонсировании всех перераспределяемых маршрутов – 10.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#default-metric 10
Switch(config-router)#redistribute rip
Switch(config-router)#
```

70.11 distance ospf

Данная команда используется, чтобы настроить расстояние (distance) для определенных маршрутов OSPF. Для отмены назначения воспользуйтесь формой **no** этой команды.

distance ospf {inter-area | intra-area | external-1 | external-2} *DISTANCE*
no distance ospf

Параметры

inter-area	Укажите расстояние для межзональных (inter-area) маршрутов OSPF.
intra-area	Укажите расстояние для внутризоновых (intra-area) маршрутов OSPF.

external-1	Укажите расстояние для внешних (external) маршрутов OSPF типа 5 и 7 с метрикой типа 1.
external-2	Укажите расстояние для внешних (external) маршрутов OSPF типа 5 и 7 с метрикой типа 2.
DISTANCE	Укажите административное расстояние (administrative distance). Диапазон значений: от 1 до 255.

По умолчанию

Параметр **intra-area** по умолчанию – 80.

Параметр **inter-area** по умолчанию – 90.

Параметр **external-1** по умолчанию – 110.

Параметр **external-2** по умолчанию – 115.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить административное расстояние для определенных маршрутов OSPF. Команда **distance ospf** действует как команда **distance**, которая определяет, какие маршруты будут установлены в таблице маршрутизации.

Как правило, чем выше значение, тем ниже рейтинг надежности.

Пример

В данном примере показано, как настроить расстояние (distance) для внешних (external) маршрутов с метрикой типа 1. Указанное значение – 50.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#distance ospf external-1 50
Switch(config-router)#
```

70.12 host area

Данная команда используется для настройки записи тупикового узла (stub host), принадлежащего определенной зоне. Чтобы удалить настройки записи узла, воспользуйтесь формой **no** этой команды.

host *IP-ADDRESS* **area** *AREA-ID* **[cost** *COST***]**

no host *IP-ADDRESS* **area** *AREA-ID*

Параметры

IP-ADDRESS	Укажите IP-адрес узла.
AREA-ID	Укажите ID зоны, которая содержит запись тупикового (stub) узла.
cost *COST*	(Опционально.) Укажите стоимость записи тупикового (stub) узла. Диапазон значений: от 1 до 65535.

По умолчанию

По умолчанию узел не настроен.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Маршрутизатор анонсирует указанные маршруты узла в качестве LSA маршрутизатора для тупикового канала (stub link).

Пример

В данном примере показано, как настроить тупиковый (stub) узел 172.16.10.100 в зоне 1.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#host 172.16.10.100 area 1
Switch(config-router)#
```

70.13 ip ospf authentication

Данная команда используется, чтобы настроить аутентификацию для OSPF. Для отключения аутентификации воспользуйтесь формой **no** этой команды.

ip ospf authentication [message-digest]

no ip ospf authentication

Параметры

message-digest	(Опционально.) Укажите, чтобы использовать аутентификацию Message Digest (дайджест сообщений).

По умолчанию

По умолчанию аутентификация не применена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если использование ключа аутентификации указано, но ключ не настроен, применяется ключ NULL. Если указан параметр **message-digest**, но ключ digest не настроен, используется ключ NULL с Key ID 0.

Пример

В данном примере показано, как включить аутентификацию Message Digest на интерфейсе VLAN 1.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip ospf authentication message-digest
Switch(config-if)#
```

70.14 ip ospf authentication-key

Данная команда используется, чтобы указать пароль для аутентификации с соседними маршрутизаторами OSPF. Для удаления пароля аутентификации OSPF воспользуйтесь формой **no** этой команды.

ip ospf authentication-key *PASSWORD*

no ip ospf authentication-key

Параметры

PASSWORD	Укажите пароль аутентификации. Максимальное количество байтов – 8. Пробелы в строке недопустимы.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда позволяет указать пароль (ключ), который будет внедрен в заголовок OSPF при отправке пакетов протокола маршрутизации. Пароли разных интерфейсов в каждой сети не должны совпадать. Для обмена данными маршрутизации OSPF маршрутизаторы в одной сети и домене должны использовать один пароль.

Пример

В данном примере показано, как создать ключ аутентификации на VLAN-интерфейсе. Настроенный ключ – test.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip ospf authentication
Switch(config-if)#ip ospf authentication-key test
Switch(config-if)#
```

70.15 ip ospf cost

Данная команда используется для указания стоимости отправки пакетов на интерфейсе. Чтобы отменить назначение, воспользуйтесь формой **no** этой команды.

ip ospf cost *COST*
no ip ospf cost

Параметры

COST	Укажите значение метрики состояния канала (link-state). Диапазон значений: от 1 до 65535.

По умолчанию

Значение по умолчанию – 1.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Стоимость интерфейса обозначает издержки отправки пакетов через интерфейс. Указанная стоимость анонсируется в качестве стоимости канала в объявлениях о состоянии каналов (link advertisement) маршрутизатора.

Пример

В данном примере показано, как указать стоимость на интерфейсе VLAN 1. Заданное значение – 10.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip ospf cost 10
Switch(config-if)#
```

70.16 ip ospf dead-interval

Данная команда используется для установки интервала, по истечении которого соседнее устройство будет считаться недоступным, если не было получено ни одного пакета hello. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip ospf dead-interval *SECONDS*
no ip ospf dead-interval

Параметры

SECONDS	Укажите интервал, по истечении которого соседнее устройство будет считаться недоступным, если не было получено ни одного пакета hello. Диапазон значений: от 1 до 65535 секунд.

По умолчанию

Значение по умолчанию – 40 секунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Интервал dead – это период времени, в течение которого маршрутизатор ожидает пакеты OSPF hello от соседних устройств, которые при отсутствии пакетов будут считаться недоступными. Данный интервал анонсируется в пакетах hello. Значение должно быть одинаковым для всех маршрутизаторов в одной сети. Чем меньше значение интервала dead, тем быстрее будут обнаружены изменения в топологии, но при этом будет увеличен маршрутный трафик.

Пример

В данном примере показано, как установить интервал dead на интерфейсе VLAN 1. Настроенное значение – 10 секунд. Заданное значение – 10.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip ospf dead-interval 10
Switch(config-if)#
```

70.17 ip ospf hello-interval

Данная команда используется для указания интервала между пакетами hello. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip ospf hello-interval *SECONDS*
no ip ospf hello-interval

Параметры

SECONDS	Укажите интервал между пакетами hello. Диапазон значений: от 1 до 65535 секунд.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Значение интервала hello анонсируется в пакетах hello и должно быть одинаковым для всех маршрутизаторов в одной сети. Чем меньше значение интервала hello, тем быстрее будут обнаружены изменения в топологии, но при этом будет увеличен маршрутный трафик.

Пример

В данном примере показано, как указать значение интервала hello на интерфейсе VLAN 1. Настроенное значение – 3 секунды.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip ospf hello-interval 3
Switch(config-if)#
```

70.18 ip ospf message-digest-key

Данная команда используется, чтобы настроить ключ MD5 для аутентификации OSPF MD5. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip ospf message-digest-key *KEY-ID* **md5** *KEY*
no ip ospf message-digest-key *KEY-ID*

Параметры

KEY-ID	Укажите ID ключа. Диапазон значений: от 1 до 255.
KEY	Укажите ключ OSPF MD5 Message Digest. Максимальное количество символов – 16.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для аутентификации OSPF-сообщений может применяться пароль или режим MD5 Digest Mode. Используйте данную команду, чтобы настроить ключ Message Digest для режима MD5 Digest Mode.

В режиме MD5 Digest Mode отправитель OSPF-сообщений определяет Message Digest на основе ключа Message Digest для TX-сообщений. Message Digest и ID ключа будут закодированы в пакете. Получатель пакета сверяет digest в сообщении с digest, определенным на основе локально настроенного ключа Message Digest, который соответствует тому же ID ключа.

Все соседние маршрутизаторы на одном интерфейсе при обмене OSPF-пакетами должны использовать одинаковый ID ключа, настроенный с помощью одной ключевой строки.

Пример

В данном примере показано, как настроить новый ключ на интерфейсе VLAN 1. Настроенный новый ключ – 10. Пароль – yourpass.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip ospf authentication message-digest
Switch(config-if)#ip ospf message-digest-key 10 md5 yourpass
Switch(config-if)#
```

70.19 ip ospf network

Данная команда используется для настройки типа сети OSPF. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip ospf network {broadcast | point-to-point}

no ip ospf network

Параметры

broadcast	Укажите тип сети broadcast (широковещательная сеть).
point-to-point	Укажите тип сети point-to-point (сеть «точка-точка»).

По умолчанию

Тип сети по умолчанию – broadcast.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы изменить тип сети OSPF на интерфейсе. При указании широковещательной сети (broadcast) из всех подключенных маршрутизаторов только назначенный маршрутизатор и резервный назначенный маршрутизатор становятся соседними устройствами (adjacent neighbor). При указании сети «точка-точка» (point-to-point) только два маршрутизатора становятся adjacent neighbor, если между ними установлено соединение.

Пример

В данном примере показано, как настроить тип сети OSPF на интерфейсе VLAN 1. Установленный тип сети – «точка-точка».

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip ospf network point-to-point
Switch(config-if)#
```

70.20 ip ospf priority

Данная команда используется для установки приоритета, согласно которому определяется назначенный маршрутизатор (Designated Router, DR) в сети. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip ospf priority *PRIORITY*
no ip ospf priority

Параметры

PRIORITY	Укажите значение приоритета маршрутизатора в диапазоне от 0 до 255.

По умолчанию

Значение по умолчанию – 1.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

OSPF-маршрутизатор определяет назначенный маршрутизатор (Designated Router, DR) для сети со множественным доступом.

Данная команда предназначена для установки приоритета, согласно которому назначается DR в сети. В качестве DR назначается маршрутизатор с наиболее высоким значением приоритета. Если приоритеты совпадают, назначается маршрутизатор с наибольшим значением Router ID.

Назначенными (designated) или резервными назначенными (backup designated) могут стать только маршрутизаторы с ненулевым значением приоритета.

Пример

В данном примере показано, как установить значение приоритета OSPF на интерфейсе VLAN 1. Настроенное значение – 3.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip ospf priority 3
Switch(config-if)#
```

70.21 log-adjacency-changes

Данная команда используется для включения отправки syslog-сообщений при обнаружении/разрыве соединения с соседними устройствами OSPF. Чтобы отключить данную опцию, воспользуйтесь формой **no** этой команды.

log-adjacency-changes [detail]
no log-adjacency-changes [detail]

Параметры

detail	(Опционально.) Укажите, чтобы при изменении состояния соседних устройств OSPF были отправлены syslog-сообщения.

По умолчанию

По умолчанию опция включена.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить или отключить отправку syslog-сообщений при обнаружении/разрыве соединения с соседними устройствами OSPF.

Пример

В данном примере показано, как включить отправку syslog-сообщений при изменении состояния соседних устройств OSPF.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#log-adjacency-changes detail
Switch(config-router)#
```

70.22 network area

Данная команда используется для включения маршрутизации OSPF с указанием ID зоны и IP-адресов, которые соответствуют или принадлежат определенному сетевому адресу. Чтобы удалить конфигурацию, воспользуйтесь формой **no** этой команды.

network *NETWORK-PREFIX NETWORK-MASK* **area** *AREA-ID*

no network *NETWORK-PREFIX NETWORK-MASK* **area** *AREA-ID*

Параметры

NETWORK-PREFIX *NETWORK-MASK*	Укажите префикс и маску подсети.
AREA-ID	Укажите ID зоны для создания в виде десятичного значения или IP-адреса.

По умолчанию

Нет.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для включения маршрутизации OSPF с указанием ID зоны на интерфейсах. На интерфейсе, который соответствует указанному сетевому адресу, должен быть включен OSPF.

Пример

В данном примере показано, как включить OSPF на интерфейсе в зоне 1.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#network 10.0.0.0 255.0.0.0 area 1
Switch(config-router)#
```

70.23 no area

Данная команда используется для удаления настроек, ассоциированных с зоной.

no area *AREA-ID*

Параметры

AREA-ID	Укажите ID зоны.

По умолчанию

Нет.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для удаления настроек, ассоциированных с зоной.

Пример

В данном примере показано, как удалить зону 3 и все ассоциированные с ней настройки.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#no area 3
Switch(config-router)#
```

70.24 passive-interface

Данная команда используется для включения пассивного режима на интерфейсе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

passive-interface {default | *INTERFACE-ID***}**
no passive-interface {default | *INTERFACE-ID***}**

Параметры

default	Укажите, чтобы включить пассивный режим на всех интерфейсах.
INTERFACE-ID	Укажите ID интерфейса, на котором необходимо включить пассивный режим.

По умолчанию

По умолчанию пассивный режим не включен ни на одном настроенном интерфейсе.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

На интерфейсе в пассивном режиме не принимаются и не отправляются пакеты обновлений маршрутизации OSPF.

Пример

В данном примере показано, как включить пассивный режим на интерфейсе VLAN 1.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#passive-interface vlan1
Switch(config-router)#
```

70.25 redistribute

Данная команда используется для перераспределения маршрутов из одного домена маршрутизации в другой. Чтобы отключить перераспределение, воспользуйтесь формой **no** этой команды.

redistribute *PROTOCOL* **[metric** *METRIC-VALUE***] [metric-type** *TYPE-VALUE***] [route-map** *MAP-NAME***]**
no redistribute *PROTOCOL* **[metric] [metric-type] [route-map]**

Параметры

PROTOCOL	Укажите исходный протокол, из которого необходимо перераспределить маршруты. Доступны следующие ключевые слова: **connected**, **rip** или **static**.
metric *METRIC-VALUE*	(Опционально.) Укажите значение метрики для перераспределяемых маршрутов. Диапазон значений: от 1 до 16777214.
metric-type *TYPE-VALUE*	(Опционально.) Укажите тип метрики для внешних (external) маршрутов, перераспределяемых в домен маршрутизации OSPF. Доступны следующие два значения: **1:** укажите, чтобы использовать внешнюю метрику типа 1. **2:** укажите, чтобы использовать внешнюю метрику типа 2. Если тип метрики не указан, по умолчанию будет выбран тип2.
route-map *MAP-NAME*	(Опционально.) Укажите карту маршрута для фильтрации импортированных маршрутов из указанного исходного протокола маршрутизации. Если параметр не указан, будут перераспределены все маршруты.

По умолчанию

По умолчанию перераспределение маршрутов отключено.

По умолчанию для внешних (external) маршрутов используется метрика типа 2.

По умолчанию карта маршрута настроена для перераспределения всех маршрутов.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Внешние (external) маршруты могут быть перераспределены в обычные зоны (normal area) как внешние маршруты типа 5, а также могут быть перераспределены в тупиковые зоны (stub area) NSSA как внешние маршруты типа 7 при помощи ASBR.

Внешние маршруты могут быть типа 1 и типа 2. Метрика перераспределяемого внешнего маршрута типа 1 представлена внутренней метрикой. Метрика перераспределяемого внешнего маршрута типа 2 представлена внешней метрикой. Внутренней метрикой считается стоимость от начала маршрута до перераспределяемого маршрута с учетом анонсированной стоимости до места назначения. Внешняя метрика предусматривает только анонсированную метрику до места назначения.

Команда **redistribute** или **default-information originate** применяется только на ASBR.

Если метрика не указана, значение метрики устанавливается командой **default metric**. Если метрика в команде **default metric** не указана, в качестве метрики маршрутов, перераспределяемых из других

протоколов, будет установлено значение 20. Исключением считается BGP, для которого в качестве метрики устанавливается значение 1.

Пример

В данном примере показан процесс перераспределения маршрутов RIP в домен OSPF.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#redistribute rip metric 100
Switch(config-router)#
```

70.26 router ospf

Данная команда используется для настройки процесса маршрутизации OSPF. Чтобы удалить процесс маршрутизации OSPF, воспользуйтесь формой **no** этой команды.

router ospf

no router ospf

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 параметры для OSPF.

Пример

В данном примере показано, как включить OSPF и войти в режим Router Configuration Mode.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#
```

70.27 router-id

Данная команда используется для того, чтобы указать ID маршрутизатора для процесса OSPF. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

router-id *ROUTER-ID*
no router-id

Параметры

ROUTER-ID	Укажите ID маршрутизатора в виде IPv4-адреса.

По умолчанию

По умолчанию ID маршрутизатора назначается автоматически.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

ID маршрутизатора – это 32-битное число, назначаемое каждому маршрутизатору, на котором включен OSPF. Данное число является уникальным идентификатором для маршрутизатора в автономной системе. На каждом маршрутизаторе должен быть указан уникальный Router ID.

Пример

В данном примере показано, как указать ID маршрутизатора. Настроенное значение – 10.10.10.60.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#router-id 10.10.10.60
Switch(config-router)#
```

70.28 show ip ospf

Данная команда используется для отображения общей информации о процессе маршрутизации OSPF.

show ip ospf

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 общую информацию о протоколе OSPF.

Пример

В данном примере показано, как отобразить общую информацию о протоколе OSPF.

```
Switch#show ip ospf

OSPF Routing Process 1
  Operational Router ID 10.90.90.90
  Process uptime is 0DT3H13M49S
  Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
  SPF schedule Hold time between two SPFs 3 secs
  Number of external LSA 0. Checksum Sum 0x0
  Number of LSA originated 0
  Number of LSA received 0
  Number of current LSA 0
  LSDB database overflow limit is 49152
  Number of areas attached to this router: 2
    Area 0.0.0.0 (BACKBONE)
        Number of interface in this area is 0, active interface number is 0
        SPF algorithm executed 3 times
        Number of LSA 0
    Area 0.0.0.1
        Number of interface in this area is 1, active interface number is 0
        SPF algorithm executed 3 times
        Number of LSA 0
        Summarize range 192.168.0.0/16 advertise

Switch#
```

70.29 show ip ospf database

Данная команда используется для отображения сводной информации базы данных OSPF.

show ip ospf database

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 сводную информацию базы данных OSPF.

Пример

В данном примере показано, как отобразить сводную информацию базы данных OSPF.

```
Switch#show ip ospf database

          OSPF Router with ID (1.1.1.1)

              Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link Count
1.1.1.1         1.1.1.1         376  0x80000003 0x7AB2 1
10.1.1.100      10.1.1.100      316  0x80000008 0xA63D 1

              Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.1.1.1        1.1.1.1         381  0x80000001 0xE6ED

              Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Route
50.1.1.0        10.1.1.100      317  0x80000002 0x2099 50.1.1.0/24
50.1.2.0        10.1.1.100      317  0x80000002 0x15A3 50.1.2.0/24
50.1.3.0        10.1.1.100      317  0x80000002 0xAAD  50.1.3.0/24

              AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route                Tag
50.1.2.0        10.1.1.100      316  0x80000002 0x9A5  E1 50.1.2.0/24       0
50.1.3.0        10.1.1.100      316  0x80000002 0xFDAF E1 50.1.3.0/24       0
50.1.4.0        10.1.1.100      316  0x80000002 0xF2B9 E1 50.1.4.0/24       0
50.1.5.0        10.1.1.100      317  0x80000002 0x6BBF E2 50.1.5.0/24       0
100.1.1.0       1.1.1.1         415  0x80000002 0x7DBE E2 100.1.1.0/24      0
100.1.2.0       1.1.1.1         415  0x80000002 0x72C8 E2 100.1.2.0/24      0
100.1.3.0       1.1.1.1         415  0x80000002 0x67D2 E2 100.1.3.0/24      0

Total Entries: 13
Switch#
```

70.30 show ip ospf database adv-router

Данная команда используется для отображения всех LSA, генерируемых анонсирующим маршрутизатором (Advertising Router).

show ip ospf database adv-router *ROUTER-ID*

Параметры

ROUTER-ID	Укажите Router ID в виде IPv4-адреса.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить все LSA, генерируемые анонсирующим маршрутизатором (Advertising Router).

Пример

В данном примере показано, как отобразить все LSA, генерируемые анонсирующим маршрутизатором (Advertising Router).

```
Switch#show ip ospf database adv-router 10.1.1.100

           OSPF Router with ID (1.1.1.1)

               Router Link States (Area 0.0.0.0)

  LS age: 476
  Options: 0x0 (*|-|-|-|-|-|-|-)
  Flags: 0x3 ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.1.1.100
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000008
  Checksum: 0xA63D
  Length: 36
  Number of Links: 1
    Link connected to a Transit Network
     (Link ID) Designated Router address: 10.1.1.1
     (Link Data) Router Interface address: 10.1.1.100
      Number of TOS metrics: 0
       TOS 0 Metric: 10

               Summary Link States (Area 0.0.0.0)

  LS age: 477
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 50.1.1.0 (summary Network Number)
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000002
  Checksum: 0x2099
  Length: 28
  Network Mask: /24
        TOS: 0 Metric: 0

  LS age: 478
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 50.1.2.0 (summary Network Number)
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000002
  Checksum: 0x15A3
  Length: 28
```

```
Network Mask: /24
      TOS: 0 Metric: 0

LS age: 478
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: summary-LSA (summary Network Number)
Link State ID: 50.1.3.0 (summary Network Number)
Advertising Router: 10.1.1.100
LS Seq Number: 0x80000002
Checksum: 0xAAD
Length: 28
Network Mask: /24
      TOS: 0 Metric: 0

              AS External Link States

LS age: 478
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: AS-external-LSA
Link State ID: 50.1.2.0 (External Network Number)
Advertising Router: 10.1.1.100
LS Seq Number: 0x80000002
Checksum: 0x9A5
Length: 36
Network Mask: /24
      Metric Type: 1
      TOS: 0
      Metric: 0
      Forward Address: 0.0.0.0
      External Route Tag: 0

LS age: 478
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: AS-external-LSA
Link State ID: 50.1.3.0 (External Network Number)
Advertising Router: 10.1.1.100
LS Seq Number: 0x80000002
Checksum: 0xFDAF
Length: 36
Network Mask: /24
      Metric Type: 1
      TOS: 0
      Metric: 0
      Forward Address: 0.0.0.0
      External Route Tag: 0

LS age: 478
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: AS-external-LSA
Link State ID: 50.1.4.0 (External Network Number)
Advertising Router: 10.1.1.100
```

```
  LS Seq Number: 0x80000002
  Checksum: 0xF2B9
  Length: 36
  Network Mask: /24
        Metric Type: 1
        TOS: 0
        Metric: 0
        Forward Address: 0.0.0.0
        External Route Tag: 0

  LS age: 479
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-external-LSA
  Link State ID: 50.1.5.0 (External Network Number)
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000002
  Checksum: 0x6BBF
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 0
        Forward Address: 0.0.0.0
         External Route Tag: 0

Total Entries: 8
Switch#
```

70.31 show ip ospf database asbr-summary

Данная команда используется для отображения информации о суммарных (summary) LSA маршрутизатора Autonomous System Boundary Router (ASBR).

show ip ospf database asbr-summary [*LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Параметры

LINK-STATE-ID	(Опционально.) Укажите link state ID в виде IP-адреса.
self-originate	(Опционально.) Укажите self-originate link state.
adv-router	(Опционально.) Укажите, чтобы отобразить все summary LSA определенного маршрутизатора ASBR.
IP-ADDRESS	(Опционально.) Укажите IP-адрес анонсирующего маршрутизатора (Advertising Router).

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 суммарных (summary) LSA маршрутизатора ASBR.

Пример

В данном примере показано, как отобразить информацию о суммарных (summary) LSA маршрутизатора ASBR.

```
Switch#show ip ospf database asbr-summary

           OSPF Router with ID (1.1.1.1)

               ASBR-Summary Link States (Area 0.0.0.0)

  LS age: 893
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: ASBR-summary-LSA
  Link State ID: 10.47.65.160 (AS Boundary Router address)
  Advertising Router: 10.47.65.181
  LS Seq Number: 80000003
  Checksum: 0xB756
  Length: 28
  Network Mask: /0
        TOS: 0  Metric: 1

               ASBR-Summary Link States (Area 0.0.0.1)

  LS age: 927
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: ASBR-summary-LSA
  Link State ID: 10.47.65.183 (AS Boundary Router address)
  Advertising Router: 10.47.65.160
  LS Seq Number: 80000001
  Checksum: 0x53BA
  Length: 28
  Network Mask: /0
        TOS: 0  Metric: 1

Total Entries: 2
Switch#
```

70.32 show ip ospf database external

Данная команда используется для отображения информации о внешних (external) LSA.

show ip ospf database external [*LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Параметры

LINK-STATE-ID	(Опционально.) Укажите link state ID в виде IP-адреса.
self-originate	(Опционально.) Укажите self-originate link state.
adv-router	(Опционально.) Укажите, чтобы отобразить все внешние (external) LSA определенного маршрутизатора.
IP-ADDRESS	(Опционально.) Укажите IP-адрес анонсирующего маршрутизатора (advertise router).

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 внешних (external) LSA.

Пример

В данном примере показано, как отобразить информацию о внешних (external) LSA.

```
Switch#show ip ospf database external

           OSPF Router with ID (1.1.1.1)

               AS External Link States

  LS age: 631
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-external-LSA
  Link State ID: 50.1.2.0 (External Network Number)
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000002
  Checksum: 0x9A5
  Length: 36
  Network Mask: /24
        Metric Type: 1
        TOS: 0
        Metric: 0
        Forward Address: 0.0.0.0
        External Route Tag: 0

Total Entries: 1
Switch#
```

70.33 show ip ospf database network

Данная команда используется для отображения информации о сетевых (network) LSA.

show ip ospf database network [*LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Параметры

LINK-STATE-ID	(Опционально.) Укажите link state ID в виде IP-адреса.
self-originate	(Опционально.) Укажите self-originate link state.
adv-router	(Опционально.) Укажите, чтобы отобразить все сетевые (network) LSA определенного маршрутизатора.
IP-ADDRESS	(Опционально.) Укажите IP-адрес анонсирующего маршрутизатора (advertise router).

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 сетевых (network) LSA.

Пример

В данном примере показано, как отобразить информацию о сетевых (network) LSA.

```
Switch#show ip ospf database network

           OSPF Router with ID (1.1.1.1)

               Net Link States (Area 0.0.0.0)

  LS age: 1024
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: network-LSA
  Link State ID: 10.1.1.1 (address of Designated Router)
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000001
  Checksum: 0xE6ED
  Length: 32
  Network Mask: /24
        Attached Router: 1.1.1.1
        Attached Router: 10.1.1.100

Total Entries: 1
Switch#
```

70.34 show ip ospf database nssa-external

Данная команда используется для отображения информации об NSSA-external LSA.

show ip ospf database nssa-external [*LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Параметры

LINK-STATE-ID	(Опционально.) Укажите link state ID в виде IP-адреса.
self-originate	(Опционально.) Укажите self-originate link state.
adv-router	(Опционально.) Укажите, чтобы отобразить все NSSA-external LSA определенного маршрутизатора.
IP-ADDRESS	(Опционально.) Укажите IP-адрес анонсирующего маршрутизатора (advertise router).

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об NSSA-external LSA.

Пример

В данном примере показано, как отобразить информацию об NSSA-external LSA.

```
Switch##show ip ospf database nssa-external

           OSPF Router with ID (30.1.1.1)

               NSSA-external Link States (Area 0.0.0.61)

  LS age: 1161
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 1.0.0.0 (External Network Number For NSSA)
  Advertising Router: 10.47.65.160
  LS Seq Number: 80000001
  Checksum: 0x82E6
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        NSSA: Forward Address: 110.201.0.1
        External Route Tag: 0
```

```
  LS age: 1097
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 47.65.55.0 (External Network Number For NSSA)
  Advertising Router: 10.47.65.160
  LS Seq Number: 80000001
  Checksum: 0xBB07
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        NSSA: Forward Address: 110.201.0.1
        External Route Tag: 0

Total Entries: 2
Switch#
```

70.35 show ip ospf database self-originate

Данная команда используется для отображения LSA, сгенерированных локальным маршрутизатором.

show ip ospf database self-originate

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 LSA, сгенерированные локальным маршрутизатором.

Пример

В данном примере показано, как отобразить LSA, сгенерированные локальным маршрутизатором.

```
Switch#show ip ospf database self-originate

           OSPF Router with ID (1.1.1.1)

               Router Link States (Area 0.0.0.0)

  LS age: 38
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x2 ASBR
  LS Type: router-LSA
  Link State ID: 1.1.1.1
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000004
  Checksum: 0x78B3
  Length: 36
  Number of Links: 1
    Link connected to a Transit Network
     (Link ID) Designated Router address: 10.1.1.1
     (Link Data) Router Interface address: 10.1.1.1
      Number of TOS metrics: 0
       TOS 0 Metric: 1

Total Entries: 1
Switch#
```

70.36 show ip ospf database router

Данная команда используется для отображения информации об LSA маршрутизатора (router LSA).

show ip ospf database router [*LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Параметры

LINK-STATE-ID	(Опционально.) Укажите link state ID в виде IP-адреса.
self-originate	(Опционально.) Укажите self-originate link state.
adv-router	(Опционально.) Укажите, чтобы отобразить все router LSA определенного маршрутизатора.
IP-ADDRESS	(Опционально.) Укажите IP-адрес анонсирующего маршрутизатора (advertise router).

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об LSA маршрутизатора (router LSA).

Пример

В данном примере показано, как отобразить информацию об LSA маршрутизатора (router LSA).

```
Switch#show ip ospf database router

           OSPF Router with ID (1.1.1.1)

               Router Link States (Area 0.0.0.0)

  LS age: 246
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x2 ASBR
  LS Type: router-LSA
  Link State ID: 1.1.1.1
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000004
  Checksum: 0x78B3
  Length: 36
  Number of Links: 1
    Link connected to a Transit Network
     (Link ID) Designated Router address: 10.1.1.1
     (Link Data) Router Interface address: 10.1.1.1
      Number of TOS metrics: 0
       TOS 0 Metric: 1

  LS age: 106
  Options: 0x0 (*|-|-|-|-|-|-|-)
  Flags: 0x3 ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.1.1.100
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000009
  Checksum: 0xA43E
  Length: 36
  Number of Links: 1
    Link connected to a Transit Network
     (Link ID) Designated Router address: 10.1.1.1
     (Link Data) Router Interface address: 10.1.1.100
      Number of TOS metrics: 0
       TOS 0 Metric: 10

Total Entries: 2
Switch#
```

70.37 show ip ospf database stub

Данная команда используется для отображения информации об LSA в тупиковой зоне (Stub Area) и зоне NSSA.

show ip ospf database stub [*LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Параметры

LINK-STATE-ID	(Опционально.) Укажите link state ID в виде IP-адреса.
self-originate	(Опционально.) Укажите self-originate link state.
adv-router	(Опционально.) Укажите, чтобы отобразить все LSA определенного маршрутизатора в тупиковой зоне (Stub Area) и зоне NSSA.
IP-ADDRESS	(Опционально.) Укажите IP-адрес анонсирующего маршрутизатора (advertise router).

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об LSA в тупиковой зоне (Stub Area) и зоне NSSA.

Пример

В данном примере показано, как отобразить информацию об LSA в тупиковой зоне (Stub Area) и зоне NSSA.

```
Switch#show ip ospf database stub

           OSPF Router with ID (1.1.1.1)

               Router Link States (Area 0.0.0.2)

  LS age: 593
  Options: 0x0 (*|-|-|-|-|-|-|-)
  Flags: 0x13 ABR ASBR
  LS Type: router-LSA
  Link State ID: 1.1.1.1
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000003
  Checksum: 0x3BEF
  Length: 36
  Number of Links: 1
    Link connected to Stub Network
     (Link ID) Network/subnet number: 10.1.1.0
     (Link Data) Network Mask: 255.255.255.0
      Number of TOS metrics: 0
        TOS 0 Metric: 1

               Summary Link States (Area 0.0.0.2)

  LS age: 632
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 20.1.1.0 (summary Network Number)
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000001
  Checksum: 0x59EA
  Length: 28
  Network Mask: /24
        TOS: 0 Metric: 1

  LS age: 632
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 30.1.1.0 (summary Network Number)
  Advertising Router: 1.1.1.1
```

```
  LS Seq Number: 0x80000001
  Checksum: 0x59EA
  Length: 28
  Network Mask: /24
        TOS: 0 Metric: 1

  LS age: 632
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 30.1.1.0 (summary Network Number)
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000001
  Checksum: 0xD663
  Length: 28
  Network Mask: /24
        TOS: 0 Metric: 1

Total Entries: 3
Switch#
```

70.38 show ip ospf database summary

Данная команда используется для отображения информации о суммарных (summary) LSA.

show ip ospf database summary [*LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Параметры

LINK-STATE-ID	(Опционально.) Укажите link state ID в виде IP-адреса.
self-originate	(Опционально.) Укажите self-originate link state.
adv-router	(Опционально.) Укажите, чтобы отобразить все суммарные (summary) LSA определенного маршрутизатора.
IP-ADDRESS	(Опционально.) Укажите IP-адрес анонсирующего маршрутизатора (advertise router).

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 суммарных (summary) LSA.

Пример

В данном примере показано, как отобразить информацию о суммарных (summary) LSA.

```
Switch#show ip ospf database summary

           OSPF Router with ID (1.1.1.1)

               Summary Link States (Area 0.0.0.0)

  LS age: 223
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 50.1.1.0 (summary Network Number)
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000003
  Checksum: 0x1E9A
  Length: 28
  Network Mask: /24
        TOS: 0 Metric: 0

  LS age: 223
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 50.1.2.0 (summary Network Number)
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000003
  Checksum: 0x13A4
  Length: 28
  Network Mask: /24
        TOS: 0 Metric: 0

  LS age: 223
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 50.1.3.0 (summary Network Number)
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000003
  Checksum: 0x8AE
  Length: 28
  Network Mask: /24
        TOS: 0 Metric: 0

Total Entries: 3
Switch#
```

70.39 show ip ospf interface

Данная команда используется для отображения информации об OSPF на интерфейсе.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса, который необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об OSPF на интерфейсе. Если интерфейс не указан, будет отображена информация об OSPF на всех интерфейсах.

Пример

В данном примере показано, как отобразить информацию об OSPF на интерфейсе.

```
Switch#show ip ospf interface

vlan1 is up, line protocol is up
  Internet Address: 10.1.1.1/24, Area 0.0.0.0
  Process ID 1 Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, Interface Address 10.1.1.1
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Current Authentication Type: none

vlan100 is up, line protocol is up
  Internet Address: 20.1.1.1/24, Area 0.0.0.0
  Process ID 2 Router ID 1.1.1.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.2, Interface Address 20.1.1.1
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Current Authentication Type: none

vlan101 is up, line protocol is up
  Internet Address: 30.1.1.1/24, Area 0.0.0.0
  Process ID 3 Router ID 1.1.1.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.3, Interface Address 30.1.1.1
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Current Authentication Type: none

Total Entries: 3
Switch#
```

70.40 show ip ospf neighbor

Данная команда используется для отображения информации о соседних устройствах OSPF.

show ip ospf neighbor [interface *INTERFACE-ID* **|** *NEIGHBOR-ID***] [detail]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите ID интерфейса, который необходимо отобразить.
NEIGHBOR-ID	(Опционально.) Укажите ID соседнего устройства.
detail	(Опционально.) Укажите, чтобы отобразить подробную информацию о соседних устройствах.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об OSPF на интерфейсе. Если интерфейс не указан, будет отображена информация об OSPF на всех интерфейсах.

Пример

В данном примере показано, как отобразить информацию о соседних устройствах OSPF.

```
Switch#show ip ospf neighbor

Neighbor ID      Pri   State           Address         Interface
---------------- ----- --------------- --------------- ------------
10.1.1.100       0     Full/DROther    10.1.1.100      vlan1
20.1.1.100       0     Full/DROther    20.1.1.100      vlan100
30.1.1.100       0     Full/DROther    30.1.1.100      vlan101

Total Entries: 3
Switch#
```

В примере ниже показано, как отобразить подробную информацию о соседних устройствах OSPF.

```
Switch#show ip ospf neighbor detail

Neighbor 10.1.1.100, interface  address 10.1.1.100
    In the area 0.0.0.0 via interface vlan1
    Neighbor priority is 0, State is Full, 6 state change
    DR is 10.1.1.1, BDR is 0.0.0.0
    Options: 0x2 (*|-|-|-|-|-|E|-)

Neighbor 20.1.1.100, interface  address 20.1.1.100
    In the area 0.0.0.0 via interface vlan100
    Neighbor priority is 0, State is Full, 6 state change
    DR is 20.1.1.1, BDR is 0.0.0.0
    Options: 0x2 (*|-|-|-|-|-|E|-)

Neighbor 30.1.1.100, interface  address 30.1.1.100
    In the area 0.0.0.0 via interface vlan101
    Neighbor priority is 0, State is Full, 6 state change
    DR is 30.1.1.1, BDR is 0.0.0.0
    Options: 0x2 (*|-|-|-|-|-|E|-)

Total Entries: 3
Switch#
```

70.41 show ip ospf virtual-links

Данная команда используется для отображения информации о виртуальных каналах (virtual link).

show ip ospf virtual-links

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 виртуальных каналах (virtual link).

Пример

В данном примере показано, как отобразить информацию о виртуальных каналах (virtual link).

```
Switch#show ip ospf virtual-links

Virtual Link to router 2.2.2.2 is down, Process ID 1
  Transit area 0.0.0.1
  Transmit Delay is 1 sec, State DOWN
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Current Authentication Type: none

Total Entries: 1
Switch#
```

70.42 debug ip ospf

Данная команда используется для включения функции отладки OSPF. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

debug ip ospf
no debug ip ospf

Параметры

Нет.

По умолчанию

По умолчанию функция отладки OSPF отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию отладки OSPF. Перед применением данной команды убедитесь, что функция отладки включена глобально.

Пример

В данном примере показано, как включить функцию отладки OSPF.

```
Switch#debug ip ospf
Switch#
```

70.43 debug ip ospf neighbor

Данная команда используется для включения функции отладки соседних устройств OSPF на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

debug ip ospf neighbor
no debug ip ospf neighbor

Параметры

Нет.

По умолчанию

По умолчанию функция отладки соседних устройств OSPF на коммутаторе отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию отладки соседних устройств OSPF на коммутаторе. Если при включенной функции статус соседнего устройства изменится или произойдет какое-то другое событие, которое касается изменения статуса соседнего устройства, то отобразится информация об отладке.

Пример

В данном примере показано, как включить функцию отладки соседних устройств OSPF на коммутаторе.

```
Switch#debug ip ospf neighbor
Switch#

NBR 2.2.2.2 state change from LOADING to FULL tic 100
NBR 3.3.3.3 state change from FULL to DOWN tic 100
```

70.44 debug ip ospf interface

Данная команда используется для включения функции отладки OSPF на интерфейсе коммутатора. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

debug ip ospf interface
no debug ip ospf interface

Параметры

Нет.

По умолчанию

По умолчанию функция отладки OSPF на интерфейсе коммутатора отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию отладки OSPF на интерфейсе коммутатора. Если при включенной функции на интерфейсе изменится статус OSPF или произойдет какое-то другое событие, которое касается изменения статуса интерфейса, то отобразится информация об отладке. Информация об отладке также отображается при назначении DR.

Пример

В данном примере показано, как включить функцию отладки OSPF на интерфейсе коммутатора.

```
Switch#debug ip ospf interface
Switch#

intf 10.1.1.1 up tic 10
intf 100.1.1.1 down tic 20
OSPF: Select DR: 2.2.2.2
OSPF: Select BDR: 1.1.1.1
```

70.45 debug ip ospf log

Данная команда используется для включения отправки syslog-сообщений OSPF на маршрутизаторе. Чтобы отключить отправку syslog-сообщений OSPF, воспользуйтесь формой **no** этой команды.

debug ip ospf log
no debug ip ospf log

Параметры

Нет.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить/отключить отправку syslog-сообщений OSPF на маршрутизаторе.

Пример

В данном примере показано, как включить отправку syslog-сообщений OSPF на маршрутизаторе.

```
Switch#debug ip ospf log
#60    2018-04-03 11:26:32 INFO(6) OSPF-6-INTFSTATECHANGE: OSPF interface vlan1 changed state
to Up.
#61    2018-04-03 11:26:34 NOTI(5) OSPF-5-NBRLOADINGTOFULL: OSPF nbr 2.2.2.2 on interface
vlan1 changed state from Loading to Full.
Switch#
```

70.46 debug ip ospf lsa-originating

Данная команда используется для включения функции отладки OSPF при возникновении LSA на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

debug ip ospf lsa-originating
no debug ip ospf lsa-originating

Параметры

Нет.

По умолчанию

По умолчанию функция отладки OSPF при возникновении LSA на коммутаторе отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию отладки OSPF при возникновении LSA на коммутаторе. Когда функция включена и возникло хотя бы одно LSA, отобразится информация об отладке.

Пример

В данном примере показано, как включить функцию отладки OSPF при возникновении LSA на коммутаторе.

```
Switch#debug ip ospf lsa-originating
Build Router LSA id 100.1.1.2 for area 0.0.0.0 seq 80000001 tic 10 proc_id 1
Switch#
```

70.47 debug ip ospf lsa-flooding

Данная команда используется для включения функции отладки OSPF при лавинном распространении LSA на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

debug ip ospf lsa-flooding
no debug ip ospf lsa-flooding

Параметры

Нет.

По умолчанию

По умолчанию функция отладки OSPF при лавинном распространении LSA на коммутаторе отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию отладки OSPF при лавинном распространении LSA на коммутаторе. Когда функция включена и хотя бы одно LSA получено, добавлено в локальную базу данных или перенаправлено на соседний маршрутизатор, отображается информация об отладке.

Пример

В данном примере показано, как включить функцию отладки OSPF при лавинном распространении LSA на коммутаторе.

```
Switch#debug ip ospf lsa-flooding
Switch#

Received LSA type 1 id 2.2.2.2 from nbr 2.2.2.2 in area 0.0.0.0 seq 80000001 csum fe3a tic 15
Flood LSAs in area 0.0.0.0 tic 15
```

70.48 debug ip ospf packet-receiving

Данная команда используется для включения функции отладки при получении пакетов OSPF на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

debug ip ospf packet-receiving
no debug ip ospf packet-receiving

Параметры

Нет.

По умолчанию

По умолчанию функция отладки при получении пакетов OSPF на коммутаторе отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию отладки при получении пакетов OSPF на коммутаторе. Когда функция включена и получено хотя бы одно сообщение протокола OSPF, отображается информация об отладке.

Пример

В данном примере показано, как включить функцию отладки при получении пакетов OSPF на коммутаторе.

```
Switch#debug ip ospf packet-receiving
Received a Hello packet from addr 10.1.1.2 at interface 10.90.90.90 tic 100
Received a Hello packet from addr 100.1.1.2 at interface 100.90.90.90 tic 102
Switch#
```

70.49 debug ip ospf packet-transmitting

Данная команда используется для включения функции отладки при отправке пакетов OSPF на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

debug ip ospf packet-transmitting
no debug ip ospf packet-transmitting

Параметры

Нет.

По умолчанию

По умолчанию функция отладки при отправке пакетов OSPF на коммутаторе отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию отладки при отправке пакетов OSPF на коммутаторе. Когда функция включена и отправлено хотя бы одно сообщение протокола OSPF, отображается информация об отладке.

Пример

В данном примере показано, как включить функцию отладки при отправке пакетов OSPF на коммутаторе.

```
Switch#debug ip ospf packet-transmitting
Send out a Hello on interface 10.1.1.1 dst 224.0.0.5 tic 200
Send out a Hello on interface 100.1.1.1 dst 224.0.0.5 tic 220
Switch#
```

70.50 debug ip ospf spf

Данная команда используется для включения функции отладки OSPF при расчете SPF на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

debug ip ospf spf
no debug ip ospf spf

Параметры

Нет.

По умолчанию

По умолчанию функция отладки OSPF при расчете SPF на коммутаторе отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию отладки OSPF при расчете SPF на коммутаторе. Когда функция включена и производится расчет SPF, отображается информация об отладке.

Пример

В данном примере показано, как включить функцию отладки OSPF при расчете SPF на коммутаторе.

```
Switch#debug ip ospf spf
Running SPF-intra for area 0.0.0.0 tic 300  proc_id 1
SPF-intra calculation completed tic 310
Switch#
```

70.51 debug ip ospf timer

Данная команда используется для включения функции отладки таймера OSPF на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

debug ip ospf timer
no debug ip ospf timer

Параметры

Нет.

По умолчанию

По умолчанию функция отладки таймера OSPF на коммутаторе отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию отладки таймера OSPF на коммутаторе. Когда функция включена и происходит событие, которое касается таймера OSPF, отображается информация об отладке.

Пример

В данном примере показано, как включить функцию отладки таймера OSPF на коммутаторе.

```
Switch#debug ip ospf timer
Start Hello timer at interface 10.90.90.90 tic 20
Wait timer expired at interface 10.90.90.90 tic 100
Switch#
```

70.52 debug ip ospf virtual-link

Данная команда используется для включения функции отладки виртуального канала OSPF (virtual link) на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

debug ip ospf virtual-link

no debug ip ospf virtual-link

Параметры

Нет.

По умолчанию

По умолчанию функция отладки виртуального канала OSPF (virtual link) на коммутаторе отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию отладки виртуального канала OSPF (virtual link) на коммутаторе. Когда произойдет событие, которое касается виртуального канала OSPF, будет отображена информация об отладке.

Пример

В данном примере показано, как включить функцию отладки виртуального канала OSPF (virtual link) на коммутаторе.

```
Switch#debug ip ospf virtual-link
Virtual link up transit area 1.1.1.1 vnbr 3.3.3.3 tic 260
Switch#
```

70.53 debug ip ospf route

Данная команда используется для включения функции отладки маршрутов OSPF на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

debug ip ospf route

no debug ip ospf route

Параметры

Нет.

По умолчанию

По умолчанию функция отладки маршрутов OSPF на коммутаторе отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию отладки маршрутов OSPF на коммутаторе. Когда при включенной функции будет добавлен, обновлен или удален хотя бы один маршрут, то отобразится информация об отладке.

Пример

В данном примере показано, как включить функцию отладки маршрутов OSPF на коммутаторе.

```
Switch#debug ip ospf route
Add an OSPF route level 1 dst 172.18.1.1 mask 255.255.255.0  nh cnt 1 cost 10 cost2: 0 tic:
300 proc_id 1
Switch#
```

70.54 debug ip ospf redistribution

Данная команда используется для включения функции отладки при перераспределении OSPF на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

debug ip ospf redistribution

no debug ip ospf redistribution

Параметры

Нет.

По умолчанию

По умолчанию функция отладки при перераспределении OSPF на коммутаторе отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию отладки при перераспределении OSPF на коммутаторе. Если при включенной функции один маршрут был перераспределен в OSPF из другого протокола или больше не перераспределяется в OSPF, то будет отображена информация об отладке.

Пример

В данном примере показано, как включить функцию отладки при перераспределении OSPF на коммутаторе.

```
Switch#debug ip ospf redistribution
Import AS external route from src 5 net 192.1.1.1  mask 255.255.255.0 type 2 cost 50 fwd
10.1.1.100 tic 500
Switch#
```

70.55 debug ip ospf show counter

Данная команда используется для отображения счетчиков статистики OSPF.

debug ip ospf show counter [packet | neighbor | spf]

Параметры

packet	(Опционально.) Укажите, чтобы отобразить счетчик OSPF-пакетов.
neighbor	(Опционально.) Укажите, чтобы отобразить счетчик соседних устройств OSPF.
spf	(Опционально.) Укажите, чтобы отобразить счетчик событий OSPF SPF.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы проверить информацию о статистике пакетов OSPF, соседних устройств OSPF или расчетов SPF.

Пример

В данном примере показано, как отобразить все счетчики статистики OSPF.

```
Switch#debug ip ospf show counter

OSPF Debug Statistic Counters
Packet Receiving:
  Total   : 5
  Hello   : 5
  DD      : 0
  LSR     : 0
  LSU     : 0
  LSAck   : 0
  Drop    : 0
  Auth Fail : 0

Packet Sending:
  Total   : 5
  Hello   : 5
  DD      : 0
  LSR     : 0
  LSU     : 0
  LSAck   : 0

Neighbor State:
  Change : 3
  SeqMismatch : 0

SPF Calculation:
  Intra  : 1
  Inter  : 1
  Extern : 1

Switch#
```

70.56 debug ip ospf clear counter

Данная команда используется для сброса счетчиков статистики OSPF.

debug ip ospf clear counter [packet | neighbor | spf]

Параметры

packet	(Опционально.) Укажите, чтобы сбросить счетчик пакетов OSPF.
neighbor	(Опционально.) Укажите, чтобы сбросить счетчик соседних устройств OSPF.
spf	(Опционально.) Укажите, чтобы сбросить счетчик событий OSPF SPF.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы сбросить счетчики статистики OSPF. После сброса значение указанных счетчиков будет изменено на 0.

Пример

В данном примере показано, как сбросить все счетчики статистики OSPF.

```
Switch#debug ip ospf clear counter
Switch#
```

70.57 debug ip ospf show database

Данная команда используется для отображения подробной информации об OSPF LSDB.

debug ip ospf show database {rt-link | net-link | summary-link | external-link | type7-link}

Параметры

rt-link	Укажите, чтобы отобразить подробную информацию об LSA маршрутизатора (router LSA).
net-link	Укажите, чтобы отобразить подробную информацию о сетевых (network) LSA.
summary-link	Укажите, чтобы отобразить подробную информацию о суммарных (summary) LSA.

external-link	Укажите, чтобы отобразить подробную информацию об AS external LSA.
type7-link	Укажите, чтобы отобразить подробную информацию об LSA типа 7.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы отобразить подробную информацию об OSPF LSDB.

Пример

В данном примере показано, как отобразить подробную информацию об LSA маршрутизатора.

```
Switch#debug ip ospf show database rt-link

OSPF Phase2 RT Link (Process ID 1):

===========
AREA 0.0.0.0:
 Router LSA:
 Link-State ID: 100.1.1.2
 Advertising Router: 100.1.1.2
 LS Age: 10 Seconds
 Options: 0x2
 .... ...0 = 0 Bit Isn't Set
 .... ..1. = E: ExternalRoutingCapability
 .... .0.. = MC: NOT Multicast Capable
 .... 0... = N/P: NSSA Bit
 ...0 .... = EA: Not Support Rcv And Fwd EA_LSA
 ..0. .... = DC: Not Support Handling Of Demand Circuits
 .0.. .... = O: O Bit Isn't Set
 0... .... = 7 Bit Isn't Set
```

```
LS Sequence Number: 0x80000001
Length: 36
Flags: 0x0
.... ...0 = B: NO Area Border Router
.... ..0. = E: NO AS Boundary Router
.... .0.. = V: NO Virtual Link Endpoint
Number Of Links: 1
Type: Stub       ID: 10.1.1.0         Data: 255.255.255.0    Metric: 1
Internal Field:
Del_flag: 0x0  I_ref_count: 0  Seq: 0x80000001  Csum: 0x4D28
Rxtime: 0  Txtime: 0  Orgage: 0
Current Time: 10

Switch#
```

70.58 debug ip ospf show request-list

Данная команда используется для отображения текущей информации об LSA внутреннего списка запросов OSPF.

debug ip ospf show request-list

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы проверить информацию об LSA, которую OSPF запрашивает у соседних устройств.

Пример

В данном примере показано, как отобразить текущие запрашиваемые LSA.

```
Switch#debug ip ospf show request-list

OSPF Request List (Process ID 1):

Area 0.0.0.0:
Circuit: 1.1.1.1
Neighbor: 90.2.0.1  IP: 1.1.1.2
 LSID: 192.194.134.0  RTID: 90.2.0.1
 LSID: 192.194.135.0  RTID: 90.2.0.1
 LSID: 192.194.136.0  RTID: 90.2.0.1
 LSID: 192.194.137.0  RTID: 90.2.0.1
 LSID: 192.194.138.0  RTID: 90.2.0.1

Switch#
```

70.59 debug ip ospf show redistribution

Данная команда используется для отображения текущего внутреннего списка перераспределения OSPF.

debug ip ospf show redistribution

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы отобразить информацию о внешних (external) маршрутах, которые импортированы в OSPF.

Пример

В данном примере показано, как отобразить внешние (external) маршруты, импортированные в OSPF.

```
Switch#debug ip ospf show redistribution

OSPF Redistribution List (Process ID 1):

IP                  Nexthop          State Type Tag
------------------  ---------------  ----- ---- ---------------
1.1.1.0/24          0.0.0.0          ON    2    0.0.0.0

OSPF ASE Table (Process ID 1):

IP                  Nexthop          State Type Tag
------------------  ---------------  ----- ---- ---------------
1.1.1.0/24          0.0.0.0          ON    2    0.0.0.0

Switch#
```

70.60 debug ip ospf show summary-list

Данная команда используется для отображения текущего внутреннего суммарного (summary) списка OSPF.

debug ip ospf show summary-list

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы отобразить информацию о суммированном маршруте.

Пример

В данном примере показано, как отобразить информацию о суммированном маршруте.

```
Switch#debug ip ospf show summary-list

OSPF Summary List (Process ID 1):

Area 0.0.0.0:
Circuit: 1.1.1.1
Neighbor: 90.2.0.1  IP: 1.1.1.2
LSID: 1.1.1.1 RTID: 1.1.1.1

Circuit: 2.2.2.1

Circuit: 10.1.1.6

Switch#
```

71. Команды Open Shortest Path First Version 3 (OSPFv3)

71.1 area default-cost

Данная команда используется, чтобы установить стоимость по умолчанию (summary-default cost) тупиковой зоны (Stub Area). Для отключения этой функции воспользуйтесь формой **no** этой команды.

area *AREA-ID* **default-cost** *COST*
no area *AREA-ID* **default-cost**

Параметры

AREA-ID	Укажите ID зоны в виде адреса IPv4.
COST	Укажите метрику или стоимость для маршрута, которую OSPF будет использовать для вычисления кратчайшего пути к адресу назначения. Диапазон значений: от 0 до 65535.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применяется только на пограничном маршрутизаторе (ABR), подключенном к тупиковой зоне (Stub Area). На всех маршрутизаторах и серверах доступа, подключенных к тупиковой зоне, зона должна быть сконфигурирована командой **area stub** как тупиковая. Используйте команду **area default-cost** только на ABR, подключенном к тупиковой зоне. Команда **area default-cost** задает метрику для маршрута по умолчанию, генерируемого ABR в тупиковую зону.

Пример

В данном примере показано, как назначить стоимость по умолчанию для тупиковой зоны 1. Установленное значение – 10.

```
Switch#configure terminal
Switch(config)#ipv6 router ospf 1000
Switch(config-rtr)#area 0.0.0.1 stub
Switch(config-rtr)#area 0.0.0.1 default-cost 10
Switch(config-rtr)#
```

71.2 area range

Данная команда используется для объединения и суммирования маршрутов на границе зоны. Для отключения этой функции воспользуйтесь формой **no** этой команды.

area *AREA-ID* **range** *IPv6-PREFIX/PREFIX-LENGTH* **[advertise | not-advertise]**
no area *AREA-ID* **range** *IPv6-PREFIX/PREFIX-LENGTH*

Параметры

AREA-ID	Укажите ID зоны, маршруты которой необходимо объединить. ID задается в виде адреса IPv4.
IPv6-PREFIX	Укажите префикс IPv6.
PREFIX-LENGTH	Укажите длину префикса IPv6.
advertise	(Опционально.) Укажите, чтобы анонсировать inter-area prefix LSA для заданного диапазона адресов.
not-advertise	(Опционально.) Укажите, чтобы отключить анонсирование inter-area prefix LSA. Маршруты, входящие в состав объединенного, по-прежнему скрыты за ним.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется только на ABR для объединения и суммирования маршрутов на границе зоны. Полученный в результате единый суммарный маршрут анонсируется ABR в другие зоны. Маршрутная информация уплотняется на границах зоны. Единый маршрут, находящийся за пределами указанной зоны, анонсируется для каждого диапазона адресов.

Пример

В данном примере показано, как сконфигурировать один суммарный маршрут, который будет анонсироваться ABR в другие зоны для префикса IPv6 2001:0DB8:0:1::/64 и для Router ID 20.0.1.10.

```
Switch#configure terminal
Switch(config)#ipv6 router ospf 1000
Switch(config-rtr)#router-id 20.0.1.10
Switch(config-rtr)#area 0.0.0.1 range 2001:0DB8:0:1::/64
Switch(config-rtr)#
```

71.3 area stub

Данная команда используется для назначения зоны в качестве тупиковой зоны (Stub Area). Для отключения этой функции воспользуйтесь формой **no** этой команды.

area *AREA-ID* **stub [no-summary]**
no area *AREA-ID* **stub [no-summary]**

Параметры

AREA-ID	Укажите ID зоны в виде IPv4-адреса.
no-summary	(Опционально.) Укажите, чтобы отключить отправку inter-area prefix LSA в тупиковую зону (Stub Area).

По умолчанию
По умолчанию данная функция отключена.

Режим ввода команды
Router Configuration Mode.

Уровень команды по умолчанию
Уровень 12.

Использование команды
При использовании команды **no area** *AREA-ID* **stub** будут удалены все настройки, связанные с назначенной тупиковой зоной (Stub Area). Зона становится нормальной зоной (Normal Area). Команда применяется на всех маршрутизаторах в тупиковой зоне.

Используйте параметр **no-summary**, чтобы назначить тупиковую зону в качестве Total Stubby Area. Маршрутизаторам в данной зоне не требуется изучение маршрутов inter-area, за исключением маршрута по умолчанию.

Пример
В данном примере показано, как настроить маршрутизатор как тупиковый (stub), который анонсирует подключенные и суммарные маршруты.

```
Switch#configure terminal
Switch(config)#ipv6 router ospf 1000
Switch(config-rtr)#router-id 20.0.1.10
Switch(config-rtr)#area 1.1.1.1 stub
Switch(config-rtr)#
```

71.4 area virtual-link

Данная команда используется для настройки виртуального канала (virtual link) через немагистральную зону (Non-Backbone Area), которая физически отделена от магистральной зоны (Backbone Area). Чтобы удалить виртуальный канал или вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

area *AREA-ID* **virtual-link** *ROUTER-ID* **[hello-interval** *SECONDS***] [dead-interval** *SECONDS***] [transmit-delay** *SECONDS***] [retransmit-interval** *SECONDS***] [instance** *INSTANCE-ID***]**

no area *AREA-ID* **virtual-link** *ROUTER-ID* **[hello-interval] [dead-interval] [transmit-delay] [retransmit-interval]**

Параметры

AREA-ID	Укажите ID зоны в виде IPv4-адреса.
ROUTER-ID	Укажите ID соседнего маршрутизатора канала. ID задается в виде IPv4-адреса.
hello-interval *SECONDS*	(Опционально.) Укажите интервал между пакетами hello, которые маршрутизатор отправляет на интерфейс. Диапазон значений: от 1 до 65535 секунд.
dead-interval *SECONDS*	(Опционально.) Укажите интервал, по истечении которого соседнее устройство считается недоступным, если за это время не было получено ни одного пакета. Диапазон значений: от 1 до 65535 секунд.
transmit-delay *SECONDS*	(Опционально.) Укажите интервал, по истечении которого маршрутизатор будет отправлять пакет. Диапазон значений: от 1 до 65535 секунд.
retransmit-interval *SECONDS*	(Опционально.) Укажите интервал, по истечении которого маршрутизатор будет повторно отправлять пакет. Диапазон значений: от 1 до 65535 секунд.
instance-id *INSTANCE-ID*	(Опционально.) Укажите ID экземпляра.

По умолчанию

Виртуальные каналы IPv6 OSPF по умолчанию не настроены.
hello-interval *SECONDS*: 10 секунд.
dead-interval *SECONDS*: 40 секунд.
transmit-delay *SECONDS*: 1 секунда.
retransmit-interval *SECONDS*: 5 секунд.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Все зоны в автономной системе IPv6 OSPF должны быть физически подключены к магистральной зоне (Area 0). В некоторых случаях, когда физическое подключение невозможно, используется виртуальный канал (virtual link) для подключения к магистрали через немагистральную зону (Non-Backbone Area). Настройка виртуального канала позволяет соединить две части разделенной магистрали через немагистральную зону. Зона, в которой настраивается виртуальный канал,

называется транзитной. Транзитная зона (Transit Area) должна иметь полную маршрутную информацию. Нельзя назначить транзитную зону в качестве тупиковой зоны (Stub Area).

Значение интервала hello должно быть одинаковым для всех маршрутизаторов, подключенных к общей сети. Чем меньше значение интервала hello, тем быстрее будут обнаружены изменения в топологии, но при этом будет увеличен маршрутный трафик.

Как и в случае с интервалом hello, значение интервала dead должно быть одинаковым для всех маршрутизаторов и серверов доступа, подключенных к общей сети.

Интервал retransmit связан с ожидаемым временем задержки приема/передачи (Round-Trip Delay) между двумя маршрутизаторами в сети. Установите значение больше ожидаемого времени задержки приема/передачи, чтобы избежать ненужных повторных передач.

Интервал transmit-delay – это время, требуемое для передачи пакета обновления состояния канала (Link State Update, LSU) на интерфейс. Перед отправкой LSU увеличиваются на это значение. Установите интервал transmit-delay больше нуля. Учитывайте также задержку передачи и прохождения, установленную для интерфейса.

Для настройки виртуального канала в IPv6 OSPF используйте Router ID вместо адреса и IPv6-префикса удаленного маршрутизатора.

Пример

В данном примере показано, как настроить виртуальный канал. Значения опциональных параметров указаны по умолчанию.

```
Switch#configure terminal
Switch(config)#ipv6 router ospf 1000
Switch(config-rtr)#area 0.0.0.1 virtual-link 192.168.255.1
Switch(config-rtr)#
```

71.5 auto-cost reference-bandwidth

Данная команда применяется для указания референсного значения пропускной способности (reference-bandwidth), используемого IPv6 OSPF при вычислении метрики для интерфейсов. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

auto-cost reference-bandwidth *MBPS*
no auto-cost reference-bandwidth

Параметры

MBPS	Укажите пропускную способность в Мбит/с. Диапазон значений: от 1 до 4294967 Мбит/с.

По умолчанию

Значение по умолчанию – 100 Мбит/с.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию
Уровень 12.

Использование команды
Данная команда позволяет указать референсное значение пропускной способности (reference-bandwidth), используемое IPv6 OSPF при вычислении метрики для интерфейсов.

Пример
В данном примере показано, как указать значение auto-cost reference bandwidth. Установленное значение – 1000 Мбит/с.

```
Switch#configure terminal
Switch(config)#ipv6 router ospf 1000
Switch(config-rtr)#auto-cost reference-bandwidth 1000
Switch(config-rtr)#
```

71.6 clear ipv6 ospf

Данная команда используется для перезапуска OSPF на основе ID процесса маршрутизации OSPF.

clear ipv6 ospf [*PROCESS-ID***] process**

Параметры

PROCESS-ID	(Опционально.) Укажите внутренний ID процесса маршрутизации IPv6 OSPF. ID назначается локально в виде любого положительного числа. Для каждого процесса маршрутизации IPv6 OSPF задается уникальное значение.

По умолчанию
Нет.

Режим ввода команды
Privileged EXEC Mode.

Уровень команды по умолчанию
Уровень 12.

Использование команды
База данных OSPF удаляется, заполняется снова, а затем выполняется алгоритм OSPF. Если параметры не указаны, удаляются все процессы OSPF.

Пример
В данном примере показано, как удалить все процессы OSPF.

```
Switch#clear ipv6 ospf process
Switch#
```

71.7 default-metric

Данная команда используется для того, чтобы установить метрику по умолчанию для IPv6 OSPF. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

default-metric *METRIC-VALUE*
no default-metric

Параметры

METRIC-VALUE	Укажите значение метрики по умолчанию. Диапазон значений: от 1 до 16777214.

По умолчанию
Значение метрики по умолчанию – 20.

Режим ввода команды
Router Configuration Mode.

Уровень команды по умолчанию
Уровень 12.

Использование команды
Команда **default-metric** применяется вместе с командой **redistribute** для настройки общего значения метрики для всех перераспределяемых маршрутов текущего протокола маршрутизации. Несовместимое значение метрики при перераспределении маршрутов будет заменено настроенным значением метрики по умолчанию.

Пример
В данном примере показан процесс перераспределения маршрутов из IPv6 RIP. Все перераспределяемые маршруты анонсируются с метрикой 10.

```
Switch#configure terminal
Switch(config)#ipv6 router ospf 1000
Switch(config-rtr)#default-metric 10
Switch(config-rtr)#redistribute rip
Switch(config-rtr)#
```

71.8 distance ospf

Данная команда используется, чтобы сконфигурировать расстояние (distance) для определенных маршрутов OSPF. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

distance ospf {external | inter-area | intra-area} *DISTANCE*
no distance ospf

Параметры

external	Укажите расстояние для внешних маршрутов OSPF.
inter-area	Укажите расстояние для маршрутов OSPF inter-area.
intra-area	Укажите расстояние для маршрутов OSPF intra-area.
DISTANCE	Укажите значение расстояния (distance) определенных маршрутов OSPF. Диапазон значений: от 1 до 254.

По умолчанию

По умолчанию значение расстояния для всех маршрутов OSPF – 110.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду **distance ospf**, чтобы настроить административное расстояние (administrative distance) для определенных маршрутов OSPF. Команда определяет, какие маршруты будут установлены в таблице маршрутизации.

Административное расстояние представляет собой число от 0 до 255. Чем выше это значение, тем ниже надежность маршрута. Если для административного расстояния указано значение 255, источник маршрутной информации не является доверенным и должен игнорироваться.

Пример

В данном примере показано, как настроить расстояние (distance) для внешних маршрутов. Установленное значение – 50.

```
Switch#configure terminal
Switch(config)#ipv6 router ospf 1
Switch(config-rtr)#distance ospf external 50
Switch(config-rtr)#
```

71.9 ipv6 ospf area

Данная команда используется для настройки зоны процесса OSPF на интерфейсе. Чтобы отключить маршрутизацию OSPF для определенных интерфейсов, воспользуйтесь формой **no** этой команды.

ipv6 ospf *PROCESS-ID* **area** *AREA-ID* **[instance** *INSTANCE-ID***]**
no ipv6 ospf *PROCESS-ID* **area** *AREA-ID* **[instance** *INSTANCE-ID***]**

Параметры

AREA-ID	Укажите ID зоны в виде IPv4-адреса.

PROCESS-ID	Укажите ID процесса. ID используется локально и должен быть уникальным.
INSTANCE-ID	(Опционально.) Укажите ID экземпляра. Диапазон значений: от 0 до 255. Если не указано, значение по умолчанию – 0.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда предназначена для настройки зоны процесса OSPF на интерфейсе. Настройки данной команды применяются только на интерфейсе IPv6. Создаваемая зона первоначально является нормальной зоной (Normal Area). Тип зоны можно изменить с помощью команды **area stub**.

На интерфейсе может быть сконфигурирована только одна зона для одного процесса OSPF. Чтобы установить сессию, ID экземпляра (Instance ID) должен совпадать с Instance ID соседнего маршрутизатора.

Пример

В данном примере показано, как создать зону OSPF на интерфейсе.

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ipv6 address 2001:DB8:0:6::/64 eui-64
Switch(config-if)#ipv6 enable
Switch(config-if)#ipv6 ospf 1000 area 0.0.0.0 instance 2
Switch(config-if)#
```

71.10 ipv6 ospf cost

Данная команда используется для точного указания стоимости отправки пакета на интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 ospf cost *COST*

no ipv6 ospf cost

Параметры

COST	Укажите значение метрики состояния канала (link-state). Значение задается в виде целого числа без знаков. Диапазон значений: от 1 до 65535.

По умолчанию
Значение по умолчанию – 10.

Режим ввода команды
Interface Configuration Mode.

Уровень команды по умолчанию
Уровень 12.

Использование команды
Установите метрику вручную с помощью команды **ipv6 ospf cost**. При использовании команды **auto-cost reference-bandwidth** стоимость канала связи (link cost) меняется до тех пор, пока не будет применена команда **ipv6 ospf cost**. Метрика состояния канала (link-state) анонсируется как стоимость канала в объявлениях о состоянии каналов (link advertisement) маршрутизатора.

Пример
В данном примере показано, как указать стоимость интерфейса. Установленное значение – 65.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 ospf cost 65
Switch(config-if)#
```

71.11 ipv6 ospf dead-interval

Данная команда используется для установки интервала, по истечении которого соседнее устройство будет считаться недоступным, если за это время не было получено ни одного пакета hello. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 ospf dead-interval *SECONDS*
no ipv6 ospf dead-interval

Параметры

SECONDS	Укажите интервал в секундах, по истечении которого соседнее устройство будет считаться недоступным, если за это время не было получено ни одного пакета hello. Диапазон значений: от 1 до 65535 с.

По умолчанию
Значение по умолчанию – 40 секунд.

Режим ввода команды
Interface Configuration Mode.

Уровень команды по умолчанию
Уровень 12.

Использование команды
Данный интервал анонсируется в пакетах hello. Значение должно быть одинаковым для всех маршрутизаторов и серверов доступа в определенной сети.

Пример
В данном примере показано, как установить интервал dead для IPv6 OSPF. Настроенное значение – 60 секунд.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 ospf dead-interval 60
Switch(config-if)#
```

71.12 ipv6 ospf hello-interval

Данная команда используется для указания интервала между пакетами hello, которые маршрутизатор отправляет на интерфейс. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 ospf hello-interval *SECONDS*
no ipv6 ospf hello-interval

Параметры

SECONDS	Укажите интервал между пакетами hello, которые маршрутизатор отправляет на интерфейс. Диапазон значений: от 1 до 65535 секунд.

По умолчанию
Значение по умолчанию – 10 секунд.

Режим ввода команды
Interface Configuration Mode.

Уровень команды по умолчанию
Уровень 12.

Использование команды
Чем меньше значение интервала hello, тем быстрее будут обнаружены изменения в топологии, но при этом будет увеличен маршрутный трафик. Значение должно быть одинаковым для всех маршрутизаторов и серверов доступа в определенной сети.

Пример
В данном примере показано, как указать интервал между пакетами hello. Установленное значение – 15 секунд.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 ospf hello-interval 15
Switch(config-if)#
```

71.13 ipv6 ospf priority

Данная команда используется для установки приоритета, согласно которому определяется назначенный маршрутизатор (Designated Router, DR) в сети. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 ospf priority *PRIORITY*

no ipv6 ospf priority

Параметры

PRIORITY	Укажите значение приоритета маршрутизатора в диапазоне от 0 до 255.

По умолчанию

Приоритет маршрутизатора по умолчанию: 1.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда устанавливает приоритет, согласно которому определяется назначенный маршрутизатор (Designated Router, DR) OSPF в сети. Если два маршрутизатора пытаются стать DR, в качестве DR будет выбран маршрутизатор с более высоким приоритетом. Если у маршрутизаторов одинаковый приоритет, будет выбран маршрутизатор с более высоким значением Router ID.

Назначенными (designated) или резервными назначенными (backup designated) могут стать только маршрутизаторы с ненулевым значением приоритета.

Пример

В данном примере показано, как установить приоритет маршрутизатора. Настроенное значение – 4.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 ospf priority 4
Switch(config-if)#
```

71.14 ipv6 ospf retransmit-interval

Данная команда используется, чтобы установить время повторной отправки LSA соседним устройствам на интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 ospf retransmit-interval *SECONDS*

no ipv6 ospf retransmit-interval

Параметры

SECONDS	Укажите время интервала, по истечении которого маршрутизатор будет повторно отправлять пакет. Диапазон значений: от 1 до 65535 секунд.

По умолчанию

Интервал по умолчанию – 5 секунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

После отправки LSA соседнему устройству маршрутизатор сохраняет пакет LSA до тех пор, пока не получит подтверждение. Если маршрутизатор не получает подтверждения в течение установленного времени (значение интервала retransmit), он повторно отправляет LSA. Во избежание ненужных повторных отправок значение интервала retransmit должно быть больше, чем ожидаемое время задержки приема/передачи (Round-Trip Delay) между двумя маршрутизаторами.

Пример

В данном примере показано, как установить интервал retransmit. Настроенное значение – 6 секунд.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 ospf retransmit-interval 6
Switch(config-if)#
```

71.15 ipv6 ospf transmit-delay

Данная команда используется, чтобы задать время, требуемое для передачи пакета обновления состояния канала (LSU) на интерфейс. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 ospf transmit-delay *SECONDS*
no ipv6 ospf transmit-delay

Параметры

SECONDS	Укажите интервал, по истечении которого маршрутизатор отправит пакет. Диапазон значений: от 1 до 65535 секунд.

По умолчанию

Значение по умолчанию – 1 секунда.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

LSU должны иметь возраст, который перед отправкой увеличивается на значение, указанное в секундах. При настройке значения необходимо учитывать задержку передачи и прохождения пакетов, установленную для интерфейса.

Если задержка не добавляется перед отправкой по каналу, время прохождения LSA по каналу не учитывается. Данная настройка больше подходит для каналов с очень низкой скоростью.

Пример

В данном примере показано, как указать значение для задержки передачи. Установленное значение – 3 секунды.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 ospf transmit-delay 3
Switch(config-if)#
```

71.16 ipv6 router ospf

Данная команда используется для настройки процесса маршрутизации IPv6 OSPF и входа в режим Router Configuration Mode. Чтобы удалить процесс IPv6 OSPF, воспользуйтесь формой **no** этой команды.

ipv6 router ospf *PROCESS-ID*

no ipv6 router ospf *PROCESS-ID*

Параметры

PROCESS-ID	Укажите ID процесса. ID используется локально и должен быть уникальным для каждого процесса IPv6 OSPF на маршрутизаторе. Диапазон значений: от 1 до 65535.

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 параметры для IPv6 OSPF.

Пример

В данном примере показано, как указать ID для процесса маршрутизации IPv6 OSPF и войти в режим Router Configuration Mode. Установленный ID – 1.

```
Switch#configure terminal
Switch(config)#ipv6 router ospf 1
Switch(config-rtr)#
```

71.17 no area

Данная команда используется для удаления определенной зоны.

no area *AREA-ID*

Параметры

AREA-ID	Укажите ID зоны.

По умолчанию

Нет.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для удаления указанной зоны OSPF и ее параметров, таких как area default-cost, area range, area stub и area virtual-link.

Пример

В данном примере показано, как удалить зону 0.0.0.3 процесса OSPF 1.

```
Switch#configure terminal
Switch(config)#ipv6 router ospf 1
Switch(config-rtr)#no area 0.0.0.3
Switch(config-rtr)#
```

71.18 passive-interface

Данная команда используется для включения пассивного режима на указанном сетевом интерфейсе или всех интерфейсах. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

passive-interface {default | *INTERFACE-ID***}**
no passive-interface {default | *INTERFACE-ID***}**

Параметры

default	Укажите, чтобы включить пассивный режим на всех интерфейсах.
INTERFACE-ID	Укажите ID интерфейса, на котором необходимо включить пассивный режим.

По умолчанию

По умолчанию пассивный режим не включен ни на одном настроенном интерфейсе.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

На интерфейсе в пассивном режиме не принимаются и не отправляются пакеты обновлений маршрутизации OSPF.

Пример

В данном примере показано, как включить пассивный режим на всех интерфейсах кроме VLAN 1.

```
Switch#configure terminal
Switch(config)#ipv6 router ospf 1
Switch(config-rtr)#passive-interface default
Switch(config-rtr)#no passive-interface vlan1
Switch(config-rtr)#
```

71.19 redistribute

Данная команда используется для перераспределения маршрутов из других доменов маршрутизации в IPv6 OSPF. Чтобы отключить перераспределение, воспользуйтесь формой **no** этой команды.

redistribute *PROTOCOL* **[metric** *METRIC-VALUE***] [metric-type** *TYPE-VALUE***]**
no redistribute *PROTOCOL* **[metric] [metric-type]**

Параметры

PROTOCOL	Укажите исходный протокол, из которого необходимо перераспределить маршруты. Доступны следующие ключевые слова: **connected**, **static**, **rip**.
metric *METRIC-VALUE*	(Опционально.) Укажите значение метрики при перераспределении других процессов в IPv6 OSPF. Если значение метрики не указано, по умолчанию метрика равна 20.
metric-type *TYPE-VALUE*	(Опционально.) Укажите тип метрики для внешних маршрутов, перераспределяемых в домен маршрутизации IPv6 OSPF. Доступны следующие два значения: **1**: укажите, чтобы использовать внешнюю метрику IPv6 OSPF типа 1. **2**: укажите, чтобы использовать внешнюю метрику IPv6 OSPF типа 2. Если тип метрики не указан, будет применена метрика типа 2.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Маршрутизатор, принимающий пакеты link-state с внутренней метрикой, будет считать стоимость маршрута до перераспределяющего маршрутизатора с учетом анонсированной стоимости до места назначения. Внешняя метрика предусматривает только анонсированную метрику до места назначения.

При вводе команды **redistribute** для перераспределения маршрутов в домен маршрутизации IPv6 OSPF маршрутизатор автоматически становится пограничным маршрутизатором автономной системы (ASBR). При этом ASBR не создает маршрут по умолчанию в домен маршрутизации IPv6 OSPF.

Если при перераспределении маршрутов в IPv6 OSPF из других протоколов метрика не указана, будет применена метрика по умолчанию, равная 20.

Маршруты, настроенные с использованием ключевых слов команды **redistribute**, не являются маршрутами, указанными командой **router configuration**.

Нельзя применить команду **default-metric**, чтобы изменить метрику, используемую для анонсирования подключенных маршрутов.

Пример

В данном примере показан процесс перераспределения маршрутов в IPv6 OSPF с изучением префиксов через IPv6 RIP.

```
Switch#configure terminal
Switch(config)#ipv6 router ospf 1
Switch(config-rtr)#redistribute rip
Switch(config-rtr)#
```

71.20 router-id

Данная команда используется, чтобы указать ID маршрутизатора для процесса OSPF. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

router-id *ROUTER-ID*
no router-id

Параметры

ROUTER-ID	Укажите ID маршрутизатора в виде IPv4-адреса.

По умолчанию

По умолчанию ID маршрутизатора назначается автоматически.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

ID маршрутизатора – это 32-битное число, назначаемое каждому маршрутизатору, на котором включен OSPF. Данное число является уникальным идентификатором для маршрутизатора в автономной системе. На каждом маршрутизаторе должен быть указан уникальный Router ID для процессов IPv6 OSPF.

Пример

В данном примере показано, как указать ID маршрутизатора. Настроенное значение – 10. 1. 1. 1.

```
Switch#configure terminal
Switch(config)#ipv6 router ospf 1
Switch(config-rtr)#router-id 10.1.1.1
Switch(config-rtr)#
```

71.21 show ipv6 ospf

Данная команда используется для отображения общей информации о процессах маршрутизации OSPF.

show ipv6 ospf [*PROCESS-ID***]**

Параметры

PROCESS-ID	(Опционально.) Укажите внутренний ID процесса маршрутизации IPv6 OSPF. ID назначается локально в виде любого положительного числа. Для каждого процесса маршрутизации IPv6 OSPF задается уникальное значение.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Информация, отображаемая по команде **show ipv6 ospf**, полезна при отладке работы маршрутизации OSPF.

Пример

В данном примере показано, как отобразить общую информацию о процессах маршрутизации OSPF.

```
Switch#show ipv6 ospf

Routing Process "OSPFv3 1" with ID 107.100.0.1
  Process uptime is  0DT1H3M50S
  Conforms to RFC 2740
  This router is an ABR; ABR Type is Standard (OSPFv3).
  This router is an ASBR (injecting external routing information).
  Redistributing External Routes (with default metric 20) from,
     rip with metric 0 with metric-type 2
  SPF schedule delay 5 secs, Hold time between SPFs 10 secs
  Number of LSA originated 69
  Number of LSA received 200
  Number of areas in this router is 6
    Area 0.0.0.0 (BACKBONE) (active)
        Number of interfaces in this area is 2 active interface number is 1
        Number of fully adjacent virtual neighbors through this area is 0
        SPF algorithm executed 3 times
        Number of LSA 30. Checksum Sum 0xf521c
        Number of Unknown LSA 0
        Area ranges are
    Area 0.0.0.1
        Number of interfaces in this area is 0 active interface number is 0
        Number of fully adjacent virtual neighbors through this area is 0
        SPF algorithm executed 0 times
        Number of LSA 0. Checksum Sum 0x0
```

```
        Number of Unknown LSA 0
        Area ranges are
    Area 0.0.0.11 (active)
        Number of interfaces in this area is 1 active interface number is 1
        Number of fully adjacent virtual neighbors through this area is 1
        SPF algorithm executed 5 times
        Number of LSA 16. Checksum Sum 0x80fcd
        Number of Unknown LSA 0
        Area ranges are
    Area 0.0.0.107 (active)
        Number of interfaces in this area is 1 active interface number is 1
        Number of fully adjacent virtual neighbors through this area is 0
        SPF algorithm executed 3 times
        Number of LSA 14. Checksum Sum 0x78472
        Number of Unknown LSA 0
        Area ranges are
    Area 1.1.1.100
        Number of interfaces in this area is 0 active interface number is 0
        Number of fully adjacent virtual neighbors through this area is 0
        It is a stub area
        SPF algorithm executed 0 times
        Number of LSA 0. Checksum Sum 0x0
        Number of Unknown LSA 0
        Area ranges are
    Area 1.1.1.101
        Number of interfaces in this area is 0 active interface number is 0
        Number of fully adjacent virtual neighbors through this area is 0
        SPF algorithm executed 0 times
        Number of LSA 0. Checksum Sum 0x0
        Number of Unknown LSA 0
        Area ranges are

Switch#
```

71.22 show ipv6 ospf border-routers

Данная команда используется, чтобы отобразить маршрутизаторы ABR и ASBR для экземпляра IPv6 OSPF.

show ipv6 ospf [*PROCESS-ID***] border-routers**

Параметры

PROCESS-ID	(Опционально.) Укажите ID процесса IPv6 OSPF. ID назначается локально в виде любого положительного числа. Для каждого процесса маршрутизации IPv6 OSPF задается уникальное значение.

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 маршрутизаторах ABR и ASBR.

Пример

В данном примере показано, как отобразить маршрутизаторы ABR и ASBR для экземпляра IPv6 OSPF.

```
Switch#show ipv6 ospf border-routers

OSPFv3 Process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 10.76.37.3 [1] is directly connected, TransitArea 0.0.0.1, ABR, Area 0.0.0.0
i 10.76.37.3 [1] is directly connected, vlan2, ABR, TransitArea 0.0.0.1

Switch#
```

71.23 show ipv6 ospf database

Данная команда используется для отображения общей информации базы данных процессов маршрутизации OSPF.

show ipv6 ospf [*PROCESS-ID***] database [external | inter-area prefix | inter-area router | link | network | prefix | router] [adv-router** *ROUTER-ID* **| self-originate] [area** *AREA-ID***]**

Параметры

PROCESS-ID	(Опционально.) Укажите ID процесса. ID используется локально и должен быть уникальным для каждого процесса IPv6 OSPF на маршрутизаторе.
adv-router *ROUTER-ID*	(Опционально.) Укажите, чтобы отобразить все LSA анонсирующего маршрутизатора. ID маршрутизатора указывается в виде IPv4-адреса.
external	(Опционально.) Укажите, чтобы отобразить информацию только об External LSA.
inter-area prefix	(Опционально) Укажите, чтобы отобразить информацию только об Inter-Area Prefix LSA.
inter-area router	(Опционально.) Укажите, чтобы отобразить информацию только об Inter-Area Router LSA.
link	(Опционально.) Укажите, чтобы отобразить информацию о Link LSA.

network	(Опционально.) Укажите, чтобы отобразить информацию о Network LSA.
prefix	(Опционально.) Укажите, чтобы отобразить информацию об Intra-Area Prefix LSA.
router	(Опционально.) Укажите, чтобы отобразить информацию только о Router LSA.
self-originate	(Опционально.) Укажите, чтобы отобразить только Self-Originate LSA (из локального маршрутизатора).
AREA-ID	(Опционально.) Укажите, чтобы отобразить все LSA указанной зоны. ID зоны указывается в виде Pv4-адреса.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Набор данных LSA маршрутизатора хранится в базе данных состояния канала. При применении алгоритма Дейкстры для содержимого базы данных создаются таблицы маршрутизации OSPF. Эти ключевые слова могут быть добавлены ко всем другим ключевым словам, используемым с командой show ipv6 ospf database, для предоставления более подробной информации.

Пример

В данном примере показано, как отобразить общую информацию базы данных процессов маршрутизации OSPF.

```
Switch#show ipv6 ospf database

            OSPFv3 Router with ID (10.76.37.30) (Process 1)

                Link-LSA (Interface vlan2)

ADV Router      Age  Seq#       CkSum   LinkCnt
10.76.37.3       512 0x80000001 0xdf6f      1
10.76.37.30      400 0x80000001 0x48fa      1

                Link-LSA (Interface vlan3)

ADV Router      Age  Seq#       CkSum   LinkCnt
10.76.37.30      400 0x80000001 0x3210      1

                Router-LSA (Area 0.0.0.0) (BACKBONE)

ADV Router      Age  Seq#       CkSum   LinkCnt
10.76.37.3       354 0x8000000a 0x717d      1
10.76.37.30      357 0x80000003 0x34c8      1
10.76.37.79      439 0x8000000c 0x7be0      0

                Inter-Area-Prefix-LSA (Area 0.0.0.0) (BACKBONE)

ADV Router      Age  Seq#       CkSum   Prefix
10.76.37.3       503 0x80000002 0x8a9f  3ffe:2::/64
10.76.37.3       503 0x80000002 0xb723  3ffe:2::10/128
10.76.37.3       346 0x80000004 0x8e95  3ffe:4::/64
10.76.37.3       346 0x80000003 0x3d6e  3ffe:4::30/128
10.76.37.30      374 0x80000002 0xd345  3ffe:3::/64
10.76.37.30      374 0x80000002 0xd73f  3ffe:4::/64
10.76.37.30      374 0x80000002 0x7e20  3ffe:4::30/128
10.76.37.30      352 0x80000003 0xa570  3ffe:2::/64
10.76.37.30      352 0x80000003 0x0fad  3ffe:2::10/128

                Inter-Area-Router-LSA (Area 0.0.0.0) (BACKBONE)

ADV Router      Age  Seq#       CkSum   Dest-RtrID
10.76.37.3       366 0x80000001 0x26dd  10.76.37.30

                Intra-Area-Prefix-LSA (Area 0.0.0.0) (BACKBONE)
```

```
ADV Router      Age  Seq#       CkSum   Ref-LsType   Ref-LSID        Prefix
10.76.37.3       348 0x8000000a 0x6a0c  Router-LSA   0.0.0.0         3ffe:1::/64
10.76.37.79      468 0x80000001 0xacdb  Network-LSA  0.0.4.1         1234::/16
10.76.37.79      458 0x80000001 0xf028  Router-LSA   0.0.0.0         1234::/16
10.76.37.79      448 0x80000001 0xe631  Router-LSA   0.0.0.0         1234::/16
10.76.37.79      438 0x80000001 0xd243  Router-LSA   0.0.0.0         1234::/16

               Router-LSA (Area 0.0.0.1)

ADV Router      Age  Seq#       CkSum   LinkCnt
10.76.37.3       354 0x80000003 0x3cd1      1
10.76.37.30      357 0x80000005 0x757e      1

               Network-LSA (Area 0.0.0.1)

ADV Router      Age  Seq#       CkSum
10.76.37.3       380 0x80000001 0xe8a7

               Inter-Area-Prefix-LSA (Area 0.0.0.1)

ADV Router      Age  Seq#       CkSum   Prefix
10.76.37.3       346 0x80000003 0x84a6  3ffe:1::/64
10.76.37.30      395 0x80000002 0xd345  3ffe:3::/64

               Intra-Area-Prefix-LSA (Area 0.0.0.1)

ADV Router   Age  Seq#       CkSum   Ref-LsType   Ref-LSID        Prefix
10.76.37.3   370 0x80000002 0xe744  Router-LSA   0.0.0.0         3ffe:2::10/128
10.76.37.3   374 0x80000001 0xd71c  Network-LSA  0.0.0.2         3ffe:2::/64
10.76.37.30  378 0x80000004 0x379b  Router-LSA   0.0.0.0         3ffe:4::30/128

               Router-LSA (Area 0.0.0.3)

ADV Router      Age  Seq#       CkSum   LinkCnt
10.76.37.30      360 0x80000003 0xbdd5      0

               Inter-Area-Prefix-LSA (Area 0.0.0.3)

ADV Router      Age  Seq#       CkSum   Prefix
10.76.37.30      395 0x80000002 0x920e  3ffe:4::30/128
10.76.37.30      395 0x80000002 0xd73f  3ffe:4::/64
10.76.37.30      352 0x80000003 0xaf67  3ffe:2::/64
10.76.37.30      352 0x80000003 0x19a4  3ffe:2::10/128
10.76.37.30      347 0x80000002 0xcb41  3ffe:1::/64

               Intra-Area-Prefix-LSA (Area 0.0.0.3)

ADV Router      Age  Seq#       CkSum   Ref-LsType   Ref-LSID        Prefix
10.76.37.30      359 0x80000003 0xda73  Router-LSA   0.0.0.0         3ffe:3::/64

Total Entries: 36
Switch#
```

В следующем примере показано, как отобразить информацию о Router LSA.

```
Switch#show ipv6 ospf database router

           OSPFv3 Router with ID (10.47.65.180) (Process 1)

               Router-LSA (Area 0.0.0.0) (BACKBONE)

  LS age: 1766
  LS Type: Router-LSA
  Link State ID: 0.0.0.0
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x8000000F
  Checksum: 0x9586
  Length: 56
  Flags: 0x03 (-|-|E|B)
  Options: 0x000013 (-|R|-|-|E|V6)
  Number of Links: 2
    Link connected to: a Virtual Link
      Metric: 1
      Interface ID: 2147483809
      Neighbor Interface ID: 2147483649
      Neighbor Router ID: 10.47.65.182
    Link connected to: a Virtual Link
      Metric: 1
      Interface ID: 2147483810
      Neighbor Interface ID: 2147483649
      Neighbor Router ID: 10.47.65.183

  LS age: 1766
  LS Type: Router-LSA
  Link State ID: 0.0.0.0
  Advertising Router: 10.47.65.182
  LS Seq Number: 0x800001C3
  Checksum: 0xAD4F
  Length: 56
  Flags: 0x03 (-|-|E|B)
  Options: 0x000013 (-|R|-|-|E|V6)
  Number of Links: 2
    Link connected to: a Virtual Link
      Metric: 1
      Interface ID: 2147483649
      Neighbor Interface ID: 2147483809
      Neighbor Router ID: 10.47.65.180
    Link connected to: a Virtual Link
      Metric: 10
      Interface ID: 2147483650
      Neighbor Interface ID: 2147483650
      Neighbor Router ID: 10.47.65.183

Total Entries: 2
Switch#
```

В примере ниже показано, как отобразить информацию о Network LSA.

```
Switch#show ipv6 ospf database network

            OSPFv3 Router with ID (47.65.49.1) (Process 1)

                Network-LSA (Area 0.0.0.0) (BACKBONE)

  LS age: 68
  LS Type: Network-LSA
  Link State ID: 0.0.4.49
  Advertising Router: 47.65.49.1
  LS Seq Number: 0x80000003
  Checksum: 0xC9D1
  Length: 32
  Options: 0x000013 (-|R|-|-|E|V6)
    Attached Router: 47.65.49.1
    Attached Router: 47.65.49.111

Total Entries: 1
Switch#
```

В следующем примере показано, как отобразить информацию об Inter-Area Prefix LSA.

```
Switch#show ipv6 ospf database inter-area prefix

            OSPFv3 Router with ID (10.47.65.180) (Process 1)

                Inter-Area-Prefix-LSA (Area 0.0.0.0) (BACKBONE)

  LS age: 1056
  LS Type: Inter-Area-Prefix-LSA
  Link State ID: 128.64.0.0
  Advertising Router: 47.65.49.111
  LS Seq Number: 0x800000B5
  Checksum: 0x7F28
  Length: 36
  Metric: 0
  Prefix: c800::/64, Prefix Options: 0

Total Entries: 1
Switch#
```

В примере ниже показано, как отобразить информацию об Inter-Area Router LSA.

```
Switch#show ipv6 ospf database inter-area router

           OSPFv3 Router with ID (10.47.65.180) (Process 1)

               Inter-Area-Router-LSA (Area 0.0.0.0) (BACKBONE)

  LS age: 162
  LS Type: Inter-Area-Router-LSA
  Link State ID: 0.0.0.1
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x80000003
  Checksum: 0x3889
  Length: 32
  Options: 0x000013 (-|R|-|-|E|V6)
  Metric: 1
  Destination Router ID: 10.47.65.183

  LS age: 162
  LS Type: Inter-Area-Router-LSA
  Link State ID: 0.0.0.2
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x80000003
  Checksum: 0x1862
  Length: 32
  Options: 0x000013 (-|R|-|-|E|V6)
  Metric: 2
  Destination Router ID: 47.65.151.111

Total Entries: 2
Switch#
```

В следующем примере показано, как отобразить информацию об External LSA.

```
Switch#show ipv6 ospf database external

           OSPFv3 Router with ID (10.47.65.180) (Process 1)

               AS-external-LSA

  LS age: 279
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.1
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x80000003
  Checksum: 0xBF8B
  Length: 32
  Metric Type: 1 (Comparable directly to link state metric)
  Metric: 16000000
  Prefix: 1151::/32, Prefix Options: 0 (-|-|-|-)

  LS age: 279
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.2
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x80000003
  Checksum: 0xD96D
  Length: 32
  Metric Type: 1 (Comparable directly to link state metric)
  Metric: 16000000
  Prefix: 1154::/32, Prefix Options: 0 (-|-|-|-)

  LS age: 279
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.3
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x80000003
  Checksum: 0xDB69
  Length: 32
  Metric Type: 1 (Comparable directly to link state metric)
  Metric: 16000000
  Prefix: 1155::/32, Prefix Options: 0 (-|-|-|-)

Total Entries: 3
Switch#
```

В примере ниже показано, как отобразить информацию о Link LSA.

```
Switch#show ipv6 ospf database link

           OSPFv3 Router with ID (10.47.65.180) (Process 4765)

               Link-LSA (Interface vlan49)

  LS age: 347
  LS Type: Link-LSA
  Link State ID: 0.0.4.49
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x80000003
  Checksum: 0x62B6
  Length: 64
  Priority: 1
  Options: 0x000013 (-|R|-|-|E|V6)
  Link-Local Address: fe80::4b0:ff:fe17:31
  Number of Prefixes: 2
    Prefix: 1149::/32, Prefix Options: 0 (-|-|-|-)
    Prefix: 2049:1::/64, Prefix Options: 0 (-|-|-|-)

Total Entries: 1
Switch#
```

В следующем примере показано, как отобразить информацию об Intra-Area Prefix LSA.

```
Switch#show ipv6 ospf database prefix

           OSPFv3 Router with ID (10.47.65.180) (Process 1)

               Intra-Area-Prefix-LSA (Area 0.0.0.1)

  LS age: 326
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 0.0.0.2
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x8000000B
  Checksum: 0x9814
  Length: 52
  Referenced LS Type: 0x2001
  Referenced Link State ID: 0.0.0.0
  Referenced Advertising Router: 10.47.65.180
  Number of Prefixes: 1
    Prefix: 1152:0:1::1/128, Prefix Options: 2 (-|-|LA|-)
    Metric: 0

  LS age: 1124
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 0.0.0.2
  Advertising Router: 10.47.65.182
  LS Seq Number: 0x80000024
  Checksum: 0x1F76
  Length: 44
  Referenced LS Type: 0x2002
  Referenced Link State ID: 0.0.8.107
  Referenced Advertising Router: 10.47.65.182
  Number of Prefixes: 1    Prefix: 2113:1::/64, Prefix Options: 0 (-|-|-|-)
    Metric: 0

Total Entries: 2
Switch#
```

В данном примере показано, как отобразить все LSA анонсирующего маршрутизатора 10.47.65.182.

```
Switch#show ipv6 ospf database router adv-router 10.47.65.182

           OSPFv3 Router with ID (10.47.65.180) (Process 4765)

               Router-LSA (Area 0.0.0.0) (BACKBONE)

  LS age: 1734
  LS Type: Router-LSA
  Link State ID: 0.0.0.0
  Advertising Router: 10.47.65.182
  LS Seq Number: 0x800001D1
  Checksum: 0x915D
  Length: 56
  Flags: 0x03 (-|-|E|B)
  Options: 0x000013 (-|R|-|-|E|V6)
  Number of Links: 2
    Link connected to: a Virtual Link
      Metric: 1
      Interface ID: 2147483649
      Neighbor Interface ID: 2147483809
      Neighbor Router ID: 10.47.65.180
    Link connected to: a Virtual Link
      Metric: 10
      Interface ID: 2147483650
      Neighbor Interface ID: 2147483650
      Neighbor Router ID: 10.47.65.183

Total Entries: 1
Switch#
```

В нижеприведенном примере показано, как отобразить Self-originate LSA.

```
Switch#show ipv6 ospf database router self-originate

           OSPFv3 Router with ID (10.47.65.180) (Process 4765)
               Router-LSA (Area 0.0.0.0) (BACKBONE)

  LS age: 1753
  LS Type: Router-LSA
  Link State ID: 0.0.0.0
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x8000001D
  Checksum: 0x7994
  Length: 56
  Flags: 0x03 (-|-|E|B)
  Options: 0x000013 (-|R|-|-|E|V6)
  Number of Links: 2
    Link connected to: a Virtual Link
      Metric: 1
      Interface ID: 2147483809
      Neighbor Interface ID: 2147483649
      Neighbor Router ID: 10.47.65.182
    Link connected to: a Virtual Link
      Metric: 1
      Interface ID: 2147483810
      Neighbor Interface ID: 2147483649
      Neighbor Router ID: 10.47.65.183

Total Entries: 1
Switch#
```

71.24 show ipv6 ospf interface

Данная команда используется для отображения информации об интерфейсе, связанном с OSPF.

show ipv6 ospf [*PROCESS-ID***] interface [***INTERFACE-ID***]**

Параметры

PROCESS-ID	(Опционально.) Укажите ID процесса. ID используется локально и должен быть уникальным для каждого процесса IPv6 OSPF на маршрутизаторе.
INTERFACE-ID	(Опционально.) Укажите ID интерфейса для отображения информации об OSPF. Если ID интерфейса не указан, будет отображена информация об OSPF по всем интерфейсам.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется, чтобы отобразить информацию об интерфейсе для OSPFv3. Если интерфейс не указан, будет отображена информация OSPFv3 по всем интерфейсам.

Пример

В данном примере показано, как отобразить информацию об интерфейсах, связанных с OSPF.

```
Switch#show ipv6 ospf interface

vlan1 is up, line protocol is up
  Link Local Address: FE80::20F:36FF:FE31:AE01/128
  Interface ID: 1
  OSPFv3 Process (1), Area 0.0.0.107 (active), Instance ID 0, MTU 1500
  Router ID 107.100.0.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 107.100.0.1,
    Local Address FE80::20F:36FF:FE31:AE01
  Backup Designated Router (ID) 0.0.0.0,
    Local Address ::
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Neighbor Count is 0, Adjacent neighbor count is 0
  Hello received 0 sent 535, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0

vlan11 is up, line protocol is up
  Link Local Address: FE80::20F:36FF:FE31:AE03/128
  Interface ID: 2
  OSPFv3 Process (1), Area 0.0.0.11 (active), Instance ID 11, MTU 1500
  Router ID 107.100.0.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State Backup, Priority 1
  Designated Router (ID) 30.90.90.90,
    Local Address FE80::206:28FF:FED8:FE94
  Backup Designated Router (ID) 107.100.0.1,
    Local Address FE80::20F:36FF:FE31:AE03
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 587 sent 491, DD received 8 sent 6
  LS-Req received 1 sent 4, LS-Upd received 26 sent 24
  LS-Ack received 23 sent 27, Discarded 0

Total Entries: 2
Switch#
```

71.25 show ipv6 ospf neighbor

Данная команда используется для отображения информации о соседних устройствах OSPF по интерфейсам.

show ipv6 ospf [*PROCESS-ID***] neighbor [***INTERFACE-ID***] [***NEIGHBOR-ID***] [detail]**

Параметры

PROCESS-ID	(Опционально.) Укажите ID процесса. Process ID назначается локально в виде любого положительного числа. Для каждого процесса маршрутизации IPv6 OSPF назначается уникальное значение.
INTERFACE-ID	(Опционально.) Укажите ID интерфейса для отображения информации о соседних устройствах.
NEIGHBOR-ID	(Опционально.) Укажите ID соседнего устройства. ID указывается в виде адреса IPv4.
detail	(Опционально.) Укажите, чтобы отобразить подробную информацию о соседних устройствах.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о соседних устройствах OSPFv3. Если интерфейс не указан, будет отображена информация о соседних устройствах OSPFv3 по всем интерфейсам.

Пример

В данном примере показано, как отобразить информацию о соседних устройствах OSPF по интерфейсам.

```
Switch#show ipv6 ospf neighbor detail

Neighbor 12.0.0.1, Link Local address FE80::201:FF:FE00:0
    In the area 0.0.0.0 via interface vlan8
    Neighbor priority is 1, State is FULL, 5 state changes
    DR is 12.0.0.1 BDR is 36.0.0.0
    Options is 0x000013 (-|R|-|-|E|V6)

Neighbor 36.20.0.0, Link Local address FE80::2C0:8FFF:FE04:1128
    In the area 0.0.0.0 via interface vlan10
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 36.20.0.0 BDR is 36.0.0.0
    Options is 0x000013 (-|R|-|-|E|V6)

Neighbor 12.0.0.2, Link Local address FE80::202:FF:FE00:0
    In the area 0.0.0.5 via interface vlan11
    Neighbor priority is 1, State is FULL, 5 state changes
    DR is 12.0.0.2 BDR is 36.0.0.0
    Options is 0x000013 (-|R|-|-|E|V6)

Total Entries: 3
Switch#
```

71.26 show ipv6 ospf virtual-links

Данная команда используется для отображения параметров и текущего состояния виртуальных каналов OSPF (virtual link).

show ipv6 ospf [*PROCESS-ID***] virtual-links**

Параметры

PROCESS-ID	(Опционально.) Укажите ID процесса IPv6 OSPF. ID назначается локально в виде любого положительного числа. Для каждого процесса маршрутизации IPv6 OSPF назначается уникальное значение.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Информация, отображаемая по команде **show ipv6 ospf virtual-links**, полезна при отладке работы маршрутизации OSPF.

Пример

В данном примере показано, как отобразить параметры и текущее состояние виртуальных каналов OSPF (virtual link).

```
Switch#show ipv6 ospf virtual-links

Virtual Link to router 10.90.90.90 is up
  Transit area 0.0.0.3 via interface vlan40, instance ID 0
  Local Peer Address FD80::2A10:7BFF:FE7D:D963/128
  Remote Peer Address 4000::A/128
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Adjacency state Full

Total Entries: 1
Switch#
```

72. Команды Packet Debug

72.1 debug clear cpu counter

Данная команда используется для обнуления счетчиков пакетов, включая входящий и исходящий трафик порта ЦПУ.

debug clear cpu counter

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду для обнуления счетчиков пакетов, включая входящий и исходящий трафик порта ЦПУ, и повторного отсчета.

Пример

В данном примере показано, как обнулить счетчики пакетов ЦПУ.

```
Switch#debug clear cpu counter

Success

Switch#
```

72.2 debug dump packet_in_buffer

Данная команда используется для проверки полученных пакетов в буфере.

debug dump packet_in_buffer [len *LENGTH***] [count** *COUNT***] [channel** *CHANNEL***]**

Параметры

len *LENGTH*	(Опционально.) Укажите длину буфера печати для каждого пакета в байтах. Диапазон значений: от 0 до 2048.
count *COUNT*	(Опционально.) Укажите счетчик пакетов для каждого канала. Диапазон значений: от 0 до 200.

channel *CHANNEL*	(Опционально.) Укажите канал, который необходимо отобразить. Диапазон значений: от 1 до 3.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Команда используется для проверки полученных пакетов в буфере. Система поддерживает буферизацию до 200 пакетов на канал. Всего доступно 3 канала. Система будет записывать новые входящие пакеты в нижнюю позицию канала. При перегруженности системы полученные пакеты будут буферизироваться в верхнюю позицию. Пакеты в верхней позиции можно использовать для проверки причин перегруженности ЦПУ.

Пример

В данном примере показано, как отобразить пакеты канала 2.

```
Switch#debug dump packet_in_buffer channel 2

================================================================================
Rx channel 2, base address=0x7f869ab8,total_size=432800,block_size=2148,
    block_num=200,max_alloc=20,alloc_blocks=8 print count=20(input 0)
=>7f869ac4--------------------------------------------------------------------
0000: f0 7d 68 34 00 10 f0 7d  68 34 00 10 81 00 00 01    .}h4...}h4......
0010: 08 00 45 00 00 28 6b 76  40 00 7f 06 c7 3c 0a 5a    ..E..(kv@....<.Z
0020: 5a 0f 0a 5a 5a 5a c0 09  00 50 0f 8f b3 6e 28 49    Z..ZZZ...P...n(I
0030: 97 c7 50 10 40 de 62 71  00 00                      ..P.@.bq..
=>7f86a338--------------------------------------------------------------------
0000: f0 7d 68 34 00 10 f0 7d  68 34 00 10 81 00 00 01    .}h4...}h4......
0010: 08 00 45 00 00 28 4c ec  40 00 7f 06 e5 c7 0a 5a    ..E..(L.@......Z
0020: 5a 0e 0a 5a 5a 5a 12 e0  00 50 6c 99 64 c8 14 05    Z..ZZZ...Pl.d...
0030: df d8 50 10 40 de cd 6a  00 00                      ..P.@..j..
=>7f86abac--------------------------------------------------------------------
0000: f0 7d 68 34 00 10 f0 7d  68 34 00 10 81 00 00 01    .}h4...}h4......
0010: 08 00 45 00 00 28 6b 78  40 00 7f 06 c7 3a 0a 5a    ..E..(kx@....:.Z
0020: 5a 0f 0a 5a 5a 5a c0 13  00 50 0e 98 e2 09 50 39    Z..ZZZ...P....P9
0030: b8 13 50 10 3f dc ed 88  00 00                      ..P.?.....
=>7f86b420--------------------------------------------------------------------
0000: f0 7d 68 34 00 10 f0 7d  68 34 00 10 81 00 00 01    .}h4...}h4......
0010: 08 00 45 00 00 28 6b 77  40 00 7f 06 c7 3b 0a 5a    ..E..(kw@....;.Z
0020: 5a 0f 0a 5a 5a 5a c0 13  00 50 0e 98 e2 09 50 39    Z..ZZZ...P....P9
0030: b7 65 50 10 40 07 ee 0b  00 00                      .eP.@.....
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

72.3 debug show cpu counter

Данная команда используется для отображения счетчиков пакетов, включая входящий и исходящий трафик порта ЦПУ.

debug show cpu counter

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Команда используется для отображения счетчиков пакетов, включая входящий и исходящий трафик порта ЦПУ.

Пример

В данном примере показано, как отобразить счетчики пакетов порта ЦПУ.

```
Switch#debug show cpu counter

PacketType    TotalCounter     Pkt/Sec  PacketType    TotalCounter     Pkt/Sec
----------- ------RX-TX------ --RX-TX-- ----------- ------RX-TX------ --RX-TX--
UNKNOWN            0-0           0-0    1X_BPDU            0-0           0-0
STP_BPDU           0-0           0-0    GVRP_BPDU          0-0           0-0
IP              1102-936         0-0    LACP_BPDU          0-0           0-0
BPDU               0-0           0-0    ARP             2313-2           2-0
GM                 0-0           0-0    IPv6               0-0           0-0
CTP                0-0           0-0    OSPF_TIC           0-0           0-0
OSPF_ACK           0-0           0-0    OSPF_PKT           0-0           0-0
LLDP               0-0           0-0    LOOPBACK           0-0           0-0
ERPS_PDU           0-0           0-0    Tunnel_STP         0-0           0-0
Tunnel_GVRP        0-0           0-0    CISCO_MAC1         0-0           0-0
CISCO_MAC2         0-0           0-0    L2PT_MAC1          0-0           0-0
L2PT_MAC2          0-0           0-0    TUNNEL_LLDP        0-0           0-0
OSPF6_TIC          0-0           0-0    OSPF6_ACK          0-0           0-0
OSPF6_PKT          0-0           0-0    DDPv4              0-0           0-0
DDPv6              0-0           0-0    DDP_L2             0-0           0-0
Stacking           0-0           0-0    Total           3415-938         2-0



CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Отображаемые параметры

PacketType	Тип полученных пакетов каждого протокола.
TotalCounter	Все полученные и отправленные пакеты порта ЦПУ.
Pkt/Sec	Скорость входящего и исходящего трафика в пакетах в секунду.

73. Команды Policy-based Routing (PBR)

73.1 ip policy route-map

Данная команда используется для указания карты маршрутов (route map) в качестве политики маршрутизации на интерфейсе. Чтобы отключить политику маршрутизации на интерфейсе, воспользуйтесь формой **no** этой команды.

ip policy route-map *MAP-NAME*

no ip policy route-map

Параметры

MAP-NAME	Укажите имя карты маршрутов (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 применима исключительно для настройки VLAN-интерфейсов.

Укажите одну карту маршрутов (route map) в качестве политики маршрутизации на интерфейсе. Настроенная политика будет применена к пакетам, полученным на заданном интерфейсе.

Воспользуйтесь командой **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 маршрутов. 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**

Данные команды не будут применены, если при указании карты маршрутов использовалась команда **no match ip-address**, а также если настроенный список доступа IP не существует или не содержит правила. В этом 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)#
```

73.2 ipv6 policy route-map

Данная команда используется для указания карты маршрутов (route map) в качестве политики маршрутизации на интерфейсе. Чтобы отключить политику маршрутизации на интерфейсе, воспользуйтесь формой **no** этой команды.

ipv6 policy route-map *MAP-NAME*
no ipv6 policy route-map

Параметры

MAP-NAME	Укажите имя карты маршрутов (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 применима исключительно для настройки VLAN-интерфейсов.

Укажите одну карту маршрутов (route map) в качестве политики маршрутизации на интерфейсе. Настроенная политика будет применена к пакетам, полученным на заданном интерфейсе.

Воспользуйтесь командой **match ipv6-address**, чтобы настроить критерии соответствия для пакетов с определенными характеристиками. Если при вводе команды **match ipv6-address** используется список доступа IP, проверяются все критерии соответствия в данном списке доступа. Пакеты, прошедшие проверку на соответствие, будут обработаны на основе настроенной карты маршрутов. 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 ipv6 next-hop**
- **set ipv6 default next-hop**

- **set ipv6 precedence**

Пример

В данном примере показано, как настроить политику маршрутизации для маршрутизации пакетов, соответствующих списку доступа IPv6 «pbr-acl». Следующий узел (next hop) – 1001::100.

```
Switch#configure terminal
Switch(config)#route-map pbr-map permit 1
Switch(config-route-map)#match ipv6 address pbr-acl
Switch(config-route-map)#set ipv6 next-hop 1001::100
Switch(config-route-map)#exit
Switch(config)#interface vlan 1
Switch(config-if)#ipv6 policy route-map pbr-map
Switch(config-if)#
```

73.3 show ip policy

Данная команда применяется для отображения карты маршрутов, используемой для маршрутизации на основе политики (Policy-Based Routing).

show ip policy

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 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#
```

73.4 show ipv6 policy

Данная команда применяется для отображения карты маршрутов, используемой для маршрутизации на основе политики (Policy-Based Routing).

show ipv6 policy

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 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 ipv6 policy

Interface    Route Map
------------ ----------------
vlan1        pbr-map

Total Entries: 1
Switch#
```

74. Команды Port Security

74.1 clear port security

Данная команда используется для удаления динамически изученных безопасных MAC-адресов.

clear port-security {all | {address *MAC-ADDR* **| interface** *INTERFACE-ID* **[, | -]} [vlan** *VLAN-ID***]}**

Параметры

all	Укажите, чтобы удалить все динамически изученные безопасные MAC-адреса.
address *MAC-ADDR*	Укажите, чтобы удалить указанные динамически изученные безопасные записи на основе введенного MAC-адреса.
interface *INTERFACE-ID*	Укажите, чтобы удалить все динамически изученные безопасные записи на указанном интерфейсе.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
vlan *VLAN-ID*	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

Используйте данную команду, чтобы 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#
```

74.2 show port-security

Данная команда используется для просмотра текущих настроек Port Security.

show port-security [[interface *INTERFACE-ID* **[, | -]] [address] | vlan** *VLAN-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите ID интерфейса для отображения.
,	(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.
address	(Опционально.) Укажите для отображения безопасных MAC-адресов, включая настроенные и изученные адреса.
vlan *VLAN-ID*	(Опционально.) Укажите для отображения настроек Port Security для VLAN.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда применяется для отображения текущих настроек Port Security.

Пример

В данном примере показано, как отобразить настройки Port Security на портах 1-3.

```
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 -                    D  Enabled  Forwarding
 eth1/0/2     10    10    Shutdown -                    D  Enabled  Err-disabled
 eth1/0/3     10    0     Shutdown -                    P  Disabled -

Switch#
```

74.3 snmp-server enable traps port-security

Данная команда используется для включения отправки SNMP-уведомлений при обнаружении функционалом Port Security недопустимых адресов. Чтобы отключить отправку SNMP-уведомлений, воспользуйтесь формой **no** этой команды.

snmp-server enable traps port-security [trap-rate *TRAP-RATE***]**

no snmp-server enable traps port-security [trap-rate]

Параметры

trap-rate *TRAP-RATE*	(Опционально.) Укажите количество trap-сообщений в секунду. 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 применяется для включения или отключения отправки SNMP-уведомлений при обнаружении функционалом Port Security недопустимых адресов.

Пример

В данном примере показано, как включить отправку trap-сообщений при обнаружении функционалом Port Security недопустимых адресов и установить количество trap-сообщений 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)#
```

74.4 switchport port-security

Данная команда используется для настройки параметров Port Security, чтобы ограничить количество пользователей, которым разрешен доступ к порту. Чтобы отключить Port Security или удалить безопасный MAC-адрес, воспользуйтесь формой **no** этой команды.

switchport port-security [maximum *VALUE* **| violation {protect | restrict | shutdown} | mode {permanent | delete-on-timeout} | mac-address [permanent]** *MAC-ADDRESS* **[vlan** *VLAN-ID***]]**

no switchport port-security [maximum | violation | mode | mac-address [permanent] *MAC-ADDRESS* **[vlan** *VLAN-ID***]]**

Параметры

maximum *VALUE*	(Опционально.) Укажите максимальное число разрешенных безопасных MAC-адресов. Если не указано, значение по умолчанию – 32. Диапазон значений: от 0 до 3328.
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.
permanent	(Опционально.) В данном режиме все изученные MAC-адреса не будут удалены, пока пользователь не удалит их вручную.
delete-on-timeout	(Опционально.) В данном режиме все изученные MAC-адреса будут удалены, когда запись устареет, или если пользователь удалит записи вручную.
mac-address *MAC-ADDRESS*	(Опционально.) Укажите, чтобы добавить безопасный MAC-адрес для получения доступа к порту.
permanent	(Опционально.) Укажите, чтобы задать безопасный постоянно настроенный MAC-адрес порта. Данная запись является такой же, как изученная в режиме Permanent Mode.
vlan *VLAN-ID*	(Опционально.) Укажите VLAN. Если VLAN не указана, MAC-адрес будет изучен в соответствии с PVID.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При включении функции Port Security с режимом **delete-on-timeout**, порт будет автоматически изучать безопасные записи и хранить их, пока не истечет их тайм-аут. Время хранения этих записей зависит от настроек, заданных командой **switchport port-security aging**. Если режим порта задан как постоянный (permanent), он будет автоматически изучать безопасные записи с неистекающим тайм-аутом. Автоматически изученные безопасные записи будут храниться в текущем файле конфигурации (running configuration).

При изменении режима Port Security счетчик нарушений будет сброшен, автоматически изученные постоянные записи будут преобразованы в соответствующие динамические записи. При отключении Port Security автоматически изученные безопасные записи будут удалены, включая динамические и постоянные, счетчик нарушений будет сброшен. При изменении настройки VLAN автоматически изученные динамические безопасные записи будут удалены.

Постоянные безопасные записи будут храниться в текущем файле конфигурации и могут быть сохранены в NVRAM при помощи команды **copy**. Настроенные пользователем безопасные MAC-адреса будут подсчитываться в максимальном количестве MAC-адресов на порт.

Если на порту включена постоянная (permanent) безопасная запись Port Security, MAC-адрес нельзя перенести на другой порт.

При увеличении максимального числа разрешенных адресов изученные адреса останутся неизменными. Если максимальное число будет изменено на меньшее, чем существующее число изученных записей, команда будет отклонена.

У функции Port Security есть следующие ограничения:

- Функция Port Security не может работать одновременно с 802.1X, MAC-based Access Control (управление доступом на основе MAC), WAC и IMPB, которые предоставляют более широкие возможности управления безопасностью.
- Если порт указан в качестве порта назначения для функции зеркалирования, функция Port Security не может быть включена.
- Если порт указан в качестве порта агрегирования каналов, функция Port Security не может быть включена.

При превышении максимального количества безопасных пользователей, может быть предпринято одно из следующих действий:

- **Protect** – когда число безопасных MAC-адресов порта достигает максимального значения пользователей, разрешенного на порту, пакеты с неизвестным адресом источника будут отбрасываться до тех пор, пока какая-нибудь безопасная запись не будет удалена.
- **Restrict** – при нарушении безопасности происходит ограничение данных, а также возрастает

счетчик нарушений безопасности.

- **Shutdown** – при нарушении безопасности интерфейс отключается.

Пример

В данном примере показано, как настроить Port Security с режимом permanent 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 примере ниже показано, как вручную добавить безопасный MAC-адрес 00-00-12-34-56-78 с VID 5 на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security mac-address 00-00-12-34-56-78 vlan 5
Switch(config-if)#
```

В следующем 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)#
```

74.5 switchport port-security aging

Данная команда используется для указания времени устаревания (Aging Time) для динамически изученных безопасных адресов на интерфейсе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

switchport port-security aging {time *MINUTES* **| type {absolute | inactivity}}**

no switchport port-security aging {time | type}

Параметры

time *MINUTES*	Укажите время устаревания (Aging Time) для динамически изученных безопасных адресов на порту в минутах. Диапазон значений: от 0 до 1440.
type	Укажите тип устаревания.
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 применяется для отключения процесса устаревания записей, а также для того чтобы указать время устаревания (Aging Time) динамически изученных безопасных записей. Для того чтобы задать тип **inactivity**, должна быть включена функция устаревания таблицы FDB.

Пример

В данном примере показано, как настроить время устаревания (Aging Time) динамически изученных безопасных MAC-адресов на порту 1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security aging time 1
Switch(config-if)#
```

В примере ниже показано, как настроить тип времени устаревания на порту 1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)#
```

74.6 port-security limit

Данная команда используется для указания максимального количества безопасных MAC-адресов в системе или на указанной VLAN. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

port-security limit {global | vlan *VLAN-ID* **[, | -]}** *VALUE*
no port-security limit {global | vlan *VLAN-ID* **[, | -]}**

Параметры

global	Укажите, если необходимо применить настройки ко всей системе.
vlan *VLAN-ID*	Укажите необходимые VLAN ID.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения группы VLAN от предыдущей. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
VALUE	Укажите максимальное число записей Port Security, которое может быть изучено в системе или в указанной VLAN. Диапазон значений: от 1 до 3328. Если указанное значение меньше текущего числа изученных записей, команда будет отклонена.

По умолчанию

По умолчанию в данной опции ограничений нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы 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)#
```

75. Команды Power over Ethernet (PoE) (только для DGS-1520-28MP и DGS-1520-52MP)

75.1 poe pd description

Данная команда используется для описания PD-устройства (питаемого устройства), подключенного к порту PoE. Чтобы удалить описание, воспользуйтесь формой **no** этой команды.

poe pd description *TEXT*
no poe pd description

Параметры

TEXT	Введите описание PD-устройства, подключенного к порту PoE. Максимальное 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 порту 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#poe pd description For VOIP usage
Switch(config-if)#
```

75.2 poe pd legacy-support

Данная команда используется для включения поддержки устаревших PD-устройств (legacy PD). Чтобы отключить поддержку, воспользуйтесь формой **no** этой команды.

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. Если поддержка отключена, подача питания на устаревшие PD-устройства не будет осуществляться.

Пример

В данном примере показано, как включить поддержку для устаревших PD-устройств (legacy PD), подключенных к порту 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#poe pd legacy-support
Switch(config-if)#
```

75.3 poe pd priority

Данная команда используется для настройки приоритета при подаче питания порту. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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 назначается низкий приоритет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки физического порта.

Поскольку бюджет мощности ограничен, при добавлении к системе новых PD-устройств источника питания может оказаться недостаточно. В этом случае система PoE будет работать в критическом режиме. Подача питания новому добавленному PD-устройству будет зависеть от политики, настроенной в команде **poe policy preempt**.

Если политика не настроена, обслуживаются те устройства, которые подключились первыми (first in first serviced). Таким образом, новое PD-устройство не будет обеспечено питанием.

При настроенной политике Preempt Mode PD-устройство с наименьшим приоритетом будет вытеснено новым подключенным PD-устройством с более высоким приоритетом.

Пример

В данном примере показано, как настроить наивысший приоритет для порта 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#poe pd priority critical
Switch(config-if)#
```

75.4 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. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

poe unit *UNIT-ID* **policy preempt**
no poe unit *UNIT-ID* **policy preempt**

Параметры

UNIT-ID	(Опционально.) Укажите Unit ID устройства для настройки. Параметр доступен только при включенном режиме стекирования.

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, при добавлении к системе новых PD-устройств источника питания может оказаться недостаточно. В этом случае система PoE будет работать в критическом режиме.

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. Если политика не настроена, обслуживаются те устройства, которые подключились первыми (first in first serviced). Таким образом, новое PD-устройство не будет обеспечено питанием.

При настроенной политике Preempt Mode PD-устройство с наименьшим приоритетом будет вытеснено новым подключенным PD-устройством с более высоким приоритетом.

Пример

В данном примере показано, как настроить политику распределения системной мощности PoE.

```
Switch#configure terminal
Switch(config)#poe unit 1 policy preempt
Switch(config)#
```

75.5 poe power-inline

Данная команда используется, чтобы настроить режим Power Management Mode (управление энергопотреблением) для портов PoE. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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. Диапазон значений: от 1000 мВт до 30000 мВт.
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

При использовании параметра **auto** PD-устройство будет обнаружено автоматически для подачи питания. Можно задать значение максимальной мощности для порта. Если значение 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.

При вводе команды **no poe power-inline** режим управления энергопотреблением будет сброшен к настройкам по умолчанию.

Настройка профиля временного диапазона является опциональной. Если профиля временного диапазона, указанного в команде, не существует, временной диапазон не назначается.



Примечание: если питаемое устройство не получает питание от коммутатора:

- проверьте, что устройство подключено к порту, поддерживающему стандарт IEEE 802.3at;
- вручную установите ограничение мощности на соответствующем порте в 30 Вт, введя команду **poe power-inline max 30000**.

Пример

В данном примере показано, как настроить автоматическое обнаружение PD-устройства для подачи питания на порту 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#poe power-inline auto
Switch(config-if)#
```

В примере ниже показано, как установить максимальную мощность 7 Вт на порту 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#poe power-inline auto max 7000
Switch(config-if)#
```

В следующем примере показано, как отключить обнаружение PD-устройства и прекратить подачу питания на порту 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#poe power-inline never
Switch(config-if)#
```

В примере ниже показан процесс привязки профиля временного диапазона «day-time» к порту 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#poe power-inline auto time-range day-time
Switch(config-if)#
```

75.6 poe usage-threshold

Данная команда используется, чтобы настроить порог потребления для записи в системный журнал. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

poe unit *UNIT-ID* **usage-threshold** *PERCENTAGE*
no poe unit *UNIT-ID* **usage-threshold**

Параметры

unit *UNIT-ID*	Укажите Unit ID устройства для отображения. Параметр применяется только при включенном стекировании.
PERCENTAGE	Укажите порог потребления для отправки уведомлений. Диапазон значений: от 1 до 99. Единица измерения – проценты.

По умолчанию

Значение по умолчанию – 99%.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При превышении настроенного порога потребления мощности на коммутаторе в системный журнал будет записано *EXCEED*. После уменьшения потребления ниже порога будет записано сообщение *RECOVER*.

Пример

В данном примере показано, как настроить порог потребления для уведомлений до 50%.

```
Switch#configure terminal
Switch(config)#poe unit 1 usage-threshold 50
Switch(config)#
```

75.7 snmp-server enable traps poe

Данная команда используется для включения отправки уведомлений о событиях PoE. Чтобы отключить отправку уведомлений о событиях PoE, воспользуйтесь формой **no** этой команды.

snmp-server enable traps poe [unit *UNIT-ID***]**

no snmp-server enable traps poe [unit *UNIT-ID***]**

Параметры

UNIT-ID	(Опционально.) Укажите Unit ID устройства для конфигурации. Параметр доступен только при использовании стекирования.

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 или отключения отправки trap-сообщений о событиях PoE.

Пример

В данном примере показано, как включить отправку trap-сообщений о событиях PoE.

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

75.8 clear poe statistic

Данная команда используется для сброса счетчиков статистики на порту.

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

Параметры

all	Укажите, чтобы удалить статистику на всех интерфейсах.
interface *INTERFACE-ID*	Укажите интерфейсы, которые необходимо использовать.
,	(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

Privilege EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для отображения счетчиков статистики введите 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 порту 3.

```
Switch#clear poe statistic interface eth1/0/3
Switch#
```

75.9 show poe power-inline

Данная команда используется для отображения статуса PoE для определенного порта или всех портов на коммутаторе.

show poe power-inline [*INTERFACE-ID* **[, | -]] {status | configuration | statistics | measurement | lldp-classification }**

Параметры

INTERFACE-ID	Укажите ID интерфейса для отображения. Если интерфейс не указан, будет отображена информация для всех интерфейсов.

,	(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.
status	Укажите для отображения статуса PoE.
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

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статус PoE на портах, конфигурацию PoE, счетчики статистики, физические параметры и классификацию data link layer. Отображаются только интерфейсы с поддержкой PoE.

Пример

В данном примере показан вывод команды **show poe power-inline status** на интерфейсах Ethernet 1/0/1-1/0/8.

```
Switch#show poe power-inline eth1/0/1-8 status

Interface   State      Class   Max(W) Used(W) Description
------------------------------------------------------------------------------
eth1/0/1    delivering class-1 4      3.4     IP-camera-1
eth1/0/2    delivering class-2 10     6.3     1234567890
eth1/0/3    delivering class-3 15.4   13.0
eth1/0/4    delivering class-3 15.4   1.4     access123
eth1/0/5    searching  n/a     0.0    0.0
eth1/0/6    searching  n/a     0.0    0.0
eth1/0/7    searching  n/a     0.0    0.0
eth1/0/8    searching  n/a     0.0    0.0

Faulty code
[1] MPS (Maintain Power Signature) Absent
[2] PD short
[3] Overload
[4] Power Denied
[5] Thermal Shutdown
[6] Startup Failure
[7] Classification Failure

Switch#
```

Отображаемые параметры

Interface	Идентификатор интерфейса (Interface ID).
State	Статусы порта: **Disabled:** функция PSE отключена. **Searching:** удаленное PD-устройство не подключено. **Requesting:** удаленное PD-устройство подключено, но PSE еще не обеспечивает подачу питания. **Delivering:** подача питания на удаленное PD-устройство обеспечена системой PoE. **Faulty[X]:** PD-устройство не обнаружено или находится в неисправном состоянии. В качестве «**X**» указывается номер кода ошибки: • **[1]** – отсутствует поддержка сигнатуры питания (MPS). • **[2]** – короткое замыкание PD-устройства. • **[3]** – перегруженность. • **[4]** – отказ питания. • **[5]** – защитное отключение при перегреве. • **[6]** - ошибка запуска. • **[7]** - ошибка классификации (IEEE 802.3at).
Class	Классификация IEEE: N/A или значение из класса IEEE от 0 до 4.
Max(W)	Максимальное значение мощности в Ваттах, которое может быть назначено для PD-устройства.
Used(W)	Текущее значение мощности, выделенное для PoE-портов в ваттах.

Description	Настроенное описание подключенного PD-устройства.

В следующем примере показано, как отобразить конфигурацию PoE power inline на интерфейсах Ethernet 1/0/1-1/0/6.

```
Switch#show poe power-inline eth1/0/1-6 configuration

Interface Admin   Priority  Legacy-Support  Time-Range
------------------------------------------------------------------
eth1/0/1  auto    low       disabled
eth1/0/2  auto    low       disabled
eth1/0/3  auto    low       disabled
eth1/0/4  auto    critical  enabled         day-time
eth1/0/5  auto    low       disabled
eth1/0/6  auto    low       disabled

Switch#
```

Отображаемые параметры

Interface	Идентификатор интерфейса (Interface ID).
Admin	Возможные режимы пользователя: **Auto:** PD-устройство будет обнаружено автоматически, а максимальная мощность будет зависеть от результата обнаружения. **Auto(M):** PD-устройство будет обнаружено автоматически, а в качестве максимальной мощности будет использовано значение, настроенное пользователем. **Never:** PD-устройство не будет обнаружено, и подача питания на порт не будет обеспечена.
Priority	Приоритет, используемый для определения очереди обслуживания во время ограничения мощности в блоке питания.
Legacy-Support	**Enabled:** устаревшее PD-устройство (legacy PD) может быть обнаружено. **Disabled:** устаревшее PD-устройство (legacy PD) не может быть обнаружено.
Time-Range	Имя профиля временного диапазона, настроенного для периода активации порта.

В данном примере показано, как отобразить статистику PoE power inline.

```
Switch#show poe power-inline statistics

Interface  MPS Absent  Overload  Short  Power Denied  Invalid Signature
---------  ----------  --------  -----  ------------  -----------------
eth1/0/1       0           0       0         0              228
eth1/0/2       0           0       0         0              229
eth1/0/3       0           0       0         0              8
eth1/0/4       0           0       0         0              76
eth1/0/5       0           0       0         0              233
eth1/0/6       0           0       0         0              229
eth1/0/7       0           0       0         0              27
eth1/0/8       0           0       0         0              230
eth1/0/9       0           0       0         0              139
eth1/0/10      0           0       0         0              139
eth1/0/11      0           0       0         0              139
eth1/0/12      0           0       0         0              139
eth1/0/13      0           0       0         0              139
eth1/0/14      0           0       0         0              134
eth1/0/15      0           0       0         0              134
eth1/0/16      0           0       0         0              134
eth1/0/17      0           0       0         0              165
eth1/0/18      0           0       0         0              249
eth1/0/19      0           0       0         0              184
eth1/0/20      0           0       0         0              151
eth1/0/21      0           0       0         0              57
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Отображаемые параметры

MPS Absent	Счетчик увеличивается, если PSE прекращает обеспечивать подачу питания на PI из-за невозможности PSE контролировать доступные MPS PD-устройства на PI.
Overload	Если PD-устройство потребляет слишком много энергии и превышает максимальную выходную мощность, которую может обеспечить порт, то счетчик перегрузки увеличивается.
Short	Счетчик увеличивается, когда по какой-то причине происходит короткое замыкание PD-устройства в зоне действия защиты.
Power Denied	**Enabled:** устаревшее PD-устройство (legacy PD) может быть обнаружено. **Disabled:** устаревшее PD-устройство (legacy PD) не может быть обнаружено.
Invalid Signature	Увеличивается, если PSE обнаруживает PD-устройство с недействительной подписью PD.

В данном примере показано, как отобразить статистику PoE power inline measurement.

```
Switch#show poe power-inline eth1/0/1-6 measurement

Interface  Voltage(V)  Current(mA)  Temperature(C)  Power(W)
---------  ----------  -----------  --------------  ---------
eth1/0/1     54.2         109          35            5.9
eth1/0/2     55           196          38            10.8
eth1/0/3     n/a          n/a          n/a           n/a
eth1/0/4     53.8         28           27            1.5
eth1/0/5     n/a          n/a          n/a           n/a
eth1/0/6     n/a          n/a          n/a           n/a

Switch#
```

В примере ниже показано, как отобразить классификацию PoE power inline LLDP.

```
Switch#show poe power-inline lldp-classification

Interface eth1/0/1
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: low
PD requested power value: 25.0W
PSE allocated power value: 25.0W

Information from PD:

Power type: type 2 PD
Power source: PSE
Power priority: unknown
PD requested power value: 25.0W
PSE allocated power value: 25.0W

Interface eth1/0/2
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: high
PD requested power value: 0.0W
PSE allocated power value: 0.0W
```

```
Information from PD:

none

Interface eth1/0/3
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: low
PD requested power value: 20.0W
PSE allocated power value: 20.0W

Information from PD:

Power type: type 2 PD
Power source: PSE
Power priority: unknown
PD requested power value: 20.0W
PSE allocated power value: 20.0W

Switch#
```

Отображаемые параметры

Interface	Идентификатор интерфейса PoE (Interface ID).
Power type	Поле типа мощности в Power via MDI TLV из пакетов LLDP устройств PSE или PD.
Power source	Поле источника мощности в Power via MDI TLV из пакетов LLDP устройств PSE или PD.
Power priority	Поле приоритета мощности в Power via MDI TLV из пакетов LLDP устройств PSE или PD.
PD requested power value	Поле значения запрошенной мощности PD-устройства в Power via MDI TLV из пакетов LLDP устройств PSE или PD.
PSE allocated power value	Поле значения назначенной мощности PD-устройства в Power via MDI TLV из пакетов LLDP устройств PSE или PD.

75.10 show poe power module

Данная команда используется для отображения настроек и фактических значений модулей питания.

show poe power module [unit *UNIT-ID***] [detail]**

Параметры

unit *UNIT-ID*	(Опционально.) Укажите Unit ID устройства для отображения. Параметр применяется только при включенном стекировании.
detail	(Опционально.) Укажите для отображения более подробной информации о питании и параметров PD-устройств.

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 параметрах чипа PoE для модулей питания.

Пример

В данном примере показано, как отобразить найстройки и фактические значения модулей питания.

```
Switch#show poe power module

Unit Delivered(W)  Power Budget(W)  Usage-Threshold(%)   Preempt   Trap State
-------------------------------------------------------------------------------
1      0             370               50              Enabled    Enabled

Switch#
```

Отображаемые параметры

Unit	ID устройства в стеке.
Delivered	Фактическая мощность, подаваемая на PD-утройство, в ваттах.
Power budget	Общий бюджет мощности в ваттах, который может обеспечить устройство.
Usage-Threshold	Порог потребления для записи в журнал.

Preempt	**Enabled:** режим управления мощностью – Policy Preempt, поэтому PD-устройство с более низким приоритетом будет вытеснено PD-устройством с более высоким приоритетом. **Disabled:** режим управления мощностью настроен на первом устройстве в очереди обслуживания.
Trap State	**Enabled:** trap-сообщение отправляется, когда указанное значение порога потребления PoE превышено. **Disabled:** trap-сообщение не отправляется, когда указанное значение порога потребления PoE превышено.

В данном примере показано, как отобразить подробную информацию о PoE для устройства (Unit 1).

```
Switch#show poe power module unit 1 detail

Unit Delivered(W)  Power Budget(W)  Usage-Threshold(%)   Preempt   Trap State
------------------------------------------------------------------------------
1      0             370               50              Enabled    Enabled

PoE system parameters:
Unit   Max Ports   Device ID    SW Version
----   ---------   ---------    ----------
1      24          E121         20

Switch#
```

Отображаемые параметры

Max Ports	Максимальное количество портов под-системы PoE.
Device ID	Аппаратная версия устройства PoE.
S/W Version	Версия программного обеспечения устройства PoE.

75.11 poe pd alive

Данная команда используется для включения функции PD Alive, которая позволяет отслеживать доступность PD-устройств, подключенных к порту PoE. Для отключения функции воспользуйтесь формой **no** этой команды.

poe pd alive [{ip {*IP-ADDRESS***} | interval** *INTERVAL-TIME* **| retry** *RETRY-COUNT* **| waiting-time** *WAITING-TIME* **| action {reset | notify | both}}]**

no poe pd alive [{ip | interval | retry | waiting-time | action}]

Параметры

ip	(Опционально.) Укажите IPv4-адрес назначенного PD-устройства для системы, выполняющей действие ping.

interval	(Опционально.) Укажите период времени, через которое системой будут отправлены запросы ping для обнаружения назначенных PD-устройств. Диапазон значений: от 10 до 300 секунд.
retry	(Опционально.) Укажите количество повторных попыток запросов ping, когда PD-устройство не отвечает. Диапазон значений: от 0 до 5.
waiting-time	(Опционально.) Укажите время ожидания восстановления PD-устройства после перезагрузки. Диапазон значений: от 30 до 300 секунд.
action	(Опционально.) Укажите действие, которое будет выполнено системой, когда PD-устройство не отвечает на запрос ping. **reset** – укажите, чтобы отключить, а затем включить порт PoE. **notify** – укажите, чтобы включить записи в журнале и trap-сообщения для уведомления администратора. **both** – укажите, чтобы сначала были включены записи в журнале и trap-сообщения, а затем сброшено состояние порта PoE.

По умолчанию

По умолчанию данная функция отключена.
По умолчанию адрес не назначен.
Интервал для отправки запросов ping по умолчанию – 30 секунд.Количество попыток запросов ping по умолчанию – 2.
Время ожидания восстановления PD-устройства после перезагрузки по умолчанию – 90 секунд.
Когда PD-устройство не отвечает на запрос ping, по умолчанию выполняется действие **both**.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная функция применяется только на портах с подачей питания по PoE.

Функция PD Alive позволяет проверять PD-устройства, которые перестают работать или не отвечают на запрос ping.

Используйте данную команду без опциональных параметров, чтобы включить/отключить функцию PD Alive.

По умолчанию IP-адрес назначенного PD-устройства для системы, отправляющей запрос ping, не настроен. IP-адрес назначенного PD-устройства необходимо настроить с помощью команды p**oe pd alive ip** перед включением функции PD Alive.

Указанные PD-устройства должны быть периодически отслежены системой с помощью запросов ping. При отсутствии ответа системой будет выполнено одно из действий, настроенное в команде **poe pd**

alive action. Интервал между повторными попытками задается с помощью команды **poe pd alive interval**.

В системе реализован механизм повторных попыток проверки состояния PD-устройств. Если PD-устройство не отвечает на повторный запрос ping, питание порта PoE будет сброшено системой. Количество повторных попыток настраивается с помощью команды **poe pd alive retry**.

При использовании параметров **reset** или **both** запрос ping будет снова отправлен системой, когда PD-устройство восстановится после перезагрузки. Время ожидания восстановления PD-устройства после перезагрузки настраивается с помощью команды **poe pd alive waiting-time**.

У функции временного диапазона PoE более высокий приоритет, чем у функции PD Alive, поэтому когда на порту одновременно включены обе функции, функция PD Alive не сработает, пока функция временного диапазона PoE активирована.



Примечание: нормальное функционирование данной функции невозможно на PD-устройстве, которое не поддерживает ICMP.



Примечание: нормальное функционирование данной функции возможно только при правильной настройке IP-адреса, который будет использоваться для достижения PD-устройства через ping.



Примечание: действие reset применяется только при прямом подключении PD-устройства. Если PD-устройство не подключено напрямую, действие **reset** не будет выполнено должным образом.



Примечание: если подключенное напрямую PD-устройство также функционирует в качестве PSE, все PD-устройства следующего уровня, подключенные к этому PSE, будут включаться и отключаться всякий раз, когда функция PD Alive будет срабатывать при выполнении действий **reset** или **both**.

Пример

В данном примере показано, как включить функцию PoE PD Alive для проверки PD-устройств на интерфейсах Ethernet 1/0/1-1/0/2.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-2
Switch(config-if-range)#poe pd alive
Switch(config-if-range)#
```

В примере ниже показано, как настроить IP-адрес назначенного PD-устройства.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive ip 192.168.1.150
Switch(config-if)#
```

В следующем примере показано, как настроить интервал между запросами ping.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive interval 60
Switch(config-if)#
```

В данном примере показан процесс настройки количества повторных попыток запросов ping.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive retry 4
Switch(config-if)#
```

В нижеприведенном примере показано, как настроить время ожидания перезагрузки PD-устройства.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive waiting-time 120
Switch(config-if)#
```

В примере ниже показано, как настроить действие **reset**, когда PD-устройство не отвечает на запрос ping.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive action reset
Switch(config-if)#
```

75.12 show poe pd alive

Данная команда используется для отображения настроек функции PoE PD Alive.

show poe pd alive [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейсы для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки функции PoE PD Alive на указанных портах. Если параметры не указаны, будет отображена информация о всех портах PoE.

Пример

В данном примере показано, как отобразить настройки функции PoE PD Alive на интерфейсах Ethernet 1/0/1-1/0/2.

```
Switch#show poe pd alive interface eth1/0/1-2

Port ID: eth1/0/1
-----------------------------------------------
    PD Alive State                : Enabled
    PD IP Address                 : 0.0.0.0
    Poll Interval                 : 30
    Retry Count                   : 2
    Waiting Time                  : 90
    Action                        : both
Port ID: eth1/0/2
-----------------------------------------------
    PD Alive State                : Enabled
    PD IP Address                 : 192.168.1.150
    Poll Interval                 : 60
    Retry Count                   : 4
    Waiting Time                  : 120
    Action                        : reset

Switch#
```

76. Команды энергосбережения

76.1 dim led

Данная команда используется для отключения индикаторов портов с целью энергосбережения. Чтобы не отключать индикаторы портов, воспользуйтесь формой **no** этой команды.

dim led

no dim led

Параметры

Нет.

По умолчанию

По умолчанию данная функция выключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для отключения или включения индикаторов портов. 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)#
```

76.2 power-saving

Данная команда используется для включения отдельных функций энергосбережения. Чтобы отключить данные функции, воспользуйтесь формой **no** этой команды.

power-saving {link-detection | port-shutdown | dim-led | hibernation}

no power-saving {link-detection | port-shutdown | dim-led | hibernation}

Параметры

link-detection	Укажите, чтобы включать функцию энергосбережения в зависимости

	от статуса соединения.
dim-led	Укажите, чтобы выполнять отключение индикаторов портов по расписанию.
port-shutdown	Укажите, чтобы выполнять отключение портов по расписанию.
hibernation	Укажите, чтобы включать режим сна системы по расписанию. 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: устройство будет отключать неактивные порты в целях энергосбережения.
dim-led: устройство будет отключать индикаторы портов в указанный диапазон времени.
port-shutdown: устройство будет отключать все порты в указанный диапазон времени.
hibernation: устройство будет включать 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 настроить функцию энергосбережения с отключением портов и режимом сна по расписанию.

```
Switch# configure terminal
Switch(config)# power-saving port-shutdown
Switch(config)# power-saving hibernation
Switch(config)#
```

76.3 power-saving eee

Данная команда используется для включения функции Energy-Efficient Ethernet (EEE) на определенных портах. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

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 применяется для включения или отключения функции Energy-Efficient Ethernet (EEE) на определенных портах. Режим EEE позволяет уменьшить энергопотребление при низком трафике пакетов на порту. Если передаваемые данные отсутствуют, на физическом интерфейсе будет включен режим Low Power Idle (LPI). В режиме EEE потребление питания изменяется в соответствии с изменениями текущей пропускной способности.



Примечание: функции EEE и ERPS являются взаимоисключающими.

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)#
```

76.4 power-saving dim-led time-range

Данная команда используется, чтобы настроить профиль временного диапазона для расписания отключения индикаторов. Для удаления профиля указанного диапазона времени воспользуйтесь формой **no** этой команды.

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. Максимальное 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. Если расписание настроено, индикаторы портов будут отключаться в соответствии с ним.

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)#
```

76.5 power-saving hibernation time-range

Данная команда используется для настройки профиля временного диапазона для расписания режима сна системы (hibernation). Используйте форму **no**, чтобы удалить профиль указанного диапазона времени.

power-saving hibernation time-range *PROFILE-NAME*
no power-saving hibernation time-range *PROFILE-NAME*

Параметры

PROFILE-NAME	Укажите имя профиля временного диапазона, который необходимо настроить. Максимальное 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 индикаторы, сетевые функции не действуют. 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)#
```

76.6 power-saving shutdown time-range

Данная команда используется, чтобы настроить профиль временного диапазона для расписания отключения порта. Для удаления профиля указанного диапазона времени воспользуйтесь формой **no** этой команды.

power-saving shutdown time-range *PROFILE-NAME*
no power-saving shutdown time-range *PROFILE-NAME*

Параметры

PROFILE-NAME	Укажите имя профиля временного диапазона, который необходимо настроить. Максимальное 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. Указанный порт будет отключаться в соответствии с настроенным расписанием.

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)#
```

76.7 show power-saving

Данная команда используется для отображения информации о настройках энергосбережения.

show power-saving [link-detection] [dim-led] [port-shutdown [hibernation] [eee]

Параметры

link-detection	(Опционально.) Укажите, чтобы отобразить настройки энергосбережения в зависимости от статуса соединения.
dim-led	(Опционально.) Укажите, чтобы отобразить состояние индикаторов.
port-shutdown	(Опционально.) Укажите, чтобы отобразить настройки энергосбережения, связанные с отключением порта.
hibernation	(Опционально.) Укажите, чтобы отобразить настройки энергосбережения для режима сна. Данный параметр можно использовать, только если отключен режим стекирования.
eee	(Опционально.) Укажите, чтобы отобразить состояние функции EEE.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если параметры не указаны, будет отображена информация обо всех настройках энергосбережения.

Пример

В данном примере показано, как отобразить информацию обо всех настройках энергосбережения.

```
Switch#show power-saving

Link Detection Power Saving
  State: Disabled

Administrative Dim-LED
  State: Disabled

Scheduled Dim-LED Power Saving
  State: Disabled

Scheduled Port-shutdown Power Saving
  State: Disabled

EEE_Enabled Ports

Switch#
```

77. Команды Priority-based Flow Control (PFC)

77.1 clear priority-flow-control counters

Данная команда используется для обнуления счетчиков PFC (управления потоком в соответствии с приоритетом) на указанных интерфейсах.

clear priority-flow-control counters {all | *INTERFACE-ID* **[, | -]} {rx | tx | both}**

Параметры

all	Укажите, чтобы обнулить PFC-счетчики на всех интерфейсах.
INTERFACE-ID	Укажите интерфейсы, которые 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.
rx	Укажите, чтобы обнулить полученные кадры PFC.
tx	Укажите, чтобы обнулить отправленные кадры PFC.
both	Укажите, чтобы обнулить счетчик полученных и отправленных кадров PFC.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда используется для обнуления PFC-счетчиков запросов и показателей на указанных интерфейсах.

Пример

В данном примере показано, как обнулить счетчики отправленных кадров PFC на интерфейсе Ethernet 1/0/21.

```
Switch#clear priority-flow-control counters eth1/0/21 tx
Switch#
```

77.2 show interfaces priority-flow-control

Данная команда используется для отображения информации о PFC на интерфейсе.

show interfaces [*INTERFACE-ID* **[, | -]] priority-flow-control**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейсы физического порта для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения информации о PFC на указанных интерфейсах.

Пример

В данном примере показано, как отобразить информацию о PFC на интерфейсах Ethernet от 1/0/25 до 1/0/26.

```
Switch#show interfaces eth1/0/25-26 priority-flow-control

Interface PFC  Admin PFC On      Oper PFC On       Rx PFC    Tx PFC
Id        Cap. Priorities        Priorities        Frame(s)  Frame(s)
--------------------------------  ----------------  --------------------
eth1/0/25  8                     (7)               0         0
eth1/0/26  8                     (7)               0         0

Switch#
```

Отображаемые параметры

PFC Cap	**Возможности PFC**: указывает количество классов трафика, поддерживаемых PFC на устройстве одновременно.

Admin PFC On Priorities	Список CoS, для которых пользователь настроил PFC.
Oper PFC On Priorities	Список CoS, для которых включен действующий PFC. Если список пуст, значит на интерфейсе нет CoS, для которых действующий PFC активен.
Rx PFC Frame(s)	Счетчик полученных кадров PFC.
Tx PFC Frame(s)	Счетчик отправленных кадров PFC.

78. Команды Private VLAN

78.1 private-vlan

Данная команда используется для настройки VLAN в качестве Private VLAN. Чтобы удалить настройку Private VLAN, воспользуйтесь формой **no** этой команды.

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 изолированной VLAN не могут обмениваться информацией друг с другом и с портами других Community VLAN на 2 уровне.
primary	Укажите для настройки VLAN в качестве основной (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 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)#
```

78.2 private-vlan association

Данная команда используется для ассоциирования второстепенной VLAN с основной VLAN. Чтобы отменить ассоциирование VLAN, воспользуйтесь формой **no** этой команды.

private-vlan association {add *SECONDARY-VLAN-ID* **[, | -] | remove** *SECONDARY-VLAN-ID* **[, | -]}**

no private-vlan association

Параметры

add *SECONDARY-VLAN-ID*	Укажите для связи указанной второстепенной VLAN с основной VLAN. Диапазон значений VLAN ID: от 2 до 4094.
remove *SECONDARY-VLAN-ID*	Укажите, чтобы удалить связь указанной второстепенной VLAN с основной 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

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

С основной VLAN могут быть связаны одна изолированная (Isolated) и несколько общедоступных (Community) VLAN. Второстепенная VLAN может быть связана только с одной основной 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)#
```

78.3 private-vlan synchronize

Данная команда используется для синхронизации второстепенных VLAN, чтобы у них был тот же самый идентификатор сопоставления MST (mapping MST ID), что и у основной 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)#
```

78.4 switchport mode private-vlan

Данная команда используется для назначения порта в качестве порта Private VLAN. Доступные типы порта – host port (порт узла) и promiscuous port (смешанный порт). Для возвращения к заводским настройкам воспользуйтесь формой **no** этой команды.

switchport mode private-vlan {host | promiscuous}
no switchport mode

Параметры

host	Укажите порт в качестве изолированного (Isolated) или общедоступного (Community).
promiscuous	Укажите порт в качестве смешанного (Promiscuous).

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 вторичной VLAN и основной VLAN.

Для порта Promiscuous введите команду **switchport mode private-vlan promiscuous**, чтобы указать режим порта, и команду **switchport private-vlan mapping**, чтобы связать порт с основной VLAN и определить сопоставление с второстепенной VLAN.

Для порта Trunk основной VLAN используйте команду **switchport mode trunk**, чтобы указать режим порта, и команду **switchport trunk allowed vlan**, чтобы определить связанные VLAN.

При смене режима порта настройки, связанные с предыдущим режимом, будут утеряны.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве порта Host Port для Private VLAN, а интерфейс Ethernet 1/0/2 в качестве 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)#
```

78.5 switchport private-vlan host-association

Данная команда используется для ассоциации Private VLAN с портом Isolated, портом Community или второстепенным портом Trunk. Чтобы отменить связь, воспользуйтесь формой **no** этой команды.

switchport private-vlan host-association *PRIMARY-VLAN-ID SECONDARY-VLAN-ID*
no switchport private-vlan host-association

Параметры

PRIMARY-VLAN-ID	Укажите ID основной VLAN, которую необходимо ассоциировать. Диапазон VLAN ID: от 2 до 4094.
SECONDARY-VLAN-ID	Укажите ID второстепенной VLAN, которую необходимо ассоциировать. Диапазон VLAN ID: от 2 до 4094.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Порт является изолированным (Isolated), если второстепенная VLAN, указанная в команде, будет изолированной (Isolated). Порт является общедоступным (Commnity), если второстепенная VLAN, указанная командой, является Community VLAN. Команда настроит порт в качестве нетегированного участника указанной основной и второстепенной VLAN.

Пример

В данном примере показано, как связать интерфейс 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)#
```

78.6 switchport private-vlan mapping

Данная команда позволяет ассоциировать членство Private VLAN с портом Promiscuous или Trunk Promiscuous. Чтобы отменить ассоциирование, воспользуйтесь формой **no** этой команды.

switchport private-vlan mapping *PRIMARY-VLAN-ID* **{add** *SECONDARY-VLAN-ID* **[, | -] | remove** *SECONDARY-VLAN-ID* **[, | -]}**

no switchport private-vlan mapping

Параметры

PRIMARY-VLAN-ID	Укажите ID основной VLAN. Диапазон VLAN ID: от 2 до 4094.
add *SECONDARY-VLAN-ID*	Укажите, чтобы добавить членство в указанной второстепенной VLAN. Диапазон VLAN ID: от 2 до 4094.
remove *SECONDARY-VLAN-ID*	Укажите, чтобы удалить членство в указанной второстепенной VLAN.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона 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

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

Используйте команду для ассоциирования Private VLAN с портом Promiscuous или Trunk Promiscuous. Команда настроит порт в качестве нетегированного участника указанной основной и второстепенной VLAN.

Пример

В данном примере показано, как настроить интерфейс 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)#
```

78.7 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.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения списка Private VLAN, находящегося в домене VLAN, и ассоциирования второстепенных и основных VLAN и портов для каждой Private VLAN.

Пример

В примере показано, как отобразить настройки Private VLAN. В данном примере настроено 2 домена

Private VLAN.

```
Switch#show vlan private-vlan

Primary VLAN   Secondary VLAN   Type        Interface
-------------  ---------------  ----------  ----------------------------
1000           1001             Isolated    eth1/0/1, eth1/0/16
               1002             Community
               1003             Community
2000           2001             Isolated    eth1/0/2, eth1/0/3
2000           2002             Community   eth1/0/2, eth1/0/3
2000           2003             Community   eth1/0/4, eth1/0/13, eth1/0/15

Total Entries: 6

Switch#
```

79. Команды Protocol Independent

79.1 distance

Данная команда используется, чтобы настроить административное расстояние (administrative distance) для протоколов маршрутизации, включая RIP и OSPF. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

distance *DISTANCE*
no distance

Параметры

DISTANCE	Укажите административное расстояние. Диапазон значений: от 1 до 255.

По умолчанию

Расстояние подключенного маршрута – 0.
Расстояние для внутренних маршрутов зоны OSPF (intra-area routes) – 80.
Расстояние для маршрутов между зонами OSPF (inter-area routes) – 90.
Расстояние для внешнего маршрута типа 1 OSPF (type-1 AS external route) – 110.
Расстояние для внешнего маршрута типа 2 OSPF (type-2 AS external route) – 115.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить расстояние, которое представляет собой рейтинг надежности маршрута. В качестве расстояния может быть указано целое число от 1 до 255. Маршрут, значение расстояния которого ниже, имеет более высокий приоритет. Маршруты, расстояние которых равно 255, не будут установлены для маршрутизации пакетов, поскольку в данном случае маршруты не являются доверенными. Если команда применяется без параметров, указанным расстоянием будет значение маршрута по умолчанию настроенного протокола.

Пример

В данном примере показано, как настроить расстояние маршрута RIP. Указанное расстояние – 75.

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#distance 75
Switch(config-router)#
```

79.2 distance default

Данная команда используется, чтобы настроить административное расстояние для статического маршрута по умолчанию. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

distance default *DISTANCE*
no distance default

Параметры

DISTANCE	Укажите административное расстояние. 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 собой рейтинг надежности маршрута. В качестве расстояния может быть указано целое число от 1 до 255. Маршрут, значение расстояния которого ниже, имеет более высокий приоритет.

Пример

В данном примере показано, как настроить расстояние статического маршрута по умолчанию. Указанное значение – 150.

```
Switch#configure terminal
Switch(config)#distance default 150
Switch(config)#
```

79.3 distance static

Данная команда используется, чтобы настроить административное расстояние для статических маршрутов. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

distance static *DISTANCE*
no distance static

Параметры

DISTANCE	Укажите административное расстояние. 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 собой рейтинг надежности маршрута. В качестве расстояния может быть указано целое число от 1 до 255. Маршрут, значение расстояния которого ниже, имеет более высокий приоритет.

Пример

В данном примере показано, как настроить расстояние статического маршрута. Указанное значение – 100.

```
Switch# configure terminal
Switch(config)# distance static 100
Switch(config)#
```

79.4 distribute-list in (OSPF)

Данная команда используется, чтобы настроить список distribute list для фильтрации обновлений маршрута OSPF на основе указанного списка доступа. Для удаления фильтра воспользуйтесь формой **no** этой команды.

distribute-list *ACCESS-LIST-NAME* **in [***INTERFACE-ID***]**
no distribute-list *ACCESS-LIST-NAME* **in [***INTERFACE-ID***]**

Параметры

ACCESS-LIST-NAME	Укажите имя стандартного списка доступа IP, определяющего, какие полученные обновления маршрута должны быть приняты, а какие – анонсированы.
INTERFACE-ID	(Опционально.) Укажите интерфейс, к которому необходимо применить настроенный список distribute list.

По умолчанию

Нет.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При применении списка доступа к интерфейсу командой **distribute-list in** обновления маршрута, полученные указанным интерфейсом, фильтруются на основе этого списка.

Если ID интерфейса не указан, список distribute list будет применен ко всем интерфейсам.

Пример

В данном примере показано, как настроить список доступа «East-ranch» для фильтрации обновлений маршрута протокола OSPF.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#distribute-list East-ranch in
Switch(config-router)#
```

79.5 distribute-list in (RIP)

Данная команда используется, чтобы настроить список distribute list для фильтрации обновлений маршрута RIP на основе указанного списка доступа. Для удаления фильтра воспользуйтесь формой **no** этой команды.

distribute-list *ACCESS-LIST-NAME* **in [***INTERFACE-ID***]**

no distribute-list *ACCESS-LIST-NAME* **in [***INTERFACE-ID***]**

Параметры

ACCESS-LIST-NAME	Укажите имя стандартного списка доступа IP, определяющего, какие полученные обновления маршрута должны быть приняты, а какие – анонсированы.
INTERFACE-ID	(Опционально.) Укажите интерфейс, к которому необходимо применить настроенный список distribute list.

По умолчанию

Нет.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При применении списка доступа к интерфейсу командой **distribute-list in** обновления маршрута, полученные указанным интерфейсом, фильтруются на основе этого списка.

Пример

В данном примере показано, как настроить список доступа «branch-route» для фильтрации обновлений маршрута протокола RIP.

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#distribute-list branch-route in vlan1
Switch(config-router)#
```

79.6 ip route

Данная команда используется для создания записи статического маршрута. Чтобы удалить запись статического маршрута, воспользуйтесь формой **no** этой команды.

ip route *NETWORK-PREFIX NETWORK-MASK* **{***IP-ADDRESS* **[primary | backup | weight** *NUMBER***] | null0}**

no ip route *NETWORK-PREFIX NETWORK-MASK* **{***IP-ADDRESS* **| null0}**

Параметры

NETWORK-PREFIX	Укажите сетевой адрес.
NETWORK-MASK	Укажите сетевую маску.
IP-ADDRESS	Укажите IP-адрес следующего узла , который будет использоваться для достижения сети назначения.
primary	(Опционально.) Указывает, что маршрут будет использоваться в качестве основного.
backup	(Опционально.) Указывает, что маршрут будет использоваться в качестве резервного.
weight *NUMBER*	(Опционально.) Укажите значение веса (weight) больше 0, но меньше максимального количества путей. Данное значение применяется, чтобы дублировать путь идентичного маршрута (несколько копий) в таблице маршрутизации. Таким образом, у пути будет больше возможностей быть выбранным для маршрутизации трафика. Если для статического маршрута не указано значение веса, то по умолчанию для пути в хэш-таблице используется одна копия.

null0	Указывает, что маршрут будет использоваться в качестве нулевого (black hole route).

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Чтобы задать маршрут по умолчанию, укажите **0.0.0.0 0.0.0.0**.

Поддерживаются резервные маршруты. Это означает, что можно создать два маршрута с одним адресом сети назначения, но с разными следующими узлами. Если параметры **primary** или **backup** не указаны, статический маршрут будет автоматически определен как основной или резервный. Основной маршрут считается предпочтительным. Если он становится недоступным, будет использоваться резервный маршрут.

Если у нескольких маршрутов в одну сеть назначения одинаковое значение веса, такая маршрутизация называется Equal-cost Multi-path (ECMP).

Например:

- ip route 100.1.1.0 255.255.255.0 10.1.1.1 weight 1
- ip route 100.1.1.0 255.255.255.0 10.1.1.2 weight 1
- ip route 100.1.1.0 255.255.255.0 10.1.1.3 weight 1
- ip route 100.1.1.0 255.255.255.0 10.1.1.4 weight 1

Если вес маршрутов отличается, это Weighted-cost Multi-path (WCMP).

Например:

- ip route 100.1.1.0 255.255.255.0 10.1.1.1 weight 1
- ip route 100.1.1.0 255.255.255.0 10.1.1.2 weight 2
- ip route 100.1.1.0 255.255.255.0 10.1.1.3 weight 3
- ip route 100.1.1.0 255.255.255.0 10.1.1.4 weight 4

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)#
```

79.7 ipv6 route

Данная команда используется для создания записи статического маршрута IPv6. Для удаления записи статического маршрута IPv6 воспользуйтесь формой **no** этой команды.

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.
NETWORK-PREFIX/PREFIX-LENGTH	Укажите сетевой префикс и длину префикса статического маршрута.
INTERFACE-ID	(Опционально.) Укажите интерфейс передачи для маршрутизации пакетов.
NEXT-HOP-ADDRESS	Укажите IPv6-адрес следующего узла (next hop), который будет использоваться для достижения сети назначения. Если адрес является адресом link-local, необходимо также указать ID интерфейса.
primary	(Опционально.) Указывает, что маршрут будет использоваться в качестве основного.
backup	(Опционально.) Указывает, что маршрут будет использоваться в качестве резервного.
DISTANCE	(Опционально.) Укажите административное расстояние статического маршрута. Диапазон значений: от 1 до 254. Чем ниже значение, тем выше приоритет маршрута. Если значение не указано, административное расстояние по умолчанию – 1.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Поддерживаются резервные маршруты. Это означает, что можно создать два маршрута с одним адресом сети назначения, но с разными следующими узлами. Если параметры **primary** или **backup** не указаны, статический маршрут будет автоматически определен как основной или резервный. Основной маршрут считается предпочтительным и всегда используется для продвижения, если

находится в активном режиме. Если он становится недоступным, будет использоваться резервный маршрут.

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 vlan1 fe80::0000:00ff:1111:2233
Switch(config)#
```

79.8 ip route ecmp load-balance

Данная команда используется, чтобы настроить алгоритм балансировки нагрузки для распределения трафика в сеть назначения между несколькими маршрутами. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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	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	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	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	Алгоритм балансировки нагрузки, включающий IP-адрес назначения.
port	Алгоритм балансировки нагрузки, включающий TCP-порт или UDP-порт.

По умолчанию

По умолчанию используется параметр **sip**.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить алгоритм балансировки нагрузки для распределения трафика в сеть назначения между несколькими маршрутами.

Пример

В данном примере показано, как настроить алгоритм балансировки нагрузки. Указанный алгоритм – dip.

```
Switch#configure terminal
Switch(config)#ip route ecmp load-balance dip
Switch(config)#
```

79.9 maximum-paths

Данная команда используется, чтобы указать максимальное количество параллельных маршрутов настроенного протокола маршрутизации, которые можно одновременно установить в таблице маршрутизации. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

maximum-paths *NUMBER-PATHS*

no maximum-paths

Параметры

NUMBER-PATHS	Укажите максимальное количество параллельных маршрутов.

По умолчанию

Значение по умолчанию – 1.

Режим ввода команды

OSPF Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Маршрут может быть получен из разных источников. Каждый маршрут ассоциирован с расстоянием. Маршрут с наименьшим расстоянием будет добавлен в таблицу маршрутизации.

Значение, указанное в команде **maximum-paths**, определяет максимальное количество параллельных маршрутов в одну сеть назначения, которые могут быть одновременно установлены в таблице маршрутизации. Установленные параллельные маршруты должны относиться к одному и тому же источнику.

Пример

В данном примере показано, как указать максимальное количество путей OSPF – 4.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#maximum-paths 4
Switch(config-router)#
```

79.10 show ip protocols

Данная команда используется, чтобы отобразить состояние процесса маршрутизации.

show ip protocols [rip | ospf]

Параметры

rip	(Опционально.) Укажите для отображения общих настроек протокола RIP.
ospf	(Опционально.) Укажите для отображения общих настроек протокола OSPF.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить состояние процессов маршрутизации. Если параметры не указаны, 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 30 seconds, next due in 9 seconds
  Invalid 180 secs, flush 120 secs
  Default redistribution metric is 0
  Redistributing: OSPF
  Default version control: send version 1, receive any version
    Interface     Send       Recv
    vlan2         1          1 2
  Maximum path: 1
  Routing for Networks:
    vlan2  (200.1.1.5/255.255.255.0)
  Routing Information Sources:
    Gateway          Last Update
  Distribute list:
    East branch (in)
    Interface   in
  Distance:100

Routing Protocol is OSPF
  Router ID 200.1.1.5
  Number of areas in this router is 2. 2 normal, 0 stub, 0 nssa
  Maximum path: 1
  Routing for Networks:
    200.1.1.5/24
  Routing Information Sources:
    Gateway
  Distribute list:
    Incoming update filter list for all interfaces is not set
  External-1 distance 110, External-2 distance 115, Inter-area distance 90, Intra-area
distance 80
Switch#
```

79.11 show ip route

Данная команда используется для отображения записей таблицы маршрутизации.

show ip route [[*IP-ADDRESS* **[***MASK***] | ***PROTOCOL*** | hardware]**

Параметры

IP-ADDRESS	(Опционально.) Укажите сетевой адрес, информацию о маршрутизации которого необходимо отобразить.
MASK	(Опционально.) Укажите маску подсети для указанной сети.
PROTOCOL	(Опционально.) Укажите протокол маршрутизации или ключевые слова: **static, connected**, **RIP**, **OSPF**.
hardware	(Опционально.) Укажите для отображения маршрутов, записанных в чипсет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

В таблицу маршрутизации занесены маршруты, информация о которых была получена из разных протоколов. Если в одну и ту же сеть есть несколько маршрутов, для перенаправления пакетов будет выбран тот, у которого меньше значение расстояния и доступен следующий узел (next hop).

Пример

В данном примере показано, как отобразить таблицу маршрутизации.

```
Switch#show ip route

Code: C - connected, S - static, R - RIP, 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, vlan11
O    1.0.0.0/8 [80/2] via 11.0.0.1, vlan11
O    2.0.0.0/8 [80/2] via 11.0.0.1, vlan11
C    11.0.0.0/8 is directly connected, vlan11
O    12.0.0.0/8 [80/3] via 11.0.0.1, vlan11
O    13.0.0.0/8 [80/3] via 11.0.0.1, vlan11
O    17.0.0.0/8 [80/3] via 11.0.0.1, vlan11
O    18.0.0.0/8 [80/3] via 11.0.0.1, vlan11
O    30.0.0.0/8 [80/2] via 11.0.0.1, vlan11
O    40.0.0.0/8 [80/3] via 11.0.0.1, vlan11
R    105.100.0.0/24 [100/2] via 11.0.0.5, vlan11
C    107.100.0.0/16 is directly connected, vlan1
C    172.18.64.0/21 is directly connected, mgmt_ipif
R    212.254.254.0/24 [100/2] via 11.0.0.254, vlan11

Total Entries: 14

Switch#
```

79.12 show ip route summary

Данная команда используется для отображения краткой информации о текущих записях маршрутизации.

show ip route summary

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется 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
Total           14
Multi-path      0

Switch#
```

79.13 show ipv6 route

Данная команда используется для отображения записей таблицы маршрутизации.

show ipv6 route [[*IPV6-ADDRESS* **|** *NETWORK-PREFIX/PREFIX-LENGTH* **[longer-prefixes]** | *INTERFACE-ID* **|** *PROTOCOL*] **[database]** | **hardware]**

Параметры

IPV6-ADDRESS	(Опционально.) Укажите IPv6-адрес, чтобы найти самый длинный префикс соответствующего IPv6-маршрута.
NETWORK-PREFIX	(Опционально.) Укажите сетевой адрес, информацию о маршрутизации которого необходимо отобразить.
PREFIX-LENGTH	(Опционально.) Укажите длину префикса для указанной сети.

longer-prefixes	(Опционально.) Укажите для отображения всех более точных маршрутов.
INTERFACE-ID	(Опционально.) Укажите интерфейс для отображения.
PROTOCOL	(Опционально.) Укажите протокол маршрутизации.
database	(Опционально.) Укажите, чтобы отобразить все соответствующие записи в таблице маршрутизации, а не только приоритетный маршрут.
hardware	(Опционально.) Укажите для отображения маршрутов, записанных в чипсет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

В таблицу маршрутизации занесены маршруты, информация о которых была получена из разных протоколов. Если в одну и ту же сеть есть несколько маршрутов, для перенаправления пакетов будет выбран тот, у которого меньше значение расстояния и доступен следующий узел (next hop).

Пример

В данном примере показано, как отобразить записи маршрутизации для IPv6.

```
Switch#show ipv6 route

IPv6 Routing Table
Code: C - connected, S - static, R - RIP, O - OSPF,
      IA - OSPF inter area
      E1 - OSPF external type 1, E2 - OSPF external type 2
      SLAAC - Stateless address autoconfiguration

S     1234::/64 [1/1] via FE80::206:28FF:FED8:FEAC, vlan11
R     2000:17::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan11
R     2000:18::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan11
C     2001:DB8:0:5::/64 [0/1] is directly connected, vlan11
O     2001:DB8:0:5::1/128 [110/10] via FE80::206:28FF:FED8:FE94, vlan11
R     2001:DB8:0:3600::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan11
R     2001:DB8:0:3620::/64 [71/2] via FE80::206:28FF:FED8:FE94, vlan11
R     2016:3630::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan11
O     2105:5000:A::/64 [110/430] via FE80::206:28FF:FED8:FE94, vlan11
C     2107:100:A::/64 [0/1] is directly connected, vlan1
O     2207:7000:AC::/64 [110/8030] via FE80::206:28FF:FED8:FE94, vlan11
O     2207:7171:ABCD::/64 [110/8040] via FE80::206:28FF:FED8:FE94, vlan11
R     6000::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan11
R     7100::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan11

Total Entries: 14 entries, 14 routes
Switch#
```

79.14 show ipv6 route summary

Данная команда используется для отображения краткой информации о текущих записях таблицы маршрутизации IPv6.

show ipv6 route summary

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если система обеспечивает маршрутизацию IPv6-трафика, проверка таблицы маршрутизации помогает понять, как в данный момент перенаправляется трафик 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
OSPF            4
SLAAC           0
Total           14
Switch#
```

80. Команды Protocol Independent Multicast (PIM)

80.1 ip pim

Данная команда используется для включения PIM на интерфейсе для работы в разреженном (Sparse Mode, SM) или уплотненном (Dense Mode, DM) режимах. Чтобы отключить данную функцию на интерфейсе, воспользуйтесь формой **no** этой команды.

ip pim {sparse-mode | dense-mode | sparse-dense-mode}
no ip pim

Параметры

sparse-mode	Укажите для работы в режиме SM.
dense-mode	Укажите для работы в режиме DM.
sparse-dense-mode	Укажите для работы в режиме SM-DM.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда доступна только на интерфейсе с настроенным IP-адресом.

Укажите один из трех режимов работы для интерфейса: разреженный, уплотненный или разреженно-уплотненный. Для изменения режима работы PIM используйте сначала команду **no ip pim** для отключения PIM, а затем установите новый режим.

Уплотненный режим (Dense Mode). PIM-DM предполагает, что когда источник начинает передачу, всем маршрутизаторам в сети требуется многоадресный поток данных. Первоначально многоадресный поток распространяется на все нисходящие маршрутизаторы и интерфейсы, на которых есть участники группы. Если нисходящие маршрутизаторы или участники группы отсутствуют, маршрутизатор отправит сообщение prune, означающее, что многоадресный поток данных не требуется.

Разреженный режим (Sparse Mode). Когда многоадресный (multicast) трафик принимается на интерфейсе в режиме Sparse Mode, маршрутизатором первого перехода (First Hop Router) будет отправлено регистрационное сообщение в точку встречи (Rendezvous Point, RP). Если маршрутизатор не является маршрутизатором первого перехода, трафик будет перенаправлен в соответствии с записью mroute.

В режиме Sparse Mode интерфейс будет помещен в таблицу mroute, только если получит сообщение join от нисходящего маршрутизатора или если на интерфейсе есть участники группы. В этом случае будет запущен процесс PIM Join для построения дерева (shared tree или source tree).

Разреженно-уплотненный режим (Sparse-Dense Mode). Когда интерфейс настроен в режиме PIM Sparse-Dense, принимаемая на интерфейсе многоадресная группа может работать либо в режиме Sparse Mode, либо в режиме Dense Mode. При приеме multicast-трафика на интерфейсе группа, у которой есть известная RP, будет работать в режиме Sparse Mode, в противном случае группа будет работать в режиме Dense Mode.

Пример

В данном примере показано, как включить протокол PIM-SM на указанном интерфейсе.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip pim sparse-mode
Switch(config-if)#
```

80.2 ip pim bsr border

Данная команда используется, чтобы избежать отправки или приема сообщений BSR на интерфейсе. Для разрешения сообщений воспользуйтесь формой **no** этой команды.

ip pim bsr-border

no ip pim bsr-border

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно на интерфейсе с включенным PIM.

Используйте команду на интерфейсе, который граничит с другим доменом, чтобы избежать обмена сообщениями BSR между доменами.

Пример

В данном примере показано, как настроить VLAN 100 в качестве пограничного интерфейса BSR.

```
Switch#configure terminal
Switch(config)#interface vlan100
Switch(config-if)#ip pim bsr-border
Switch(config-if)#
```

80.3 ip pim bsr-candidate

Данная команда используется для назначения роли Candidate Bootstrap Router (CBSR) маршрутизатору. Чтобы отменить назначение роли CBSR маршрутизатору, воспользуйтесь формой **no** этой команды.

ip pim bsr-candidate *INTERFACE-ID* **[***HASH-MASK-LENGTH* **[***PRIORITY***]] [interval** *SECONDS***]**
no ip pim bsr-candidate

Параметры

INTERFACE-ID	Укажите интерфейс, IP-адрес которого будет анонсирован как адрес Bootstrap Router.
HASH-MASK-LENGTH	(Опционально.) Укажите длину хэш-маски для выбора RP. Диапазон значений: от 0 до 32. Если значение не указано, длина маски по умолчанию – 30.
PRIORITY	(Опционально.) Укажите приоритет для CBSR. Диапазон значений: от 0 до 255. Если значение не указано, приоритет по умолчанию – 64. BSR с более высоким приоритетом является предпочтительным. Если значения приоритета совпадают, в качестве BSR будет назначен маршрутизатор с наибольшим IP-адресом.
interval *SECONDS*	(Опционально.) Укажите интервал между сообщениями bootstrap. Диапазон значений: от 1 до 255. Если значение не указано, интервал по умолчанию – 60 секунд.

По умолчанию

По умолчанию маршрутизатор не назначен в качестве CBSR.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно на интерфейсе с настроенным IP-адресом в режиме PIM-SM.

Команда позволяет маршрутизатору отправлять сообщения bootstrap, используя адрес назначенного интерфейса в качестве адреса CBSR. Хэш-маска используется всеми маршрутизаторами внутри

домена, чтобы привязать группу к какой-либо RP из соответствующего набора карт group-range-to-RP (этот набор имеет одинаковую маску наибольшей длины и одинаковый наивысший приоритет). Алгоритм в качестве вводных данных берет за основу адрес группы и адреса кандидатов в RP из карт и выдает один адрес RP, который будет применяться.

Пример

В данном примере показано, как указать IP-адрес маршрутизатора в качестве CBSR на интерфейсе VLAN 1 с длиной хэш-маски 20, приоритетом 192 и интервалом 120 секунд.

```
Switch#configure terminal
Switch(config)#ip pim bsr-candidate vlan1 20 192 interval 120
Switch(config)#
```

80.4 ip pim dr-priority

Данная команда используется для изменения значения приоритета назначенного маршрутизатора (Designated Router, DR). Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip pim dr-priority *PRIORITY*
no ip pim dr-priority

Параметры

PRIORITY	Укажите значение приоритета DR в диапазоне от 0 до 4294967295. Чем больше значение, тем выше приоритет.

По умолчанию

Значение по умолчанию – 1.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно на интерфейсе в режиме PIM-SM.

В режиме DM опция DR Priority не будет внесена в сообщение Hello. В качестве DR назначается маршрутизатор с наивысшим значением приоритета. Если несколько маршрутизаторов имеют наивысший приоритет, то DR становится маршрутизатор с наибольшим значением IP-адреса. Если есть маршрутизатор, у которого отсутствует значение приоритета в Hello-сообщениях, то все маршрутизаторы в локальной сети будут игнорировать приоритет DR и использовать только IP-адрес при выборе DR.

Пример

В данном примере показано, как установить приоритет DR на интерфейсе VLAN 1. Настроенное значение – 200.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip pim dr-priority 200
Switch(config-if)#
```

80.5 ip pim jp-timer

Данная команда используется для настройки значения интервала между сообщениями Join/Prune. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip pim jp-timer *SECONDS*
no ip pim jp-timer

Параметры

SECONDS	Укажите интервал между сообщениями Join/Prune. Диапазон значений: от 1 до 18000 секунд.

По умолчанию

Значение по умолчанию – 60 секунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно на интерфейсе в режиме PIM-SM.

При настройке значения интервала между сообщениями Join/Prune необходимо учитывать следующие факторы: настроенную полосу пропускания и ожидаемое среднее количество записей многоадресной маршрутизации для подключенной сети. В режиме SM маршрутизаторы отправляют периодические сообщения Join в соответствии с данным интервалом. Время ожидания (Hold Time) в сообщениях Join/Prune превышает интервал Join/Prune в 3,5 раза. На основе этого времени ожидания принимающий маршрутизатор запустит таймер и по его истечении отключит интерфейс, если на нем не было получено ни одного сообщения Join.

Пример

В данном примере показано, как установить таймер PIM Join/Prune. Настроенное значение – 120 секунд.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip pim jp-timer 120
Switch(config-if)#
```

80.6 ip pim passive

Данная команда используется для включения пассивного режима на интерфейсе. Для отключения пассивного режима воспользуйтесь формой **no** этой команды.

ip pim passive
no ip pim passive

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 доступна только на интерфейсе с включенным PIM.

При включении пассивного режима интерфейс не будет отправлять и принимать PIM-сообщения, а маршрутизатор не будет распознавать другие соседние устройства.

Данная команда применяется, когда в сети находится только один PIM-маршрутизатор.

Пример

В данном примере показано, как включить пассивный режим на VLAN-интерфейсе 100.

```
Switch#configure terminal
Switch(config)#interface vlan 100
Switch(config-if)#ip pim passive
Switch(config-if)#
```

80.7 ip pim query-interval

Данная команда используется для настройки частоты сообщений PIM Hello. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip pim query-interval *SECONDS*
no ip pim query-interval

Параметры

SECONDS	Укажите интервал между сообщениями Hello.

По умолчанию

Значение по умолчанию – 30 секунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно на интерфейсе с включенным PIM.

Маршрутизатор PIMv2 изучает соседние устройства PIM с помощью сообщений Hello. Используйте данную команду, чтобы настроить частоту сообщений Hello. Маршрутизаторы, настроенные для многоадресной рассылки, отправляют сообщения Hello, чтобы обнаружить другие маршрутизаторы PIM. В режиме SM сообщения Hello также используются для определения назначенного маршрутизатора в каждом сегменте локальной сети. Заданный интервал запросов также применяется как значение времени ожидания (Hold Time). Чем меньше значение интервала, тем быстрее соседнее устройство может быть обнаружено, и таким образом будет повышена отказоустойчивость.

Пример

В данном примере показано, как установить интервал запросов PIM. Настроенное значение – 45 секунд.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip pim query-interval 45
Switch(config-if)#
```

80.8 ip pim register-checksum-wholepkt

Данная команда используется для включения вычисления контрольной суммы для всего пакета Register. Для отключения подсчета контрольной суммы по всему пакету воспользуйтесь формой **no** этой команды.

ip pim register-checksum-wholepkt rp-address-list *ACCESS-LIST-NAME*
no ip pim register-checksum-wholepkt

Параметры

ACCESS-LIST-NAME	Укажите имя списка доступа IP с адресами RP. Это адрес в поле «адрес источника» записи списка доступа.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды
Global Configuration Mode.

Уровень команды по умолчанию
Уровень 12.

Использование команды

Если данная функция отключена, контрольная сумма пакетов Register подсчитывается только по заголовку. Команда может быть введена только один раз. Последующая команда перезапишет предыдущие настройки.

Пример

В данном примере показано, как включить подсчет контрольной суммы для всего пакета Register, отправляемого на RP 10.1.1.1.

```
Switch#configure terminal
Switch(config)#ip access-list rp_filter
Switch(config-ip-acl)#permit host 10.1.1.1
Switch(config-ip-acl)#exit
Switch(config)#ip pim register-checksum-wholepkt rp-address-list rp_filter
Switch(config)#
```

80.9 ip pim register-probe

Данная команда используется для настройки времени register probe. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip pim register-probe *SECONDS*
no ip pim register-probe

Параметры

SECONDS	Укажите значение времени register probe. Диапазон значений: от 1 до 127 секунд.

По умолчанию
Значение по умолчанию – 5 секунд.

Режим ввода команды
Global Configuration Mode.

Уровень команды по умолчанию
Уровень 12.

Использование команды

Register probe – это время до истечения таймера Register Stop Timer (RST), в течение которого DR может отправлять Null-Register на RP для повторной отправки сообщения Register-Stop.

Пример

В данном примере показано, как установить время register probe. Настроенное значение – 7 секунд.

```
Switch#configure terminal
Switch(config)#ip pim register-probe 7
Switch(config)#
```

80.10 ip pim register-suppression

Данная команда используется для настройки времени register suppression. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip pim register-suppression *SECONDS*

no ip pim register-suppression

Параметры

SECONDS	Укажите значение времени register suppression. Диапазон значений: от 3 до 65535 секунд.

По умолчанию

Значение по умолчанию – 60 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Когда DR получает сообщение Register stop, запускается таймер suppression. В течение настроенного времени подавления DR перестает отправлять сообщения Register на RP.

Используйте данную команду на маршрутизаторе первого перехода (first hop router). Для корректной настройки таймера register stop значение времени register probe должно быть меньше половины времени register suppression. Минимальное значение времени register suppression составляет 3 секунды.

Пример

В данном примере показано, как установить время register suppression. Настроенное значение – 30 секунд.

```
Switch#configure terminal
Switch(config)#ip pim register-suppression 30
Switch(config)#
```

80.11 ip pim rp-address

Данная команда используется, чтобы настроить статический адрес RP для многоадресных групп. Для удаления адреса RP воспользуйтесь формой **no** этой команды.

ip pim rp-address *IP-ADDRESS* **[group-list** *ACCESS-LIST-NAME***]**
no ip pim rp-address *IP-ADDRESS*

Параметры

IP-ADDRESS	Укажите IP-адрес RP.
group-list *ACCESS-LIST-NAME*	(Опционально.) Укажите стандартный список доступа, содержащий многоадресные группы. Если список групп не указан, RP будет привязана ко всем многоадресным группам.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для статической привязки многоадресных групп к RP. В многоадресном домене статическая привязка к RP может быть использована вместе с BSR. Привязка многоадресных групп к RP должна быть согласована для всех маршрутизаторов в одном домене. Маршрутизатор первого перехода (first hop router), который инициирует сообщение Register, будет использовать записи привязки, чтобы определить RP при отправке сообщений PIM Register для указанной группы. Маршрутизатор последнего перехода (last hop router), который инициирует сообщение Join, будет использовать записи привязки, чтобы определить RP при отправке сообщений Join/Prune для указанной группы. Полученное сообщение Join будет перенаправлено маршрутизатором после проверки записей привязки. Когда RP получает сообщение Register, а маршрутизатор не является соответствующим RP для многоадресной группы, отправляется сообщение Register stop.

Возможна настройка нескольких RP, для каждой из которой задается отдельный список доступа.

Пример

В данном примере показано, как настроить адрес RP 10.90.90.90 только для многоадресной группы 225.2.2.2.

```
Switch#configure terminal
Switch(config)#ip access-list PIM-Control
Switch(config-ip-acl)#permit any host 225.2.2.2
Switch(config-ip-acl)#exit
Switch(config)#ip pim rp-address 10.90.90.90 group-list PIM-Control
Switch(config)#
```

80.12 ip pim rp-candidate

Данная команда используется для назначения роли RP Candidate маршрутизатору. Чтобы отменить назначение, воспользуйтесь формой **no** этой команды.

ip pim rp-candidate {*INTERFACE-ID* **[group-list** *ACCESS-LIST-NAME***] | interval** *SECONDS* **| priority** *PRIORITY* **| wildcard-prefix-cnt {0 | 1}}**

no ip pim rp-candidate [*INTERFACE-ID***]**

Параметры

INTERFACE-ID	Укажите интерфейс, IP-адрес которого будет анонсирован как адрес Candidate RP.
group-list *ACCESS-LIST-NAME*	(Опционально.) Укажите имя стандартного списка доступа IP, который определяет префиксы группы, анонсируемые в связи с адресом RP. Если список доступа не указан, коммутатор будет являться Candidate RP для всех групп.
interval *SECONDS*	Укажите интервал между объявлениями Candidate RP. Диапазон значений: от 1 до 16383 секунд.
priority *PRIORITY*	Укажите значение приоритета RP. Диапазон значений: от 0 до 255.
wildcard-prefix-cnt	Укажите для установки в сообщении C-RP префикса произвольной wildcard-группы (224.0.0.0/4). Доступны значения: 1 или 0.

По умолчанию

По умолчанию маршрутизатор не назначен в качестве Candidate RP.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда доступна только на интерфейсе в режиме PIM-SM. Для каждого интерфейса может быть указан только один список доступа группы. После применения команды маршрутизатор отправит на BSR сообщение PIMv2 с объявлением себя в качестве Candidate RP.

Пример

В данном примере показано, как настроить маршрутизатор, чтобы он объявлял себя Candidate RP в своем домене PIM. Основной список доступа IP под названием «PIM-Control», который указывает префикс группы (239.0.0.0/8), ассоциирован с RP с адресом интерфейса VLAN 1.

```
Switch#configure terminal
Switch(config)#ip access-list PIM-Control
Switch(config-ip-acl)#permit any 239.0.0.0 0.255.255.255
Switch(config-ip-acl)#exit
Switch(config)#ip pim rp-candidate vlan1 group-list PIM-Control
Switch(config)#
```

80.13 ip pim rp-register-kat

Данная команда используется для настройки времени keep-alive записи (S, G) на RP при получении регистрационных сообщений. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip pim rp-register-kat *SECONDS*
no ip pim rp-register-kat

Параметры

SECONDS	Укажите значение времени keep-alive. Диапазон значений: от 1 до 65525 секунд.

По умолчанию

Значение по умолчанию – 185 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При получении многоадресного потока DR отправляет регистрационное (register) сообщение на RP группы. При получении данного сообщения на RP будет установлен таймер для этой записи (S, G). Используйте данную команду, чтобы настроить значение этого таймера.

Пример

В данном примере показано, как установить время PIM keep-alive. Настроенное значение – 500 секунд.

```
Switch#configure terminal
Switch(config)#ip pim rp-register-kat 500
Switch(config)#
```

80.14 ip pim spt-threshold

Данная команда используется используется для настройки порогового значения PIM Shortest Path Tree (SPT). Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip pim spt-threshold {0 | infinity}
no ip pim spt-threshold

Параметры

0	Укажите, чтобы дерево источника (source tree) было создано сразу же после получения первого пакета.
infinity	Укажите, чтобы всегда использовать общее дерево (shared tree).

По умолчанию

Режим по умолчанию – **infinity**.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду на маршрутизаторе последнего перехода (Last Hop Router). В режиме PIM-SM первоначально multicast-трафик передается от источника к получателю по общему дереву RPT. После получения первых пакетов на маршрутизаторе последнего перехода для каждой группы трафика возможна работа в одном из двух режимов. В режиме **infinity** трафик продолжает идти по общему дереву. В режиме **0** будет построено дерево источника, и трафик переключится на него.

Пример

В данном примере показано, как включить режим **infinity** для порогового значения SPT.

```
Switch#configure terminal
Switch(config)#ip pim spt-threshold infinity
Switch(config)#
```

80.15 ip pim ssm

Данная команда используется для настройки диапазона адресов multicast SSM-группы. Для отключения PIM-SSM воспользуйтесь формой **no** этой команды.

ip pim ssm {default | range *ACCESS-LIST***}**
no ip pim ssm

Параметры

default	Укажите, чтобы использовать диапазон адресов SSM-группы по умолчанию, равный 232.0.0.0/8.
ACCESS-LIST	Укажите стандартный список доступа IP, в котором будут определены заданные пользователем адреса SSM-группы. Адрес группы должен быть указан в поле «IP-адрес назначения» записи правила.

По умолчанию

По умолчанию PIM-SSM отключен.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется только на маршрутизаторе последнего перехода (Last Hop Router) в режиме PIM-SM.

При включении SSM маршрутизатор последнего перехода будет инициировать построение дерева для канала (S,G) при приеме IGMPv3 от подключенных узлов с запросом (S, G), который попадает в диапазон SSM.

Пример

В данном примере показано, как настроить стандартный список доступа IP с указанием диапазона адресов SSM-группы.

```
Switch#configure terminal
Switch(config)#ip access-list SSM-GROUP
Switch(config-ip-acl)#permit any 224.2.0.0 0.0.255.255
Switch(config-ip-acl)#exit
Switch(config)#ip pim ssm range SSM-GROUP
Switch(config)#
```

80.16 show ip pim

Данная команда используется для отображения общей информации о PIM.

show ip pim

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения общей информации о PIM.

Пример

В данном примере показано, как отобразить общую информацию о PIM.

```
Switch#show ip pim

PIM Configurations:

Register Checksum Wholepkt: (Not configured)
Register Probe Time            : 5 seconds
Register Suppression Time      : 60 seconds
Register Keepalive Time on RP  : 185 seconds
SPT Threshold                  : Infinity

RP Address
  90.1.1.1, group-list: static-rp

RP Candidate
  priority: 192, interval: 60 seconds, wildcard-prefix-cnt: 0
  vlan100, group-list: rp-cand

BSR Candidate
  vlan100, hash-mask-length: 30, priority: 1, interval: 60 seconds

SSM group : Movies

Switch#
```

80.17 show ip pim bsr-router

Данная команда используется для отображения информации о BSR.

show ip pim bsr-router

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о выбранном BSR и объявлениях о локально сконфигурированном Candidate RP.

Пример

В данном примере показано, как отобразить информацию о BSR на маршрутизаторе BSR с информацией о Candidate RP на интерфейсе VLAN 100.

```
Switch# show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 90.1.1.3
  BSR Priority: 3, Hash mask length: 30
  Next bootstrap message in 0DT00H00M21S
  Candidate RP: 90.1.1.3(vlan100), Group ACL: crp-list
  Next Cand_RP_advertisement in 0DT00H00M13S
Switch#
```

В примере ниже показано, как отобразить информацию о BSR на маршрутизаторе, не являющимся BSR, с информацией о Candidate RP на интерфейсе маршрутизатора.

```
Switch# show ip pim bsr-router
PIMv2 Bootstrap information
  BSR address: 192.168.53.113
  BSR Priority: 255, Hash mask length: 30
  Next bootstrap message in 0DT00H02M04S
  Candidate RP: 192.168.38.111(loopback2), Group ACL: d235.1.3-4/24
  Next Cand_RP_advertisement in 0DT00H00M41S
Switch#
```

80.18 show ip pim interface

Данная команда используется для отображения информации об интерфейсе PIM.

show ip pim interface [dense-mode | sparse-mode | sparse-dense-mode] [*INTERFACE-ID***] [detail]**

Параметры

dense-mode	(Опционально.) Укажите, чтобы отобразить информацию только для режима PIM-DM.
sparse-mode	(Опционально.) Укажите, чтобы отобразить информацию только для режима PIM-SM.

sparse-dense-mode	(Опционально.) Укажите, чтобы отобразить информацию для режима PIM-SM-DM.
INTERFACE-ID	(Опционально.) Укажите интерфейс, о котором необходимо отобразить информацию. Допускаются только ID VLAN-интерфейсов.
detail	(Опционально.) Укажите, чтобы отобразить подробную информацию об интерфейсе.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации об интерфейсе. Если интерфейс не указан, будет показана информация PIM для всех допустимых интерфейсов.

Пример

В данном примере показано, как отобразить информацию об интерфейсе.

```
Switch#show ip pim interface

p: passive, Nbr Cnt: Neighbor Count
Address         Interface    Mode     Nbr DR         DR              Generation
                                      Cnt Priority                   ID
--------------- ------------ -------- --- ---------- --------------- ----------
10.90.90.90     vlan1        DM       0   1          0.0.0.0         0

Total Entries: 1

Switch#
```

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

```
Switch#show ip pim interface detail

vlan1
  Address             : 10.90.90.90
  PIM                 : Disabled
  Mode                : Dense
  Neighbor Count      : 0
  Generation ID       : 0
  Query Interval      : 30 seconds
  PIM Passive Mode    : Disabled


Total Entries: 1

Switch#
```

80.19 show ip pim neighbor

Данная команда используется для отображения информации о соседних устройствах PIM-SM.

show ip pim neighbor [*INTERFACE-ID***]**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейс, для которого необходимо отобразить информацию о соседних устройствах PIM-SM. Если ID интерфейса не указан, будет отображена информация для всех интерфейсов.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы определить, какие маршрутизаторы в локальной сети настроены для PIM.

Пример

В данном примере показано, как отобразить информацию о соседних устройствах PIM на всех интерфейсах.

```
Switch#show ip pim neighbor

Mode: DR - Designated Router, N - Default DR Priority,
      G - Generation ID
Neighbor        Interface  Uptime/Expires            Ver            DR Pri/Mode
--------------------------------------------------------------------------------
10.10.0.9       vlan1      0DT00H55M33S/0DT00H01M44S  v2             1 /G
10.10.0.136     vlan1      0DT00H55M20S/0DT00H01M25S  v2             1 /G
10.10.0.172     vlan1      0DT00H55M33S/0DT00H01M32S  v2             1 /DR,G
192.168.0.100   vlan2      0DT00H55M30S/0DT00H01M20S  v2             N /G

Total Entries: 4

Switch#
```

80.20 show ip pim rp mapping

Данная команда используется для отображения точек встреч (Rendezvous Point, RP) и привязок групп к RP.

show ip pim rp mapping

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 активные точки встречи (Rendezvous Point, RP), связанные с записями в таблице multicast-маршрутизации. Команда также применяется для отображения информации о привязках RP, существующих на маршрутизаторе.

Пример

В данном примере показано, как отобразить RP и привязки групп к RP.

```
Switch#show ip pim rp mapping

Group(s): 224.0.0.0/4
RP: 90.1.1.3
Info source: 90.1.1.3, via bootstrap, priority 0
Uptime: 0DT16H52M39S, expires: 0DT00H02M50S
Group(s): 225.0.0.0/8
RP: 1.1.1.10
Info source: static

Switch#
```

Отображаемые параметры

RP	Адрес RP для указанной группы.
Info source	Указывает, из какой системы маршрутизатором была получена данная информация об RP.
Via bootstrap	Информация о привязках RP была получена от BSR.
Priority	Приоритет RP.
Uptime	Продолжительность времени (в днях, часах, минутах и секундах), в течение которого маршрутизатор знает об этой RP.
Expires	Время (в днях, часах, минутах и секундах), по истечении которого информация об RP будет удалена, если маршрутизатором не получено сообщений об обновлении.

80.21 show ip pim rp-hash

Данная команда используется для отображения RP, которая должна быть выбрана для указанной группы.

show ip pim rp-hash *GROUP-ADDRESS*

Параметры

GROUP-ADDRESS	Укажите адрес группы, RP которой необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения RP, которая должна быть выбрана для указанной группы.

Пример

В данном примере показано, как отобразить RP для адреса группы 238.10.10.10.

```
Switch#show ip pim rp-hash 238.10.10.10

RP: 10.20.30.1
Info source: 10.20.30.1, via bootstrap
Uptime: 0DT01H42M15S, expires: 0DT00H02M16S

Switch#
```

В примере ниже показано, как отобразить RP с адресом группы 225.1.1.1.

```
Switch#show ip pim rp-hash 225.1.1.1

RP: 1.1.1.10
Info source: static

Switch#
```

81. Команды Protocol Independent Multicast (PIM) IPv6

81.1 ipv6 pim

Данная команда используется для включения IPv6 PIM на интерфейсе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ipv6 pim {sparse-mode | dense-mode}

no ipv6 pim [sparse-mode]

Параметры

sparse-mode	Укажите, чтобы включить режим PIM-SM для IPv6 PIM.
dense-mode	Укажите, чтобы включить режим PIM-DM для IPv6 PIM.

По умолчанию

По умолчанию режимы PIM-SM и PIM-DM отключены для IPv6 на всех интерфейсах.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Перед тем как запустить PIM на интерфейсе, необходимо включить маршрутизацию IPv6 multicast при помощи команды **ipv6 multicast-routing** в режиме Global Configuration Mode.

Пример

В данном примере показано, как включить PIM-SM для IPv6 на указанном интерфейсе.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 pim sparse-mode
Switch(config-if)#
```

81.2 ipv6 pim bsr border

Данная команда используется для настройки интерфейса в качестве пограничного PIM-домена. Чтобы отключить данную настройку, воспользуйтесь формой **no** этой команды.

ipv6 pim bsr border

no ipv6 pim bsr border

Параметры

Нет.

По умолчанию

По умолчанию интерфейс не настроен в качестве пограничного PIM-домена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду на интерфейсе, который граничит с другим доменом, чтобы избежать обмена сообщениями BSR между доменами.

Пример

В данном примере показано, как настроить VLAN-интерфейс 1 в качестве пограничного (border).

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 pim bsr border
Switch(config-if)#
```

81.3 ipv6 pim bsr candidate bsr

Данная команда используется для назначения роли Candidate BSR маршрутизатору. Чтобы отменить назначение роли Candidate BSR маршрутизатору, воспользуйтесь формой **no** этой команды.

ipv6 pim bsr candidate bsr *INTERFACE-ID* **[***HASH-MASK-LENGTH***] [priority** *PRIORITY-VALUE***]**
no ipv6 pim bsr candidate bsr

Параметры

INTERFACE-ID	Укажите интерфейс, IPv6-адрес которого анонсирован как адрес BootStrap Router (BSR).
HASH-MASK-LENGTH	(Опционально.) Укажите длину хэш-маски для выбора RP. Диапазон значений: от 0 до 128. Максимальное значение – 128 бит. Перед применением хэш-функции необходимо, чтобы маска была логической *AND* с адресом группы. Все группы, имеющие одинаковый seed hash, соответствуют одной общей RP. Поэтому одна RP может быть назначена для нескольких групп
priority *PRIORITY-VALUE*	(Опционально.) Укажите приоритет для Candidate BSR. Диапазон значений: от 0 до 255. BSR с более высоким приоритетом является предпочтительным. Если значения приоритета совпадают, в качестве BSR будет назначен маршрутизатор с наибольшим значением IPv6-адреса.

По умолчанию

По умолчанию маршрутизатор не назначен в качестве Candidate BSR.

Длина хэш-маски по умолчанию – 126.
Приоритет по умолчанию – 64.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется только в режиме PIM-SM и позволяет маршрутизатору отправлять сообщения bootstrap всем соседним устройствам PIM, используя адрес назначенного интерфейса в качестве адреса BSR. Домен PIM-SM должен содержать уникальный BSR, который отвечает за сбор и анонсирование информации о RP.

Пример

В данном примере показано, как настроить IPv6-адрес маршрутизатора, которому назначена роль Candidate BSR на VLAN-интерфейсе 1, с длиной хэш-маски 20 и приоритетом 192.

```
Switch#configure terminal
Switch(config)#ipv6 pim bsr candidate bsr vlan1 120 priority 192
Switch(config)#
```

81.4 ipv6 pim bsr candidate rp

Данная команда используется для настройки интерфейса в качестве Candidate RP и отправки сообщений PIM RP по направлению к BSR. Чтобы отключить отправку PIM RP на BSR, воспользуйтесь формой **no** этой команды.

ipv6 pim bsr candidate rp *INTERFACE-ID* **[group-list** *ACCESS-LIST***] [priority** *PRIORITY-VALUE***] [interval** *SECONDS***]**

no ipv6 pim bsr candidate rp *INTERFACE-ID*

Параметры

INTERFACE-ID	Укажите интерфейс, IPv6-адрес которого будет назначен в качестве Candidate RP (C-RP).
group-list *ACCESS-LIST*	(Опционально.) Укажите имя списка доступа IPv6, в котором заданы префиксы группы, ассоциированные с адресом RP. Если параметр не указан, коммутатор выступает в роли Candidate RP для всех групп.
priority *PRIORITY-VALUE*	(Опционально.) Укажите приоритет RP. Диапазон значений: от 0 до 255.
interval *SECONDS*	(Опционально.) Укажите интервал между сообщениями объявления Candidate RP. Диапазон значений: от 1 до 16383 секунд.

По умолчанию

По умолчанию маршрутизатор не назначен в качестве Candidate RP.
Приоритет по умолчанию – 192.
Интервал по умолчанию – 60 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется только в режиме PIM-SM и позволяет отправлять сообщения PIMv2 по направлению к BSR для обнаружения себя в роли Candidate RP.

Для каждого интерфейса можно указать только один список группы доступа. Ранее настроенная конфигурация перезаписывается новой. Использовать команду можно несколько раз для каждого интерфейса.

Пример

В данном примере показано, как назначить роль Candidate RP маршрутизатору на VLAN-интерфейсе 1. Настроенный приоритет – 10.

```
Switch#configure terminal
Switch(config)#ipv6 pim bsr candidate rp vlan1 priority 10
Switch(config)#
```

81.5 ipv6 pim dr-priority

Данная команда используется для изменения значения приоритета назначенного маршрутизатора (Designated Router, DR) при помощи опции DR Priority в сообщениях PIM hello. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ipv6 pim dr-priority *PRIORITY*
no ipv6 pim dr-priority

Параметры

PRIORITY	Укажите значение приоритета DR. Диапазон значений: от 0 до 4294967295. Чем больше значение, тем выше приоритет.

По умолчанию

Значение по умолчанию – 1.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно в режиме PIM-SM. При назначении маршрутизатора в качестве DR применяются следующие правила:

- В качестве DR назначается маршрутизатор с наиболее высоким значением приоритета, настроенным на интерфейсе. Если несколько маршрутизаторов имеют наивысший приоритет, в качестве DR назначается маршрутизатор с наибольшим значением IPv6-адреса, заданного на интерфейсе.
- Маршрутизатор, у которого отсутствует значение приоритета в hello-сообщениях, обычно имеет наивысший приоритет и становится DR. Если у нескольких маршрутизаторов отсутствует приоритет в hello-сообщениях, в качестве DR назначается маршрутизатор с наибольшим значением IPv6-адреса.

Пример

В данном примере показано, как настроить приоритет DR на VLAN-интерфейсе 1. Настроенное значение – 200.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 pim dr-priority 200
Switch(config-if)#
```

81.6 ipv6 pim hello-interval

Данная команда используется для настройки частоты сообщений PIM hello. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ipv6 pim hello-interval *SECONDS*
no ipv6 pim hello-interval

Параметры

SECONDS	Укажите интервал между hello-сообщениями в диапазоне от 1 до 18000 секунд.

По умолчанию

Значение по умолчанию – 30 секунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

PIM-маршрутизатор изучает соседние устройства PIM с помощью сообщений hello, отправленных маршрутизаторами, которые настроены для многоадресной IP-рассылки. В режиме SM Mode hello-сообщения также используются для определения назначенного маршрутизатора в каждом сегменте локальной сети.

Пример

В данном примере показано, как установить интервал PIM hello. Настроенное значение – 45 секунд.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 pim hello-interval 45
Switch(config-if)#
```

81.7 ipv6 pim sr-interval

Данная команда используется для настройки интервала сообщений state refresh. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ipv6 pim sr-interval *SECONDS*
no ipv6 pim sr-interval

Параметры

SECONDS	Укажите интервал между сообщениями state refresh в диапазоне от 4 до 100 секунд.

По умолчанию

Значение по умолчанию – 60 секунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для настройки интервала сообщений state refresh.

Пример

В данном примере показано, как установить интервал для сообщений state refresh. Настроенный интервал – 45 секунд.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 pim sr-interval 45
Switch(config-if)#
```

81.8 ipv6 pim join-prune-interval

Данная команда используется для настройки периодических PIM-сообщений join/prune. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ipv6 pim join-prune-interval *SECONDS*
no ipv6 pim join-prune-interval

Параметры

SECONDS	Укажите интервал между сообщениями join/prune в диапазоне от 1 до 18000 секунд.

По умолчанию

Значение по умолчанию – 60 секунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно в режиме PIM-SM.

При настройке значения интервала между сообщениями join/prune необходимо учитывать следующие факторы: настроенную полосу пропускания и ожидаемое среднее количество записей многоадресной маршрутизации во время подключения к сети или соединения. Например, для каналов связи с более низкими скоростями или для маршрутизаторов, которые обычно имеют больше количества записей из-за нахождения в центре сети, настраивается более длинный интервал.

В режиме SM-Mode маршрутизаторы отправляют периодические сообщения join на основе настроенного интервала. Время ожидания (Hold Time) в сообщениях join/prune превышает интервал join/prune в 3,5 раза. Таймер получающего маршрутизатора запускается на основе настроенного времени ожидания. Интерфейс, на котором не было получено ни одного сообщения join, отключается.

Пример

В данном примере показано, как установить таймер PIM join/prune на VLAN-интерфейсе 1.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 pim join-prune-interval 120
Switch(config-if)#
```

81.9 ipv6 pim passive

Данная команда используется для включения пассивного режима на интерфейсе. Чтобы отключить пассивный режим, воспользуйтесь формой **no** этой команды.

ipv6 pim passive

no ipv6 pim passive

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 доступна только на интерфейсе с включенным IPv6 PIM. При включении пассивного режима интерфейс не будет отправлять и принимать PIM-сообщения, а маршрутизатор не будет распознавать другие соседние устройства. Данная команда применяется, когда в локальной сети находится только один PIM-маршрутизатор.

Пример

В данном примере показано, как включить пассивный режим на интерфейсе VLAN 100.

```
Switch#configure terminal
Switch(config)#interface vlan100
Switch(config-if)#ipv6 pim passive
Switch(config-if)#
```

81.10 ipv6 pim register-checksum-wholepkt

Данная команда используется на коммутаторе, чтобы подсчитать контрольную сумму регистрационного (register) сообщения для всего PIM-сообщения, включая часть данных. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ipv6 pim register-checksum-wholepkt
no ipv6 pim register-checksum-wholepkt

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.
По умолчанию опция Register Checksum совместима с PIM RFC, за исключением части данных в регистрационном (register) сообщении.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда доступна только в режиме PIM-SM. При использовании команды настройки применяются ко всем адресам RP.

Пример

В данном примере показано, как подсчитать контрольную сумму для всего регистрационного (register) сообщения.

```
Switch#configure terminal
Switch(config)#ipv6 pim register-checksum-wholepkt
Switch(config)#
```

81.11 ipv6 pim register-probe

Данная команда используется для настройки времени register probe. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ipv6 pim register-probe *SECONDS*
no ipv6 pim register-probe

Параметры

SECONDS	Укажите значение времени register probe в диапазоне от 1 до 127 секунд.

По умолчанию

Значение по умолчанию – 5 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Register probe – это время до истечения таймера Register Stop Timer (RST), в течение которого DR может отправлять Null-Register по направлению к RP для повторной отправки сообщения register-stop.

Пример

В данном примере показано, как установить время register probe. Настроенное значение – 10 секунд.

```
Switch#configure terminal
Switch(config)#ipv6 pim register-probe 10
Switch(config)#
```

81.12 ipv6 pim register-suppression

Данная команда используется для настройки времени register suppression. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ipv6 pim register-suppression *SECONDS*
no ipv6 pim register-suppression

Параметры

SECONDS	Укажите значение времени register suppression в диапазоне от 3 до 65535 секунд.

По умолчанию

Значение по умолчанию – 60 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда доступна только в режиме PIM-SM.

Когда DR получает сообщение register stop, запускается таймер suppression. В течение настроенного времени подавления (suppression) DR перестает отправлять регистрационно-инкапсулированные (register-encapsulated) данные по направлению к RP. Таймер должен быть настроен на DR. Для корректной настройки таймера register stop значение времени register probe должно быть меньше половины значения времени register suppression. Минимальное значение времени register suppression составляет 3 секунды.

Пример

В данном примере показано, как настроить время register suppression. Установленное значение – 30 секунд.

```
Switch#configure terminal
Switch(config)#ipv6 pim register-suppression 30
Switch(config)#
```

81.13 ipv6 pim rp embedded

Данная команда используется для включения поддержки Embedded RP в PIMv6. Чтобы отключить поддержку Embedded RP, воспользуйтесь формой **no** этой команды.

ipv6 pim rp embedded
no ipv6 pim rp embedded

Параметры
Нет.

По умолчанию
По умолчанию данная функция включена.

Режим ввода команды
Global Configuration Mode.

Уровень команды по умолчанию
Уровень 12.

Использование команды
Данная команда доступна только на интерфейсе в режиме PIM-SM.

При включении поддержки Embedded RP определяется политика распределения адресов, в которой адрес RP зашифрован в IPv6-адресе многоадресной группы. Это способствует легкому развертыванию масштабируемой междоменной многоадресной рассылки, а также упрощению ее конфигурации. IPv6-адреса многоадресной группы, встроенные (embedded) в информацию о RP, начинаются с ff70::/12, где значения флага, равное 7, означает Embedded RP.

Поддержка Embedded-RP по умолчанию включена. Чтобы отключить поддержку Embedded-RP, воспользуйтесь формой **no** этой команды. Данная команда применяется только к диапазонам ff7x::/12 группы Embedded RP.

Пример
В данном примере показано, как отключить поддержку Embedded RP в PIMv6 PIM-SM.

```
Switch#configure terminal
Switch(config)#no ipv6 pim rp embedded
Switch(config)#
```

81.14 ipv6 pim rp-address

Данная команда используется для настройки адреса PIM RP для диапазона определенной группы. Чтобы удалить адрес RP, воспользуйтесь формой **no** этой команды.

ipv6 pim rp-address *IPV6-ADDRESS* **[***GROUP-ACCESS-LIST***] [override]**
no ipv6 pim rp-address *IPV6-ADDRESS*

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес маршрутизатора, который необходимо настроить как PIM RP.
GROUP-ACCESS-LIST	(Опционально.) Укажите имя списка доступа, в котором будут определены многоадресные группы, используемые для RP. Если список доступа не настроен, RP используется для всех групп.

override	(Опционально.) Укажите, чтобы динамически изученный RP был перезаписан статическим RP.

По умолчанию

По умолчанию RP-адреса не настроены.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду только в режиме PIM-SM, чтобы статически настроить адрес RP для многоадресных групп.

Один RP может использоваться для нескольких групп. Группы, для которых будет использоваться RP, определяются настроенным списком доступа. Возможна настройка нескольких RP, для каждого из которых настраивается один список доступа. Предыдущие настройки перезаписываются новыми.

Привязка многоадресных групп к RP должна быть согласована для всех маршрутизаторов в одном домене. Маршрутизатор первого перехода (First Hop Router), который инициирует регистрационное (register) сообщение, будет использовать записи привязки для определения RP при отправке сообщений PIM register для определенной группы. Маршрутизатор последнего перехода (Last Hop Router), который инициирует сообщение join, будет использовать записи привязки (mapping), чтобы определить RP при отправке сообщений join/prune для указанной группы. Полученное сообщение join будет перенаправлено маршрутизатором после проверки записей привязки. Когда RP получает сообщение register, а маршрутизатор не является соответствующим RP для многоадресной группы, отправляется сообщение register stop.

Если в PIM-домене используется Embedded-RP, только RP нуждается в статической конфигурации как RP для диапазонов Embedded-RP. Другие маршрутизаторы будут узнавать адрес RP из адреса группы IPv6. Если вместо Embedded-RP необходимо выбрать статический RP, в списке доступа статистического RP должен быть настроен определенный диапазон групп Embedded-RP.

Пример

В данном примере показано, как настроить адрес RP для списка доступа группы «G1». Настроенный адрес – 3ffe:6000:3000::123.

```
Switch#configure terminal
Switch(config)#ipv6 access-list G1
Switch(config-ipv6-acl)#permit any ff75::/16
Switch(config-ipv6-acl)#exit
Switch(config)#ipv6 pim rp-address 3ffe:6000:3000::123 G1
Switch(config)#
```

81.15 ipv6 pim spt-threshold

Данная команда используется для настройки порогового значения PIM Shortest Path Tree (SPT) для определенных групп. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой

команды.

ipv6 pim spt-threshold {0 | infinity}

no ipv6 pim spt-threshold

Параметры

0	Укажите, чтобы дерево источника (source tree) было создано сразу же после получения первого пакета.
infinity	Укажите, чтобы всегда использовать общее дерево (shared tree).

По умолчанию

По умолчанию используется параметр **infinity**.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте параметр **infinity**, чтобы все источники указанных групп использовали общее дерево (shared tree). Используйте параметр **0**, чтобы присоединиться к SPT сразу же после получения первого пакета от нового источника.

Пример

В данном примере показано, как настроить PIM LHR (Last Hop Router) для использования общего дерева (shared tree).

```
Switch#configure terminal
Switch(config)#ipv6 pim spt-threshold infinity
Switch(config)#
```

81.16 ipv6 pim ssm

Данная команда используется для настройки диапазона адресов многоадресной SSM-группы. Чтобы отключить PIM-SSM, воспользуйтесь формой **no** этой команды.

ipv6 pim ssm {default | range *ACCESS-LIST***}**

no ipv6 pim ssm

Параметры

default	Укажите, чтобы использовать диапазон адресов SSM-группы по умолчанию, равный FF3x::/32.

ACCESS-LIST	Укажите стандартный список доступа IP, в котором будут определены заданные пользователем адреса SSM-группы.

По умолчанию

По умолчанию PIM-SSM отключен.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда доступна только в режиме PIM-SM.

PIM-SSM строит деревья, основываясь только на одном источнике. При включении SSM трафик датаграмм отправляется только из тех источников многоадресной рассылки, к которым получатели были явно присоединены. В результате полоса пропускания оптимизируется, а нежелательный широковещательный трафик блокируется. Более того, вместо RP и общих деревьев (shared tree) используется информация, найденная в адресах источника многоадресной группы. Получатели сразу же предоставляют данную информацию устройствам последнего перехода по адресам источника с помощью ответов о принадлежности MLD по кратчайшему пути (Shortest Path Tree).

При включении SSM датаграммы отправляются на основе каналов (S, G). Трафик для одного канала (S, G) состоит из датаграмм с индивидуальным IPv6-адресом источника (S) и адресом многоадресной группы (G) в качестве IPv6-адреса назначения (destination). Данный трафик отправляется только в системы, ставшие участниками канала (S, G). Передача сигналов не требуется, однако для получения трафика из определенных источников необходимо подписаться на каналы (S, G) или отписаться от них, чтобы не получать трафик. Для включения SSM требуется MLD v2.

Чтобы в полной мере воспользоваться преимуществами SSM, все маршрутизаторы в одном домене должны иметь согласованную конфигурацию диапазона адресов SSM-группы.

Пример

В данном примере показано, как настроить обслуживание SSM для диапазона IPv6-адресов, определенного в списке доступа «ssm-group». Диапазон IPv6-адресов – ff30::/96.

```
Switch#configure terminal
Switch(config)#ipv6 access-list ssm-group
Switch(config-ipv6-acl)#permit any ff30::/96
Switch(config-ipv6-acl)#exit
Switch(config)#ipv6 pim ssm range ssm-group
Switch(config)#
```

81.17 ipv6 pim sg-keepalive-time

Данная команда используется, чтобы настроить время keep alive для записи маршрутизации PIM6-SM multicast. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 pim sg-keepalive-time *SECONDS*

no ipv6 pim sg-keepalive-time

Параметры

SECONDS	Укажите период времени, в течение которого PIM-маршрутизатор будет поддерживать состояние (S, G) при отсутствии явных (S, G) локальных membership/join-сообщений. Диапазон значений: от 120 до 65535 секунд.

По умолчанию

Значение по умолчанию – 210 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду только для IPv6 PIM-SM, чтобы настроить период времени keep alive, в течение которого PIM-маршрутизатор будет поддерживать состояние (S, G) при отсутствии явных (S, G) локальных membership/join-сообщений.

Пример

В данном примере показано, как установить время (S, G) keep alive. Настроенное значение – 300 секунд.

```
Switch#configure terminal
Switch(config)#ipv6 pim sg-keepalive-time 300
Switch(config)#
```

81.18 show ipv6 pim

Данная команда используется для отображения общей информации о PIM-SM.

show ipv6 pim sparse-mode

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 общую информацию о PIM-SM.

Пример

В данном примере показано, как отобразить общую информацию о PIM-SM.

```
Switch#show ipv6 pim sparse-mode

Register checksum wholepkt  : Enabled
Register probe time         : 10 seconds
Register suppression time   : 60 seconds
SPT Threshold               : Infinity
(S,G) keepalive time        : 300 seconds
Embedded RP support         : Enabled
RP Address
  3FFE:6000:3000::123, group-list: G1

RP Candidate
  vlan100, group-list: rp-cand, interval: 60, priority: 192

BSR Candidate
  vlan100, hash-mask-length: 30, priority: 1

SSM Group : Movies

Switch#
```

81.19 show ipv6 pim bsr

Данная команда используется для отображения информации о BSR.

show ipv6 pim bsr {candidate-rp | election | rp-cache}

Параметры

candidate-rp	Укажите, чтобы отобразить состояние C-RP на маршрутизаторах, настроенных в качестве C-RP.
election	Укажите, чтобы отобразить состояние и назначение BSR, а также таймеры BootStrap Message (BSM).
rp-cache	Укажите, чтобы отобразить кэш точки встречи (Candidate Rendezvous Point, C-RP), информация о котором была получена из одноадресных (unicast) объявлений, полученных на назначенном BSR.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить подробную информацию о состоянии и назначении BSR, а также о кэше C-RP. Информация отображается только на маршрутизаторе, настроенном как C-RP.

Пример

В данном примере показано, как отобразить информацию о назначении BSR.

```
Switch#show ipv6 pim bsr election

PIMv2 BSR Information
BSR Election Information
This system is the Bootstrap Router (BSR)
BSR Address: 3FFE:6000:3000::123
Uptime: 0DT00H18M50S, BSR Priority: 0, Hash mask length: 126
BS Timer: 0DT00H00M21S

Switch#
```

В примере ниже показано, как отобразить информацию, полученную на BSR от разных C-RP. В данном примере два C-RP отправили сообщения объявления (advertisement) для FF00::/8 или для диапазона многоадресной рассылки IPv6 по умолчанию.

```
Switch#show ipv6 pim bsr rp-cache

PIMv2 BSR C-RP Cache
BSR Candidate RP Cache
Group(s) FF00::/8
  RP 3FFE:1000:10:5::153
    Priority 192
    Uptime: 0DT00H08M36S, expires: 0DT00H01M21S
  RP 3FFE:2000:10:5::100
    Priority 192
    Uptime: 0DT00H08M36S, expires: 0DT00H01M21S

Switch#
```

В следующем примере показано, как отобразить информацию о C-RP, настроенном на маршрутизаторе.

```
Switch#show ipv6 pim bsr candidate-rp

PIMv2 C-RP Information
Candidate RP: 3FFE:1000:10:5::100 (vlan10)
  Priority 192, Holdtime 150
  Advertisement interval 60 seconds
  Next advertisement in 0DT00H00M54S

Switch#
```

Отображаемые параметры

This system is the Bootstrap Router (BSR)	Указывает, что данный маршрутизатор настроен в качестве BSR, и отображает информацию о параметрах, связанных с ним.
BS Timer	Таймер BS назначенного BSR показывает время, в течение которого появится следующее BSM. На всех других маршрутизаторах в этом домене таймер BS показывает, когда истечет время срока назначения BSR.

81.20 show ipv6 pim group-map

Данная команда используется для отображения информации о привязках RP группы.

show ipv6 pim group-map [IPV6-GROUP-ADDR/PREFIX-LENGTH] [info-source {bsr | embedded-rp | static}]

Параметры

IPV6-GROUP-ADDR/PREFIX-LENGTH	(Опционально.) Укажите диапазон IPv6-адресов многоадресной группы.
info-source	(Опционально.) Укажите, чтобы отобразить все привязки, информация о которых была получена из определенного источника, например, BSR или статической конфигурации.
bsr	Укажите, чтобы отобразить диапазоны групп, информация о которых была получена от BSR.
embedded-rp	Укажите, чтобы отобразить диапазоны группы, информация о которых была получена от Embedded RP.
static	Укажите, чтобы отобразить диапазоны групп, которые были статически сконфигурированы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если параметры не указаны, будут отображены все привязки группы. Для фильтрации привязок группы укажите диапазон адресов группы или изученный источник.

Пример

В данном примере показано, как отобразить привязки RP для группы FF04::10.

```
Switch#show ipv6 pim group-map ff04::10/128

FF04::10/128
  RP: 3FFE:10:10:5::153
  Info source: 3FFE:10:10:5::153, via bootstrap

Switch#
```

В примере ниже показано, как отобразить привязки RP, информация о которых была получена из определенного источника, настроенного в статической конфигурации.

```
Switch#show ipv6 pim group-map info-source static

FF00::/8
    RP: 2013:1:1:11::1
   Info source:  static

Switch#
```

В следующем примере показано, как отобразить привязки RP, информация о которых была получена от Embedded RP.

```
Switch#show ipv6 pim group-map info-source embedded-rp

FF7E:640:2002:6666::/96
    RP: 2002:6666::6
    Info source: embedded

Switch#
```

81.21 show ipv6 pim interface

Данная команда используется для отображения конфигурации для PIM на интерфейсе/интерфейсах.

show ipv6 pim interface [sparse-mode | dense-mode] [*INTERFACE-ID*] [detail]

Параметры

sparse-mode	(Опционально.) Укажите, чтобы отобразить информацию об интерфейсе с включенным PIM-SM.

dense-mode	(Опционально.) Укажите, чтобы отобразить информацию об интерфейсе с включенным PIM-DM.
INTERFACE-ID	(Опционально.) Укажите интерфейс для отображения.
detail	(Опционально.) Укажите, чтобы отобразить подробную информацию об интерфейсе.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы проверить, включен ли PIM на интерфейсе, а также чтобы узнать количество соседних устройств и назначенный маршрутизатор (Designated Router, DR). Если интерфейс не указан, будет отображена информация для всех интерфейсов с включенным IPv6 PIM.

Пример

В данном примере показано, как отобразить информацию об интерфейсе, на котором включен режим PIM Sparse Mode.

```
Switch#show ipv6 pim interface sparse-mode

Nbr Count: Neighbor Count

PIM6 Interface Table

Interface     Mode    Nbr     DR          Hello     J/P       BSR
                      Count   Priority    Interval  Interval  Border
------------  ------  -----   ----------  --------  --------  --------
vlan1         Sparse  0       2           30        60        disabled
    Address       : FE80::211:11FF:FE11:1111
    Global Address: 2000:1::3630
    DR            : this system
vlan2         Sparse  1       1           30        60        disabled
    Address       : FE80::211:11FF:FE11:1114
    Global Address: 2000:2::3630
    DR            : FE80::202:2FF:FE03:401

Total Entries : 2

Switch#
```

В примере ниже показано, как отобразить подробную информацию о PIM на VLAN-интерфейсе 1.

```
Switch#show ipv6 pim interface sparse-mode vlan1 detail

Interface                          : vlan1
Interface Link-Local Address       : FE80::207:E9FF:FE02:81D
Interface Global Address           : 3FFE:192:168:1::53
Mode                               : Sparse
Designated Router                  : FE80::20E:CFF:FE01:FACC
Designated Router Priority         : 1
Designated Router Priority Enabled : True
Generation ID                      : 0
Hello Interval                     : 30 seconds
Triggered Hello Interval           : 5 seconds
Hello Holdtime                     : 105 seconds
Join Prune Interval                : 60 seconds
Join Prune Holdtime                : 210 seconds
LAN Delay Enabled                  : True
Propagation Delay                  : 1 seconds
Override Interval                  : 3 seconds
Effective Propagation Delay        : 1 seconds
Effective Override Interval        : 3 seconds
Join Suppression Enabled           : False
Bidirectional Capable              : False
BSR Domain Border                  : Disabled
PIM Passive Mode                   : Disabled

Total Entries : 1

Switch#
```

Отображаемые параметры

Interface	ID интерфейса, на котором включен PIM.
Mode	Режим PIM на интерфейсе.
Nbr Count	Количество соседних устройств PIM, изученных на интерфейсе.
DR Priority	Приоритет DR, настроенный на интерфейсе.
Hello Interval	Значение интервала hello, настроенного на интерфейсе.
J/P Interval	Значение интервала join/prune, настроенного на интерфейсе.
BSR Border	Указывает, включено или отключено состояние BSR Border.
Address	IPv6-адрес Link-Local на интерфейсе.
Global Address	Глобальный IPv6-адрес на интерфейсе.
DR	Pv6-адрес назначенного порта на интерфейсе.
Designated Router Priority Enabled	Указывает, все ли маршрутизаторы на интерфейсе используют опцию DR Priority.

LAN Delay Enabled	Указывает, все ли маршрутизаторы на интерфейсе используют опцию LAN Prune Delay.
Propagation Delay	Значение Propagation Delay на интерфейсе.
Override Interval	Значение Override Interval на интерфейсе.
Effective Propagation Delay	Effective Propagation Delay на интерфейсе.
Effective Override Interval	Effective Override Interval на интерфейсе.
Join Suppression Enabled	Указывает, включено ли Join Suppression на интерфейсе.

81.22 show ipv6 pim mroute

Данная команда используется для отображения таблицы маршрутизации IPv6 PIM-SM multicast.

show ipv6 pim mroute sparse-mode

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 все записи таблицы маршрутизации IPv6 PIM-SM multicast. В таблице представлены записи источника, группы (S,G) и (*,G), где знак (*) обозначает все адреса источника, «S» – один адрес источника, а «G» – адрес назначения многоадресной группы. При создании записей (S, G) в таблице unicast-маршрутизации к указанной группе назначения используется кратчайший путь Reverse Path Forwarding (RPF).

Пример

В данном примере показано, как отобразить таблицу маршрутизации IPv6 PIM-SM multicast.

```
Switch#show ipv6 pim mroute sparse-mode

PIM-SM Multicast Routing Table:
JP State- Join Prune State, ET - Expiry Timer, PPT - Prune Pending Timer,
KAT - Keep Alive Timer

Flags: S - Sparse, T - SPT-bit set, s - SSM Group.

(*, FF13::10) Uptime: 0DT00H04M43S, Flags:S
  RP: 3FFE:6000:1005::36, RPF nbr: FE80::217:55FF:FEC0:16, RPF interface: vlan101
  Upstream interface:
   Join State: Joined, Join Timer: 17 secs
  Downstream Interface List:
   vlan11:
     JP State: Join, ET: 166 secs, PPT: off
     Assert State: No Info, Assert Timer: off
      Assert Winner: ::, Metric: 0, Pref: 0

(3FFE:6000:1005::DD, FF13::10) Uptime: 0DT00H00M05S, Flag:ST
  RPF nbr: FE80::217:55FF:FEC0:16, RPF Interface: vlan101
  Upstream Interface:
   Join State: Joined, Join Timer: 55 secs, KAT: off
  Downstream Interface List:
   vlan11:
     JP State: Join, ET: 205 secs, PPT: off
     Assert State: No Info, Assert Timer: off
      Assert Winner: ::, Metric: 0, Pref: 0

(3FFE:6000:1005::DD, FF13::10, rpt) Uptime: 0DT00H00M05S, Flags:S
  RP: 3FFE:6000:1005::36, RPF nbr: FE80::217:55FF:FEC0:16, RPF Interface: vlan101
  Upstream Interface:
   Prune State: Not Pruned, Override Timer: off
  Downstream Interface List:
   vlan11:
     Prune State: No Info, ET: off, PPT: off

Total Entries: 3

Switch#
```

Отображаемые параметры

Uptime	Время существования записи.
Flags	Информация о записях Sparse/SPT-bit.
RP	Rendezvous Point (RP) из (*, G) mroute-записи.
RPF nbr	Адрес соседнего устройства Reserve Path Forwarding (RPF).
RPF interface	Имя локального интерфейса, подключенного к восходящему маршрутизатору.

Join State	Указывает, к чему необходимо подключиться локальному маршрутизатору: к дереву RP для группы или к Shortest Path Tree для источника и группы, представленных записью.
Join Timer	Время, через которое локальный маршрутизатор отправит следующее сообщение join.
Downstream Interface List	Информация о состоянии протокола нисходящих интерфейсов.
vlan11	Имя нисходящего интерфейса.
JP State	Состояние интерфейса после получения сообщений (*, G) или (S, G) join/prune.
PPT	Prune Pending Timer – время, в течение которого другой маршрутизатор может отменить отправку join/prune.
ET	Expiry Timer – время до истечения состояния join на интерфейсе.
Assert State	Состояние Assert State на интерфейсе.
Assert Timer	Assert Timer – время перед отправкой сообщения assert интерфейсом Assert Winner; для интерфейса Assert Loser – время перед истечением состояния Assert State.
Assert Winner	Если состояние Assert State является Loser, данное поле указывает IP-адрес Assert Winner. В противном случае поле всегда будет «::».
Metric	Если состояние Assert State является Loser, данное поле указывает метрику маршрута к RP/источнику (source), установленном Assert Winner.
Pref	Если состояние Assert State является Loser, данное поле указывает приоритетность метрики маршрута к RP/источнику (source), установленном Assert Winner.

81.23 show ipv6 pim neighbor

Данная команда используется для отображения информации о соседних устройствах PIM.

show ipv6 pim neighbor [sparse-mode | dense-mode] [detail] [*INTERFACE-ID***]**

Параметры

sparse-mode	(Опционально.) Укажите, чтобы отобразить информацию о соседних устройствах PIM-SM.
dense-mode	(Опционально.) Укажите, чтобы отобразить информацию о соседних устройствах PIM-DM.
detail	(Опционально.) Укажите, чтобы отобразить подробную информацию о соседних устройствах PIM-SM.

INTERFACE-ID	(Опционально.) Укажите интерфейс, информацию о соседних устройствах которого необходимо отобразить. Если ID интерфейса не указан, будет отображена информация обо всех интерфейсах.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы узнать, какие маршрутизаторы в локальной сети настроены для PIMv6.

Пример

В данном примере показано, как отобразить информацию о соседних устройствах PIM.

```
Switch#show ipv6 pim neighbor

Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      G - Supports Generation ID, R - State Refresh Capable
Neighbor-Address Interface Uptime/Expires              Ver   DR Pri/Mode
---------------------------------------------------------------------------
FE80::233:38FF:FE10:1700
                 vlan2     0DT01H14M18S  /0DT00H01M16S   v2    N /RG
FE80::200:FF:FE26:6667
                 vlan4     4DT18H22M00S  /0DT00H01M43S   v2    1 /DR,G

Total Entries: 2

Switch#
```

Отображаемые параметры

Neighbor-Address	IPv6-адрес соседнего устройства PIM (адрес Link-Local).
Interface	Имя интерфейса соседнего устройства.
Uptime	Период времени, в течение которого маршрутизатор узнает соседнее устройство.
Expires	Время, по истечении которого информация о соседнем устройстве удаляется. Если за это время маршрутизатор не получает ни одного hello-сообщения, информация о соседнем устройстве будет удалена.

Ver	Версия PIM, используемая соседним устройством.
DR Pri/Mode	Приоритет и режим назначенного маршрутизатора. **DR Priority:** используйте **N**, чтобы указать, что соседнее устройство не поддерживает опцию DR Priority в hello-сообщениях. В противном случае значение приоритета DR будет отображено. Значение кодов для указания режима: **DR –** соседним устройством является назначенный маршрутизатор (Designated Router). **B –** соседнее устройство поддерживает PIM в двунаправленном режиме. **G –** соседнее устройство поддерживает Generation ID, которое позволяет сократить время повторной сходимости после перезагрузки. **R** – соседнее устройство готово перейти в состояние refresh.

82. Команды Protocol Independent Multicast (PIM) Snooping

82.1 ip pim snooping

Данная команда используется для включения функции PIM Snooping. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ip pim snooping
no ip pim snooping

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена глобально и на всех VLAN-интерфейсах.

Режим ввода команды

Global Configuration Mode.

VLAN Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для работы VLAN с PIM Snooping функция должна быть включена как глобально, так и на интерфейсе.

Пример

В данном примере показано, как включить PIM Snooping глобально.

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

В примере ниже показано, как включить PIM Snooping на VLAN 1.

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

82.2 clear ip pim snooping statistics

Данная команда используется для удаления статистики, относящейся к PIM Snooping.

clear ip pim snooping statistics {all | vlan *VLAN-ID***}**

Параметры

all	Укажите, чтобы удалить всю статистику PIM Snooping для всех VLAN.
vlan *VLAN-ID*	Укажите, чтобы удалить всю статистику PIM Snooping для определенной VLAN.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применяется для удаления статистики, относящейся к PIM snooping.

Пример

В данном примере показано, как удалить статистику PIM Snooping.

```
Switch#clear ip pim snooping statistics all
Switch#
```

82.3 show ip pim snooping

Данная команда используется для отображения информации о PIM Snooping на коммутаторе.

show ip pim snooping [vlan *VLAN-ID***]**

Параметры

vlan *VLAN-ID*	(Опционально.) Укажите VLAN, для которой необходимо отобразить информацию о PIM Snooping.

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 PIM Snooping на коммутаторе.

Пример

В данном примере показано, как отобразить общую информацию о PIM Snooping на коммутаторе.

```
Switch#show ip pim snooping

PIM snooping global state       : Enabled
Number of user enabled VLANs    : 2
User enabled VLANs: 1, 2

Switch#
```

В данном примере показано, как отобразить информацию о PIM Snooping для определенной VLAN.

```
Switch#show ip pim snooping vlan 1

2 neighbors, 10 mroutes, DR is 36.90.90.100
Learned neighbor on ports:
  1/0/23, Local

Switch#
```

82.4 show ip pim snooping neighbor

Данная команда используется для отображения информации о соседних устройствах PIM Snooping на коммутаторе.

show ip pim snooping neighbor [vlan *VLAN-ID***]**

Параметры

vlan *VLAN-ID*	(Опционально.) Укажите VLAN, для которой необходимо отобразить информацию.

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 соседних устройствах PIM Snooping на коммутаторе.

Пример

В данном примере показано, как отобразить информацию о соседних устройствах PIM Snooping на коммутаторе.

```
Switch#show ip pim snooping neighbor

Mode: DR - Designated Router, L - LAN Prune Delay , T - Tracking

VLAN  Neighbor        Port         Uptime/Expires               Option Flags
1     36.90.90.90     1/0/23        0DT00H09M30S/0DT00H01M45S
1     36.90.90.100    Local         0DT00H09M28S/0DT00H01M18S      DR

Total Entries: 2

Switch#
```

82.5 show ip pim snooping mroute

Данная команда используется для отображения информации о многоадресной маршрутизации PIM Snooping на коммутаторе.

show ip pim snooping mroute [vlan *VLAN-ID* **| group** *GROUP-ADDRESS***]**

Параметры

vlan *VLAN-ID*	(Опционально.) Укажите VLAN, для которой необходимо отобразить информацию.
group *GROUP-ADDRESS*	(Опционально.) Укажите групповой адрес, таблицу маршрутизации mroute которого необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о многоадресной маршрутизации PIM Snooping на коммутаторе.

Пример

В данном примере показано, как отобразить информацию о многоадресной маршрутизации PIM Snooping на коммутаторе.

```
Switch#show ip pim snooping mroute

Timers: PPT - Prune Pending Timer, ET - Expiry Timer

VLAN 1, (*, 226.1.1.1)
  Uptime/Expire: 0DT00H07M21S/0DT00H03M08S
  Downstream ports: 1/0/23
  Outgoing ports: 1/0/23, Local
    Port 1/0/23, JPState:Join, Exp:0DT00H03M08S
        Upstream neighbor: 36.90.90.100 learned on port Local
            PPT/ET: -/0DT00H03M08S

VLAN 1, (*, 226.1.1.2)
  Uptime/Expire: 0DT00H07M21S/0DT00H03M08S
  Downstream ports: 1/0/23
  Outgoing ports: 1/0/23, Local
    Port 1/0/23, JPState:Join, Exp:0DT00H03M08S
        Upstream neighbor: 36.90.90.100 learned on port Local
            PPT/ET: -/0DT00H03M08S

VLAN 1, (1.3.3.5, 226.1.1.2, rpt)
  Uptime/Expire: 0DT00H07M18S/0DT00H03M08S
  Downstream ports: 1/0/23
  Outgoing ports: 1/0/23, Local
    Port 1/0/23, JPState:Pruned, Exp:0DT00H03M08S
        Upstream neighbor: 36.90.90.100 learned on port Local
            PPT/ET: -/0DT00H03M08S

Total Entries: 3

Switch#
```

82.6 show ip pim snooping statistics

Данная команда используется для отображения статистики PIM Snooping на коммутаторе.

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

Параметры

vlan *VLAN-ID*	(Опционально.) Укажите VLAN, для которой необходимо отобразить информацию.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статистику PIM Snooping на коммутаторе.

Пример

В данном примере показано, как отобразить статистику PIM Snooping на коммутаторе.

```
Switch#show ip pim snooping statistics

VLAN ID: 1
Received PIMv2 hello: 41
Received PIMv2 join/prune: 18
Received PIM error: 0
Received PIMv1 messages in total: 0
Received PIMv2 messages in total: 69

VLAN ID: 2
Received PIMv2 hello: 0
Received PIMv2 join/prune: 0
Received PIM error: 0
Received PIMv1 messages in total: 0
Received PIMv2 messages in total: 0

Total Entries: 2

Switch#
```

83. Команды Quality of Service (QoS)

83.1 class

Данная команда используется, чтобы указать имя карты класса (class map) для привязки к политике трафика и войти в режим Policy-map Configuration Mode. Чтобы удалить описание политики указанного класса, воспользуйтесь формой **no** этой команды.

class *NAME*
no class *NAME*
class class-default

Параметры

NAME	Укажите имя карты класса (class map) для привязки к политике трафика.

По умолчанию

Нет.

Режим ввода команды

Policy-map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

После ввода данной команды будет выполнен вход в режим Policy-map Configuration Mode. Весь трафик, который не соответствует текущему настроенному классу, будет классифицирован как класс по умолчанию (class-default). Если указанного имени карты класса (class map) 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)#
```

83.2 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. Чтобы удалить существующую карту класса на коммутаторе, воспользуйтесь формой **no** этой команды.

class-map [match-all | match-any] *NAME*
no class-map *NAME*

Параметры

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**.
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**.
NAME	Укажите имя карты класса. Максимальное количество символов – 32.

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 применено 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. Указанное 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 заданную карту класса «class_home_user».

```
Switch#configure terminal
Switch(config)#class-map match-all class_home_user
Switch(config-cmap)#match access-group name acl_home_user
Switch(config-cmap)#match protocol ipv6
Switch(config-cmap)#
```

83.3 match

Данная команда используется, чтобы настроить критерии соответствия для карты класса. Для удаления критериев соответствия воспользуйтесь формой **no** этой команды.

match {access-group name *ACCESS-LIST-NAME* **| cos [inner]** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP-PRECEDENCE-LIST* **| protocol** *PROTOCOL-NAME* **| vlan [inner]** *VLAN-LIST***}**

no match {access-group name *ACCESS-LIST-NAME* **| cos [inner]** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP-PRECEDENCE-LIST* **| protocol** *PROTOCOL-NAME* **| vlan [inner]** *VLAN-ID-LIST***}**

Параметры

access-group name *ACCESS-LIST-NAME*	Укажите список доступа в качестве критерия соответствия. Трафик, разрешенный указанным списком доступа, будет классифицирован.
cos [inner] *COS-LIST*	Укажите значение (-я) определенного IEEE 802.1Q в качестве критерия соответствия. 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 *DSCP-LIST*	Укажите значения DSCP-метки в качестве критерия соответствия. 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, критерий соответствия настраивается для пакетов IPv4 и IPv6.
[ip] precedence *IP-PRECEDENCE-LIST*	Укажите значения приоритета IP в качестве критерия соответствия. Диапазон значений: от 0 до 7. Для перечисления нескольких значений приоритета используется запятая, а для обозначения диапазона значений – дефис. **ip** – (Опционально.) Укажите, чтобы настроить критерий соответствия только для пакетов IPv4. Если не указано, критерий соответствия настраивается для пакетов IPv4 и IPv6. Для пакетов IPv6 приоритетом являются три наиболее значимых бита класса трафика заголовка IPv6.
protocol *PROTOCOL-NAME*	Укажите имя протокола в качестве критерия соответствия.

vlan [inner] *VLAN-LIST*	Укажите номер (-а) или диапазон номеров идентификации VLAN в качестве критерия соответствия. 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.
Команда **match access-group** позволяет указать список доступа для соответствия. Пакеты, разрешенные данным списком, будут включены в класс. Правило «запретить» в списке доступа учитываться не будет. Если группа доступа применяется при помощи команды **expert access-group**, **ip access-group**, **ipv6 access-group**, или **mac access-group**, а пакет соответствует правилам ACL и QoS, будет использоваться карта класса

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 заданной карты класса – class-home-user. Имя указанного 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 примере ниже показано, как настроить карту класса и значения CoS, которые будут использованы в качестве критериев соответствия для данного класса. Имя заданной карты класса – cos. Указанные 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 следующем примере показано, как настроить классы для классификации трафика на основе значений CoS. Имена заданных 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. Указанная 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 eth1/0/1
Switch(config-if)#service-policy input cos-based-treatment
Switch(config-if)#
```

83.4 mls qos aggregate-policer

Данная команда предназначена для настройки aggregate policer, который будет использован в картах политики. Чтобы удалить aggregate policer, воспользуйтесь формой **no** этой команды. Команда **mls**

qos aggregate-policer применяется для использования single rate policing, а команда **mls qos aggregate-policer cir** для использования two-rate policing.

mls qos aggregate-policer *NAME KBPS* **[***BURST-NORMAL* **[***BURST-MAX***]] [conform-action** *ACTION***] exceed-action** *ACTION* **[violate-action** *ACTION***] [color-aware]**

mls qos aggregate-policer *NAME* **cir** *CIR* **[bc** *CONFORM-BURST***] pir** *PIR* **[be** *PEAK-BURST***] [conform-action** *ACTION***] [exceed-action** *ACTION* **[violate-action** *ACTION***]] [color-aware]**

no mls qos aggregate-policer *NAME*

Параметры

NAME	Укажите имя правила aggregate policing. Максимально допустимое количество символов – 32. Символы, используемые в данном параметре, чувствительны к регистру. Имена aggregate policer не должны совпадать и начинаться с цифры. Первым символом в имени обязательно должна быть буква.
KBPS	Укажите среднюю скорость в Кбит/с.
BURST-NORMAL	(Опционально.) Укажите нормальный размер всплеска (burst). Единица измерения – Кбайт.
BURST-MAX	(Опционально.) Укажите максимальный размер всплеска (burst). Единица измерения – Кбайт.
CIR	Укажите гарантированную полосу пропускания (committed information rate) в Кбит/с. Данный параметр является первым в алгоритме «корзина маркеров» (token bucket) для two-rate Metering.
PIR	Укажите пиковую скорость передачи (peak information rate) в Кбит/с. Данный параметр является вторым в алгоритме «корзина маркеров» (token bucket) для two-rate Metering.
CONFORM-BURST	(Опционально.) Укажите размер всплеска (burst) для первого параметра алгоритма «корзина маркеров» (token bucket). Единица измерения – Кбайт.
PEAK-BURST	(Опционально.) Укажите размер всплеска (burst) для второго параметра алгоритма «корзина маркеров» (token bucket). Единица измерения – Кбайт.
conform-action	(Опционально.) Укажите, чтобы действие было применено к green color packets (пакетам, «окрашенным» в зелёный цвет). Если не указано, будет применено действие по умолчанию **transmit** (передача пакетов).
exceed-action	Укажите, чтобы действие было применено к пакетам, превышающим разрешенную скорость. Если при использовании two rate policer данный параметр не указан, будет применено действие по умолчанию **drop** (отбрасывание).

violate-action	(Опционально.) Укажите, чтобы при использовании single rate policing действие было применено 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 применено действие по умолчанию **drop** (отбрасывание).
ACTION	Укажите, чтобы действие было применено к пакетам. Ниже указаны ключевые слова: **drop** – отбрасывание пакетов. **set-dscp-transmit** *VALUE* – укажите значение IP DSCP и передачу пакетов с новым заданным значением IP DSCP. **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. Указанное 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)#
```

83.5 mls qos cos

Данная команда используется, чтобы настроить значение CoS по умолчанию для порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 интерфейсе Ethernet 1/0/1. Заданное значение – 3.

```
Switch#configure terminal
Switch(config)#interface  eth1/0/1
Switch(config-if)#mls qos cos 3
Switch(config-if)#
```

83.6 mls qos dscp-mutation

Данная команда используется для привязки карты изменения входящего DSCP (DSCP Mutation) к интерфейсу. Чтобы удалить привязку карты DSCP Mutation к интерфейсу, воспользуйтесь формой **no** этой команды.

mls qos dscp-mutation *DSCP-MUTATION-TABLE-NAME*
no mls qos dscp-mutation

Параметры

DSCP-MUTATION-TABLE-NAME	Укажите имя таблицы DSCP Mutation без пробелов. Максимальное 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 интерфейсу 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 eth1/0/1
Switch(config-if)#mls qos dscp-mutation mutemap1
Switch(config-if)#
```

83.7 mls qos map cos-color

Данная команда используется для настройки цветовой привязки CoS пакета. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

mls qos map cos-color *COS-LIST* **to {green | yellow | red}**
no mls qos map cos-color

Параметры

COS-LIST	Укажите список значений CoS для привязки к цвету. Диапазон значений: от 0 до 7. Используйте дефис, чтобы отделить диапазон значений. Используйте запятую, чтобы разделить несколько значений. Пробелы до и после символов недопустимы.
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, 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 eth1/0/1
Switch(config-if)#mls qos map cos-color 1-7 to red
Switch(config-if)#
```

83.8 mls qos map dscp-color

Данная команда используется для настройки цветовой привязки DSCP пакета. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

mls qos map dscp-color *DSCP-LIST* **to {green | yellow | red}**
no mls qos map dscp-color *DSCP-LIST*

Параметры

DSCP-LIST	Укажите список DSCP-меток для привязки к цвету. Диапазон значений: от 0 до 63. Используйте дефис, чтобы отделить диапазон значений. Используйте запятую, чтобы разделить несколько значений. Пробелы до и после символов недопустимы.
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 применяется 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 eth1/0/1
Switch(config-if)#mls qos map dscp-color 61-63 to yellow
Switch(config-if)#
```

83.9 mls qos map dscp-cos

Данная команда используется для привязки DSCP-меток к CoS. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

mls qos map dscp-cos *DSCP-LIST* **to** *COS-VALUE*
no mls qos map dscp-cos *DSCP-LIST*

Параметры

dscp-cos *DSCP-LIST* **to** *COS-VALUE*	Укажите список DSCP-меток для привязки к значению CoS. Диапазон значений: от 0 до 63. Используйте дефис, чтобы отделить диапазон значений. Используйте запятую, чтобы разделить несколько значений. Пробелы до и после символов недопустимы.
DSCP-LIST	Укажите диапазон DSCP-меток.

По умолчанию

Значение CoS:	0	1	2	3	4	5	6	7
Значение DSCP:	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда позволяет привязать DSCP-метку доверенного порта DSCP к значению внутреннего CoS. Данное значение CoS будет привязано к очереди CoS на основе CoS в карте очереди, настроенной в команде **priority-queue cos-map**.

Пример

В данном примере показано, как привязать DSCP к CoS на интерфейсе Ethernet 1/0/6. DSCP-метки 12, 16 и 18 привязаны к CoS 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/6
Switch(config-if)#mls qos map dscp-cos 12,16,18 to 1
Switch(config-if)#
```

83.10 mls qos map dscp-mutation

Данная команда используется для настройки карты DSCP Mutation. Чтобы удалить карту Mutation, воспользуйтесь формой **no** этой команды.

mls qos map dscp-mutation *MAP-NAME INPUT-DSCP-LIST* **to** *OUTPUT-DSCP*

no mls qos map dscp-mutation *MAP-NAME*

Параметры

MAP-NAME	Укажите имя карты DSCP Mutation без пробелов. Максимальное количество символов – 32. Пробелы недопустимы.
INPUT-DSCP-LIST	Укажите список DSCP, значения которых необходимо «мутировать». Диапазон значений: от 0 до 63. Используйте дефис, чтобы отделить диапазон значений. Используйте запятую, чтобы разделить несколько значений. Пробелы до и после символов недопустимы.
OUTPUT-DSCP	Укажите значение DSCP, которое будет применено после «мутации» Mutation. 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 каждых новых значений DSCP, которые нужно изменить, и для каждых новых значений, 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)#
```

83.11 mls qos scheduler

Данная команда используется для настройки механизма обслуживания очередей. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

mls qos scheduler {sp | rr | wrr | wdrr}
no mls qos scheduler

Параметры

sp	Укажите алгоритм Strict Priority, SP для всех очередей.
rr	Укажите алгоритм Round-Robin, RR для всех очередей.
wrr	Укажите алгоритм Weighted Round-Robin, WRR по числу кадров для всех очередей. Если настроенный вес (weight) очереди равен нулю, для данной очереди будет включен алгоритм Strict Priority, SP.
wdrr	Укажите алгоритм Weighted Deficit Round-Robin, WDRR по длине кадров (quantum) для очередей всех портов. Если настроенный вес (weight) очереди равен нулю, для данной очереди включен алгоритм Strict Priority, SP.

По умолчанию

Алгоритм механизма обслуживания очередей для очереди по умолчанию – WRR.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Укажите алгоритм обслуживания очередей (WRR, SP, RR или WDRR) для выходной очереди. Алгоритм обслуживания очередей для очереди по умолчанию – WRR. WDRR предназначен для набора накопившихся кредитов в очереди передачи в режиме Round-Robin. Изначально для каждой очереди установлен свой счетчик кредита (настроенное значение quantum). Каждый раз, когда пакет отправляется из очереди CoS, размер пакета вычитается из соответствующего счетчика кредитов, и право на обслуживание переходит к очереди с более низким CoS. Если счетчик кредитов опускается ниже нуля, очередь не обслуживается до тех пор, пока ее кредиты не будут снова пополнены. Счетчики кредитов всех очередей CoS при достижении нуля пополняются за одни раз.

Обслуживание всех пакетов прекращается, когда их счетчики достигают нуля или становятся меньше нуля, а также после полного осуществления передачи последнего пакета. При выполнении данного условия к каждому счетчику в очереди CoS будет добавлено значение quantum кредитов. Значение quantum для каждой очереди может отличаться в зависимости от пользовательских настроек.

Для включения режима Strict Priority для очереди CoS необходимо, чтобы для всех других очередей CoS с более высоким приоритетом также был установлен режим Strict Priority.

WRR предназначен для передачи разрешенных пакетов в очереди передачи в режиме Round-Robin. Изначально вес каждой очереди установлен на основе настроенного веса. Каждый раз, когда пакет отправляется из очереди CoS с более высоким приоритетом, из соответствующего веса вычитается 1, и право на обслуживание переходит к пакету из очереди CoS с приоритетом ниже предыдущего. Если вес очереди CoS достигает нуля, очередь не обслуживается до тех пор, пока ее вес не будет возобновлен. Вес всех очередей CoS при достижении нуля возобновляется за один раз.

Пример

В данном примере показано, как настроить алгоритм Strict Priority, SP для очереди.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos scheduler sp
Switch(config-if)#
```

83.12 mls qos trust

Данная команда используется, чтобы настроить доверенный статус (trust) на порту для поля CoS или DSCP поступающего пакета для последующих QoS-операций. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

mls qos trust {cos | dscp}

no mls qos trust

Параметры

cos	Укажите, чтобы назначить биты CoS поступающих пакетов доверенными для последующих QoS-операций.
dscp	Укажите, чтобы назначить биты ToS/DSCP (если доступны в поступающих пакетах) доверенными для последующих операций. Для не IP-пакетов: доверенной будет назначена информация 2 уровня CoS для классификации трафика.

По умолчанию

По умолчанию доверенным является CoS.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

После настройки статуса trust для DSCP на интерфейсе, для последующих QoS-операций DSCP приходящих пакетов будет доверенным. Сначала DSCP будет привязан к значению внутреннего CoS, которое в дальнейшем будет использовано для определения очереди CoS. Привязка DSCP к CoS настраивается с помощью команды **mls qos map dscp-cos**. Чтобы настроить CoS в карте очереди, используйте команду **priority-queue cos-map**. Если приходящий пакет не IP-пакет, доверенным будет CoS. В передаваемом пакете также будет CoS, полученный в результате привязки DSCP.

После настройки статуса trust для CoS на интерфейсе, CoS приходящих пакетов будет применен в качестве внутреннего CoS и использован для определения очереди CoS. Очередь CoS определяется на основе таблицы соответствия CoS и очереди.

Пакету, прибывшему на порт 802.1Q VLAN tunnel, будет добавлен внешний тег VLAN для передачи через VLAN tunnel. Если на порту настроен статус trust для CoS, тег внутреннего CoS будет являться CoS пакета и значением CoS во внешнем теге VLAN пакета. Если при вводе команды **mls qos cos** был указан параметр **override**, то внутренним CoS пакета и значением CoS во внешнем теге VLAN пакета будет CoS, настроенный в команде **mls qos cos**. Если на порту настроен статус trust для DSCP, то внутренним CoS пакета и значением CoS во внешнем теге VLAN пакета будет CoS, полученный в результате привязки DSCP.

Пакет, полученный портом, будет инициализирован с цветом на основе команды **mls qos map dscp-color** (если на порту настроен статус trust для DSCP) или с цветом на основе MLS QoS преобразованного CoS (если на порту настроен статус trust для CoS).

Пример

В данном примере показано, как настроить режим trust для DSCP на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos trust dscp
Switch(config-if)#
```

83.13 police

Данная команда используется для настройки Traffic Policing (ограничения трафика) с использованием single rate. Чтобы оменить Traffic Policing, воспользуйтесь формой **no** этой команды.

police *KBPS* **[***BURST-NORMAL* **[***BURST-MAX***]] [conform-action** *ACTION***] exceed-action** *ACTION* **[violate-action** *ACTION***] [color-aware]**

no police

Параметры

KBPS	Укажите среднюю скорость в Кбит/с.
BURST-NORMAL	(Опционально.) Укажите нормальный размер всплеска (burst). Единица измерения – Кбайт.

BURST-MAX	(Опционально.) Укажите максимальный размер всплеска (burst). Единица измерения – Кбайт.
conform-action	(Опционально.) Укажите, чтобы действие было выполнено к green color packets (пакетам «окрашенным» в зелёный цвет). Если не указано, будет выполнено действие по умолчанию **transmit** (передача пакетов).
exceed-action	Укажите, чтобы действие было выполнено к yellow color packets (пакетам, «окрашенным» в желтый цвет), превышающим разрешенную скорость.
violate-action	(Опционально.) Укажите, чтобы действие было выполнено к red color packets (пакетам, «окрашенным» в красный цвет). Если данный параметр не указан, используется single rate two color policer. Если данный параметр указан, используется single rate three color policer.
ACTION	Укажите, чтобы действие было выполнено к пакетам. Ниже указаны ключевые слова: **drop** – отбрасывание пакетов. **set-dscp-transmit** *VALUE* – укажите значение IP DSCP-метки и передачу пакетов с новой IP DSCP-меткой. **set-1p-transmit** – укажите значение 802.1p и передачу пакетов с новым значением. **transmit** – передача пакетов без изменений.
color-aware	(Опционально.) Укажите данный параметр для single rate three color policer. Если данный параметр не указан, policer работает в режиме Color Blind. Если данный параметр указан, policer работает в режиме Color Aware.

По умолчанию

Нет.

Режим ввода команды

Policy-map Class Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду **police**, чтобы отбросить или отметить пакеты со значениями QoS, не соответствующими уровню пакета.

Введите команду **police** *KBPS*, чтобы создать single rate policer. Примените 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 заданному 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. Указанная 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 eth1/0/1
Switch(config-if)#service-policy input police-setting
Switch(config-if)#
```

83.14 police aggregate

Данная команда используется, чтобы настроить aggregate policer в качестве политики для класса трафика в карте политик. Для удаления aggregate policer из политики класса воспользуйтесь формой **no** этой команды.

police aggregate *NAME*

no police

Параметры

NAME	Укажите ранее настроенное имя aggregate policer в качестве aggregate policer для класса трафика.

По умолчанию

Нет.

Режим ввода команды

Policy-map Class Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду **mls qos aggregate-policer** в режиме Global Configuration Mode, чтобы создать aggregate policer. Затем примените 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 задан 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)#
```

83.15 police cir

Данная команда используется для настройки two-rate Traffic Policing (CIR и PIR). Чтобы отменить two-rate Traffic Policing, воспользуйтесь формой **no** этой команды.

police cir *CIR* **[bc** *CONFORM-BURST***] pir** *PIR* **[be** *PEAK-BURST***] [conform-action** *ACTION***] [exceed-action** *ACTION* **[violate-action** *ACTION***]] [color-aware]**

no police

Параметры

CIR	Укажите гарантированную полосу пропускания (committed information rate) в Кбит/с. Данный параметр является первым в алгоритме «корзина маркеров» (token bucket) для two-rate Metering.
PIR	Укажите пиковую скорость передачи (peak information rate) в Кбит/с. Данный параметр является вторым в алгоритме «корзина маркеров» (token bucket) для two-rate Metering.
CONFORM-BURST	(Опционально.) Укажите размер всплеска (burst) для первого параметра алгоритма «корзина маркеров» (token bucket). Единица измерения – Кбайт.
PEAK-BURST	(Опционально.) Укажите размер всплеска (burst) для второго параметра алгоритма «корзина маркеров» (token bucket). Единица измерения – Кбайт.
conform-action	(Опционально.) Укажите, чтобы действие было выполнено к green color packets (пакетам, «окрашенным» в зелёный цвет). Если не указано, будет выполнено действие по умолчанию **transmit** (передача пакетов).
exceed-action	(Опционально.) Укажите, чтобы действие было выполнено к yellow color packets (пакетам, «окрашенным» в желтый цвет), которые соответствуют PIR, но не соответствуют CIR. Если не указано, будет выполнено действие по умолчанию **drop** (отбрасывание).
violate-action	(Опционально.) Укажите, чтобы действие было выполнено к red color packets (пакетам, «окрашенным» в красный цвет), которые не соответствуют CIR и PIR. Если не указано, будет выполнено действие по умолчанию **drop** (отбрасывание).
ACTION	(Опционально.) Укажите, чтобы действие было выполнено к пакетам. Ниже указаны ключевые слова: **drop** – отбрасывание пакетов. **set-dscp-transmit** *VALUE* – укажите значение IP DSCP и передачу пакетов с новым заданным значением IP DSCP. **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 eth1/0/3
Switch(config-if)#service-policy output policy1
Switch(config-if)#
```

83.16 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. Чтобы удалить карту политики, воспользуйтесь формой **no** этой команды.

policy-map *NAME*
no policy-map *NAME*

Параметры

NAME	Укажите имя карты политики. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду **policy-map**, 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 0
Switch(config-pmap-c)#
```

83.17 priority-queue cos-map

Данная команда используется для привязки CoS к карте очереди. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

priority-queue cos-map *QUEUE-ID COS1* **[***COS2* **[***COS3* **[***COS4* **[***COS5* **[***COS6* **[***COS7* **[***COS8***]]]]]]]**

no priority-queue cos-map

Параметры

QUEUE-ID	Укажите ID очереди, к которой будет привязан CoS.
CoS 1	Укажите значение CoS для привязки. Диапазон значений: от 0 до 7.
COS2...COS8	(Опционально.) Укажите значение CoS для привязки. Диапазон значений: от 0 до 7.

По умолчанию

По умолчанию привязка приоритета CoS к очереди: 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)#
```

83.18 queue rate-limit

Данная команда позволяет указать/изменить полосу пропускания (bandwidth), предназначенную для очереди. Чтобы удалить полосу пропускания, предназначенную для очереди, воспользуйтесь формой **no** этой команды.

queue *QUEUE-ID* **rate-limit {***MIN-BANDWIDTH-KBPS* **| percent** *MIN-PERCENTAGE***} {***MAX-BANDWIDTH-KBPS* **| percent** *MAX-PERCENTAGE***}**

no queue *QUEUE-ID* **rate-limit**

Параметры

QUEUE-ID	Укажите ID очереди, для которой необходимо настроить минимальную разрешенную и максимальную полосу пропускания.
MIN-BANDWIDTH-KBPS	Укажите минимальную разрешенную полосу пропускания в Кбит/с для указанной очереди.
MAX-BANDWIDTH-KBPS	Укажите максимальную полосу пропускания в Кбит/с для указанной очереди.
MIN-PERCENTAGE	Укажите минимальную полосу пропускания в процентах. Диапазон значений: от 1 до 100.
MAX-PERCENTAGE	Укажите максимальную полосу пропускания в процентах. 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 применима исключительно 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» заданы минимальная разрешенная полоса пропускания 100 Кбит/с и максимальная полоса пропускания 2000 Кбит/с. Для очереди 2 «queue 2» указаны минимальная разрешенная полоса пропускания 10% и максимальная полоса пропускания 50%.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#queue 1 rate-limit 100 2000
Switch(config-if)#queue 2 rate-limit percent 10 percent 50
Switch(config-if)#
```

83.19 rate-limit {input | output}

Данная команда используется, чтобы настроить значения ограничения полосы пропускания для входящего и исходящего трафика на интерфейсе. Для отмены ограничения полосы пропускания воспользуйтесь формой **no** этой команды.

rate-limit {input | output} {*NUMBER-KBPS* **| percent** *PERCENTAGE***} [***BURST-SIZE***]**

no rate-limit {input | output}

Параметры

input	Укажите ограничение полосы пропускания для входящих пакетов.
output	Укажите ограничение полосы пропускания для исходящих пакетов.
NUMBER-KBPS	Укажите ограничение максимальной полосы пропускания в Кбит/с.
PERCENTAGE	Укажите для настройки ограничения в процентах. Диапазон значений: от 1 до 100.
BURST-SIZE	(Опционально.) Укажите ограничение для трафика всплеска (burst). Единица измерения – Кбайт.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Настроенное ограничение не должно превышать максимальную скорость на указанном интерфейсе. Если полученный трафик превышает заданное 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. Заданные ограничения входящей полосы пропускания: 2000 Кбит/с и 4096 Кбайт для трафика всплеска (burst).

```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#rate-limit input 2000 4096
Switch(config-if)#
```

83.20 service-policy

Данная команда используется для привязки карты политики к типу input или output на интерфейсе. Чтобы удалить политику обслуживания из входящего интерфейса (input), воспользуйтесь формой **no** этой команды.

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.
NAME	Укажите имя карты политики обслуживания. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применима исключительно для настройки интерфейсов физического порта.

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, заданная согласованная скорость передачи – 800 Кбит/с; карта класса «silver» настроена для привязки CoS 5 с использованием single rate policer, заданная согласованная скорость передачи – 2000 Кбит/с; карта класса «bronze» настроена для привязки CoS 0 с использованием single rate policer, заданная согласованная скорость передачи – 8000 Кбит/с.

Для cust2-classes: карта класса «gold» настроена с использованием очереди CoS 6 и single rate policer, заданная согласованная скорость передачи – 1600 Кбит/с; карта класса «silver» настроена с использованием single rate policer, заданная согласованная скорость передачи – 4000 Кбит/с; карта класса «bronze» настроена с использованием single rate policer, заданная согласованная скорость передачи – 16000 Кбит/с.

Указанная 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 eth1/0/1
Switch(config-if)#service-policy input cust1-classes
Switch(config-if)#exit
Switch(config)#interface eth1/0/2
Switch(config-if)#service-policy input cust1-classes
Switch(config-if)#
```

83.21 set

Данная команда используется для настройки полей нового приоритета (precedence), DSCP и CoS исходящего пакета. Также возможна настройка очереди CoS для пакета. Чтобы удалить заданные настройки, воспользуйтесь формой **no** этой команды.

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

[ip] precedence *PRECEDENCE*	Укажите новый приоритет пакета. Диапазон значений: от 0 до 7. **ip** – (Опционально) укажите, чтобы отметить 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.
[ip] dscp *DSCP*	Укажите новый DSCP пакета. Диапазон значений: от 0 до 63. **ip** – (Опционально) укажите, чтобы отметить IPv4 DSCP. Если не указано, будут отмечены IPv4 и IPv6 DSCP. Настройка DSCP не повлияет на выбор очереди CoS.

cos *COS*	Укажите новое значение CoS пакета. Диапазон значений: от 0 до 7. Настройка CoS повлияет на выбор очереди CoS, если карта политики применена на входящем интерфейсе.
cos-queue *COS-QUEUE*	Укажите очередь CoS для пакетов. Новое значение очереди CoS заменит первоначальное. Очередь CoS не будет назначена, если карта политики привязана к исходящему потоку на интерфейсе.

По умолчанию

Нет.

Режим ввода команды

Policy-map Class Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для настройки полей нового приоритета (precedence), DSCP и CoS исходящего пакета. Введите 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 указанном классе «class1» будут помечены DSCP 10 с использованием single rate policer, заданная 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)#
```

83.22 show class-map

Данная команда используется для отображения настроек карты класса.

show class-map [*NAME***]**

Параметры

NAME	(Опционально.) Укажите имя карты класса. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить все карты класса и их критерии соответствия.

Пример

В данном примере показано, как настроены две карты класса. Пакеты, соответствующие списку доступа «acl_home_user», принадлежат заданному классу «c3». IP-пакеты принадлежат настроенному классу «c2».

```
Switch#show class-map

Class Map match-any class-default
   Match any

 Class Map match-all c2
   Match protocol ip

Class Map match-all c3
   Match access-group acl_home_user

Switch#
```

83.23 show mls qos aggregate-policer

Данная команда используется для отображения настроенного aggregated policer.

show mls qos aggregate-policer [*NAME***]**

Параметры

NAME	(Опционально.) Укажите имя aggregated policer.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настроенный aggregated policer.

Пример

В данном примере показано, как отобразить aggregated policer.

```
Switch#show mls qos aggregate-policer

mls qos aggregate-policer agg-policer5 10 1000 conform-action transmit exceed-action drop
mls qos aggregate-policer agg-policer5 cir 500 bc 10 pir 1000 be 10 conform-action transmit
exceed-action set-dscp-transmit 2 violate-action drop

Switch#
```

83.24 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-ID	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
cos	Укажите, чтобы отобразить CoS по умолчанию.
scheduler	Укажите, чтобы отобразить настройки механизма обслуживания очереди передачи.
trust	Укажите, чтобы отобразить статус trust порта.

rate-limit	Укажите, чтобы отобразить ограничение полосы пропускания, настроенной для порта.
queue-rate-limit	Укажите, чтобы отобразить ограничение полосы пропускания, настроенной для очереди.
dscp-mutation	Укажите, чтобы отобразить карту DSCP Mutation, привязанную к интерфейсу.
map dscp-color	Укажите, чтобы отобразить цветовую привязку DSCP.
map cos-color	Укажите, чтобы отобразить цветовую привязку CoS.
map dscp-cos	Укажите, чтобы отобразить привязку DSCP к CoS.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Когда в команде используется параметр **rate-limit** или **queue-rate-limit**, при отображении информации указываются проценты и фактическая скорость, если соединение порта активно. Если соединение порта неактивно, при отображении информации указываются только проценты.

Пример

В данном примере показано, как отобразить CoS по умолчанию для диапазона интерфейсов от Ethernet 1/0/2 до Ethernet 1/0/5.

```
Switch#show mls qos interface eth1/0/2-5 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 примере ниже показано, как отобразить статус trust порта для диапазона интерфейсов от Ethernet 1/0/2 до Ethernet 1/0/5.

```
Switch#show mls qos interface eth1/0/2-5 trust

 Interface     Trust State
 ------------  ------------
 eth1/0/2      trust DSCP
 eth1/0/3      trust CoS
 eth1/0/4      trust DSCP
 eth1/0/5      trust CoS

Switch#
```

В следующем примере показано, как отобразить настройки механизма обслуживания очередей для интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch#show mls qos interface eth1/0/1-2 scheduler

 Interface     Scheduler Method
 ------------  -----------------
 eth1/0/1      sp
 eth1/0/2      wrr

Switch#
```

В нижеприведенном 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 eth1/0/1-2 dscp-mutation

 Interface     DSCP Mutation Map
 ------------  --------------------
 eth1/0/1      Mutate Map 1
 eth1/0/2      Mutate Map 2

Switch#
```

В нижеследующем примере показано, как отобразить ограничение полосы пропускания для диапазона интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/4.

```
Switch#show mls qos interface eth1/0/1-4 rate-limit

 Interface Rx Rate             TX Rate             Rx Burst       Tx Burst
 --------- ------------------- ------------------- -------------- -------------
 eth1/0/1  1000 kbps           No Limit            64 kbyte       No Limit
 eth1/0/2  No Limit            2000 kbps           No Limit       2000 kbyte
 eth1/0/3  10%(100000 kbps)    20%(200000 kbps)    64 kbyte       64 kbyte
 eth1/0/4  2%                  2000 kbps           64 kbyte       64 kbyte

Switch#
```

В примере ниже показано, как отобразить ограничение полосы пропускания CoS для интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch#show mls qos interface eth1/0/1-2 queue-rate-limit


eth1/0/1
 QID   Min Bandwidth        Max Bandwidth
 ----  -------------------  -------------------
 0     No Limit             No Limit
 1     16 kbps              10%(100000 kbps)
 2     32 kbps              -
 3     2%                   50%
 4     64 kbps              -
 5     64 kbps              -
 6     32 kbps              -
 7     -                    128 kbps

eth1/0/2
 QID   Min Bandwidth        Max Bandwidth
 ----  -------------------  -------------------
 0     -                    -
 1     16 kbps              -
 2     32 kbps              -
 3     32 kbps              -
 4     64 kbps              -
 5     64 kbps              -
 6     32 kbps              -
 7     -                    128 kbps

Switch#
```

В следующем примере показано, как отобразить цветовую привязку DSCP для интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch#show mls qos interface eth1/0/1-2 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 0-63 are mapped to green

Switch#
```

В нижеприведенном примере показано, как отобразить цветовую привязку CoS для интерфейсов Ethernet1/0/3 и Ethernet 1/0/4.

```
Switch#show mls qos interface eth1/0/3-4 map cos-color


eth1/0/3
  CoS 0-2,5,7 are mapped to green
  CoS 3-4 are mapped to yellow
  CoS 6 are mapped to red

eth1/0/4
  CoS 0-6 are mapped to green
  CoS 7 are mapped to yellow

Switch#
```

В нижеследующем примере показано, как отобразить привязку DSCP к CoS для интерфейса Ethernet 1/0/1.

```
Switch#show mls qos interface eth1/0/1 map dscp-cos

eth1/0/1
       0  1  2  3  4  5  6  7  8  9
     ---------------------------------
   00  00 00 00 00 00 00 00 00 01 01
   10  01 01 01 01 01 01 02 02 02 02
   20  02 02 02 02 03 03 03 03 03 03
   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#
```

83.25 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 для отображения.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется 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#
```

83.26 show mls qos queueing

Данная команда используется, чтобы отобразить информацию об очередях QoS и настройках веса (weight) для разных алгоритмов обслуживания очередей на определенном интерфейсе или интерфейсах.

show mls qos queuing [interface I*NTERFACE-ID* [, | -]]

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите ID интерфейса, для которого необходимо отобразить информацию о настройках веса (weight) разных алгоритмов обслуживания очередей.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

При указании ключевого слова **interface**, на определенном интерфейсе или интерфейсах будет отображен настроенный вес для разных алгоритмов обслуживания очередей (WRR или WDRR). Если **interface** не указан, отображается только системная карта привязки CoS к ID очереди.

Режим Scheduling, который настроен при помощи команды **mls qos scheduler**, определяет, какие настройки будут действовать для веса. Используйте команду **show mls qos interface scheduler**, чтобы отобразить настроенный алгоритм обслуживания очередей на интерфейсе.

Пример

В данном примере показано, как отобразить информацию об очередях QoS.

```
Switch#show mls qos queueing

 CoS-queue map:
   CoS   QID
   ---   ---
    0     2
    1     0
    2     1
    3     3
    4     4
    5     5
    6     6
    7     7


Switch#
```

В примере ниже показано, как отобразить настройки веса для разных алгоритмов обслуживания очередей на интерфейсе Ethernet 1/0/3.

```
Switch#show mls qos queueing interface eth1/0/3

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
 wdrr bandwidth weights:
   QID  Quantum
   ---  -------
    0      1
    1      1
    2      1
    3      1
    4      1
    5      1
    6      1
    7      1

Switch#
```

83.27 show policy-map

Данная команда используется для отображения настроек карты политики.

show policy-map [*POLICY-NAME* **| interface** *INTERFACE-ID***]**

Параметры

POLICY-NAME	(Опционально.) Укажите имя карты политики. Если не указано, будут отображены все карты политики.
interface *INTERFACE-ID*	(Опционально.) Укажите интерфейсы физического порта, которые необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить политики класса, настроенные для карты политики.

Пример

В данном примере показано, как настроить two-rate Traffic Policing в карте политики под именем «policy1» для класса «police». Для ограничения трафика заданы 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 eth1/0/1
Router(config-if)#service-policy output policy1
Router(config-if)#
```

В примере ниже показано, как отобразить карту 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 следующем примере показано, как отобразить все карты политики на интерфейсе Ethernet 1/0/1.

```
Switch#show policy-map interface eth1/0/1

 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#
```

83.28 wdrr-queue bandwidth

Данная команда используется, чтобы настроить значения quantum для очередей, обслуживаемых механизмом WDRR. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

wdrr-queue bandwidth *QUANTUM1...QUANTUM8*
no wdrr-queue bandwidth

Параметры

QUANTUM1 ...QUANTUM8	Укажите значение quantum (число длины кадров) для каждой очереди, обслуживаемой механизмом WDRR.

По умолчанию

Значение quantum для каждой очереди по умолчанию – 1.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Чтобы использовать данную команду, необходимо перейти в режим обслуживания очередей WDRR с помощью команды **mls qos scheduler wdrr**.

Пример

В данном примере показано, как настроить значения quantum для очередей в режиме обслуживания очередей WDRR на интерфейсе Ethernet 1/0/1. Для очереди 0 задано значение 1, для очереди 1 – 2, для очереди 2 – 3, для очереди 3 – 4, для очереди 5 – 6, для очереди 6 – 7 и для очереди 7 – 8.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos scheduler wdrr
Switch(config-if)#wdrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

83.29 wrr-queue bandwidth

Данная команда позволяет указать/изменить полосу пропускания (bandwidth), предназначенную для очереди. Чтобы удалить полосу пропускания, предназначенную для очереди, воспользуйтесь формой **no** этой команды.

wrr-queue bandwidth *WEIGHT1...WEIGHT8*
no wrr-queue bandwidth

Параметры

WEIGHT1 ...WEIGHT8	Укажите значение веса (число кадров) для каждой очереди, обслуживаемой механизмом WRR. Диапазон значений: от 0 до 127.

По умолчанию

Значение веса для параметров от *WEIGHT1* до *WEIGHT7* по умолчанию – 1.

Значение веса для *WEIGHT8* по умолчанию – 0.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Чтобы применить 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 задано значение 1, для очереди 1 – 2, для очереди 2 – 3, для очереди 3 – 4, для очереди 5 – 6, для очереди 6 – 7 и для очереди 7 – 8.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos scheduler wrr
Switch(config-if)#wrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

84. Команды QoS Amendment Data Center Bridge (DCB)

84.1 class type network-qos

Данная команда используется, чтобы указать имя карты классов (class map) сетевого QoS для привязки к политике трафика и войти в режим конфигурации класса policy-map type network QoS.

class type network-qos *NAME*

Параметры

NAME	Укажите имя карты классов (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

Сетевой QoS применяется на коммутаторе, который поддерживает функцию DCB. Если указанного имени карты классов не существует, трафик не будет ассоциирован с данным классом, о чем будет выведено предупреждающее сообщение.

Используйте команду **policy-map type network-qos** в режиме Global Configuration Mode, чтобы идентифицировать карту политик (policy map) сетевого QoS и войти в режим Policy-map Configuration Mode.

Пример

В данном примере показано, как создать карту классов сетевого QoS для классификации трафика, который соответствует приоритету 1, 3 или 5.

```
Switch#configure terminal
Switch(config)#class-map type network-qos match-any my_class_map
Switch(config-cmap-nq)#match cos 3
Switch(config-cmap-nq)#match cos 1
Switch(config-cmap-nq)#match cos 5
Switch(config-cmap-nq)#exit
Switch(config)#policy-map type network-qos my_policy_map
Switch(config-pmap-nq)#class type network-qos my_class_map
Switch(config-pmap-c-nq)#pause
Switch(config-pmap-c-nq)#
```

84.2 class-map type network-qos match-any

Данная команда используется для создания или изменения карты классов сетевого QoS, в которой определены критерии соответствия пакетов.

class-map type network-qos match-any *NAME*

Параметры

NAME	Укажите имя карты класса. Максимальное количество символов – 32.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда глобальной конфигурации **class-map type network-qos match-any** используется для указания имени карты классов сетевого QoS или создания/изменения критериев соответствия карты классов. В карте классов могут быть установлены несколько критериев соответствия на основе логического оператора OR (ИЛИ). Команда **class-map type network-qos match-any** и ее подкоманды применяется для того, чтобы определить классификацию пакетов. С помощью этой команды осуществляется вход в режим конфигурации карты классов (Class-map Configuration Mode).

Для определения или изменения критериев соответствия используйте следующие команды:

- **match cos**: определение класса трафика в карте классов сетевого QoS.
- **no match cos**: удаление критериев соответствия из карты классов.

Пример

В данном примере показано, как создать карту классов сетевого QoS под именем «my_class_map».

```
Switch#configure terminal
Switch(config)#class-map type network-qos match-any my_class_map
Switch(config-cmap-nq)#
```

84.3 pause

Данная команда используется, чтобы включить управление потоком на основе приоритета (Priority-based Flow Control, PFC) в классе, указанном в карте политик сетевого QoS. Для отключения PFC в классе воспользуйтесь формой **no** этой команды.

pause

no pause

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Policy Map Type Network-QoS Class Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Priority-based Flow Control (PFC) используется на интерфейсах Ethernet, чтобы обеспечить сервис без потерь пакетов.

PFC, определенный стандартом IEEE 802.1Qbb, расширяет основную спецификацию IEEE 802.3x PAUSE и применяет значения приоритетов IEEE 802.1p CoS в теге IEEE 802.1Q VLAN для определения до восьми классов CoS, для которых может независимо осуществляться управление потоком.

Если PFC всех приоритетов отключен, интерфейс возвращается к настройкам управления потоком IEEE 802.3x по умолчанию. При включении PFC какого-либо приоритета на интерфейсе будут распознаны кадры PFC PAUSE. Другими словами, на коммутаторе будет приостановлен тот класс CoS, на котором включен PFC и для которого принят кадр PFC PAUSE. Кадр PFC PAUSE будет передаваться при обнаружении перегрузки в CoS с включенным PFC.

Для включения PFC по классам CoS необходимо выполнить следующее:

- Введите команду **class-map type network-qos match-any global configuration** для создания карты классов сетевого QoS.

  ◦ Воспользуйтесь командой **match cos class-map configuration,** чтобы указать класс CoS для конфигурации.

- Используйте команду **policy-map type network-qos** для создания карты политик сетевого QoS.

  ◦ Примените команду **class type network-qos policy-map configuration** для указания карты классов сетевого QoS, которая будет ассоциирована с политикой трафика, с дальнейшим переходом в режим конфигурации класса policy-map type network QoS.

  ◦ Введите команду **pause policy map type network-qos class configuration** для включения PFC в классе, указанном в карте политик сетевого QoS.

- Используйте команду **service-policy type network-qos input** в режиме Interface Configuration Mode для применения карты политик сетевого QoS.

Пример

В данном примере показано, как включить PFC на приоритетах 3 и 4 на интерфейсе Ethernet 1/0/3.

Шаг 1: Создайте карту классов сетевого QoS под именем «my_class_map» и установите критерии для соответствия CoS 3 или 4.

```
Switch#configure terminal
Switch(config)#class-map type network-qos match-any my_class_map
Switch(config-cmap-nq)#match cos 3
Switch(config-cmap-nq)#match cos 4
Switch(config-cmap-nq)#
```

Шаг 2: Создайте карту политик сетевого QoS под именем «my_policy_map» и включите PFC для класса «my_class_map», который был создан в шаге 1.

```
Switch#configure terminal
Switch(config)#policy-map type network-qos my_policy_map
Switch(config-pmap-nq)#class type network-qos my_class_map
Switch(config-pmap-c-nq)#pause
Switch(config-pmap-c-nq)#exit
Switch(config-pmap-nq)#
```

Шаг 3: Примените карту политик сетевого QoS «my_policy_map», созданную в шаге 2 на интерфейсе Ethernet 1/0/3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#service-policy type network-qos input my_policy_map
Switch(config-if)#
```

84.4 policy-map type network-qos

Данная команда используется для входа в режим Policy-map Configuration Mode и создания или изменения карты политик сетевого QoS, которая может быть присоединена к одному или нескольким интерфейсам.

policy-map type network-qos *NAME*

Параметры

NAME	Укажите имя карты политик сетевого QoS. Максимальное количество буквенно-цифровых 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 для настройки или изменения политики для класса трафика.

Для настройки критерия соответствия для класса используйте команды **class-map type network-qos match-any** и **match cos**.

Одна карта политик может быть присоединена одновременно к нескольким интерфейсам. Последующий ввод команды policy-map type network QoS перезаписывает предыдущие настройки.

Примените следующие команды в режиме Policy-map Configuration Mode для присоединения карты классов к карте политик или ее отсоединения:

- **class type network-qos:** присоединение карты классов сетевого QoS, определяющей критерии классификации, к карте политик и осуществление входа в режим Policy-map Configuration Mode.
- **no class:** удаление карты классов из этой карты политик.

Карты политик сетевого QoS могут содержать более одного класса трафика при использовании команды **class type network-qos policy-map**.

Присоедините карту политик сетевого QoS к интерфейсу в точке входа с помощью команды **service-policy type network-qos input interface configuration**.

Пример

В данном примере показано, как войти в режим Policy-map Configuration Mode.

```
Switch#configure terminal
Switch(config)#policy-map type network-qos my_policy_map
Switch(config-pmap-nq)#
```

84.5 service-policy type network-qos input

Данная команда используется для присоединения карты политик сетевого QoS к входному интерфейсу.

service-policy type network-qos input *NAME*

Параметры

NAME	Укажите имя карты политик сетевого QoS, созданное командой **policy-map type network-qos**, для присоединения. Максимальное количество буквенно-цифровых символов – 32.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для присоединения единой карты политик сетевого QoS к входным интерфейсам. Карта политик не обязательно должна быть создана до указания ее в этой команде. При ассоциации с несуществующей политикой команда не будет применена. Если в карте политик ничего не указано, никаких действий выполняться не будет.

Кроме одной карты политики (без указания названия типа) для каждого типа (входящего или исходящего) на интерфейсе, можно применить до одной карты политики сетевого QoS на физическом входном порту.

Пример

В данном примере показано, как применить карту политик «policy1» к физическому входному интерфейсу.

```
Switch#configure terminal
Switch(config)#interface eth1/0/26
Switch(config-if)#service-policy type network-qos input my_policy_map
Switch(config-if)#
```

84.6 show class-map type network-qos

Данная команда используется для отображения конфигурации карты классов сетевого QoS.

show class-map type network-qos [*NAME***]**

Параметры

NAME	(Опционально.) Укажите имя карты классов. Максимальное количество буквенно-цифровых символов – 32.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения карт классов сетевого QoS. Если указан параметр *NAME*, будет отображена информация об указанной в параметре карте классов сетевого QoS и ее критерии соответствия.

Пример

В данном примере показано, как отобразить все карты классов сетевого QoS.

```
Switch#show class-map type network-qos

Type network-qos class-maps
===========================
Class Map my_class_map
match cos 3,4

Class Map my_class_map_2
  match cos 2

Class Map my_class_map_3
  match cos 5

Switch#
```

84.7 show policy-map interface

Данная команда используется для отображения конфигурации карт политик на указанном интерфейсе.

show policy-map interface *INTERFACE-ID*

Параметры

INTERFACE-ID	Укажите ID интерфейса.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения конфигурации карты политик, если она была присоединена к указанному интерфейсу.

Пример

В данном примере показано, как отобразить конфигурацию карты политик, если она была присоединена к указанному интерфейсу.

```
Switch#show policy-map interface eth1/0/1

Policy Map: policy1(network-qos) : input
Class Map my_class_map_2

pause
Policy Map: policy2 : input
  Class Map police
police cir 500000 bc 10000 pir 1000000 be 10000 exceed-action set-dscp-transmit 2 violate-
action drop

Switch#
```

84.8 show policy-map type network-qos

Данная команда используется для отображения конфигурации карты политик сетевого QoS.

show policy-map type network-qos [*POLICY-NAME* **| interface** *INTERFACE-ID***]**

Параметры

POLICY-NAME	(Опционально.) Укажите имя карты политик. Если имя не указано, будут отображаться все карты политик сетевого QoS.
interface *INTERFACE-ID*	(Опционально.) Укажите номер модуля и порта.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения политик классов, настроенных в карте политик сетевого QoS. Чтобы отобразить все существующие карты политик, примените команду **show policy-map** без указания ключевого слова **type network-qos**. Для отображения конфигурации карты политик сетевого QoS укажите интерфейс с ключевым словом **interface**.

Пример

В данном примере показано, как отобразить все карты политик сетевого QoS.

```
Switch#show policy-map type network-qos

 Type network-qos policy-maps
 ============================
 Policy Map my_policy_map
  Class Map my_class_map
    pause

Switch#
```

85. Команды Remote Network MONitoring (RMON)

85.1 rmon collection stats

Данная команда используется для включения статистики RMON на настраиваемом интерфейсе. Чтобы отключить статистику, воспользуйтесь формой **no** этой команды.

rmon collection stats *INDEX* **[owner** *NAME***]**
no rmon collection stats *INDEX*

Параметры

INDEX	Укажите индекс таблицы RMON. Диапазон значений: от 1 до 65535.
owner *NAME*	Укажите имя владельца. Максимальное 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

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

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 eth1/0/2
Switch(config-if)#rmon collection stats 65 owner guest
Switch(config-if)#
```

85.2 rmon collection history

Данная команда используется для включения сбора истории статистики RMON MIB на настраиваемом интерфейсе. Чтобы отключить сбор истории статистики на интерфейсе, воспользуйтесь формой **no** этой команды.

rmon collection history *INDEX* **[owner** *NAME***] [buckets** *NUM***] [interval** *SECONDS***]**
no rmon collection history *INDEX*

Параметры

INDEX	Укажите индекс таблицы RMON. Диапазон значений: от 1 до 65535.
owner *NAME*	Укажите имя владельца. Максимальное количество символов в строке – 127.
buckets *NUM*	Укажите количество ячеек для сбора истории по группе статистики RMON. 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). 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

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

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 eth1/0/8
Switch(config-if)#rmon collection history 101 owner it@domain.com interval 2000
Switch(config-if)#
```

85.3 rmon alarm

Данная команда используется для настройки записи уровня alarm (тревога) для мониторинга интерфейса. Чтобы удалить запись уровня alarm, воспользуйтесь формой **no** этой команды.

rmon alarm *INDEX VARIABLE INTERVAL* **{delta | absolute} rising-threshold** *VALUE* **[***RISING-EVENT-NUMBER***] falling-threshold** *VALUE* **[***FALLING-EVENT-NUMBER***] [owner** *STRING***]**

no rmon alarm *INDEX*

Параметры

INDEX	Укажите индекс alarm. Диапазон значений: от 1 до 65535.
VARIABLE	Укажите идентификатор объекта переменной для выборки.
INTERVAL	Укажите интервал в секундах для выборки переменной и проверки соответствия пороговых значений. 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. Диапазон значений: от 0 до 2147483647.
RISING-EVENT-NUMBER	(Опционально.) Укажите индекс записи события, при котором превышено заданное верхнее пороговое значение. 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. Диапазон значений: от 0 до 2147483647.
FALLING-EVENT-NUMBER	(Опционально.) Укажите индекс записи события, при котором достигнуто заданное нижнее пороговое значение. 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 допустимое количество символов – 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)#
```

85.4 rmon event

Данная команда используется для настройки записи события. Чтобы удалить запись события, воспользуйтесь формой **no** этой команды.

rmon event *INDEX* **[log] [[trap** *COMMUNITY***] [owner** *NAME***] [description** *TEXT***]**

no rmon event *INDEX*

Параметры

INDEX	Укажите индекс записи alarm. Доступный диапазон значений: от 1 до 65535.
log	(Опционально.) Укажите, чтобы генерировать сообщения в системном журнале для уведомлений.
trap *COMMUNITY*	(Опционально.) Укажите, чтобы генерировать сообщения SNMP trap для уведомлений. Максимальное количество символов – 127.
owner *NAME*	Укажите имя владельца. Максимальное количество символов – 127.
description *TEXT*	(Опционально.) Укажите описание для записи события RMON. Максимальное 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)#
```

85.5 show rmon alarm

Данная команда используется для отображения конфигурации alarm.

show rmon alarm

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить таблицу RMON alarm.

Пример

В данном примере показано, как отобразить таблицу RMON alarm.

```
Switch#show rmon alarm

Alarm index 23, owned by IT
  Monitors OID: 1.3.6.1.2.1.2.2.1.10.1
  every 120 second(s)
  Taking delta samples, last value was 2500
  Rising threshold is 2000, assigned to event 12
  Falling threshold is 1100, assigned to event 12
  On startup enable rising or falling alarm

Switch#
```

85.6 show rmon events

Данная команда используется для отображения таблицы событий RMON.

show rmon events

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить таблицу событий RMON.

Пример

В данном примере показано, как отобразить таблицу событий RMON.

```
Switch#show rmon events

Event 1, owned by manager1
  Description is Errors
  Event trigger action: log & trap sent to community manager
  Last triggered time: 13:12:15, 2013-03-02

Event 2, owned by manager2
  Description is Errors
  Event trigger action: log & trap
  Last triggered time:

Switch#
```

85.7 show rmon history

Данная команда используется для отображения информации об истории статистики RMON.

show rmon history

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить историю статистики для всех настроенных записей.

Пример

В данном примере показано, как отобразить историю статистики RMON Ethernet.

```
Switch#show rmon history

Index 23, owned by Manager, Data source is eth1/0/2
  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#
```

85.8 show rmon statistics

Данная команда используется для отображения статистики RMON Ethernet.

show rmon statistics

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статистику для всех настроенных записей.

Пример

В данном примере показано, как отобразить статистику RMON.

```
Switch#show rmon statistics

Index 32, owned by it@domain.com, Data Source is  eth1/0/3
  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#
```

85.9 snmp-server enable traps rmon

Данная команда используется для включения отправки RMON trap. Чтобы отключить отправку RMON trap, воспользуйтесь формой **no** этой команды.

snmp-server enable traps rmon [rising-alarm | falling-alarm]

no snmp-server enable traps rmon [rising-alarm | falling-alarm]

Параметры

rising-alarm	(Опционально.) Укажите, чтобы настроить отправку trap, уведомляющих о поднятии тревоги.
recursive	(Опционально.) Укажите, чтобы настроить отправку trap, уведомляющих об отмене тревоги.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить/отключить отправку RMON trap.

Пример

В данном примере показано, как включить отправку RMON trap, уведомляющих о поднятии и об отмене тревоги.

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

86. Команды Reset Button

86.1 reset-button reboot

Данная команда используется, чтобы включить для кнопки Reset функцию перезапуска коммутатора. Для отключения функции воспользуйтесь формой **no** этой команды.

reset-button reboot enable
no reset-button reboot

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 включить для кнопки Reset функцию перезапуска коммутатора. Если функция включена, нажмите и удерживайте кнопку Reset в течение 5 секунд, чтобы перезапустить коммутатор.

Пример

В данном примере показано, как отключить функцию перезапуска для кнопки Reset.

```
Switch#configure terminal
Switch(config)#no reset-button reboot
Switch(config)#
```

86.2 reset-button ztp

Данная команда используется, чтобы включить для кнопки Reset функцию Zero Touch Provisioning (ZTP). Для отключения функции воспользуйтесь формой **no** этой команды.

reset-button ztp enable
no reset-button ztp

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 включить для кнопки Reset функцию ZTP. Если функция включена, нажмите и удерживайте кнопку Reset от 5 до 10 секунд, чтобы запустить функцию ZTP. После запуска функции ZPT на коммутаторе будут получены и применены изображение и настройки интерфейса VLAN 1 при помощи DHCP и TFTP. Если процесс ZPT активен, все индикаторы будут мигать зеленым.

После перезапуска коммутатор будет использовать загруженное изображение и настройки. При ошибке загрузки все индикаторы будут гореть оранжевым, изображение и настройки останутся неизменными, а перезапуск коммутатора выполнен не будет. Чтобы вернуть нормальный режим работы индикаторов, нажмите кнопку Reset.

Пример

В данном примере показано, как отключить функцию ZPT для кнопки Reset.

```
Switch#configure terminal
Switch(config)#no reset-button ztp
Switch(config)#
```

86.3 reset-button factory

Данная команда используется, чтобы включить для кнопки Reset функцию возврата к заводским настройкам. Для отключения функции воспользуйтесь формой **no** этой команды.

reset-button factory enable
no reset-button factory

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 включить для кнопки Reset функцию возврата к заводским настройкам. Если функция включена, нажмите и удерживайте кнопку Reset более 10 секунд, чтобы вернуться к заводским настройкам.

Пример

В данном примере показано, как отключить функцию возврата к заводским настройкам для кнопки Reset.

```
Switch#configure terminal
Switch(config)#no reset-button factory
Switch(config)#
```

87. Команды Route Map

87.1 match interface

Данная команда используется для настройки правила соответствия маршрутов исходящим интерфейсам. Чтобы отменить правило, воспользуйтесь формой **no** этой команды.

match interface *INTERFACE-ID*
no match interface

Параметры

INTERFACE-ID	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 vlan1
Switch(config-route-map)#
```

87.2 match ip address

Данная команда используется для настройки правила соответствия маршрута на основе стандартного списка доступа IP или списка IP-префиксов. Чтобы отменить правило, воспользуйтесь формой **no** этой команды.

match ip address *ACCESS-LIST-NAME*
no match ip address *ACCESS-LIST-NAME*

Параметры

ACCESS-LIST-NAME	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)#
```

87.3 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

ACCESS-LIST-NAME	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, чтобы настроить правило соответствия маршрутов следующему узлу, 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 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)#
```

87.4 match ip route-source

Данная команда используется для настройки правила соответствия маршрутов IP-адресу исходного маршрутизатора на основе стандартного списка доступа IP. Чтобы отменить правило, воспользуйтесь формой **no** этой команды.

match ip route-source *ACCESS-LIST-NAME*

no match ip route-source

Параметры

ACCESS-LIST-NAME	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)#
```

87.5 match ipv6 address

Данная команда используется для настройки правила соответствия маршрутов на основе стандартного списка доступа IPv6. Чтобы отменить правило, воспользуйтесь формой **no** этой команды.

match ipv6 address *ACCESS-LIST-NAME*
no match ipv6 address *ACCESS-LIST-NAME*

Параметры

ACCESS-LIST-NAME	Укажите имя стандартного или расширенного списка доступа IPv6.

По умолчанию

Нет.

Режим ввода команды

Route-map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить правило соответствия маршрутов списку доступа IPv6.

Пример

В данном примере показано, как создать список доступа IPv6 «myacl6»и запись карты маршрутов с соответствием списку доступа IPv6.

```
Switch#configure terminal
Switch(config)#ipv6 access-list myacl6
Switch(config-ipv6-acl)#permit 1000::/64
Switch(config-ipv6-acl)#exit
Switch(config)#route-map mypolicy permit 1
Switch(config-route-map)#match ipv6 address myacl6
Switch(config-route-map)#
```

87.6 match ipv6 next-hop

Данная команда используется для настройки правила соответствия маршрутов следующему узлу (next hop) на основе стандартного списка доступа IPv6. Чтобы отменить правило, воспользуйтесь формой **no** этой команды.

match ipv6 next-hop *ACCESS-LIST-NAME*
no match ipv6 next-hop *ACCESS-LIST-NAME*

Параметры

ACCESS-LIST-NAME	Укажите имя списка доступа IPv6.

По умолчанию

Нет.

Режим ввода команды

Route-map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить правило соответствия маршрутов следующему узлу (next hop), IP-адрес которого будет проверен в соответствии со стандартным списком доступа IPv6.

Пример

В данном примере показано, как создать список доступа IPv6 «myacl6» и запись карты маршрутов с соответствием следующему узлу (next hop) на основе списка доступа IPv6.

```
Switch#configure terminal
Switch(config)#ipv6 access-list myacl6
Switch(config-ipv6-acl)#permit 1000::/64 any
Switch(config-ipv6-acl)#exit
Switch(config)#route-map mypolicy permit 1
Switch(config-route-map)#match ipv6 next-hop myacl6
Switch(config-route-map)#
```

87.7 match metric

Данная команда используется для настройки правила соответствия метрики (metric) маршрутов. Чтобы отменить правило, воспользуйтесь формой **no** этой команды.

match metric *VALUE*
no match 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 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)#
```

87.8 match route-type

Данная команда используется для настройки правила соответствия типа маршрутов OSPF. Чтобы отменить правило, воспользуйтесь формой **no** этой команды.

match route-type {internal | external [type-1 | type-2]}

no match route-type {internal | external [type-1 | type-2]}

Параметры

internal	Укажите внутризоновые (intra-area) и межзоновые (inter-area) маршруты OSPF.
external	Укажите внешний маршрут OSPF автономной системы. Если параметры **type-1** и **type-2** не указаны, включены оба типа внешних маршрутов.
type-1	(Опционально.) Укажите внешний маршрут OSPF type-1.
type-2	(Опционально.) Укажите внешний маршрут OSPF type-2.

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 типа маршрутов OSPF.

Пример

В данном примере показано, как создать запись карты маршрутов с соответствием внутреннему (internal) маршруту OSPF.

```
Switch#configure terminal
Switch(config)#route-map myPolicy permit 1
Switch(config-route-map)#match route-type internal
Switch(config-route-map)#
```

87.9 route map

Данная команда используется для создания записи правила карты маршрутов (route map). Чтобы удалить запись правила карты маршрутов, воспользуйтесь формой **no** этой команды.

route-map *MAP-NAME* **{permit | deny}** *SEQ-NUMBER*
no route-map *MAP-NAME* **{permit | deny}** *SEQ-NUMBER*

Параметры

MAP-NAME	Укажите имя карты маршрутов.
permit	Укажите, чтобы разрешить маршруты, соответствующие записи правила.
deny	Укажите, чтобы заблокировать маршруты, соответствующие записи правила.
SEQ-NUMBER	Укажите порядковый номер записи карты маршрутов. 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, при этом записи разрешения (permit) и запрета (deny) могут быть указаны одновременно. 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)#
```

87.10 show route-map

Данная команда используется для отображения информации о карте маршрутов.

show route-map [*ROUTE-MAP-NAME***]**

Параметры

ROUTE-MAP-NAME	(Опционально.) Укажите карту маршрутов для отображения.

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 карте маршрута.

Пример

В данном примере показано, как отобразить информацию о карте маршрута.

```
Switch#show route-map

Route Map mypolicy, 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#
```

87.11 set ip default next-hop

Данная команда используется, чтобы настроить следующий узел по умолчанию (default next hop) для маршрутизации пакетов, которые соответствуют настроенным правилам последовательностей карты маршрутов. Для удаления определенных следующих узлов по умолчанию воспользуйтесь формой **no** этой команды.

set ip default next-hop *IP-ADDRESS* **[...***IP-ADDRESS***]**

no set ip default next-hop *IP-ADDRESS* **[...***IP-ADDRESS***]**

Параметры

IP-ADDRESS	Укажите IP-адрес default next hop 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. Настроенный список – Strict-Control. Затем создается карта маршрутов, соответствующая IP-адресу из списка префиксов созданного списка «Strict-Control». Заданная 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 default next-hop 120.1.2.2
Switch(config-route-map)#exit
Switch(config)#interface vlan100
Switch(config-if)#ip policy route-map myPolicy
Switch(config-if)#
```

87.12 set ip next-hop

Данная команда используется, чтобы настроить на маршрутизаторе следующий узел (next hop) для маршрутизации пакетов, которые соответствуют настроенным правилам последовательностей карты маршрутов. Для удаления определенных next hop воспользуйтесь формой **no** этой команды.

set ip next-hop {*IP-ADDRESS* **[...***IP-ADDRESS***] | recursive** *IP-ADDRESS***}**
no set ip next-hop {*IP-ADDRESS* **[...***IP-ADDRESS***] | recursive** *IP-ADDRESS***}**

Параметры

IP-ADDRESS	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

Используйте данную команду, чтобы настроить несколько 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.

IP-адрес рекурсивного next hop установлен в таблице маршрутизации и может существовать в подсети, напрямую не подключенной к нему. Если IP-адрес рекурсивного next hop недоступен, для маршрутизации пакетов используется маршрут по умолчанию.

Если IP-адрес next hop и рекурсивного next hop находятся в одной записи карты маршрута, используется IP-адрес следующего next hop. Если IP-адрес следующего next hop недоступен, используется IP-адрес рекурсивного next hop.

Если в команде policy-based routing используются другие правила, их приоритет должен быть следующим:

1. **set ip next-hop**
2. **set ip 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. Настроенный список – Strict-Control. Затем создается карта маршрутов, соответствующая

IP-адресу из списка префиксов созданного списка «Strict-Control». Заданная 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 vlan100
Switch(config-if)#ip policy route-map myPolicy
Switch(config-if)#
```

87.13 set ip precedence

Данная команда используется, чтобы настроить значение приоритета (precedence) для заголовка IP. Для удаления настроек воспользуйтесь формой **no** этой команды.

set ip precedence {*NUMBER* **|** *NAME***}**

no set ip precedence

Параметры

NUMBER	Укажите одно из нижеперечисленных значений приоритета для заголовка IP: • 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. Указанное 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)#
```

87.14 set ipv6 default next-hop

Данная команда используется, чтобы настроить следующий узел по умолчанию (default next hop) для маршрутизации пакетов, которые соответствуют настроенным правилам последовательностей карты маршрутов. Чтобы удалить определенные следующие узлы по умолчанию, воспользуйтесь формой **no** этой команды.

set ipv6 default next-hop *IPV6-ADDRESS* **[...***IPV6-ADDRESS***]**
no set ipv6 default next-hop *IPV6-ADDRESS* **[...***IPV6-ADDRESS***]**

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес default next hop для маршрутизации пакетов.

По умолчанию

Нет.

Режим ввода команды

Route-map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для маршрутов на основе политики IPv6. 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 показано, как настроить default next hop для маршрутизации пакетов, которые соответствуют настроенным правилам последовательностей карты маршрутов.

```
Switch#configure terminal
Switch(config)#ipv6 access-list ipacl1
Switch(config-ip-acl)#permit 1000::/64 any
Switch(config-ip-acl)#exit
Switch(config)#route-map mypolicy permit 1
Switch(config-route-map)#match ipv6 address ipacl1
Switch(config-route-map)#set ipv6 default next-hop 2000::1
Switch(config-route-map)#exit
Switch(config)#interface vlan1
Switch(config-if)#ip policy route-map mypolicy
Switch(config-if)#
```

87.15 set ipv6 next-hop

Данная команда используется, чтобы настроить следующий узел (next hop) для маршрутизации пакетов, которые соответствуют настроенным правилам последовательностей карты маршрутов. Чтобы удалить определенные следующие узлы, воспользуйтесь формой **no** этой команды.

set ipv6 next-hop {*IPV6-ADDRESS* **[...***IPV6-ADDRESS***] | recursive** *IPV6-ADDRESS***}**
no set ipv6 next-hop {*IPV6-ADDRESS* **[...***IPV6-ADDRESS***] | recursive** *IPV6-ADDRESS***}**

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес next hop для маршрутизации пакетов.
recursive	Укажите IPv6-адрес рекурсивного next hop маршрутизатора.

По умолчанию

Нет.

Режим ввода команды

Route-map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применяется для указания нескольких IPv6 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.

IP-адрес рекурсивного next hop установлен в таблице маршрутизации и может существовать в подсети, напрямую не подключенной к нему. Если IP-адрес рекурсивного next hop недоступен, для маршрутизации пакетов используется маршрут по умолчанию.

Если IP-адрес next hop и рекурсивного next hop находятся в одной записи карты маршрута, используется IP-адрес следующего next hop. Если IP-адрес следующего next hop недоступен, используется IP-адрес рекурсивного next hop.

Если в команде policy-based routing используются другие правила, их приоритет должен быть следующим:

1. **set ipv6 next-hop**
2. **set ipv6 default next-hop**

Пример

В данном примере показано, как настроить next-hop для маршрутизации пакетов, которые соответствуют настроенным правилам последовательностей карты маршрутов.

```
Switch#configure terminal
Switch(config)#ipv6 access-list ipacl1
Switch(config-ipv6-acl)#permit 1000::/64 any
Switch(config-ipv6-acl)#exit
Switch(config)#route-map mypolicy permit 1
Switch(config-route-map)#match ipv6 address ipacl1
Switch(config-route-map)#set ipv6 next-hop 2000::1
Switch(config-route-map)#
```

87.16 set ipv6 precedence

Данная команда используется, чтобы настроить значение приоритета (precedence) для заголовка IPv6. Для удаления настроек воспользуйтесь формой **no** этой команды.

set ipv6 precedence {*NUMBER* **|** *NAME***}**
no set ipv6 precedence

Параметры

NUMBER	Укажите одно из нижеперечисленных значений приоритета для заголовка IP: • 0 – Routine • 1 – Priority • 2 – Immediate • 3 – Flash • 4 – Flash-override • 5 – Critical • 6 – Internet

	• 7 – Network
NAME	Укажите имя приоритета для заголовка IPv6.

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 IPv6. Команда доступна, только если политика маршрутизации включает в себя пакеты IPv6. Приоритет можно установить при помощи номера или соответствующего имени.

Пример

В данном примере показано, как настроить значение приоритета IPv6 для пакетов, соответствующих карте маршрутов. Указанное значение – 5 (критическое).

```
Switch#configure terminal
Switch(config)#route-map example permit 10
Switch(config-route-map)#match ip address ipacl1
Switch(config-route-map)#set ipv6 precedence 5
Switch(config-route-map)#
```

87.17 set metric

Данная команда используется для изменения метрики маршрутов. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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. Указанная 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)#
```

87.18 set metric-type

Данная команда используется для указания типа внешнего (external) маршрута OSPF автономной системы.

set metric-type {type-1 | type-2}

no set metric-type

Параметры

type-1	Укажите, чтобы использовать внешний (external) маршрут OSPF с метрикой type-1.
type-2	Укажите, чтобы использовать внешний (external) маршрут OSPF с метрикой type-2.

По умолчанию

Нет.

Режим ввода команды

Route-map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы указать тип внешнего маршрута OSPF автономной системы.

Пример

В данном примере показано, как настроить тип внешних маршрутов OSPF автономной системы, которые соответствуют карте маршрутов. Указанный тип маршрута – type-2.

```
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-type type-2
Switch(config-route-map)#
```

88. Команды Router Advertisement (RA) Guard

88.1 ipv6 nd raguard policy

Данная команда используется для создания политики Router Advertisement (RA) Guard Policy и для входа в режим RA Guard Policy Configuration Mode. Чтобы удалить политику RA Guard Policy, воспользуйтесь формой **no** этой команды.

ipv6 nd raguard policy *POLICY-NAME*
no ipv6 nd raguard policy *POLICY-NAME*

Параметры

POLICY-NAME	Укажите имя политики IPv6 RA Guard Policy.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы создать политику RA Guard Policy и войти в режим RA Guard Policy Configuration Mode.

Пример

В данном примере показано, как создать политику RA Guard Policy под именем «policy1».

```
Switch#configure terminal
Switch(config)#ipv6 nd raguard policy policy1
Switch(config-ra-guard)#
```

88.2 device-role

Данная команда используется для настройки роли подключенного устройства. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

device-role {host | router}
no device-role

Параметры

host	Укажите, чтобы настроить подключенное устройство в качестве узла.
router	Укажите, чтобы настроить подключенное устройство в качестве маршрутизатора.

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)#
```

88.3 match ipv6 access-list

Данная команда используется для фильтрации RA-сообщений на основе IPv6-адреса отправителя. Чтобы отключить фильтрацию, воспользуйтесь формой **no** этой команды.

match ipv6 access-list *IPV6-ACCESS-LIST-NAME*

no match ipv6 access-list

Параметры

IPV6-ACCESS-LIST-NAME	Укажите стандартный список доступа IPv6.

По умолчанию

Нет.

Режим ввода команды

RA Guard Policy Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для устройства в роли маршрутизатора (router), чтобы отфильтровать RA-сообщения на основе IP-адреса отправителя. Если команда **match ipv6 access-list** не настроена, все RA-сообщения будут игнорироваться. Список доступа настраивается с помощью команды **ipv6 access-list**.

Пример

В данном примере показано, как создать политику RA Guard Policy и настроить проверку соответствия IPv6-адресов списку доступа «list1».

```
Switch#configure terminal
Switch(config)#ipv6 nd raguard policy raguard1
Switch(config-ra-guard)#match ipv6 access-list list1
Switch(config-ra-guard)#
```

88.4 ipv6 nd raguard attach-policy

Данная команда используется для применения политики RA Guard Policy на определенном интерфейсе. Чтобы удалить привязку, воспользуйтесь формой **no** этой команды.

ipv6 nd raguard attach-policy [*POLICY-NAME***]**
no ipv6 nd raguard

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики RA Guard Policy.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Может быть применена только одна политика RA Policy. Если имя политики не указано, политика по умолчанию настроит устройство в качестве узла.

Пример

В данном примере показано, как применить политику RA Guard Policy на интерфейсе Ethernet 1/0/3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 nd raguard attach-policy raguard1
Switch(config-if)#
```

88.5 show ipv6 nd raguard policy

Данная команда используется для отображения информации о политике IPv6 RA Guard Policy.

show ipv6 nd raguard policy [*POLICY-NAME***]**

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики IPv6 RA Guard Policy.

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 политике RA Guard Policy. Если параметры не указаны, будет отображена информация для всех политик.

Пример

В данном примере показано, как отобразить информацию о политике RA Guard Policy «raguard1».

```
Switch(config)#show ipv6 nd raguard policy raguard1

Policy raguard1 configuration:
    Device Role: host
    Source Address Match Access List: list1
    Target: eth1/0/3

Switch(config)#
```

89. Команды Routing Information Protocol (RIP)

89.1 default-metric (RIP)

Данная команда используется, чтобы указать значение метрики (metric) по умолчанию для маршрутов, перераспределяемых RIP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

default-metric *METRIC-VALUE*
no default-metric

Параметры

METRIC-VALUE	Укажите значение метрики по умолчанию. Диапазон значений: 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 RIP. Для синхронизации метрики необходимо указать ее значение повторно.

Пример

В данном примере показано, как настроить значение метрики по умолчанию для маршрутов, перераспределяемых OSPF. Заданное значение – 5.

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#default-metric 5
Switch(config-router)#redistribute ospf
Switch(config-router)#
```

89.2 distance (RIP)

Данная команда используется, чтобы указать административное расстояние (administrative distance) маршрутов, информация о которых была получена от протоколов маршрутизации IPv4. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

distance *DISTANCE*
no distance

Параметры

DISTANCE	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 надежности маршрута. В качестве расстояния может быть указано целое число от 1 до 255. У маршрута, значение расстояния которого ниже, будет более высокий приоритет, чем у маршрута со значением выше.

Пример

В данном примере показано, как настроить расстояние маршрутов RIP. Заданное значение – 100.

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#distance 100
Switch(config-router)#
```

89.3 ip rip authentication mode

Данная команда позволяет указать тип аутентификации, который используется для пакетов RIP version 2. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 vlan2
Switch(config-if)#ip rip authentication mode text
Switch(config-if)#
```

89.4 ip rip authentication text-password

Данная команда позволяет включить аутентификацию для пакетов RIP version 2 и указать ключ, который будет использоваться на интерфейсе. Чтобы отменить аутентификацию, воспользуйтесь формой **no** этой команды.

ip rip authentication text-password *PASSWORD*
no ip rip authentication text-password

Параметры

PASSWORD	Укажите пароль.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется, чтобы включить аутентификацию для пакетов RIP version 2 и указать ключ, который будет использоваться на интерфейсе.

Пример

В данном примере показано, как настроить аутентификацию на интерфейсе VLAN 3.

```
Switch#configure terminal
Switch(config)#interface vlan3
Switch(config-if)#ip rip authentication mode text
Switch(config-if)#ip rip authentication text-password test1
Switch(config-if)#
```

89.5 ip rip receive version

Данная команда используется, чтобы указать RIP version для пакетов, которые будут получены на интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 vlan1
Switch(config-if)#ip rip receive version 1 2
Switch(config-if)#
```

89.6 ip rip send version

Данная команда используется, чтобы указать RIP version для пакетов, которые будут отправлены с интерфейса. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 vlan100
Switch(config-if)#ip rip send version 1
Switch(config-if)#
```

89.7 ip rip v2-broadcast

Данная команда используется для включения отправки пакетов обновлений состояния сети RIP version 2 в качестве широковещательных (broadcast) пакетов, а не многоадресных (multicast) пакетов. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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 многоадресные пакеты вместо широковещательных пакетов в целях снижения нагрузки на ненужных узлах в локальной сети при обработке широковещательных пакетов.

Используйте данную команду, чтобы настроить широковещательную рассылку обновлений RIP version 2 на устройствах, 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  vlan100
Switch(config-if)#ip rip send version 2
Switch(config-if)#ip rip v2-broadcast
Switch(config-if)#
```

89.8 network

Данная команда применяется для указания сети, в которой будет использоваться RIP. Чтобы удалить запись, воспользуйтесь формой **no** этой команды.

network *NETWORK-PREFIX*
no network *NETWORK-PREFIX*

Параметры

NETWORK-PREFIX	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)#
```

89.9 passive-interface

Данная команда используется для отключения отправки обновлений маршрутизации на интерфейсе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

passive-interface {default | *INTERFACR-ID***}**

no passive-interface {default | *INTERFACR-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. 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 отправку обновлений маршрутизации на интерфейсе VLAN 1.

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#passive-interface vlan1
Switch(config-router)#
```

89.10 redistribute (RIP)

Данная команда используется для перераспределения маршрутов из других доменов маршрутизации в RIP. Чтобы отменить перераспределение маршрута из определенного протокола, воспользуйтесь формой **no** этой команды.

redistribute *PROTOCOL* **[metric** *METRIC-VALUE*] **[route-map** *MAP-NAME*]
no redistribute *PROTOCOL* **[metric** *METRIC-VALUE*] **[route-map** *MAP-NAME*]

Параметры

PROTOCOL	Укажите протокол, маршруты которого необходимо перераспределить. Доступны следующие ключевые слова: **connected**, **ospf** и **static**. Укажите **static** для перераспределения статических IP-маршрутов. Укажите **connected** для перераспределения маршрутов, установленных автоматически на основе настроек IP-адреса на интерфейсе.
metric *METRIC-VALUE*	(Опционально.) Укажите значение метрики для перераспределяемых маршрутов. Диапазон значений: от 0 до 16.
route-map *MAP-NAME*	(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. Новое значение метрики – 10.

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#redistribute ospf  metric 10
Switch(config-router)#
```

89.11 router rip

Данная команда используется для настройки маршрутизации RIP. Чтобы отключить маршрутизацию RIP, воспользуйтесь формой **no** этой команды.

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. Для удаления настройки в режиме RIP Router Mode и отключения функции RIP воспользуйтесь формой no этой команды.

Пример

В данном примере показано, как настроить маршрутизацию RIP.

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#
```

89.12 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

IP-ADDRESS MASK	(Опционально.) Укажите адрес, информацию о маршрутизации которого необходимо отобразить.
NETWORK-PREFIX/PREFIX-LENGTH	(Опционально.) Укажите префикс подсети и длину префикса сети, которую необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

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, A - Aggregate

    Network            Next Hop        Metric  From            If       Time

Rc  11.0.0.0/8                           1                   vlan11
R   105.100.0.0/24     11.0.0.5          2     11.0.0.5        vlan11   0DT0H0M2S
Rc  107.100.0.0/16                       1                   vlan1
R   212.254.254.0/24   11.0.0.254        2     11.0.0.254      vlan11   0DT0H0M10S

Total Entries: 4 entries, 4 routes
Switch#
```

89.13 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.

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

vlan11 is up, line protocol is up:
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Send v2-broadcast: Disabled
    Authentication Mode: none
    Passive interface: Disabled
    IP interface address:
      11.0.0.3/8

vlan1 is up, line protocol is up:
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Send v2-broadcast: Disabled
    Authentication Mode: none
    Passive interface: Disabled
    IP interface address:
      107.100.0.1/16

Total Entries : 2
Switch#
```

89.14 timers basic

Данная команда используется для настройки значений таймеров сетевого протокола RIP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

timers basic *UPDATE INVALID FLUSH*

no timers basic

Параметры

UPDATE	Укажите интервал update, по истечении которого будет отправлено сообщение с обновлениями. Диапазон значений: от 5 до 65535 секунд.
INVALID	Укажите таймер invalidate. Диапазон значений: от 1 до 65535 секунд.
FLUSH	Укажите таймер flush. 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 значения таймеров протокола RIP.

Пример

В данном примере показано, как настроить значения таймеров RIP. Заданные значения: 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)#
```

89.15 version

Данная команда используется, чтобы глобально настроить RIP version по умолчанию для всех интерфейсов. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

version {1 | 2}
no version

Параметры

1	Укажите, чтобы получать и отправлять только пакеты RIP version 1.
2	Укажите, чтобы получать и отправлять только 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)#
```

90. Команды Routing Information Protocol Next Generation (RIPng)

90.1 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#
```

90.2 default-metric (RIPng)

Данная команда используется, чтобы указать значение метрики (metric) по умолчанию для маршрутов, перераспределяемых RIPng. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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. Заданное значение – 5.

```
Switch#configure terminal
Switch(config)#ipv6 router rip
Switch(config-rtr)#default-metric 5
Switch(config-rtr)#redistribute ospf
Switch(config-rtr)#
```

90.3 distance (RIPng)

Данная команда используется, чтобы указать административное расстояние (administrative distance) маршрутов, информация о которых была получена от RIPng. Для возврата к настройкам воспользуйтесь формой **no** этой команды.

distance *DISTANCE*

no distance

Параметры

DISTANCE	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 надежности маршрута. В качестве расстояния может быть указано целое число от 1 до 254. У маршрута, значение расстояния которого ниже, будет более высокий приоритет, чем у маршрута со значением выше.

Пример

В данном примере показано, как настроить расстояние маршрутов RIPng. Заданное значение – 100.

```
Switch#configure terminal
Switch(config)#ipv6 router rip
Switch(config-rtr)#distance 100
Switch(config-rtr)#
```

90.4 ipv6 rip enable

Данная команда используется, чтобы включить маршрутизацию RIP для IPv6 на интерфейсе. Для отключения маршрутизации воспользуйтесь формой **no** этой команды.

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 vlan1
Switch(config-if)#ipv6 rip enable
Switch(config-if)#
```

90.5 ipv6 rip metric-offset

Данная команда используется, чтобы указать значение, которое необходимо добавить к метрике маршрута IPv6 RIP, полученного на настраиваемом интерфейсе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 rip metric-offset *METRIC-VALUE*

no ipv6 rip metric-offset

Параметры

METRIC-VALUE	Укажите значение, которое необходимо добавить к метрике маршрута IPv6 RIP, полученного на настраиваемом интерфейсе. 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 vlan1
Switch(config-if)#ipv6 rip metric-offset 3
Switch(config-if)#
```

90.6 ipv6 router rip

Данная команда используется, чтобы настроить маршрутизацию RIP для IPv6. Для отключения маршрутизации воспользуйтесь формой **no** этой команды.

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. Чтобы отключить маршрутизацию RIP для IPv6, воспользуйтесь формой **no** этой команды.

Пример

В данном примере показано, как настроить маршрутизацию RIP для IPv6.

```
Switch#configure terminal
Switch(config)#ipv6 router rip
Switch(config-rtr)#
```

90.7 poison-reverse

Данная команда используется, чтобы включить технологию обратного исправления (Poison Reverse) для IPv6 RIP. Для отключения Poison Reverse воспользуйтесь формой **no** этой команды.

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)#
```

90.8 redistribute (RIPng)

Данная команда используется для перераспределения маршрутов из других доменов маршрутизации в RIP. Чтобы отменить перераспределение маршрута с определенных протоколов, воспользуйтесь формой **no** этой команды.

redistribute *PROTOCOL* **[metric** *METRIC-VALUE***]**
no redistribute *PROTOCOL*

Параметры

PROTOCOL	Укажите протокол, маршруты которого необходимо перераспределить. Доступны следующие ключевые слова: **connected**, **ospf** и **static**. Укажите **static** для перераспределения статических IPv6-маршрутов. Укажите **connected** для перераспределения маршрутов, установленных автоматически на основе настроек IPv6-адреса на интерфейсе.
metric *METRIC-VALUE*	(Опционально.) Укажите метрику для перераспределяемых маршрутов. 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. Новое значение метрики – 10.

```
Switch#configure terminal
Switch(config)#ipv6 router rip
Switch(config-rtr)#redistribute ospf metric 10
Switch(config-rtr)#
```

90.9 passive-interface

Данная команда используется для отключения отправки обновлений маршрутизации на интерфейсе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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 vlan1
Switch(config-rtr)#
```

90.10 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.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о настройках протокола RIP.

Для отображения записи базы данных маршрутизации RIP примените команду **show ipv6 rip database**.

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 120
     Updates every 30 seconds, expire after 180 seconds
     Garbage collect after 120 seconds
     Split horizon is on; poison reverse is off
     Periodic updates 44, trigger updates 1

  Interfaces:
     vlan1
     vlan2
     vlan3
  Redistribution:
     Redistributing static with metric 2

Switch#
```

90.11 split-horizon

Данная команда используется, чтобы включить технологию Split Horizon для IPv6 RIP. Для отключения Split Horizon воспользуйтесь формой **no** этой команды.

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)#
```

90.12 timers

Данная команда используется для настройки таймеров сетевого протокола IPv6 RIP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

timers *UPDATE INVALID FLUSH*

no timers

Параметры

UPDATE	Укажите интервал update, по истечении которого будет отправлено сообщение с обновлениями. Диапазон значений: от 5 до 65535 секунд.
INVALID	Укажите таймер invalidate. Диапазон значений: от 1 до 65535 секунд.
FLUSH	Укажите таймер flush. 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 значения таймеров протокола IPv6 RIP.

Пример

В данном примере показано, как настроить значения таймеров RIP. Заданные значения: 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)#
```

90.13 debug ipv6 rip

Данная команда используется для включения функции отладки IPv6 RIP. Чтобы отключить функцию отладки IPv6 RIP, воспользуйтесь формой **no** этой команды.

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#
```

90.14 debug ipv6 rip interface

Данная команда используется для включения функции отладки IPv6 RIP на интерфейсе коммутатора. Чтобы отключить функцию отладки IPv6 RIP на интерфейсе коммутатора, воспользуйтесь формой **no** этой команды.

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 vlan1 has changed the link state to UP
```

90.15 debug ipv6 rip packet-transmitting

Данная команда используется для включения отладки IPv6 RIP при передаче пакетов на коммутаторе. Чтобы отключить отладку IPv6 RIP при передаче пакетов на коммутаторе, воспользуйтесь формой **no** этой команды.

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 FF02::9 , Index 1
```

90.16 debug ipv6 rip packet-receiving

Данная команда используется для включения отладки IPv6 RIP при получении пакетов на коммутаторе. Чтобы отключить отладку IPv6 RIP при получении пакетов на коммутаторе, воспользуйтесь формой **no** этой команды.

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
```

90.17 debug ipv6 rip route

Данная команда используется для включения отладки маршрутов IPv6 RIP на коммутаторе. Чтобы отключить отладку маршрутов IPv6 RIP на коммутаторе, воспользуйтесь формой **no** этой команды.

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 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= 2016:3630:: nexthop= FE80::206:28FF:FED8:FEAC

Switch#
Switch#
```

91. Команды Safeguard Engine

91.1 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#
```

91.2 cpu-protect safeguard

Данная команда используется для включения или настройки функции Safeguard Engine. Для выключения функции Safeguard Engine воспользуйтесь формой **no** этой команды.

cpu-protect safeguard [threshold *RISING-THRESHOLD FALLING-THRESHOLD***]**
no cpu-protect safeguard [threshold]

Параметры

threshold	(Опционально.) Укажите, чтобы настроить пороговые значения загрузки, при которой будет включаться/отключаться функция Safeguard Engine.
RISING-THRESHOLD	(Опционально.) Укажите, чтобы установить значение в процентах верхнего порога загрузки ЦПУ, при котором включается функция Safeguard Engine. Если загрузка ЦПУ превысит указанное значение, механизм Safeguard Engine начнет функционировать. Диапазон значений: от 20 до 100.
FALLING-THRESHOLD	(Опционально.) Укажите, чтобы установить значение в процентах нижнего порога загрузки ЦПУ, при котором выключается функция Safeguard Engine. Если загрузка ЦПУ снизится до указанного значения, механизм Safeguard Engine перестанет функционировать. 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)#
```

91.3 cpu-protect sub-interface

Данная команда используется для настройки пропускной способности (Rate Limit) трафика, предназначенного для ЦПУ по типам под-интерфейсов. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

cpu-protect sub-interface {manage | protocol | route} pps *RATE*
no cpu-protect sub-interface {manage | protocol | route}

Параметры

pps *RATE*	Укажите пороговое значение. Единица измерения – пакеты в секунду. Если установлено значение 0, будут отброшены все пакеты указанных типов под-интерфейса.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Причины, по которым пакеты предназначаются для ЦПУ, могут быть классифицированы по следующим трем группам: **manage**, **protocol** и **route**. Под-интерфейс – это логический интерфейс, предназначенный для разделения полученных пакетов ЦПУ на разные группы. Как правило, для корректной работы функций пакеты протокола должны иметь более высокий приоритет. Обычно ЦПУ не участвует в маршрутизации пакетов. В некоторых случаях, например, при изучении нового IP-адреса, или если не указан маршрут по умолчанию, некоторые пакеты будут оправлены в ЦПУ для программной маршрутизации. Используйте данную команду, чтобы ограничить скорость маршрутизируемых пакетов. Это позволит ЦПУ не тратить много времени на маршрутизацию пакетов.

Пример

В данном примере показано, как настроить пропускную способность (Rate Limit) пакетов для под-интерфейса управления (management). Настроенное пороговое значение – 1000 пакетов в секунду.

```
Switch#configure terminal
Switch(config)#cpu-protect type ospf pps 100
Switch(config)#
```

91.4 cpu-protect type

Данная команда используется для настройки пропускной способности (Rate Limit) трафика, предназначенного для ЦПУ, по типу протокола. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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** – пакеты управления протоколом, 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.



Примечание: сначала ЦПУ проверяет, содержит ли принимаемый пакет виртуальный под-интерфейс протокола. Далее ЦПУ проверит, содержит ли принимаемый пакет виртуальный под-интерфейс управления (management). Пакет, который не содержит виртуальный под-интерфейс протокола или управления, будет классифицирован как виртуальный под-интерфейс

маршрутизации.

В таблице ниже перечислены имена поддерживаемых протоколов для данной команды:

Имя протокола	Описание	Классификация (под-интерфейс)
8021x	Port-based Network Access Control	Protocol
arp	IP Address Resolution Protocol (ARP)	Protocol
dhcp	Dynamic Host Configuration	Protocol
dns	Domain Name Services	Protocol
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
lacp	Link Aggregation Control Protocol	Protocol
ntp	Network Time Protocol	Protocol
ospf	Open Shortest Path First	Protocol
pim	Protocol Independent Multicast	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 – 100 пакетов в секунду.

```
Switch#configure terminal
Switch(config)#cpu-protect type ospf pps 100
Switch(config)#
```

91.5 show cpu-protect safeguard

Данная команда используется для отображения настроек и статуса функции Safeguard Engine.

show cpu-protect safeguard

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки и статус функции Safeguard Engine.

Пример

В данном примере показано, как отобразить настройки и текущий статус Safeguard Engine.

```
Switch#show cpu-protect safeguard

Safeguard Engine State: Disabled
Safeguard Engine Status: Normal
Utilization Thresholds:
 Rising   :50%
 Falling  :20%

Switch#
```

Отображаемые параметры

Safeguard Engine Status	Текущий режим загрузки ЦПУ. Возможны следующие строки для отображения: **Exhausted**: если загрузка ЦПУ превышает установленный верхний порог, коммутатор переходит в режим Exhausted Mode, и механизм Safeguard Engine начинает функционировать. Safeguard Engine не выключается до тех пор, пока загрузка не снизится до нижнего порога. **Normal**: Safeguard Engine не срабатывает.

91.6 show cpu-protect sub-interface

Данная команда используется для отображения пропускной способности (Rate Limit) и статистики под-интерфейса.

show cpu-protect sub-interface {manage | protocol | route} [*UNIT-ID***]**

Параметры

UNIT-ID	(Опционально.) Укажите unit ID устройства, для под-интерфейса которого необходимо отобразить пропускную способность (rate limit) и статистику. Данный параметр доступен только при включенном режиме стекирования (Stacking Mode).

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настроенные значения Rate Limit и Drop Count механизма Safeguard Engine указанной группы. Данные счетчики подсчитываются программно.

Пример

В данном примере показано, как отобразить настроенные значения Rate Limit и Drop Count механизма Safeguard Engine указанной группы.

```
Switch#show cpu-protect sub-interface manage

Sub-Interface: manage
Rate Limit: 10 pps

Unit  Total                          Drop
----- ------------------------------ ------------------------------
1     103                            12

Switch#
```

91.7 show cpu-protect type

Данная команда используется для отображения пропускной способности (Rate Limit) и статистики защиты ЦПУ.

show cpu-protect type {*PROTOCOL-NAME* **[***UNIT-ID***] | unit** *UNIT-ID***}**

Параметры

PROTOCOL-NAME **[***UNIT-ID***]**	Укажите для отображения настроенного значения Rate Limit и статистики указанного протокола, если дополнительный unit ID не указан. В противном случае будет отображена информация только для устройства, unit ID которого был указан. Параметр *UNIT-ID* доступен только при включенном режиме стекирования.
unit *UNIT-ID*	Укажите unit ID устройства для отображения настроенного значения Rate Limit и статистики. Данный параметр доступен только при включенном режиме стекирования.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить Rate Limit и статистику механизма Safeguard Engine.

Пример

В данном примере показано, как отобразить Rate Limit и статистику механизма Safeguard Engine.

```
Switch#show cpu-protect type dhcp

Type: dhcp
Rate Limit: 200 pps

Unit  Total                          Drop
----- ------------------------------ ------------------------------
1     0                              0

Switch#
```

91.8 snmp-server enable traps safeguard-engine

Данная команда используется для включения отправки SNMP-уведомлений для Safeguard Engine. Для отключения отправки SNMP-уведомлений для Safeguard Engine воспользуйтесь формой **no** этой команды.

snmp-server enable traps safeguard-engine
no snmp-server enable traps safeguard-engine

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить/отключить отправку SNMP-уведомлений при изменении текущего режима Safeguard Engine.

Пример

В данном примере показано, как включить отправку trap-сообщений об изменении текущего режима Safeguard Engine.

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

92. Команды клиента Secure File Transfer Protocol (SFTP)

92.1 ip ssh client authmethod

Данная команда используется для настройки метода аутентификации SFTP-клиента на коммутаторе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip ssh client authmethod {password | publickey}

no ip ssh client authmethod

Параметры

password	Укажите, чтобы использовать метод аутентификации по паролю для SFTP-клиента.
publickey	Укажите, чтобы использовать метод аутентификации с открытым ключом для SFTP-клиента.

По умолчанию

По умолчанию используется метод аутентификации по паролю (**password**).

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда предназначена для настройки метода аутентификации SFTP-клиента на коммутаторе.

Ниже перечислены доступные шифрования (cipher) для SFTP-клиента:

- алгоритмы обмена ключами: diffie-hellman-group1-sha1
- алгоритмы MAC: hmac-sha1
- алгоритмы шифрования: 3des-cbc

При настройке метода аутентификации по паролю (**password**) примените следующие шаги для успешного подключения к SFTP-серверу:

1. Введите команду **ip ssh client authmethod password** на коммутаторе.
2. Настройте имя пользователя и пароль на SFTP-сервере.
3. Используйте команду **copy**, чтобы загрузить файлы с SFTP-сервера или выгрузить файлы на SFTP-сервер. При подключении к SFTP-серверу требуется ввести имя пользователя и пароль.

При настройке метода аутентификации с открытым ключом (**publickey**) воспользуйтесь следующими шагами для успешного подключения к SFTP-серверу.

1. Введите команду **ip ssh client authmethod publickey** на коммутаторе.
2. Сгенерируйте пару ключей RSA. На коммутаторе поддерживается только формат RSA, 1024-битовая длина и OpenSSH.
3. Загрузите пару ключей RSA с SFTP-сервера.

4. Загрузите открытый ключ RSA с SFTP-сервера.
5. Настройте путь открытого ключа на SFTP-сервере.
6. Примените команду **copy**, чтобы загрузить файлы с SFTP-сервера или выгрузить файлы на SFTP-сервер. При подключении к SFTP-серверу требуется ввести имя пользователя и пароль.

Пример

В данном примере показано, как настроить метод аутентификации по паролю для SFTP-клиента.

```
Switch#configure terminal
Switch(config)#ip ssh client authmethod password
Switch(config)#
```

92.2 ip ssh client keypath

Данная команда используется, чтобы настроить путь файла закрытого ключа для SFTP-клиента. Чтобы удалить путь ключа, воспользуйтесь формой **no** этой команды.

ip ssh client keypath {publickey *STRING* **| privatekey** *STRING***}**

no ip ssh client keypath {publickey | privatekey}

Параметры

publickey *STRING*	Укажите путь файла открытого ключа для SFTP-клиента. Максимальное количество символов – 200.
privatekey *STRING*	Укажите путь файла закрытого ключа для SFTP-клиента. Максимальное количество символов – 200.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить путь файла закрытого ключа для SFTP-клиента. Когда применяется открытый ключ в качестве метода аутентификации SFTP-клиента, необходимо настроить следующую команду.

Пример

В данном примере показано, как настроить путь файла открытого ключа для SFTP-клиента.

```
Switch#configure terminal
Switch(config)#ip ssh client keypath publickey /c:/Identity.pub
Switch(config)#
```

92.3 show ip ssh client

Данная команда используется для отображения настроек SFTP-клиента.

show ip ssh client

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки SFTP-клиента.

Пример

В данном примере показано, как отобразить настройки SFTP-клиента.

```
Switch#show ip ssh client

 auth method : Publickey
 Public key path  : /c:/Identity.pub
 Private key path : /c:/Identity

Switch#
```

93. Команды Secure File Transfer Protocol (SFTP) Server

93.1 ip sftp server

Данная команда используется для включения SFTP-сервера. Чтобы отключить SFTP-сервер, воспользуйтесь формой **no** этой команды.

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 применяется 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)#
```

93.2 ip sftp timeout

Данная команда используется для настройки таймера пассивного состояния (Idle Timer) для SFTP-сервера на коммутаторе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip sftp timeout *SECONDS*
no ip sftp timeout

Параметры

SECONDS	Укажите значение таймера пассивного состояния (Idle Timer) для SFTP-сервера. 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. Указанное значение – 600 секунд.

```
Switch#configure terminal
Switch(config)#ip sftp timeout 600
Switch(config)#
```

93.3 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.

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#
```

94. Команды Secure Shell (SSH)

94.1 crypto key generate

Данная команда используется для генерирования пары ключей RSA или DSA.

crypto key generate {rsa [modulus *MODULUS-SIZE*] **| dsa}**

Параметры

rsa	Укажите для генерирования пары ключей RSA.
modulus *MODULUS-SIZE*	(Опционально.) Укажите количество битов в модуле. Доступные значения для RSA: 360, 512, 768, 1024 и 2048. Если не указано, будет получено сообщение о необходимости указать значение.
dsa	Укажите для генерирования пары ключей DSA. Фиксированный размер ключа DSA – 1024 битов.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда применяется 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#
```

94.2 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#
```

94.3 ip ssh timeout

Данная команда используется для настройки параметров контроля SSH на коммутаторе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip ssh {timeout *SECONDS* **| authentication-retries** *NUMBER***}**

no ip ssh {timeout | authentication-retries}

Параметры

timeout *SECONDS*	Укажите временной интервал ожидания ответа от SSH-клиента для этапа согласования SSH. Диапазон значений: от 30 до 600.

authentication-retries *NUMBER*	Укажите количество попыток аутентификации. Сессия завершается после всех неудачных попыток. 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 для SSH. Указанное значение – 160 секунд.

```
Switch#configure terminal
Switch(config)#ip ssh timeout 160
Switch(config)#
```

В примере ниже показано, как настроить значение попыток аутентификации. Указанное значение – 2. Соединение будет прервано после 2 неудачных попыток.

```
Switch#configure terminal
Switch(config)#ip ssh authentication-retries 2
Switch(config)#
```

94.4 ip ssh server

Данная команда используется для включения SSH-сервера. Чтобы отключить SSH-сервер, воспользуйтесь формой **no** этой команды.

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/отключить SSH-сервер.

Пример

В данном примере показано, как включить SSH-сервер.

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

94.5 ip ssh service-port

Данная команда используется для указания сервисного порта для SSH. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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

Параметры

TCP-PORT	Укажите номер TCP-порта. Диапазон значений: от 1 до 65535. Как правило, для протокола SSH назначается TCP-порт 22.

По умолчанию

По умолчанию номер TCP-порта – 22.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить номер TCP-порта для SSH-сервера.

Пример

В данном примере показано, как изменить номер сервисного порта. Новый настроенный номер – 3000.

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

94.6 show crypto key mypubkey

Данная команда используется для отображения пар открытых ключей RSA или DSA.

show crypto key mypubkey {rsa | dsa}

Параметры

rsa	Укажите, чтобы отобразить информацию об открытом ключе RSA.
dsa	Укажите, чтобы отобразить информацию об открытом ключе DSA.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы отобразить пары открытых ключей RSA или DSA.

Пример

В данном примере показано, как отобразить информацию об открытом ключе RSA.

```
Switch#show crypto key mypubkey rsa

% Key pair was generated at: 09:48:40, 2013-11-29
Key Size: 768 bits
Key Data:
AAAAB3Nz aC1yc2EA AAADAQAB AAAAQwCN 6IRFHCBf jsHvYjQG iCL0p2kz 2v38ULC8
kAKra/Ze mG7IW3eC 8STcrkr5 s7l9H/bh jG/oqkwj SlUJSGqR e/sj6Ws=

Switch#
```

94.7 show ip ssh

Данная команда используется для отображения пользовательских настроек конфигурации SSH.

show ip ssh

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить 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#
```

94.8 show ssh

Данная команда используется для отображения статуса подключений SSH-сервера.

show ssh

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статус подключений SSH на коммутаторе.

Пример

В данном примере показано, как отобразить информацию о подключениях SSH.

```
Switch#show ssh

SID Ver. Cipher                       Userid           Client IP Address
--- --- ---------------------------- ---------------- ------------------------
0   V2  3des-cbc/hmac-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.

94.9 ssh user authentication-method

Данная команда используется для настройки методов аутентификации SSH для учетной записи пользователя. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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. Максимальное количество символов – 32.
password	Укажите метод аутентификации по паролю для указанной учетной записи пользователя. Данный метод аутентификации используется по умолчанию.
publickey *URL*	Укажите метод аутентификации с открытым ключом для указанной учетной записи пользователя. Введите URL локального файла, который будет использоваться в качестве открытого ключа указанного пользователя.
hostbased *URL*	Укажите метод аутентификации на основе узла для указанной учетной записи пользователя. Введите URL локального файла, который будет использоваться в качестве ключа узла клиента.
host-name *HOSTNAME*	Укажите доступное имя узла для аутентификации на основе узла. Имя узла клиента проверяется во время аутентификации. Диапазон значений: от 1 до 255.
IP-ADDRESS	(Опционально.) Укажите, необходима ли дополнительная проверка IP-адреса клиента для аутентификации на основе узла. Если IPv4/IPv6-адрес не указан, будет проверено только имя узла.
IPV6-ADDRESS	(Опционально.) Укажите, необходима ли дополнительная проверка IPv6-адреса клиента для аутентификации на основе узла. Если IPv4/IPv6-адрес не указан, 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. Максимальная длина строки составляет 8 Kb.
- Каждый ключ состоит из следующих разделенных пробелами полей: *keytype*, *base64-encoded key*, *comment*. Ввод полей *keytype* и *base64-encoded key* обязателен, ввод поля *comment* – необязатетелен. Поле *keytype* может являться *ssh-dss* или *ssh-rsa*.

Пример

В данном примере показано, как настроить метод аутентификации с открытым ключом для пользователя «user1».

```
Switch#configure terminal
Switch(config)#ssh user user1 authentication-method publickey c:/user1.pub
Switch(config)#
```

95. Команды sFlow

95.1 sflow receiver

Данная команда используется для настройки получателя для агента sFlow. Получатели не могут быть добавлены или удалены из агента sFlow. Чтобы вернуть настройки по умолчанию для одного получателя, воспользуйтесь формой **no** этой команды.

sflow receiver *INDEX* **[owner** *NAME***] [expiry {***SECONDS* **| infinite}] [max-datagram-size** *SIZE***] [host {***IP-ADDRESS* **|** *IPV6-ADDRESS***}] [udp-port** *PORT***]**

no sflow receiver *INDEX*

Параметры

INDEX	Укажите индекс получателя.
owner *NAME*	(Опционально.) Укажите имя владельца получателя. Максимальное 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 датаграммы sFlow. 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. 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 датаграммы 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)#
```

95.2 sflow sampler

Данная команда используется для создания или настройки выборки для агента sFlow. Чтобы удалить одну выборку, воспользуйтесь формой **no** этой команды.

sflow sampler *INSTANCE* **[receiver** *RECEIVER***] [inbound | outbound] [sampling-rate** *RATE***] [max-header-size** *SIZE***]**

no sflow sampler *INSTANCE*

Параметры

INSTANCE	Укажите индекс экземпляра, если с одним интерфейсом ассоциировано несколько выборок. Диапазон значений: от 1 до 65535.
receiver *RECEIVER*	(Опционально.) Укажите индекс получателя указанной выборки. Если параметр не указан, значение равно нулю. Пользователь не может указать «0» в качестве данного значения.
inbound	(Опционально.) Укажите для выборки входящих пакетов. По умолчанию используется данное направление выборки.
outbound	(Опционально.) Укажите для выборки исходящих пакетов.

sampling-rate *RATE*	(Опционально.) Укажите частоту выборки пакетов. Доступный диапазон: от 0 до 65536. Если параметр не указан или указан «0», выборка будет отключена.
max-header-size *SIZE*	(Опционально.) Укажите максимальное количество байтов, которое необходимо скопировать из пакетов выборки. Диапазон значений: от 18 до 256. Если параметр не указан, значение по умолчанию составляет 128.

По умолчанию

По умолчанию ни одной выборки не создано.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду без ключевых слов, чтобы создать выборку по умолчанию или вернуть значения по умолчанию для существующей выборки. При использовании формы **no** укажите индекс экземпляра выборки, которую необходимо удалить.

Пользователь может указать только получателя, для которого настроено имя владельца. Если имя владельца получателя сброшено, ассоциированная с ним выборка вернется к настройкам по умолчанию. ID получателя выборки по умолчанию составляет 0.

Возможна настройка двух режимов для экземпляра: inbound или outbound. Если режим не указан, по умолчанию используется inbound, который применяется для контроля входящих пакетов.

На интерфейсе возможна настройка нескольких выборок. Настроенная частота нескольких выборок может отличаться, но частота всех других выборок в одном направлении должна быть кратна минимальной настроенной частоте выборки во второй степени.

Во время перегрузки системы текущая частота выборки может быть автоматически понижена.

Пример

В данном примере показано, как создать выборку экземпляра 1. Получатель – 1. Режим – inbound. Частота – 1024. Размер – 128 байтов.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#sflow sampler 1 receiver 1 inbound sampling-rate 1024 max-header-size 128
Switch(config-if)#
```

95.3 sflow poller

Данная команда используется для создания или настройки опроса для агента sFlow. Чтобы удалить опрос, воспользуйтесь формой **no** этой команды.

sflow poller *INSTANCE* **[receiver** *RECEIVER***] [interval** *SECONDS***]**
no sflow poller *INSTANCE*

Параметры

INSTANCE	Укажите индекс экземпляра, если с одним интерфейсом ассоциировано несколько опросов. Диапазон значений: от 1 до 65535.
receiver *RECEIVER*	(Опционально.) Укажите индекс получателя указанного опроса. Если параметр не указан, значение равно нулю. Пользователь не может указать «0» в качестве данного значения.
interval *SECONDS*	(Опционально.) Укажите максимальное количество секунд между последовательными выборками опроса. Диапазон значений: от 0 до 120. Если параметр не указан или указан «0», опрос будет отключен.

По умолчанию

Опросы по умолчанию не созданы.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду без ключевых слов, чтобы создать опрос по умолчанию или вернуть значения по умолчанию для существующего опроса. При использовании формы **no** укажите индекс экземпляра опроса, который необходимо удалить.

Пользователь может указать только получателя, 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 eth1/0/1
Switch(config-if)#sflow poller 1 receiver 1 interval 20
Switch(config-if)#
```

95.4 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 обо всех получателях.
sampler	(Опционально.) Укажите для отображения информации обо всех выборках.
poller	(Опционально.) Укажите для отображения информации обо всех опросах.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об sFlow. При отсутствии поддержки MIB, строка sFlow Agent Version с указанием версии MIB будет пустой. При изменении vendor имя организации в строке sFlow Agent Version также будет изменено.

Пример

В данном примере показано, как отобразить информацию обо 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                     : 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 датаграммы sFlow.
Address	IPv4/IPv6-адрес удаленного получателя sFlow.
Port	UDP-порт удаленного получателя sFlow.
Datagram Version	Версия датаграммы 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.

Active Rate	Частота для выборки пакетов, установленная в чипсете.
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.

96. Команды Simple Mail Transfer Protocol (SMTP)

96.1 smtp server

Данная команда применяется для настройки SMTP-сервера и порта. Используйте команду **no smtp server** для удаления SMTP-сервера. Для возврата порта к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

smtp server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [port** *PORT***]**

no smtp server

no smtp server port

Параметры

IP-ADDRESS	Укажите IPv4-адрес SMTP-сервера.
IPV6-ADDRESS	Укажите IPv6-адрес SMTP-сервера.
port *PORT*	(Опционально.) Укажите номер TCP-порта для подключения к SMTP-серверу. 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)#
```

96.2 smtp self

Данная команда используется, чтобы настроить адрес электронной почты коммутатора для отправки сообщений по электронной почте. Для удаления адреса электронной почты коммутатора воспользуйтесь формой **no** этой команды.

smtp self *EMAIL-ADDRESS*
no smtp self

Параметры

self *EMAIL-ADDRESS*	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. Указанный адрес – switch@domain.com.

```
Switch#configure terminal
Switch(config)#smtp self switch@domain.com
Switch(config)#
```

96.3 smtp recipient

Данная команда используется для настройки получателя электронных писем. Чтобы удалить получателя, воспользуйтесь формой **no** этой команды.

smtp recipient *EMAIL-ADDRESS*
no smtp recipient {all | *EMAIL-ADDRESS***}**

Параметры

EMAIL-ADDRESS	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 отправку 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)#
```

96.4 smtp interval

Данная команда используется для настройки SMTP-интервала. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

smtp interval *MINUTES*
no smtp interval

Параметры

MINUTES	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)#
```

96.5 show smtp

Данная команда используется для отображения информации об SMTP.

show smtp

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

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#
```

96.6 smtp send-testmsg

Данная команда используется для проверки доступности SMTP-сервера.

smtp send-testmsg

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC 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.



Примечание: клавиша ENTER используется, чтобы указать завершение текста, введенного в полях объекта (subject) и содержимого (content).

```
Switch# smtp send-testmsg

Subject:This is a test of smtp
Content:Hello, everybody!

Sending mail, please wait...
< send line, > receive line, [] message
[Trying to connect IPv4 server......]
[Connect to IPv4 server 10.1.1.1 port 25]
>220 mail.test.com ESMTP MAIL Service ready at Thu, 16 Jan 2020 13:59:30 +0800
<HELO Switch
>250 mail.test.com Hello [10.90.90.90]
<MAIL FROM:<sender@test.com>
>250 2.1.0 Sender OK
<RCPT TO:<reciever@test.com >
>250 2.1.5 Recipient OK
<DATA
>354 Start mail input; end with <CRLF>.<CRLF>
<From: sender@test.com
<To: reciever@test.com
<Subject: Test mail from DGS-1520 : This is a test of smtp
<
From device DGS-1520 10.90.90.90
<Jan 16 2020 05:59:44.470
<
<Hello, everybody!
<
<.
>250 2.6.0 <8d54887926b140a3958e5bc0f7382f52@mail.test.com> [InternalId=13421772800270,
Hostname=mail.test.com] Queued mail for delivery
<QUIT
Switch#
```

97. Команды Simple Network Management Protocol (SNMP)

97.1 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 об SNMP local engine ID.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения информации об 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 примере ниже 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 следующем 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 нижеприведенном 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 нижеследующем примере показано, как отобразить SNMP engine ID.

```
Switch#show snmp engineID

Local SNMP engineID: 800000ab03f07d6834001000

Switch#
```

97.2 show snmp user

Данная команда используется для отображения информации о настроенном SNMP-пользователе.

show snmp user [*USER-NAME***]**

Параметры

USER-NAME	(Опционально.) Укажите имя SNMP-пользователя, о котором необходимо отобразить информацию.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если имя пользователя не указано, будут отображены все настроенные пользователи. С помощью данной команды нельзя отобразить созданную строку community string.

Пример

В данном примере показано, как отобразить SNMP-пользователей.

```
Switch#show snmp user

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#
```

97.3 snmp-server community

Данная команда используется, чтобы настроить строку сообщества (community string) для доступа к SNMP. Для удаления строки community string воспользуйтесь формой **no** этой команды.

snmp-server community [0 | 7] *COMMUNITY-STRING* **[view** *VIEW-NAME***] [ro | rw] [access** *IP-ACL-NAME***] [context** *CONTEXT***]**

no snmp-server community [0 | 7] *COMMUNITY-STRING*

Параметры

0 *COMMUNITY-STRING*	(Опционально.) Укажите строку community string в форме обычного текста. Максимальное количество символов в строке – 32. Данное значение используется по умолчанию. Использовать решетку (#) запрещено.
7 *COMMUNITY-STRING*	(Опционально.) Укажите строку community string в зашифрованном виде.
view *VIEW-NAME*	(Опционально.) Укажите имя ранее настроенного view, которое доступно указанному SNMP-сообществу.

ro	(Опционально.) Укажите право «только чтение».
rw	(Опционально.) Укажите право «чтение/запись».
access *IP-ACL-NAME*	(Опционально.) Укажите имя стандартного списка доступа, дающего возможность пользователю использовать указанную строку community string при доступе к агенту SNMP. Укажите доступного пользователя в поле адреса источника записи списка доступа.
context *CONTEXT*	(Опционально.) Укажите имя SNMP-контекста.

По умолчанию

Community	View Name	Access right
private	CommunityView	Read/Write (чтение/запись)
public	CommunityView	Read Only (только чтение)

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда предоставляет простой способ для создания строки community string для управления SNMPv1 и SNMPv2c. При настройке 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)#
```

97.4 snmp-server engineID local

Данная команда используется для указания SNMP engine ID на локальном устройстве. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

snmp-server engineID local *ENGINEID-STRING*
no snmp-server engineID local

Параметры

ENGINEID-STRING	Укажите строку engine ID. Максимальное 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 332200000000000000000000.

```
Switch#configure terminal
Switch(config)#snmp-server engineID local 3322
Switch(config)#
```

97.5 snmp-server group

Данная команда используется для настройки SNMP-группы. Чтобы удалить SNMP-группу или удалить группу из используемой указанной модели безопасности, воспользуйтесь формой **no** этой команды.

snmp-server group *GROUP-NAME* **{v1 | v2c | v3 {auth | noauth | priv}} [read** *READ-VIEW***] [write** *WRITE-VIEW***] [notify** *NOTIFY-VIEW***] [access** *IP-ACL-NAME***] [context** *CONTEXT***]**

no snmp-server group *GROUP-NAME* **{v1 | v2c | v3 {auth | noauth | priv}}**

Параметры

GROUP-NAME	Укажите имя группы. Максимальное количество символов в строке – 32. Пробелы в строке недопустимы.
v1	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv1.

v2c	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv2c.
v3	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv3.
auth	Укажите для аутентификации пакетов. Данный параметр не используется для шифрования пакетов.
noauth	Укажите для отмены аутентификации и шифрования пакетов.
priv	Укажите для аутентификации и шифрования пакетов.
read *READ-VIEW*	(Опционально.) Укажите, чтобы обеспечить доступ к чтению пользователю данной группы.
write *WRITE-VIEW*	(Опционально.) Укажите, чтобы обеспечить доступ к записи пользователю данной группы.
notify *NOTIFY-VIEW*	(Опционально.) Укажите, чтобы обеспечить доступ для уведомлений пользователю данной группы. В данном уведомлении описывается объект, о состоянии которого пользователь данной группы узнает с помощью SNMP trap.
access *IP-ACL-NAME*	(Опционально.) Укажите стандартный IP-адрес списка управления доступом (ACL) для ассоциирования с группой.
context *CONTEXT*	(Опционально.) Укажите имя контекста SNMP.

По умолчанию

Group Name	Version	Security Level	Read View Name	Write View Name	Notify View
initial	SNMPv3	noauth	Restricted	None	Restricted
public	SNMPv1	None	CommunityView	None	CommunityView
public	SNMPv2c	None	CommunityView	None	CommunityView
private	SNMPv1	None	CommunityView	CommunityView	CommunityView
private	SNMPv2c	None	CommunityView	CommunityView	CommunityView

По умолчанию нет списка управления доступом (ACL), ассоциированного с какой-либо SNMP-группой.

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 применять 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)#
```

97.6 snmp-server host

Данная команда используется для указания получателя SNMP-уведомлений. Чтобы удалить получателя, воспользуйтесь формой **no** этой команды.

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***} [***COMMUNITY-STRING***]**

Параметры

IP-ADDRESS	Укажите IPv4-адрес узла-получателя сервера для SNMP-уведомлений.
IPV6-ADDRESS	Укажите IPv6-адрес узла-получателя сервера для SNMP-уведомлений.

version	(Опционально.) Укажите версию SNMP, которую необходимо использовать для отправки SNMP trap. Если версия не указана, по умолчанию используется SNMPv1. **1** – SNMPv1. **2c** – SNMPv2c. **3** – SNMPv3.
auth	(Опционально.) Укажите для аутентификации пакетов. Данный параметр не используется для шифрования пакетов.
noauth	(Опционально.) Укажите для отмены аутентификации и шифрования пакетов.
priv	(Опционально.) Укажите для аутентификации и шифрования пакетов.
COMMUNITY-STRING	Введите строку community string, которую необходимо отправить с notify-пакетами уведомлений. При указании версии 3 строка community string используется в качестве имени пользователя, как показано в примере команды **snmp-sever user**.
port *PORT-NUMBER*	(Опционально.) Укажите номер UDP-порта. Номер UDP-порта trap по умолчанию – 162. 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 команды **snmp-server user** сначала необходимо создать пользователя.

При отправке SNMP trap система проверит уведомления view, ассоциированные с указанным пользователем или именем сообщества. Если вариабельные привязки (binding variables), которые должны быть отправлены с SNMP trap, отсутствуют в уведомлениях view, уведомления не будут отправлены на данный сервер.

Пример

В данном примере показано, как настроить SNMP trap-получателя с указанием версии 1 и со строкой community string «comaccess». SNMP trap-получатель – 163.10.50.126.

```
Switch#configure terminal
Switch(config)#snmp-server community comaccess rw
Switch(config)#snmp-server host 163.10.50.126 version 1 comaccess
Switch(config)#
```

В примере ниже 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 следующем 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)#
```

97.7 snmp-server source-interface traps

Данная команда используется, чтобы указать интерфейс, IP-адрес которого будет применен в качестве адреса источника для отправки пакетов SNMP trap. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

snmp-server source-interface traps *INTERFACE-ID*

no snmp-server source-interface traps

Параметры

INTERFACE-ID	Укажите интерфейс, IP-адрес которого будет использован в качестве адреса источника для отправки пакетов SNMP trap.

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда применяется, чтобы указать интерфейс, IP-адрес которого будет применен 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 vlan100
Switch(config)#
```

97.8 snmp-server user

Данная команда используется для создания SNMP-пользователя. Чтобы удалить SNMP-пользователя, воспользуйтесь формой **no** этой команды.

snmp-server user *USER-NAME GROUP-NAME* **[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*

Параметры

USER-NAME	Укажите имя пользователя. Максимальное количество символов в строке – 32. Пробелы в строке недопустимы.
GROUP-NAME	Укажите имя группы, к которой принадлежит данный пользователь. Пробелы в строке недопустимы.
encrypted	(Опционально.) Укажите для шифрования пароля.
auth	(Опционально.) Укажите тип аутентификации.
md5	(Опционально.) Укажите использование аутентификации HMAC-MD5-96.
sha	(Опционально.) Укажите использование аутентификации HMAC-SHA-96.

AUTH-PASSWORD	(Опционально.) Укажите пароль аутентификации в форме обычного текста. Для MD5 пароль может содержать от 8 до 16 символов, для SHA – от 8 до 20. При указании параметра **encrypted** длина пароля для MD5 составляет 32, для SHA – 40. В данном параметре используются шестнадцатеричные значения.
priv	(Опционально.) Укажите тип шифрования.
des	(Опционально.) Укажите использование алгоритма DES для шифрования.
aes	(Опционально.) Укажите использование алгоритма AES для шифрования.
PRIV-PASSWORD	Укажите пароль Private в форме обычного текста. Максимально допустимое количество символов – 64. При указании параметра **encrypted** фиксированная длина пароля – 16 символов.
access *IP-ACL-NAME*	(Опционально.) Укажите стандартный IP-адрес ACL для ассоциирования с пользователем.

По умолчанию

По умолчанию настроен один пользователь.
Имя пользователя – initial.
Имя группы – initial.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Для создания SNMP-пользователя укажите модель безопасности, которая будет использована данным пользователем, и группу, для которой создан данный пользователь. Для создания SNMPv3-пользователя необходимо указать пароль для аутентификации и шифрования.

Невозможно удалить SNMP-пользователя, который был ассоциирован с SNMP-сервером.

Пример

В данном примере показано, как настроить пароль в форме обычного текста для пользователя «user1» в группе «public»в версии SNMPv3.

```
Switch#configure terminal
Switch(config)#snmp-server user user1 public auth md5 authpassword
Switch(config)#
```

В примере ниже показано, как использовать строку MD5 digest вместо пароля в форме обычного текста.

```
Switch#configure terminal
Switch(config)#snmp-server user user1 public encrypted auth md5
00112233445566778899AABBCCDDEEFF
Switch(config)#
```

97.9 snmp-server view

Данная команда используется для создания или изменения записи view. Чтобы удалить указанную запись SNMP view, воспользуйтесь формой **no** этой команды.

snmp-server view *VIEW-NAME OID-TREE* **{included | excluded}**
no snmp-server view *VIEW-NAME*

Параметры

VIEW-NAME	Укажите имя записи view. Диапазон значений: от 1 до 32 символов. Пробелы в строке недопустимы.
OID-TREE	Укажите идентификатор объекта (Object IDentifier, OID) под-дерева ASN.1, который необходимо включить или исключить из View. Для идентификации под-дерева введите строку, состоящую либо из чисел, например, 1.3.6.2.4, либо из слов, например, system.
included	Укажите под-дерево, которое необходимо включить в SNMP View.
excluded	Укажите под-дерево, которое необходимо исключить из SNMP view.

По умолчанию

VIEW-NAME	OID-TREE	View Type
Restricted	1.3.6.1.2.1.1	Included
Restricted	1.3.6.1.2.1.11	Included
Restricted	1.3.6.1.6.3.10.2.1	Included
Restricted	1.3.6.1.6.3.11.2.1	Included
Restricted	1.3.6.1.6.3.15.1.1	Included
CommunityView	1	Included
CommunityView	1.3.6.1.6.3	Excluded
CommunityView	1.3.6.1.6.3.1	Included

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы создать view MIB-объектов.

Пример

В данном примере показано, как создать MIB view и предоставить доступ для чтения SNMP-группе, ассоциированной с данным MIB view. Настроенный MIB view – interfacesMibView. SNMP-группа – guestgroup.

```
Switch#configure terminal
Switch(config)#snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)#snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)#
```

97.10 show snmp trap link-status

Данная команда используется для отображения состояния trap-статуса канала на интерфейсе.

show snmp trap link-status [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения состояния trap-статуса при обнаружении/разрыве соединения (link-up / link-down) на интерфейсе.

Пример

В данном примере показано, как отобразить trap-статус соединения для диапазона интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/9.

```
Switch#show snmp trap link-status interface eth1/0/1-9

Interface           Trap state
-------------       -------------
eth1/0/1            Enabled
eth1/0/2            Enabled
eth1/0/3            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#
```

97.11 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.

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, введите 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 примере ниже 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#
```

97.12 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

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить состояние отправки SNMP trap на порту. Если параметры не указаны, будут отображены все порты.

Пример

В данном примере показано, как отобразить состояние отправки SNMP trap для диапазона интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/9.

```
Switch#show snmp-server trap-sending interface eth1/0/1-9

      Port                          Trap Sending
-----------------                  ---------------
 eth1/0/1                             Enabled
 eth1/0/2                             Enabled
 eth1/0/3                             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#
```

97.13 snmp-server

Данная команда используется для включения агента SNMP. Чтобы выключить агента SNMP, воспользуйтесь формой **no** этой команды.

snmp-server
no snmp-server

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Менеджер SNMP управляет агентом SNMP: отправляет SNMP-запросы агенту и получает ответы и SNMP-уведомления от агента. Для управления агентом необходимо включить на нем SNMP-серевер.

Пример

В данном примере показано, как включить SNMP-сервер.

```
Switch#configure terminal
Switch(config)#snmp-server
Switch(config)#
```

97.14 snmp-server contact

Данная команда используется, чтобы настроить системную контактную информацию для устройства. Для удаления настроек воспользуйтесь формой no этой команды.

snmp-server contact *TEXT*
no snmp-server contact

Параметры

TEXT	(Опционально.) Укажите системную контактную информацию. Максимальное 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. Настроенная строка – MIS Department II.

```
Switch#configure terminal
Switch(config)#snmp-server contact MIS Department II
Switch(config)#
```

97.15 snmp-server enable traps

Данная команда используется для глобального включения отправки SNMP trap. Чтобы отключить отправку SNMP trap, воспользуйтесь формой **no** этой команды.

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/отключить отправку SNMP trap глобально на устройстве.

Пример

В данном примере показано, как включить отправку SNMP trap глобально.

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

97.16 snmp-server enable traps snmp

Данная команда используется для включения отправки всех или определенных SNMP-уведомлений. Чтобы отключить отправку всех или определенных SNMP-уведомлений, воспользуйтесь формой **no** этой команды.

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 сообщества (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 примере ниже показано, как включить SNMP trap об ошибке аутентификации.

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

97.17 snmp-server location

Данная команда используется для указания информации о системном местоположении. Чтобы удалить настройки, воспользуйтесь формой **no** этой команды.

snmp-server location *TEXT*
no snmp-server location

Параметры

TEXT	Укажите системное местоположение. Максимальное 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)#
```

97.18 snmp-server name

Данная команда используется для указания информации о системном имени. Чтобы удалить настройки, воспользуйтесь формой **no** этой команды.

snmp-server name *NAME*

no snmp-server name

Параметры

NAME	Укажите имя сервера. Максимальное количество символов в строке – 255. Оптимальное количество символов в строке – не более 10. Имя узла должно начинаться с буквы, заканчиваться буквой или цифрой, внутри можно использовать буквы, цифры и дефисы.

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. Указанное имя – SiteA-switch.

```
Switch#configure terminal
Switch(config)#snmp-server name SiteA-switch
SiteA-switch(config)#
```

97.19 snmp-server trap-sending disable

Данная команда используется для отключения отправки SNMP trap на порту. Чтобы включить отправку SNMP trap на порту, воспользуйтесь формой **no** этой команды.

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, чтобы включить/отключить отправку сгенерированных системой SNMP trap с определенного порта. Данная команда не применима для SNMP trap, сгенерированных другой системой и переадресованных на порт.

Пример

В данном примере показано, как отключить отправку SNMP trap на интерфейсе с интерфейса Ethernet 1/0/8.

```
Switch#configure terminal
Switch(config)#interface eth1/0/8
Switch(config-if)#snmp-server trap-sending disable
Switch(config-if)#
```

97.20 snmp-server service-port

Данная команда используется для настройки номера UDP-порта SNMP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

snmp-server service-port *PORT-NUMBER*
no snmp-server service-port

Параметры

PORT-NUMBER	Укажите номер UDP-порта. Диапазон значений: от 1 до 65535. Некоторые номера могут конфликтовать с другими протоколами.

По умолчанию

Номер по умолчанию – 161.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для настройки номера UDP-порта SNMP на коммутаторе. Агент будет прослушивать пакеты SNMP request на сервисном UDP-порту настроенного номера.

Пример

В данном примере показано, как настроить номер UDP-порта SNMP.

```
Switch#configure terminal
Switch(config)#snmp-server service-port 50000
Switch(config)#
```

97.21 snmp-server response broadcast-request

Данная команда позволяет разрешить серверу отвечать на широковещательные пакеты SNMP GetRequest. Чтобы запретить серверу отвечать на широковещательные пакеты SNMP GetRequest, воспользуйтесь формой **no** этой команды.

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)#
```

97.22 snmp trap link-status

Данная команда используется для включения отправки уведомлений об обнаружении/разрыве соединения (link-up / link-down), произошедшем на интерфейсе. Чтобы отключить отправку, воспользуйтесь формой **no** этой команды.

snmp trap link-status

no snmp trap link-status

Параметры

Нет.

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для включения или отключения отправки SNMP trap об обнаружении/разрыве соединения (link-up / link-down) на интерфейсе.

Пример

В данном примере показано, как отключить отправку SNMP trap об обнаружении/разрыве соединения (link-up / link-down) на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no snmp trap link-status
Switch(config-if)#
```

97.23 snmp-server context-map

Данная команда используется для конфигурирования таблицы соответствий SNMP-контекста. Чтобы удалить конфигурацию, воспользуйтесь формой **no** этой команды.

snmp-server context-map *CONTEXT* **[instance-id** *INT***] [instance-name** *NAME***]**
no snmp-server context-map *CONTEXT*

Параметры

CONTEXT	Укажите имя контекста VACM. Максимальное количество символов – 32.
instance-id *INT*	Укажите ID экземпляра протокола. Диапазон значений: от 1 до 65535.
instance-name *NAME*	Укажите имя экземпляра протокола. Максимальное количество символов – 12.

По умолчанию

По умолчанию имя контекста VACM – Contex1.

По умолчанию instance ID – 0.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для конфигурирования таблицы соответствий SNMP-контекста на коммутаторе.

Пример

В данном примере показано, как указать SNMP-контекст «snmp-context».

```
Switch#configure terminal
Switch(config)#snmp-server context-map snmp-context
Switch(config)#
```

97.24 show snmp context-map

Данная команда используется для отображения информации о сконфигурированной таблице соответствий SNMP-контекста.

show snmp context-map

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о сконфигурированной таблице соответствий SNMP-контекста.

Пример

В данном примере показано, как отобразить информацию о сконфигурированной таблице соответствий SNMP-контекста.

```
Switch#show snmp context-map

 SNMP Context Mapping Table:

Context Name : Context1
 Instance ID : 0
 Instance Name :


Switch#
```

98. Команды Single IP Management (SIM)

98.1 sim

Данная команда используется для включения функции Single IP Management. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

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)#
```

98.2 sim role

Данная команда используется для смены роли Candidate Switch на Commander Switch или Commander Switch на Candidate Switch.

sim role {commander [*GROUP-NAME***] | candidate}**

Параметры

commander	Укажите для передачи роли Commander Switch устройству.
GROUP-NAME	(Опционально.) Укажите имя группы, назначая устройству роль Commander Switch.

candidate	Укажите для передачи роли Candidate Switch устройству.

По умолчанию

Имя группы Single IP Management по умолчанию – default.

Роль устройства по умолчанию – Candidate Switch.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Технология Single IP Management предусматривает три роли: Candidate Switch и Commander Switch (назначаются пользователем), а также Member Switch (назначается при помощи команды **sim group-member** на Commander Switch).

В SIM-группу входит Commander Switch и множество Member Switch. При смене роли устройства, например, с Commander Switch на Candidate Switch все роли участников SIM-группы будут изменены на Candidate Switch.

Пример

В данном примере показано, как создать SIM-группу.

```
Switch#configure terminal
Switch(config)#sim role commander my-group
Switch(config)#
```

98.3 sim group-member

Данная команда используется для добавления одного Candidate Switch в SIM-группу. Чтобы удалить одного участника из данной SIM-группы, воспользуйтесь формой **no** этой команды.

sim group-member *CANDIDATE-ID* **[***PASSWORD***]**

no sim group-member *MEMBER-ID*

Параметры

CANDIDATE-ID	Укажите одно устройство в роли Candidate Switch в одной SIM-группе.
MEMBER-ID	Укажите одно устройство в роли Member Switch в одной SIM-группе.
PASSWORD	(Опционально.) Укажите пароль устройства в роли Candidate Switch.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

После того как Candidate Switch пройдет аутентификацию 15-уровнего пароля, Commander Switch позволит данному Candidate Switch присоединиться к SIM-группе в качестве Member Switch.

Пример

В данном примере показано, как добавить один Candidate Switch к SIM-группе.

```
Switch#configure terminal
Switch(config)#sim group-member 1 secret
Switch(config)#
```

98.4 sim holdtime

Данная команда используется для настройки времени ожидания (Hold Time) в секундах. Если устройство (Commander Switch или Candidate Switch) по истечении данного времени не получит сообщения Single IP Management, информация о другом устройстве будет удалена. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

sim holdtime *SECONDS*

no sim holdtime

Параметры

SECONDS	Укажите значение времени ожидания (Hold Time). 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 времени ожидания (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 время ожидания (Hold Time) для SIM.

```
Switch#configure terminal
Switch(config)#sim holdtime 120
Switch(config)#
```

98.5 sim interval

Данная команда используется для настройки SIM-интервала в секундах для отправки сообщений протокола Single IP Management. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

sim interval *SECONDS*
no sim interval

Параметры

SECONDS	Укажите значение интервала. 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)#
```

98.6 sim management vlan

Данная команда используется для настройки SIM Management VLAN. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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. Указанное значение – 100.

```
Switch#configure terminal
Switch(config)#sim management vlan 100
Switch(config)#
```

98.7 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#
```

98.8 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 диапазона значений используйте дефис, для отделения нескольких значений используйте запятую. Пробелы до и после символов недопустимы.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда может применяться 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 примере ниже 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#
```

98.9 snmp-server enable traps sim

Данная команда используется для включения отправки trap-сообщений для SIM. Чтобы отключить отправку, воспользуйтесь формой **no** этой команды.

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)#
```

98.10 show sim

Данная команда используется для отображения информации о Single IP Management.

show sim [{candidates [*CANDIDATE-ID***] | members [***MEMBER-ID***] | group [***COMMANDER-MAC***] |**
neighbor}]

Параметры

candidates	(Опционально.) Укажите, чтобы отобразить информацию обо всех Candidate Switch.
CANDIDATE-ID	(Опционально.) Укажите, чтобы отобразить подробную информацию об одном определенном Candidate Switch.
members	(Опционально.) Укажите, чтобы отобразить информацию обо всех Member Switch.
MEMBER-ID	(Опционально.) Укажите, чтобы отобразить подробную информацию об одном определенном Member Switch.

group	(Опционально.) Укажите, чтобы отобразить информацию о других SIM-группах.
COMMANDER-MAC	(Опционально.) Укажите, чтобы отобразить подробную информацию об одной определенной группе.
neighbor	(Опционально.) Укажите, чтобы отобразить информацию о соседних устройствах.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется 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    : 1.00.022
    Management VLAN     : 1
    Device Name         : Switch
    MAC Address         : 80-26-89-15-28-00
    Platform            : DGS-1520-28MP
    SIM State           : Enabled
    Role State          : Commander
    Discovery Interval  : 30 sec
    Hold Time           : 100 sec
    Trap                : Disabled

Switch#
```

В примере ниже показано, как отобразить подробную информацию о локальной SIM на Member Switch.

```
Switch#show sim

    SIM Version        : VER-1.61
    Firmware Version   : 1.00.022
    Device Name        :
    MAC Address        : 80-26-00-15-28-00
    Platform           : DGS-1520-28MP
    SIM State          : Enabled
    Role State         : Member
    Discovery Interval : 30 sec
    Hold Time          : 100 sec
----------------CS Info----------------
    CS Group Name    : my-group
    CS MAC Address   : 80-26-89-15-28-00
    CS Hold Time     : 90 s

Switch#
```

В данном примере показано, как отобразить список участников SIM-группы.

```
Switch#show sim members

Member                                          Hold Firmware
  ID   MAC Address       Platform                Time Version   Device Name
-------------------------------------------------------------------------------
  1    80-26-00-15-28-00 DGS-1520-28MP           100  1.00.022
  2    80-26-01-15-28-00 DGS-1520-28MP            80  1.00.022

Total Entries : 2

Switch#
```

В примере ниже показано, как отобразить подробную информацию об участнике SIM-группы.

```
Switch#show sim members 1

 Sim Member Information :
    Member ID             : 1
    Firmware Version      : 1.00.022
    Device Name           :
    MAC Address           : 80-26-00-15-28-00
    Platform              : DGS-1520-28MP
    Hold Time             : 100 sec

Switch#
```

В данном примере показано, как отобразить список Candidate Switch SIM-группы.

```
Switch#show sim candidates

Candidate                                                Hold Firmware
   ID     MAC Address       Platform                    Time Version   Device Name
-------------------------------------------------------------------------------
   1      EE-FF-00-00-12-12 DGS-1520-28MP                90  1.00.022

Total Entries : 1

Switch#
```

В примере ниже 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      : 1.00.022
 Device Name           :
 MAC Address           : EE-FF-00-00-12-12
 Platform              : DGS-1520-28MP
 Hold Time             : 100 sec

Switch#
```

В данном примере показано, как отобразить краткую информацию о группе.

```
Switch#show sim group
* -means Commander switch.

SIM Group Name : default
                                      Hold  Firmware
ID  MAC Address         Platform        Time  Version    Device Name
-------------------------------------------------------------------
*1  00-02-00-00-08-12   DGS-1520-28MP   40    1.00.022
 2  00-07-15-34-00-50
 3  00-01-02-03-00-10

SIM Group Name : SIM2
                                      Hold  Firmware
ID  MAC Address         Platform        Time  Version    Device Name
-------------------------------------------------------------------
*1  00-01-02-03-04-11   DGS-1520-28MP   40    1.00.022
 2  00-55-55-00-55-11

Total Entries : 2

Switch#
```

В примере ниже 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      : 1.00.022
Platform              : DGS-1520-28MP
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#
```

99. Команды Spanning Tree Protocol (STP)

99.1 clear spanning-tree detected-protocols

Данная команда используется для перезапуска процесса миграции протокола.

clear spanning-tree detected-protocols {all | interface *INTERFACE-ID***}**

Параметры

all	Укажите, чтобы запустить действие обнаружения для всех портов.
interface *INTERFACE-ID*	Укажите интерфейс порта, на котором необходимо запустить действие обнаружения.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

С помощью данной команды во время миграции протокола порт будет переведен в состояние *SEND_RSTP*. Данное действие можно использовать, чтобы проверить, все ли устаревшие мосты на LAN были удалены. При отсутствии моста STP на данной LAN порт будет работать в выбранном режиме RSTP или MSTP. В противном случае порт будет работать в режиме STP.

Пример

В данном примере показано, как запустить процесс миграции протокола для всех портов.

```
Switch#clear spanning-tree detected-protocols all

Clear spanning-tree detected-protocols? (y/n) [n] y

Switch#
```

99.2 show spanning-tree

Данная команда используется для отображения информации о работе протокола Spanning Tree и применяется только для STP и RSTP.

show spanning-tree [interface [_INTERFACE-ID_ **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите ID интерфейса для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения настроек Spanning Tree одного связующего дерева в режиме, совместимом с RSTP или STP.

Пример

В данном примере показано, как отобразить информацию о Spanning Tree при включенном STP.

```
Switch#show spanning-tree

 Spanning Tree: Enabled
 Protocol Mode: RSTP
 Tx-hold-count: 6
 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

                                          Priority Link
 Interface      Role       State      Cost      .Port#   Type   Edge
 ---------      ----       -----      ----      -------  -----  ----
 eth1/0/1       designated forwarding 200000    128.1    p2p    edge

Switch#
```

99.3 show spanning-tree configuration interface

Данная команда используется для отображения информации о настройках интерфейса STP.

show spanning-tree configuration interface [*INTERFACE-ID* **[, | -]]**

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки интерфейса Spanning Tree. Команда может применяться 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 eth1/0/1

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#
```

99.4 snmp-server enable traps stp

Данная команда позволяет включить отправку SNMP-уведомлений для STP. Чтобы отключить отправку уведомлений для STP, воспользуйтесь формой **no** этой команды.

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, 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)#
```

99.5 spanning-tree global state

Данная команда используется для включения/отключения глобального состояния STP. Чтобы отключить глобальное состояние STP, воспользуйтесь формой **no** этой команды.

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, чтобы включить/отключить 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)#
```

99.6 spanning-tree (timers)

Данная команда используется для настройки значений таймеров Spanning Tree. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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. 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. Диапазон значений: от 4 до 30 секунд.
max-age *SECONDS*	Укажите максимальное время жизни сообщения BDPU. Диапазон значений: от 6 до 40 секунд.

По умолчанию

Значение параметра **hello-time** по умолчанию – 2 секунды.
Значение параметра **forward-time** по умолчанию – 15 секунд.
Значение параметра **max-age** по умолчанию – 20 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить значения таймеров Spanning Tree.

Пример

В данном примере показано, как настроить значения таймеров Spanning Tree.

```
Switch#configure terminal
Switch(config)#spanning-tree hello-time 1
Switch(config)#spanning-tree forward-time 16
Switch(config)#spanning-tree max-age 21
Switch(config)#
```

99.7 spanning-tree state

Данная команда используется для включения/отключения STP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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 данная 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 eth1/0/1
Switch(config-if)#spanning-tree state enable
Switch(config-if)#
```

99.8 spanning-tree cost

Данная команда используется для настройки значения стоимости пути на указанном порту. Чтобы определить стоимость пути автоматически, воспользуйтесь формой **no** этой команды.

spanning-tree cost *COST*
no spanning-tree cost

Параметры

COST	Укажите стоимость пути для порта. 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. Указанное значение – 20000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree cost 20000
Switch(config-if)#
```

99.9 spanning-tree guard root

Данная команда используется для включения функции STP Root Guard. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree guard root
no spanning-tree guard root

Параметры

Нет.

По умолчанию

По умолчанию 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 eth1/0/1
Switch(config-if)#spanning-tree guard root
Switch(config-if)#
```

99.10 spanning-tree link-type

Данная команда используется, чтобы настроить тип соединения (link type) для порта. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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 параметры не указаны, 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 типа «точка-точка»; 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 типа соединения модулем STP.

Данные настройки доступны для всех режимов Spanning Tree.

Пример

В данном примере показано, как настроить тип соединения «точка-точка» для интерфейса Ethernet 1/0/7.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree link-type point-to-point
Switch(config-if)#
```

99.11 spanning-tree mode

Данная команда используется для настройки режима STP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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 отбрасывания (discarding).

Пример

В данном примере показано, как настроить текущую версию протокола STP на RSTP.

```
Switch#configure terminal
Switch(config)#spanning-tree mode rstp
Switch(config)#
```

99.12 spanning-tree portfast

Данная команда используется для настройки режима Port Fast Mode на порту. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree portfast {disable | edge| network}
no spanning-tree portfast

Параметры

disable	Укажите для включения режима Fast Disable Mode на порту.
edge	Укажите для включения режима Fast Edge Mode на порту.
network	Укажите для включения режима Fast Network Mode на порту.

По умолчанию

Параметр по умолчанию – **network**.

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 Mode:

- **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 Mode для интерфейса Ethernet- 1/0/7.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree portfast edge
Switch(config-if)#
```

99.13 spanning-tree port-priority

Данная команда используется для настройки значения приоритета STP на указанном порту. Команда применима только для версий RSTP и STP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree port-priority *PRIORITY*
no spanning-tree port-priority

Параметры

PRIORITY	Укажите приоритет порта в диапазоне от 0 до 240.

По умолчанию

Значение по умолчанию – 128.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При присвоении роли порту используется его идентификатор, который состоит из приоритета и номера порта. Чем ниже число, тем выше приоритет. Данный параметр применим только в режимах RSTP или STP.

Пример

В данном примере показано, как настроить приоритет для интерфейса Ethernet 1/0/7 со значением 0.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree port-priority 0
Switch(config-if)#
```

99.14 spanning-tree priority

Данная команда используется для настройки приоритета моста. Команда применима только для версий RSTP и STP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree priority *PRIORITY*
no spanning-tree priority

Параметры

PRIORITY	Укажите Bridge-ID Spanning Tree, который состоит из приоритета и MAC-адреса моста. Bridge-ID является важным фактором в топологии Spanning Tree. Диапазон значений: от 0 до 61440.

По умолчанию

Значение по умолчанию – 32768.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Выбор корневого моста зависит от значение приоритета моста и системного MAC-адреса. Значение приоритета моста должно делиться на 4096. Чем меньше число, тем выше приоритет.

Данные настройки применимы для версий STP и RSTP протокола Spanning Tree. В режиме MSTP используйте команду **spanning-tree mst priority**, чтобы настроить приоритет для MSTP-экземпляра.

Пример

В данном примере показано, как настроить приоритет моста STP со значением 4096.

```
Switch#configure terminal
Switch(config)#spanning-tree priority 4096
Switch(config)#
```

99.15 spanning-tree tcnfilter

Данная команда используется для включения фильтрации уведомлений об изменении топологии сети TCN (Topology Change Notification) на указанном интерфейсе. Чтобы отключить фильтрацию TCN, воспользуйтесь формой **no** этой команды.

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 интерфейсе Ethernet 1/0/7.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree tcnfilter
Switch(config-if)#
```

99.16 spanning-tree tx-hold-count

Данная команда используется для ограничения максимального количества BPDU, которые могут быть отправлены перед паузой в одну секунду. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree tx-hold-count *VALUE*

no spanning-tree tx- hold-count

Параметры

VALUE	Укажите максимальное количество BPDU, которые могут быть отправлены перед паузой в одну секунду. 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)#
```

99.17 spanning-tree forward-bpdu

Данная команда используется для включения BDPU Forwarding в Spanning Tree. Чтобы отключить BDPU Forwarding в Spanning Tree, воспользуйтесь формой **no** этой команды.

spanning-tree forward-bpdu
no spanning-tree forward-bpdu

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При использовании данной команды полученные STP BPDU будут перенаправлены на все member-порты VLAN без тега. Данная команда не будет применена, если функция L2PT включена для STP.

Пример

В данном примере показано, как включить BDPU Forwarding в Spanning Tree.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#spanning-tree forward-bpdu
Switch(config-if)#
```

99.18 spanning-tree nni-bpdu-address

Данная команда используется для настройки адреса назначения STP BPDU на стороне провайдера. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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-C2-00-00-08) 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)#
```

99.19 spanning-tree loop-guard

Данная команда используется для включения функции Loop Guard. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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 eth1/0/3
Switch(config-if)#spanning-tree loop-guard
Switch(config-if)#
```

100. Команды Stacking

100.1 stack

Данная команда используется для включения функции линейного стекирования. Чтобы отключить функцию линейного стекирования, воспользуйтесь формой **no** этой команды.

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 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#
```

100.2 stack bandwidth

Данная команда используется для изменения пропускной способности порта стекирования. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

stack bandwidth {2-port-sfp+ | 2-port-10g-base-t | 4-port-hybrid}
no stack bandwidth

Параметры

2-port-sfp+	Укажите, чтобы использовать для стекирования 2 порта SFP+.
2-port-10g-base-t	Укажите, чтобы использовать для стекирования 2 порта 10GBase-T.
4-port-hybrid	Укажите, чтобы использовать для стекирования 2 порта SFP+ и 2 порта 10GBase-T.

По умолчанию

По умолчанию используются 2 порта SFP+.

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.

Для стекирования коммутаторов данной серии можно использовать оптоволоконный кабель, ethernet-кабель или кабель прямого подключения с разъемом SFP+. Для стекирования можно использовать только последние 4 порта коммутатора.

Порты стекирования или порты, объединенные в логический стек, называются SIO1 (Stacking Input/Output 1) и SIO2. Логический стек должен всегда быть подключен к другому коммутатору в стеке в качестве группы.

В таблице ниже перечислены конфигурации стекирования для соответствующих пар портов SIO.

Конфигурация	**Коммутатор**	**Логический порт SIO1**	**Логический порт SIO2**	**Полоса пропускания**
2-port-10g-base-t	DGS-1520-28	Порт 25	Порт 26	40 Гбит/с (полный дуплекс)
	DGS-1520-28MP	Порт 25	Порт 26	40 Гбит/с (полный дуплекс)
	DGS-1520-52	Порт 49	Порт 50	40 Гбит/с (полный дуплекс)
	DGS-1520-52MP	Порт 49	Порт 50	40 Гбит/с (полный дуплекс)
2-port-sfp+	DGS-1520-28	Порт 27	Порт 28	40 Гбит/с (полный дуплекс)
	DGS-1520-28MP	Порт 27	Порт 28	40 Гбит/с (полный дуплекс)
	DGS-1520-52	Порт 51	Порт 52	40 Гбит/с (полный дуплекс)
	DGS-1520-52MP	Порт 51	Порт 52	40 Гбит/с (полный дуплекс)

4-port-hybrid	DGS-1520-28	Порт 25 и 26	Порт 27 и 28	80 Гбит/с (полный дуплекс)
	DGS-1520-28MP	Порт 25 и 26	Порт 27 и 28	80 Гбит/с (полный дуплекс)
	DGS-1520-52	Порт 49 и 50	Порт 51 и 52	80 Гбит/с (полный дуплекс)
	DGS-1520-52MP	Порт 49 и 50	Порт 51 и 52	80 Гбит/с (полный дуплекс)

Чтобы получить информацию о топологиях стекирования, обратитесь к главе «Приложение G. Информация о стекировании».

Пример

В данном примере показано, как изменить пропускную способность и использовать для стекирования 4 порта.

```
Switch#stack bandwidth 4-port-hybrid

 WARNING: The command does not take effect until the next reboot.
Switch#
```

100.3 stack renumber

Данная команда используется для назначения Unit ID коммутатору вручную. Чтобы назначить Unit ID коммутатору автоматически, воспользуйтесь формой **no** этой команды.

stack *CURRENT-UNIT-ID* **renumber** *NEW-UNIT-ID*
no stack *CURRENT-UNIT-ID* **renumber**

Параметры

CURRENT-UNIT-ID	Укажите текущий Unit ID коммутатора.
NEW-UNIT-ID	Укажите новый Unit ID, который необходимо назначить коммутатору.

По умолчанию

По умолчанию Unit ID назначается автоматически.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Изначально у коммутатора отсутствует Unit ID. При инициализации или добавлении в стек коммутатора Unit ID будет автоматически назначен основным устройством (Master). Unit ID можно сохранить в конфигурационном файле после его назначения, применив команду **copy running-config**

startup-config. Сохранившийся Unit ID будет использован при следующем запуске устройства.

Введите данную команду для переназначения Unit ID указанного коммутатора. Назначенный Unit ID будет применен при следующем запуске устройства.

При автоматическом назначении Unit ID основным устройством (Master) используются 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#
```

100.4 stack priority

Данная команда используется для настройки приоритета коммутатора в стеке. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

stack *CURRENT-UNIT-ID* **priority** *NEW-PRIORITY-NUMBER*
no stack *CURRENT-UNIT-ID* **priority**

Параметры

CURRENT-UNIT-ID	Укажите текущий Unit ID коммутатора.
NEW-PRIORITY-NUMBER	Укажите приоритет, который необходимо назначить Unit коммутатора в стеке. 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#
```

100.5 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. Чтобы отключить функцию Preempt, воспользуйтесь формой **no** этой команды.

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 preempt
Switch#
```

100.6 snmp-server enable traps stack

Данная команда используется для включения отправки trap-сообщений, касающихся стекирования. Чтобы отключить отправку trap-сообщений, касающихся стекирования, воспользуйтесь формой **no** этой команды.

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)#
```

100.7 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_Ring
My Box ID            : 1
Master ID            : 1
BK Master ID         : 2
Box Count            : 2

Box User Module              Prio-                    Prom      Runtime   H/W
ID  Set  Name          Exist rity  MAC                Version   Version   Version
--- ---- ------------- ----- ----- ------------------ --------- --------- -------
1   Auto DGS-1520-28MP Exist 32    80-26-89-15-28-00 1.00.010  1.00.022  A1
2   Auto DGS-1520-28   Exist 32    80-26-89-15-28-A0 1.00.010  1.00.022  A1
3   -    NOT_EXIST     No
4   -    NOT_EXIST     No
5   -    NOT_EXIST     No
6   -    NOT_EXIST     No
```

```
7    -     NOT_EXIST      No
8    -     NOT_EXIST      No

 Stack Bandwidth:
 Box     User Set           SIO1 Active    SIO2 Active
 ID      Bandwidth          Bandwidth      Bandwidth
 ----    ------------------ ---------      ---------
 1       2-port(sfp+)       1-port         1-port
 2       2-port(sfp+)       1-port         1-port
 3
 4
 5
 6
 7
 8

Switch#
```

101. Команды Storm Control

101.1 snmp-server enable traps storm-control

Данная команда используется, чтобы включить и настроить отправку SNMP-уведомлений для Storm Control. Для отключения отправки SNMP-уведомлений воспользуйтесь формой **no** этой команды.

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/отключения отправки SNMP-уведомлений для Storm Control. Если параметры не указаны, включены/отключены оба типа уведомлений. Если указан один из параметров, включен/отключен определенный тип уведомлений.

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)#
```

101.2 storm-control

Данная команда используется для защиты устройства от штормовых атак широковещательных и многоадресных пакетов или пакетов с неизвестным адресом назначения. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

storm-control {{broadcast | multicast | unicast} level {pps *PPS-RISE* **[***PPS-LOW***] | kbps** *KBPS-RISE* **[***KBPS-LOW***] |** *LEVEL-RISE* **[***LEVEL-LOW***]} | action {shutdown | drop | none}}**

no storm-control {broadcast | multicast | unicast | action}

Параметры

broadcast	Укажите для ограничения скорости широковещательной рассылки.
multicast	Укажите для ограничения скорости многоадресной рассылки.
unicast	Укажите, чтобы в режиме **shutdown** применять команду как к известным, так и к неизвестным одноадресным пакетам. При достижении на порту установленного лимита пакетов порт будет отключен. Если указан другой режим, команда будет применена только к неизвестным одноадресным пакетам.
level pps *PPS-RISE* **[***PPS-LOW***]**	Укажите пороговое значение пакетов в секунду. Диапазон значений: от 1 до 2147483647. Если минимальный уровень (Low Level) PPS не указан, значение по умолчанию составляет 80% от указанного максимального (Rise) PPS.
level kbps *KBPS-RISE* **[***KBPS-LOW***]**	Укажите пороговое значение скорости передачи трафика, полученного на порту, в битах в секунду. Диапазон значений: от 1 до 2147483647. Если минимальный уровень (Low Level) KBPS не указан, значение по умолчанию составляет 80% от указанного максимального (Rise) KBPS.
level *LEVEL-RISE* **[***LEVEL-LOW***]**	Укажите пороговое значение трафика, полученного на порту, в процентах от общей пропускной способности. 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

По умолчанию функция Storm Control для защиты от атак широковещательных, многоадресных и одноадресных (DLF) пакетов отключена.

При возникновении шторма действие по умолчанию – drop.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда может использоваться только для настройки интерфейса физического порта.

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.

Пороговое значение можно указать в виде процентного отношения полосы пропускания на порту, килобайт в секунду или количества пакетов в секунду.

Невозможно указать точный уровень подавления для процентного отношения (от 1 до 100) общей полосы пропускания для определенного интерфейса порта. В текущей формуле расчета предусмотрен размер пакета в 64 байта.

Если для Storm Control установлено действие **drop**, то пакет будет отброшен в случае, если скорость трафика превысит пороговое значение.

Если для Storm Control установлено действие **shutdown**, то в случае, когда нагрузка трафика отслеживаемых пакетов лавинной рассылки flooding превышает пороговое значение, порт переходит в отключенное состояние по причине ошибки.

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 2 установлен максимальный порог 70% с минимальным уровнем (Low Level) 60% и действием отбрасывания (drop).

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#storm-control broadcast level pps 500
Switch(config-if)#storm-control action shutdown
Switch(config-if)#exit
Switch(config)#interface eth1/0/2
Switch(config-if)#storm-control broadcast level 70 60
Switch(config-if)#storm-control action drop
Switch(config-if)#
```

101.3 storm-control polling

Данная команда используется для настройки интервала опроса (Polling Interval) для подсчета количества полученных пакетов. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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. Диапазон значений: от 5 до 600 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. 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 со значением 15 секунд.

```
Switch#configure terminal
Switch(config)#storm-control polling interval 15
Switch(config)#
```

101.4 show storm-control

Данная команда используется для отображения текущих настроек функции Storm Control.

show storm-control interface *INTERFACE-ID* **[, | -] [broadcast | multicast | unicast]**

Параметры

interface *INTERFACE-ID*	Укажите ID интерфейса порта.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.

-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
broadcast	(Опционально.) Укажите, чтобы отобразить текущие настройки шторма широковещательных пакетов (Broadcast Storm).
multicast	(Опционально.) Укажите, чтобы отобразить текущие настройки шторма многоадресных пакетов (Multicast Storm).
unicast	(Опционально.) Укажите, чтобы отобразить текущие настройки шторма одноадресных пакетов (DLF).

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если 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 в диапазоне интерфейсов Ethernet 1/0/1-1/0/6.

```
Switch#show storm-control interface eth1/0/1-6 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 примере ниже показано, как отобразить все настройки Storm Control для диапазона интерфейсов Ethernet 1/0/1-1/0/2.

```
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.

102. Команды Super VLAN

102.1 supervlan

Данная команда используется для настройки VLAN в качестве Super VLAN. Чтобы удалить назначение Super VLAN, воспользуйтесь формой **no** этой команды.

supervlan
no supervlan

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется 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)#
```

102.2 subvlan

Данная команда используется для добавления одной или нескольких Sub-VLAN в Super VLAN. Чтобы удалить Sub-VLAN, воспользуйтесь формой **no** этой команды.

subvlan *VLAN-ID* **[, | -]**
no subvlan [*VLAN-ID* **[, | -]]**

Параметры

VLAN-ID	Укажите VLAN ID в качестве Sub-VLAN. Диапазон значений: от 1 до 4094.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

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)#
```

102.3 subvlan-address-range

Данная команда используется для настройки диапазона IP-адресов Sub-VLAN. Чтобы удалить диапазон IP-адресов Sub-VLAN, воспользуйтесь формой **no** этой команды.

subvlan-address-range *START-IP-ADDRESS END-IP-ADDRESS*
no subvlan-address-range [*START-IP-ADDRESS END-IP-ADDRESS***]**

Параметры

START-IP-ADDRESS	Укажите начальный IP-адрес необходимой Sub-VLAN.
END-IP-ADDRESS	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)#
```

102.4 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 для отображения.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду 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           Inactive        192.168.10.1 - 192.168.10.50
               6           Inactive
               7           Inactive

Switch#
```

103. Команды Surveillance VLAN

103.1 surveillance vlan

Данная команда используется для глобального включения функции Surveillance VLAN и ее настройки. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

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 member-порт 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)#
```

103.2 surveillance vlan aging

Данная команда используется для настройки времени устаревания (Aging Time) для устаревших динамических member-портов Surveillance VLAN. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

surveillance vlan aging *MINUTES*
no surveillance vlan aging

Параметры

MINUTES	Укажите время устаревания Surveillance VLAN в диапазоне от 1 до 65535 минут.

По умолчанию

Значение по умолчанию – 720 минут.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для настройки времени устаревания для устройства видеонаблюдения (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. Указанное значение – 30 минут.

```
Switch#configure terminal
Switch(config)#surveillance vlan aging 30
Switch(config)#
```

103.3 surveillance vlan enable

Данная команда используется для включения функции Surveillance VLAN на портах. Чтобы отключить функцию Surveillance VLAN на портах, воспользуйтесь формой **no** этой команды.

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

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

Команда применяется 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 member-порт 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 интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#surveillance vlan enable
Switch(config-if)#
```

103.4 surveillance vlan mac-address

Данная команда используется для добавления уникального идентификатора организации (OUI), определяемого с устройства системы видеонаблюдения в Surveillance VLAN. Чтобы удалить OUI устройства Surveillance, воспользуйтесь формой **no** этой команды.

surveillance vlan mac-address *MAC-ADDRESS MASK* **[component-type {vms | vms-client | video-encoder | network-storage | other} description** *TEXT***]**

no surveillance vlan mac-address *MAC-ADDRESS MASK*

Параметры

MAC-ADDRESS	Укажите MAC-адрес OUI.
MASK	Укажите соответствующую битовую маску MAC-адреса OUI.
component-type	(Опционально.) Укажите устройство системы видеонаблюдения, которое может быть автоматически обнаружено при помощи Surveillance VLAN.
vms	(Опционально.) Укажите сервер VMS (Video Management Server – сервер для управления системой видеонаблюдения).
vms-client	(Опционально.) Укажите клиента VMS в системе видеонаблюдения.
video-encoder	(Опционально.) Укажите видеокодер в системе видеонаблюдения.
network-storage	(Опционально.) Укажите сетевое хранилище в системе видеонаблюдения.
other	(Опционально.) Укажите другие устройства в системе видеонаблюдения (IP Surveillance Devices).
description *TEXT*	(Опционально.) Укажите описание OUI. Максимальное количество символов – 32.

По умолчанию

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



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 применяется 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)#
```

103.5 surveillance vlan qos

Данная команда используется для настройки приоритета CoS для входящего трафика Surveillance VLAN. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

surveillance vlan qos *COS-VALUE*

no surveillance vlan qos

Параметры

COS-VALUE	Укажите приоритет Surveillance VLAN в диапазоне от 0 до 7.

По умолчанию

Значение по умолчанию – 5.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется 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. Указанное значение – 7.

```
Switch#configure terminal
Switch(config)#surveillance vlan qos 7
Switch(config)#
```

103.6 show surveillance vlan

Данная команда используется для отображения настроек Surveillance VLAN.

show surveillance vlan [interface [*INTERFACE-ID* **[, | -]]]**
show surveillance vlan device [interface [*INTERFACE-ID* **[, | -]]]**

Параметры

device	Укажите, чтобы отобразить информацию об изученных устройствах Surveillance.
interface	(Опционально.) Укажите, чтобы отобразить информацию о Surveillance VLAN на портах.
INTERFACE-ID	(Опционально.) Укажите порт, о котором необходимо отобразить информацию.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
–	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется 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, введите 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#
```

В данном примере показано, как отобразить изученные устройства Surveillance на интерфейсах Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch#show surveillance vlan device interface eth1/0/1-2

                                                Component Type/
 Interface       Device             Start Time  Description
 --------------  -----------------  ----------  ---------------
 eth1/0/1        00-01-02-03-00-01  2011-10-06  VMS
                                    09:00       IP Surveillance Device
 eth1/0/2        00-01-02-03-00-02  2011-10-06  VMS
                                    14:10       IP Surveillance Device
 eth1/0/2        F0-7D-68-03-44-A1  2011-10-06  D-Link Device
                                    17:15       user1

 Total Entries : 3

Switch#
```

104. Команды портов коммутатора

104.1 duplex

Данная команда используется для настройки режима дуплекса на интерфейсе физического порта. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

duplex {full | half | auto}
no duplex

Параметры

full	Укажите для работы порта в режиме полного дуплекса (Full-Duplex Mode).
half	Укажите для работы порта в режиме полудуплекса (Half-Duplex Mode).
auto	Укажите, чтобы режим дуплекса на порту был определен автосогласованием (Auto-Negotiation).

По умолчанию

Для интерфейсов 100Base-T, 2500Base-T и 10GBase-T параметр по умолчанию – **auto**.
Для интерфейсов 10GBase-R параметр по умолчанию – **full**.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Для модулей 2500Base-T и 10GBase-T нельзя использовать режим полудуплекса.

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.

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 eth1/0/1
Switch(config-if)#speed 100
Switch(config-if)#duplex auto
Switch(config-if)#
```

104.2 flowcontrol

Данная команда используется для настройки возможности управления потоком (Flow Control) на интерфейсе порта. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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 eth1/0/1
Switch(config-if)#flowcontrol on
Switch(config-if)#
```

104.3 mdix

Данная команда используется для настройки состояния MDIX порта. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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

Параметр по умолчанию – **auto**.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда неприменима на порту, к которому подключен оптоволоконный кабель.

Пример

В данном примере показано, как настроить режим Auto-MDIX Mode на интерфейсе Ethernet 1/0/1.

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

104.4 speed

Данная команда используется для настройки скорости интерфейса физического порта. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.



Примечание: скорости 10 Мбит/с, 100 Мбит/с и 2,5 Гбит/с недоступны на портах 10G.

speed {10 | 100 | 1000 [master | slave] | 2500 [master | slave] | 10giga [master | slave] | auto [*SPEED-LIST***]}**

no speed

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).
2500	Укажите, чтобы установить скорость 2,5 Гбит/с.
master | slave	Укажите статус порта: Master (основное устройство) или Slave (дополнительное устройство). Данный параметр применим только к устройствам, подключенным к порту 1000Base-T или 2500Base-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 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: **10**, **100**, **1000, 2500** и/или **10giga**. Если список не указан, будут анонсированы все скорости. Используйте дефис, чтобы разделить диапазоны значений. Используйте запятую для перечисления нескольких значений. Пробелы до и после символов недопустимы.

По умолчанию

Для интерфейсов 100Base-T, 2500Base-T и 10GBase-T по умолчанию скорость определяется

автоматически.

Для интерфейса 10GBase-R по умолчанию устанавливается фиксированная скорость 10 Гбит/с.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Если указанная скорость не поддерживается аппаратно, будет отображено сообщение об ошибке.

При подключении к интерфейсу 1000Base-T на скорости 1000 порт необходимо настроить как Master (основное устройство) или Slave (дополнительное устройство).

При подключении к интерфейсу 2500Base-T на скорости 1000 или 2500 порт необходимо настроить как Master (основное устройство) или Slave (дополнительное устройство).

При подключении к интерфейсу 10GBase-T на скорости 1000 или 10giga порт необходимо настроить как Master (основное устройство) или Slave (дополнительное устройство).

Если выбрана скорость 10giga, нельзя выбрать режим полудуплекса и наоборот.

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.

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 eth1/0/1
Switch(config-if)#speed auto 10,100
Switch(config-if)#
```

105. Команды управления системными файлами

105.1 boot config

Данная команда используется для указания конфигурационного файла, который будет использован при следующем запуске устройства.

boot config *URL*

Параметры

URL	Укажите URL конфигурационного файла, который будет использован при следующем запуске устройства.

По умолчанию

По умолчанию используется файл config.cfg.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы указать конфигурационный файл, который будет использован при следующем запуске устройства. По умолчанию используется файл config.cfg. 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)#
```

105.2 boot image

Данная команда используется для указания файла образа, который будет использован при следующем запуске устройства.

boot image [check] [all] *URL*

Параметры

check	(Опционально.) Укажите данный параметр для отображения информации о программном обеспечении для указанного файла (номер версии и описание модели).
all	(Опционально.) Укажите, чтобы применить файл образа для всех коммутаторов в стеке.
URL	Укажите URL файла образа для загрузки.

По умолчанию

По умолчанию используется один файл образа для загрузки.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы указать файл образа, который будет использован при следующем запуске устройства. После проверки и утверждения системой модели и контрольной суммы файл образа будет допущен.

Используйте параметр **check**, чтобы проверить, может ли быть допущен указанный файл образа для загрузки. Настройка команды **boot image** будет сохранена в энергонезависимой памяти NVRAM, благодаря которой сохраненный файл будет использован при следующем запуске устройства.

Образ резервного копирования определяется автоматически. Обычно ранее загруженный образ заменяется новым.

Пример

В данном примере показано, как указать файл под именем «switch-image1.had» в качестве файла образа для загрузки.

```
Switch#configure terminal
Switch(config)#boot image c:/switch-image1.had
Switch(config)#
```

В примере ниже 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.switch.had

----------------------
Image information
----------------------
Version: 1.00.022
Description: D-Link Corporation Gigabit Ethernet Smart Managed Switch

Switch(config)#
```

В следующем 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)#
```

105.3 clear running-config

Данная команда используется для удаления текущей конфигурации системы (running configuration).

clear running-config

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы удалить конфигурацию системы, сохраненную в DRAM-память. Данные конфигурации вернутся к настройкам по умолчанию. Перед использованием данной команды сохраните резервную копию конфигурации с помощью команды **copy** или выгрузите профиль конфигурации на TFTP-сервер.

При удалении настроек конфигурации системы информация о стеке не удаляется, однако, стираются параметры IP. Таким образом, все существующие удаленные подключения будут прерваны. После применения данной команды необходимо настроить IP-адрес через локальную консоль.

Пример

В данном примере показано, как удалить текущую конфигурацию системы.

```
Switch#clear running-config

This command will clear the system's configuration to the factory
default settings, including the IP address.
Clear running configuration? (y/n) [n] y

Switch#
```

105.4 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...
```

105.5 configure replace

Данная команда используется для замены текущей конфигурации указанным конфигурационным файлом.

configure replace {{tftp: *//LOCATION/FILENAME* **| sftp:** *//LOCATION/FILENAME***} | flash:** *FILENAME***}**
[force]

Параметры

tftp:	Укажите конфигурационный файл с TFTP-сервера.
//LOCATION/FILENAME	Укажите URL конфигурационного файла на TFTP-сервере.
sftp:	Укажите конфигурационный файл с SFTP-сервера. Перед тем, как использовать данный параметр, необходимо настроить SFTP-клиент.
//LOCATION/FILENAME	Укажите URL конфигурационного файла на SFTP-сервере.
flash:	Укажите конфигурационный файл из NVRAM.
FILENAME	Укажите имя конфигурационного файла, который хранится в NVRAM.
force	(Опционально.) Укажите, чтобы принудительно применить команду без дополнительного подтверждения.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы заменить текущую конфигурацию указанным конфигурационным файлом. Текущая конфигурация будет удалена перед применением указанной конфигурации.

Примечание: при выполнении данной команды текущая конфигурация полностью меняется на конфигурацию указанного файла. В указанном конфигурационном файле должна быть представлена полная конфигурация, а не частичная.

Перед использованием данной команды сохраните резервную копию конфигурации с помощью команды **copy** или выгрузите профиль конфигурации на TFTP-сервер.

Пример

В данном примере показано, как заменить текущую конфигурацию файлом «config.cfg», загруженным с TFTP-сервера.

```
Switch#configure replace tftp: //10.0.0.66/config.cfg

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. [y/n]:  y

 Accessing tftp://10.0.0.66/config.cfg...
 Transmission start...
 Transmission finished, file length 45422 bytes.
 Executing script file config.cfg ......
 Executing done

Switch#
```

В примере ниже 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#
```

105.6 copy

Данная команда используется для копирования файлов.

copy *SOURCE-URL DESTINATION-URL*

copy *SOURCE-URL* **{tftp: [***//LOCATION/DESTINATION-URL***] | sftp: [***//LOCATION/DESTINATION-URL***]}**

copy {tftp: [*//LOCATION/SOURCE-URL***] | sftp: [***//LOCATION/SOURCE-URL***]}** *DESTINATION-URL*

Параметры

SOURCE-URL	Укажите URL источника исходного файла, который необходимо скопировать. Особые формы URL представлены следующими ключевыми словами: Укажите **startup-config** в качестве URL источника, чтобы выгрузить конфигурацию, которая будет применена после запуска коммутатора, сохранить ее как файл в файловой системе или использовать в качестве текущей конфигурации. Укажите **running-config** в качестве URL источника, чтобы выгрузить текущую конфигурацию, сохранить ее в качестве загрузочной конфигурации или как файл в файловой системе. Укажите **flash**: **[***PATH-FILE-NAME***]** в качестве URL источника, чтобы скопировать исходный файл в файловую систему. Укажите **log** в качестве URL, чтобы выгрузить системный журнал на TFTP-сервер или сохранить его как файл в файловую систему. Укажите **attack-log** *UNIT-ID* в качестве URL источника, чтобы выгрузить журнал атак указанного unit.
DESTINATION-URL	Укажите URL назначения скопированного файла. Особые формы URL представлены следующими ключевыми словами: Укажите **running-config** в качестве URL назначения, чтобы применить конфигурацию к текущей конфигурации. Укажите **startup-config** в качестве URL назначения, чтобы сохранить конфигурацию, которую необходимо применить при следующем запуске. Текущая конфигурация будет сохранена в NVRAM, а имя файла будет совпадать с именем файла, указанным при использовании команды **boot config**. Укажите **flash: [***PATH-FILE-NAME***]** в качестве URL назначения, чтобы указать имя копируемого файла в файловой системе. При указании относительного пути файл будет загружен на все устройства в стеке и сохранен в текущем пути каждого unit. При указании абсолютного пути файл будет загружен в место, которое было задано абсолютным путем. При отсутствии информации о unit в абсолютном пути будет назначен основное устройство (Master).
LOCATION	(Опционально.) Укажите IPv4-адрес TFTP/SFTP-сервера или IPv6-адрес TFTP-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/SFTP-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 при помощи метода 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/SFTP-сервере, необходимо использовать URL с префиксом «tftp: //» или «sftp: //».

Чтобы загрузить образ программного обеспечения, используйте команду **copy tftp:** // или **copy sftp:** // для загрузки файла с TFTP/SFTP-сервера в файловую систему. Чтобы указать данный файл в качестве файла образа для загрузки, используйте команду **boot image**.

Пример

В данном примере показано, как настроить на коммутаторе текущую конфигурацию, загруженную с TFTP-сервера 10.1.1.254, используя метод increment. Имя конфигурационного файла: switch-config.cfg.

```
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 примере ниже 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 следующем 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#
```

Ниже показан пример немедленного сохранения файла «switch-config.cfg» в NVRAM с использованием метода 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 нижеприведенном 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 15710864 bytes.
 Transmission to slave start.................. Done.
 Transmission to slave finished, file length 15710864 bytes.
 Please wait, programming flash.............. 100 %
 Please wait, programming flash for language files .............Done.
 Wait slave programming flash complete...
 Done.

Switch#
```

В данном примере показано, как заменить текущую конфигурацию файлом, загруженным на SFTP-сервер.

```
Switch#configure replace sftp: //10.90.90.23/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

Address of remote host [10.90.90.23]?
Source filename [config.cfg]?
Destination filename [config.cfg]?
 Start, aborted by CTRL+C or Esc, remote_file_path is config.cfg
 Connecting to remote server 10.90.90.23
 Server's host key fingerprint (MD5):
 89:40:F4:5D:70:8B:97:13:44:D4:F2:79:1B:4E:EF:AB
 Unknown server, Are you sure you want to continue connecting (y/n)?:y
 User Name [Anonymous]:admin
 Password:****
 Download ................ 100 %
 Please wait, programming flash.............. Done.
 Executing script file config.cfg ......
 Executing done

Switch#
```

В нижеприведенном примере показано, как загрузить файл образа с SFTP-сервера на все устройства в стеке.

```
Switch#copy sftp: //10.90.90.23/sftpfile.had flash: sftpfile.had

Address of remote host [10.90.90.23]?
Source filename [sftpfile.had]?
Destination filename [sftpfile.had]?
 Start, aborted by CTRL+C or Esc, remote_file_path is sftpfile.had
 Connecting to remote server 10.90.90.23
 Server's host key fingerprint (MD5):
 89:40:F4:5D:70:8B:97:13:44:D4:F2:79:1B:4E:EF:AB
 Unknown server, Are you sure you want to continue connecting (y/n)?:y
 User Name [Anonymous]:admin
 Password:****
 Download ................ 100 %
 Please wait, programming flash.............. Done.
 Please wait, programming flash for language files .............Done.
 Wait slave programming flash complete...
 Done.

Switch#
```

105.7 ip tftp source-interface

Данная команда используется для указания интерфейса, IP-адрес которого будет использоваться в качестве адреса источника для инициирования TFTP-пакетов. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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

Параметры

INTERFACE-ID	Укажите IP-адрес интерфейса, который будет использоваться в качестве адреса источника для инициирования TFTP-пакетов.

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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 (только для DGS-1520-28 и DGS-1520-52) и VLAN.

Пример

В данном примере показано, как загрузить программное обеспечение с VLAN 1.

```
Switch#configure terminal
Switch(config)#ip tftp source-interface vlan 1
Switch(config)#
```

105.8 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 применяется для перезагрузки коммутатора.

Пример

В данном примере показано, как перезагрузить коммутатор.

```
Switch# reboot force_agree

Please wait, the switch is rebooting...
```

105.9 show boot

Данная команда используется для отображения настроек конфигурационного файла и загрузочного образа.

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

Параметры

UNIT-ID	(Опционально.) Укажите модуль (unit) для отображения.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется 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:/config.cfg


Switch#
```

105.10 show running-config

Данная команда используется для отображения команд текущего конфигурационного файла.

show running-config [effective | all] [interface *INTERFACE-ID* **| vlan** *VLAN-ID***]**

Параметры

effective	(Опционально.) Укажите, чтобы отобразить настройки команды, которые влияют на работу устройства. Все другие настройки STP (настройки более низкого уровня) не отображаются. Настройки более низкого уровня отображаются, только когда включены настройки более высокого уровня.
all	(Опционально.) Укажите, чтобы отобразить все команды конфигурации, включая команды, которые соответствуют параметрам по умолчанию.
interface *INTERFACE-ID*	(Опционально.) Укажите, чтобы отобразить команды конфигурации указанного интерфейса.
vlan *VLAN-ID*	(Опционально.) Укажите, чтобы отобразить команды конфигурации указанной VLAN.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда применяется для отображения текущей конфигурации. Если не указаны дополнительные параметры, будет отображена только изменяемая часть конфигурации, а не конфигурация по умолчанию.

Пример

В данном примере показано, как отобразить содержимое текущего конфигурационного файла.

```
Switch#show running-config
Building configuration...

Current configuration : 1891 bytes

!-----------------------------------------------------------------------------
!                 DGS-1520-28MP Gigabit Ethernet Smart Managed Switch
!                                 Configuration
!
!                             Firmware: Build 1.00.022
!           Copyright(C) 2020 D-Link Corporation. All rights reserved.
!-----------------------------------------------------------------------------

stack
!
ip http timeout-policy idle 36000
ignore wizard
!
line console
 session-timeout 0
!
line telnet
!
line ssh
!
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

105.11 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

Данная команда применяется 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-1520-28MP Gigabit Ethernet Smart Managed Switch
!                                Configuration
!
!                            Firmware: Build 1.00.022
!           Copyright(C) 2020 D-Link Corporation. All rights reserved.
!----------------------------------------------------------------------------

# AAA START
# AAA END
!
# COMMAND LEVEL START
# COMMAND LEVEL END
# LEVEL START
# LEVEL END
# ACCOUNT START
# ACCOUNT END
!
ip http timeout-policy idle 36000
ignore wizard
!
# LOGIN START
line console
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

106. Команды System Log

106.1 clear logging

Данная команда используется для удаления сообщений из внутреннего буфера.

clear logging

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда позволяет удалить все сообщения из внутреннего буфера.

Пример

В данном примере показано, как удалить все сообщения из внутреннего буфера.

```
Switch#clear logging

Clear logging? (y/n) [n] y

Switch#
```

106.2 logging on

Данная команда используется для включения логирования системных сообщений. Используйте форму **no**, чтобы отключить логирование системных сообщений.

logging on
no logging on

Параметры

Нет.

По умолчанию

По умолчанию опция включена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для включения логирования системных сообщений используйте команду **logging on** в режиме Global Configuration Mode. Данная команда регистрирует отладочные сообщения (debug) и сообщения об ошибках (error) в системном журнале (логе). Процесс сохранения сообщений идет асинхронно процессам, генерирующим данные сообщения. Используйте форму **no** этой команды для отключения данной функции.

Процесс логирования контролирует распределение сообщений по нескольким направлениям, таким как буфер логирования, консоль или syslog-сервер. Для включения или отключения функции логирования для каждого направления индивидуально можно использовать команды глобального режима конфигурирования **logging buffered** и **logging server**. Однако если команда **logging on** отключена, сообщения по данным направлениям отправляться не будут. Если команда **logging on** включена, одновременно с ней будет активирована команда **logging buffered**.

Пример

В данном примере показано, как включить логирование системных сообщений.

```
Switch#configure terminal
Switch(config)#logging on
WARNING: The command takes effect and the logging buffered is enabled at the same time.
Switch(config)#
```

106.3 logging buffered

Данная команда используется для включения логирования системных сообщений во внутренний буфер. При использовании формы **no** команда отключит логирование системных сообщений во внутренний буфер. Используйте команду **default logging buffered**, чтобы вернуться к настройкам по умолчанию.

logging buffered [severity {*SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***] [write-delay {***SECONDS* **| infinite}]**

no logging buffered

default logging buffered

Параметры

SEVERITY-LEVEL	(Опционально.) Укажите уровень важности системных сообщений. Сообщения с заданным уровнем важности или выше передаются во внутренний буфер. Доступны значения от 0 до 7, где 0 – наиболее высокий уровень важности. Уровни важности сообщений: **0** – emergencies – чрезвычайные ситуации, система не работоспособна; **1** – alerts – тревога, система требует немедленного вмешательства; **2** – critical – состояние системы критическое; **3** – errors – сообщения об ошибках; **4** – warnings – предупреждения о возможных проблемах; **5** – notifications – уведомления о нормальных, но важных событиях; **6** – informational – информационные сообщения; **7** – debugging – отладочные сообщения. Если значение не указано, по умолчанию используется уровень важности warnings (**4**).
SEVERITY-NAME	(Опционально.) Укажите название уровня важности системных сообщений: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
discriminator	(Опционально.) Укажите discriminator для фильтрации сообщений, отправляемых во внутренний буфер.
write-delay *SECONDS*	(Опционально.) Укажите, чтобы отложить периодическую запись буфера логирования во flash на указанное количество секунд. Если параметр не указан, значение по умолчанию – 300 секунд.

По умолчанию

По умолчанию используется уровень важности warning (4).

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Системные сообщения можно передать в локальный буфер и другие точки назначения. Перед отправкой в другие точки назначения сообщения должны поступить в локальный буфер.

Команда не применяется, если указанный discriminator не существует. В этом случае применяются настройки по умолчанию.

Укажите уровень важности сообщений для ограничения системных сообщений, логируемых в буфер (это позволит уменьшить количество зарегистрированных сообщений). Сообщения указанного уровня или выше логируются в буфер. При заполнении буфера старые записи удаляются, чтобы освободить место для новых сообщений.

Содержимое буфера периодически сохраняется во flash-память, чтобы при перезагрузке сообщения можно было восстановить. При необходимости можно задать интервал для сохранения записей из буфера во FLASH-память. При перезагрузке содержимое сообщений, сохраняемых во flash-память, будет перезагружено в буфер логирования.

Пример

В данном примере показано, как включить логирование сообщений в буфер и ограничить логирование сообщений с уровнем важности errors или выше.

```
Switch#configure terminal
Switch(config)#logging buffered severity errors
Switch(config)#
```

106.4 logging console

Данная команда используется для включения логирования системных сообщений в локальной консоли. При использовании формы **no** команда отключит логирование сообщений в локальной консоли и вернет настройки по умолчанию.

logging console [severity {*SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***]**
no logging console

Параметры

SEVERITY-LEVEL	(Опционально.) Укажите уровень важности системных сообщений. Сообщения с заданным уровнем важности или выше передаются во внутренний буфер. Доступны значения от 0 до 7, где 0 – наиболее высокий уровень важности. Уровни важности сообщений: **0** – emergencies – чрезвычайная ситуация, система не работоспособна, **1** – alerts – тревога, система требует немедленного вмешательства, **2** – critical – состояние системы критическое, **3** – errors – сообщения об ошибках, **4** – warnings – предупреждения о возможных проблемах, **5** – notifications – уведомления о нормальных, но важных событиях, **6** – informational – информационные сообщения, **7** – debugging – отладочные сообщения. Если значение не указано, по умолчанию используется уровень важности warnings (**4**).

SEVERITY-NAME	(Опционально.) Укажите название уровня важности системных сообщений: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
discriminator	(Опционально.) Укажите discriminator для фильтрации сообщений, отправляемых в локальный буфер.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Системные сообщения можно логировать в локальный буфер сообщений, локальную консоль или другие точки назначения. Перед отправкой на консоль сообщения должны предварительно поступить в локальный буфер.

Команда не применяется, если указанный discriminator не существует. В этом случае будут применяться настройки по умолчанию.

Укажите уровень важности сообщений для ограничения системных сообщений, логируемых в консоли. Сообщения указанного уровня или выше будут логироваться в локальную консоль.

Пример

В данном примере показано, как включить логирование сообщений в локальную консоль и ограничить логирование сообщений с уровнем важности errors или выше.

```
Switch#configure terminal
Switch(config)#logging console severity errors
Switch(config)#
```

106.5 logging monitor

Данная команда используется для включения логирования системных сообщений на терминалы, например, Telnet и SSH. Используйте форму **no**, чтобы отключить данную функцию.

logging monitor [severity {*SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***]**
no logging monitor

Параметры

SEVERITY-LEVEL	(Опционально.) Укажите уровень важности системных сообщений. Сообщения с заданным уровнем важности или выше передаются во внутренний буфер. Доступны значения от 0 до 7, где 0 – наиболее высокий уровень важности. Уровни важности сообщений: **0** – emergencies – чрезвычайная ситуация, система не работоспособна, **1** – alerts – тревога, система требует немедленного вмешательства, **2** – critical – состояние системы критическое, **3** – errors – сообщения об ошибках, **4** – warnings – предупреждения о возможных проблемах, **5** – notifications – уведомления о нормальных, но важных событиях, **6** – informational – информационные сообщения, **7** – debugging – отладочные сообщения. Если значение не указано, по умолчанию используется уровень важности warnings (**4**).
SEVERITY-NAME	(Опционально.) Укажите название уровня важности системных сообщений: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
discriminator	(Опционально.) Укажите discriminator для фильтрации сообщений, отправляемых во внутренний буфер.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Системные сообщения можно передать в локальный буфер и другие точки назначения. Перед отправкой в другие точки назначения сообщения должны поступить в локальный буфер.

Команда не применяется, если указанный discriminator не существует. В этом случае применяются настройки по умолчанию.

Укажите уровень важности сообщений для ограничения системных сообщений, логируемых в терминал. Сообщения указанного уровня или выше логируются в терминал.

Пример

В данном примере показано, как включить логирование сообщений в терминал и ограничить логирование сообщений с уровнем важности errors или выше.

```
Switch#configure terminal
Switch(config)#logging monitor severity errors
Switch(config)#
```

106.6 logging discriminator

Данная команда используется при создании discriminator для дальнейшей фильтрации сообщений syslog, отправляемых в различные точки назначения. При использовании формы **no** команда удалит discriminator.

logging discriminator *NAME* **[facility {drops** *STRING* **| includes** *STRING***}] [severity {drops** *SEVERITY-LIST* **| includes** *SEVERITY-LIST***}]**

no discriminator *NAME*

Параметры

NAME	Укажите имя discriminator.
facility	(Опционально.) Укажите, чтобы использовать под-фильтр на основе категории facility.
STRING	Укажите одно или более имен facility. Если используется несколько имен, они должны быть разделены запятой без пробелов.
includes	Укажите для включения совпадающих сообщений. Несовпадающие сообщения будут фильтроваться.
drops	Укажите для фильтрации совпадающих сообщений.
severity	(Опционально.) Укажите под-фильтр на основе совпадений с уровнем важности.
SEVERITY- LIST	Укажите список уровней важности для фильтрации или включения.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Настраивается существующий параметр discriminator. При вводе команды предыдущие настройки будут заменены новыми. Ассоциируйте discriminator с командами **logging buffered** и **logging server**.

Пример

В данном примере показано, как создать discriminator с именем «buffer-filter», указывающим два подфильтра: один на основе уровня важности, а другой на основе facility.

```
Switch#configure terminal
Switch(config)#logging discriminator buffer-filter facility includes STP severity includes 1-4,6
Switch(config)#
```

106.7 logging server

Данная команда используется для включения логирования системных сообщений на указанный syslog-сервер. При использовании формы **no** команда удалит syslog-сервер с указанным адресом из списка syslog-серверов.

logging server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [severity {***SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [facility {***FACILITY-NUM* **|** *FACILITY-NAME***}] [discriminator** *NAME***] [port** *UDP-PORT***]**

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

Параметры

IP-ADDRESS	Укажите IP-адрес syslog-сервера.
IPV6-ADDRESS	Укажите IPv6-адрес серверного узла логирования.
SEVERITY-LEVEL	(Опционально.) Укажите уровень важности системных сообщений. Сообщения с заданным уровнем важности или выше передаются во внутренний буфер. Доступны значения от 0 до 7, где 0 – наиболее высокий уровень важности. Уровни важности сообщений: **0** – emergencies – чрезвычайная ситуация, система не работоспособна, **1** – alerts – тревога, система требует немедленного вмешательства, **2** – critical – состояние системы критическое, **3** – errors – сообщения об ошибках, **4** – warnings – предупреждения о возможных проблемах, **5** – notifications – уведомления о нормальных, но важных событиях, **6** – informational – информационные сообщения, **7** – debugging – отладочные сообщения. Если значение не указано, по умолчанию используется уровень важности warnings (**4**).

SEVERITY-NAME	(Опционально.) Укажите название уровня важности системных сообщений. Имена уровней важности: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
FACILITY-NUM	(Опционально.) Укажите десятичное значение от 0 до 23 для facility. Если значение не указано, по умолчанию будет использоваться local7 (**23**). Для более подробной информации обратитесь к параграфу Использование команды.
FACILITY-NAME	(Опционально.) Укажите имя 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, на локальную консоль или удаленные узлы. Перед отправкой на сервер логирования сообщения должны поступить в локальный буфер сообщений.

Ниже представлена таблица значений Facility.

Номер Facility	**Имя Facility**	**Описание**
0	kern	Сообщения ядра
1	user	Сообщения пользовательского уровня
2	mail	Почтовая система
3	daemon	Системные службы (daemons)

4	auth1	Сообщения системы безопасности/авторизации
5	syslog	Сообщения, генерируемые syslog
6	lpr	Подсистема печати (Line Printer)
7	news	Подсистема сетевых новостей
8	uucp	Подсистема UUCP
9	clock1	Службы времени (Clock daemon)
10	auth2	Сообщения системы безопасности/авторизации
11	ftp	Служба FTP
12	ntp	Подсистема NTP
13	logaudit	Журнал аудита
14	logalert	Аварийный журнал
15	clock2	Служба времени (примечание 2)
16	local0	Локальное использование 0 (local0)
17	local1	Локальное использование 1 (local1)
18	local2	Локальное использование 2 (local2)
19	local3	Локальное использование 3 (local3)
20	local4	Локальное использование 4 (local4)
21	local5	Локальное использование 5 (local5)
22	local6	Локальное использование 6 (local6)
23	local7	Локальное использование 7 (local7)

Пример

В данном примере показано, как включить логирование системных сообщений с уровнем важности выше warnings на удаленном узле 20.3.3.3.

```
Switch#configure terminal
Switch(config)#logging server  20.3.3.3 severity warnings
Switch(config)#
```

106.8 logging smtp

Данная команда позволяет настроить отправку логов на электронную почту. При использовании формы **no** команда отключит отправку системных сообщений на электронную почту и вернет настройки по умолчанию.

logging smtp [severity {*SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***]**
no logging smtp

Параметры

SEVERITY-LEVEL	(Опционально.) Укажите уровень важности системных сообщений. Сообщения с заданным уровнем важности или выше передаются во внутренний буфер. Доступны значения от 0 до 7, где 0 – наиболее высокий уровень важности. Уровни важности сообщений: **0** – emergencies – чрезвычайная ситуация, система не работоспособна, **1** – alerts – тревога, система требует немедленного вмешательства, **2** – critical – состояние системы критическое, **3** – errors – сообщения об ошибках, **4** – warnings – предупреждения о возможных проблемах, **5** – notifications – уведомления о нормальных, но важных событиях, **6** – informational – информационные сообщения, **7** – debugging – отладочные сообщения. Если значение не указано, по умолчанию используется уровень важности warnings (**4**).
SEVERITY-NAME	(Опционально.) Укажите название уровня важности системных сообщений. Имена уровней важности: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
discriminator *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)#
```

106.9 logging source-interface

Данная команда используется для указания IP-адреса интерфейса, который будет использоваться в качестве адреса источника для отправки пакетов syslog. При использовании формы **no** команда вернется к настройкам по умолчанию.

logging source-interface *INTERFACE-ID*

no logging source-interface

Параметры

INTERFACE-ID	Укажите IP-адрес интерфейса, который будет использоваться в качестве адреса источника для отправки пакетов syslog.

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда используется для указания IP-адреса интерфейса, который будет использоваться в качестве адреса источника для отправки пакетов syslog.

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 vlan100
Switch(config)#
```

106.10 show logging

Данная команда используется для просмотра системных сообщений, хранящихся во внутреннем буфере.

show logging [all | [*REF-SEQ*] [+ *NN* | - *NN*]]

Параметры

all	(Опционально.) Укажите для вывода всех записей журнала, начиная с последних.
REF-SEQ	(Опционально.) Укажите порядковый номер, с которого начнется вывод записей.
+ *NN*	(Опционально.) Укажите количество сообщений, которое необходимо отобразить после указанного порядкового номера. Если номер не указан, отображение начинается с самого раннего сообщения в буфере.
- *NN*	(Опционально.) Укажите количество сообщений, которое необходимо отобразить до указанного номера. Если номер не указан, отображение начинается с последнего сообщения в буфере.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда используется для просмотра сообщений, хранящихся во внутреннем буфере.

Каждое сохраненное в буфер сообщение соотносится с определенным порядковым номером. При регистрации сообщению назначается порядковый номер, начиная с 1. При достижении значения 100000 нумерация вновь начнется с 1.

Если задается количество сообщений, которые необходимо отобразить после указанного порядкового номера, то вывод сообщений начнется с более ранних записей. Если задается количество сообщений, которые предшествуют указанному порядковому номеру, то вывод сообщений начнется с более поздних записей.

Если команда введена без опций, система выводит 200 записей, начиная с последнего сообщения.

Пример

В данном примере показано, как отобразить сообщения в локальном буфере сообщений.

```
Switch#show 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#
```

106.11 show attack-logging

Данная команда используется для просмотра зарегистрированных сообщений об атаках.

show attack-logging unit *UNIT-ID* **[index** *INDEX***]**

Параметры

UNIT-ID	Укажите модуль (Unit), для которого необходимо отобразить зарегистрированные сообщения об атаке.
index *INDEX*	Укажите список порядковых номеров записей, которые необходимо отобразить. Если значение не указано, отображаться будут все записи из журнала атак.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для просмотра сообщений об атаках в журнале. К таким сообщениям относятся записи, связанные с функционалом DOS и port-security. В этом случае может генерироваться большое количество подобных сообщений, из-за чего в системе быстро заканчивается память для хранения записей журнала. Чтобы этого избежать, в системный журнал сохраняется только первое сообщение данного типа, генерируемое каждую минуту, а остальные хранятся в отдельной таблице с именем attack log (журнал атак).

Пример

В данном примере показано, как отобразить первое зарегистрированное сообщение об атаке.

```
Switch#show attack-logging index 1
Attack log messages:
1  2015-03-24 15:00:14 CRIT(2) Land attack is blocked from (IP: 10.72.24.1 Port: 7)
Switch#
```

106.12 clear attack-logging

Данная команда используется для удаления сообщений об атаках.

clear attack-logging {unit *UNIT-ID* **| all}**

Параметры

unit *UNIT-ID*	Укажите модуль (Unit), для которого необходимо удалить зарегистрированные сообщения об атаке.
all	Укажите для удаления всех записей.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для удаления сообщений об атаках.

Пример

В данном примере показано, как удалить все логированные сообщения об атаках.

```
Switch#clear attack-logging all
Switch#
```

107. Команды времени и SNTP

107.1 clock set

Данная команда используется для установки системного времени вручную.

clock set *HH:MM:SS DAY MONTH YEAR*

Параметры

HH:MM:SS	Укажите текущее время: часы (24-часовой формат), минуты и секунды.
DAY	Укажите текущий день месяца.
MONTH	Укажите текущий месяц (January, Jan, February, Feb и т. д.).
YEAR	Укажите текущий год без сокращений.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если система синхронизируется с помощью любого действующего внешнего механизма синхронизации, такого как SNTP, необходимо установить системное время. Используйте данную команду, если другие источники времени недоступны. Время, указанное в данной команде, принадлежит к часовому поясу, заданному конфигурацией команды **clock timezone**. Если устройство поддерживает функцию RTC (часы реального времени), время синхронизируется с RTC. Настроенные часы не будут сохранены в файле конфигурации.

Сервер SNTP является основным источником времени: даже если системное время было настроено вручную, при подключении к серверу SNTP время будет синхронизировано с его показателями.

Пример

В 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#
```

107.2 clock summer-time

Данная команда используется для настройки автоматического перехода на летнее время. Чтобы отключить автоматический переход на летнее время, воспользуйтесь формой **no** этой команды.

clock summer-time recurring *WEEK DAY MONTH HH:MM WEEK DAY MONTH HH:MM* **[***OFFSET***]**

clock summer-time date *DATE MONTH YEAR HH:MM DATE MONTH YEAR HH:MM* **[***OFFSET***]**

no clock summer-time

Параметры

recurring	Укажите дату начала и окончания летнего времени (день недели и месяц).
date	Укажите точную дату начала и окончания летнего времени.
WEEK	Укажите номер недели месяца (от 1 до 4) или слово «last», с помощью которого будет указана последняя неделя месяца.
DAY	Укажите день недели (sun, mon и т. д.).
DATE	Укажите день месяца (от 1 до 31).
MONTH	Укажите порядковый номер месяца в диапазоне от 1 до 12, где 1 – это январь, 2 – февраль и т. д.
YEAR	Укажите года, чтобы задать необходимый интервал для применения перехода на летнее время.
HH:MM	Укажите время (24-часовой формат) в часах и минутах.
OFFSET	(Опционально.) Укажите количество минут, которое нужно добавить при переходе на летнее время. Значение по умолчанию – 60. 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 apr 2:00 last sun oct 2:00
Switch(config)#
```

107.3 clock timezone

Данная команда используется для настройки и отображения часового пояса. Чтобы настроить время в формате UTC (всемирное координированное время), воспользуйтесь формой **no** этой команды.

clock timezone {+ | -} *HOURS-OFFSET* **[***MINUTES-OFFSET***]**
no clock timezone

Параметры

+	Укажите количество часов, которое необходимо прибавить к UTC.
-	Укажите количество часов, которое необходимо вычесть из UTC.
HOURS-OFFSET	Укажите разницу во времени с UTC в часах.
MINUTES-OFFSET	(Опционально.) Укажите разницу во времени с UTC в минутах.

По умолчанию

Часовой пояс по умолчанию – UTC.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Время, полученное с сервера SNTP, синхронизируется с форматом UTC. При настройке местного времени учитывается формат UTC, часовой пояс и настройки перехода на летнее время.

Пример

В данном примере показано, как настроить часовой пояс PST (Северноамериканское Тихоокеанское Стандартное Время), который на 8 часов опережает время UTC.

```
Switch#configure terminal
Switch(config)#clock timezone - 8
Switch(config)#
```

107.4 show clock

Данная команда используется для отображения информации о времени и дате.

show clock

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Также данная команда применяется 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          : 00:02:17, 2019-01-01
    Time Zone             : UTC +00:00
    Daylight Saving Time  : Disabled

Switch#
```

107.5 show sntp

Данная команда используется для отображения информации о сервере SNTP.

show sntp

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о сервере SNTP.

Пример

В данном примере показано, как отобразить информацию об SNTP.

```
Switch#show sntp

SNTP Status               : Enabled
SNTP Poll Interval        : 720 sec

SNTP Server Status:

SNTP Server                                    Version Last Receive
---------------------------------------------- ------- ---------------
10.0.0.11                                      4       00:02:02
10::2                                          ------- ---------------
FE80::1111%vlan1                               ------- ---------------
---------------------------------------------- ------- ---------------

Total Entries:3

Switch#
```

107.6 sntp server

Данная команда используется для синхронизации системного времени с сервером SNTP. Чтобы удалить сервер из списка серверов SNTP, воспользуйтесь формой **no** этой команды.

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

Параметры

IP-ADDRESS	Укажите IP-адрес сервера, который обеспечивает синхронизацию времени.
IPV6-ADDRESS	Укажите IPv6-адрес сервера времени.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

SNTP – это упрощенная клиентская версия NTP. В отличие от NTP, SNTP может получать время только от серверов NTP; его нельзя использовать для предоставления времени другим системам. SNTP обеспечивает время с погрешностью 100 миллисекунд от точного времени, но, в отличии от NTP, не обеспечивает сложных механизмов фильтрации и статистической обработки. Кроме того, SNTP не проверяет подлинность трафика, хотя с помощью настройки расширенного списка доступа можно обеспечить определённую степень защиты.

Введите данную команду один раз для каждого сервера NTP. 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)#
```

107.7 sntp enable

Данная команда используется для включения функции SNTP. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

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 применяется для включения/отключения функции SNTP.

Пример

В данном примере показано, как включить функцию SNTP.

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

107.8 sntp interval

Данная команда используется для настройки интервала синхронизации часов SNTP-клиента с сервером. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

sntp interval *SECONDS*
no sntp interval

Параметры

SECONDS	Укажите интервал синхронизации в диапазоне от 30 до 99999 секунд.

По умолчанию

Значение по умолчанию – 720 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для настройки интервала опроса (Polling Interval).

Пример

В данном примере показано, как настроить интервал опроса. Указанное значение – 100 секунд.

```
Switch#configure terminal
Switch(config)#sntp interval 100
Switch(config)#
```

108. Команды временного диапазона

108.1 periodic

Данная команда используется для указания профиля диапазона времени. Чтобы удалить указанный временной диапазон, воспользуйтесь формой **no** этой команды.

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*	Укажите день недели (monday, tuesday, wednesday, thursday, friday, saturday, sunday) и время в формате ЧЧ:ММ. Конечный день недели, совпадающий с начальным, можно не указывать.

По умолчанию

Нет.

Режим ввода команды

Time-range Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Новый период может частично совпадать с предыдущим. Если начало и завершение нового периода соответствуют началу и завершению предыдущего периода, будет отображено сообщение об ошибке и новый период не будет задан. При удалении необходимо полностью указать заданный ранее период. Если период указан не полностью или указано сразу несколько периодов, будет отображено сообщение об ошибке.

Пример

В данном примере показано, как создать временной интервал, включающий промежутки с 09:00 до 12:00 ежедневно и с 00:00 субботы до 00:00 понедельника, а также как удалить период с 09:00 до 12:00 ежедневно.

```
Switch#configure terminal
Switch(config)#time-range rdtime
Switch(config-time-range)#periodic daily 9:00 to 12:00
Switch(config-time-range)#periodic weekly saturday 00:00 to monday 00:00
Switch(config-time-range)#no periodic daily 9:00 to 12:00
Switch(config-time-range)#
```

108.2 show time-range

Данная команда используется для отображения конфигурации профиля диапазона времени.

show time-range [*NAME***]**

Параметры

NAME	(Опционально.) Укажите имя профиля диапазона времени для отображения.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если параметр не указан, будут отображены все настроенные профили диапазона времени.

Пример

В данном примере показано, как отобразить все настроенные профили.

```
Switch#show time-range

Time Range Profile: rdtime
Daily 09:00 to 12:00
Weekly Saturday   00:00 to Monday     00:00

Total Entries: 1

Switch#
```

108.3 time-range

Данная команда используется для указания профиля диапазона времени и входа в режим Time-Range Configuration Mode. Чтобы удалить временной диапазон, воспользуйтесь формой **no** этой команды.

time-range *NAME*
no time-range *NAME*

Параметры

NAME	Укажите имя профиля диапазона времени, который необходимо настроить. Максимальное 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)#
```

109. Команды Traffic Segmentation

109.1 show traffic-segmentation forward

Данная команда используется для отображения конфигурации Traffic Segmentation на указанных или всех портах.

show traffic-segmentation forward [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейсы для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Если параметр не указан, будет отображена конфигурация Traffic Segmentation для всех портов.

Пример

В данном примере показано, как отобразить конфигурацию Traffic Segmentation для интерфейса Ethernet 1/0/1.

```
Switch#show traffic-segmentation forward interface eth1/0/1

Interface        Forwarding Domain
-------------    ----------------------------------------------------------------
eth1/0/1         eth1/0/3-1/0/6

Total Entries: 1

Switch#
```

109.2 traffic-segmentation forward

Данная команда используется для ограничения продвижения пакетов в L2 домене, приходящих на настроенный порт. Чтобы удалить ограничение продвижения пакетов в L2 домене, воспользуйтесь формой **no** этой команды.

traffic-segmentation forward interface *INTERFACE-ID* **[, | -]**
no traffic-segmentation forward interface *INTERFACE-ID* **[, | -]**

Параметры

INTERFACE-ID	Укажите разрешенные интерфейсы необходимых физических портов.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если домен продвижения пакетов задан Traffic Segmentation, то пакеты, получаемые портом, будут ограничены пакетами, отправленными интерфейсами внутри заданного L2 домена. Если ограничение продвижения пакетов в домене L2 не указано, то получение портом пакетов не ограничено.

Команду **traffic-segmentation forward** можно применять 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 интерфейса Ethernet 1/0/1. Установленное ограничение: от интерфейса Ethernet 1/0/3 до Ethernet 1/0/6.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#traffic-segmentation forward interface eth1/0/3-6
Switch(config-if)#
```

110. Команды Transport Layer Security (TLS)

110.1 no certificate

Данная команда используется для удаления импортированного сертификата.

no certificate *NAME*

Параметры

NAME	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. Доверенная точка (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)#
```

110.2 crypto pki import pem

Данная команда используется для импорта сертификата ЦС (Центра Сертификации/Certificate Authority) или сертификата коммутатора и ключей в доверенной точке (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

TRUSTPOINT	Укажите имя trust point, которое ассоциировано с импортированными сертификатами и парами ключей.
FILE-SYSTEM	Укажите файловую систему для сертификатов и пар ключей. После указанной файловой системы необходимо использовать двоеточие «:». Например, «flash:» указывает, что файловая система является локальной.
DIRECTORY	(Опционально.) Укажите имя каталога для импорта сертификатов и пар ключей. Возможен импорт в коммутатор или на TFTP-сервер.
FILE-NAME	Укажите имя сертификатов и пар ключей, которые необходимо импортировать. По умолчанию к имени сертификата ЦС добавляется .ca, к закрытому ключу – .prv, к сертификату – .crt.
password *PASSWORD-PHRASE*	(Опционально.) Укажите зашифрованную фразу пароля для отмены шифрования при импорте закрытых ключей. Максимальное количество символов в строке – 64. Если фраза пароля не указана, используется пустая строка.
tftp	Укажите URL источника для сетевого TFTP-сервера.
IP-ADDRESS	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

Global Configuration 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. Доверенная точка 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 доверенную точку (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)#
```

110.3 crypto pki trustpoint

Данная команда используется для настройки доверенной точки trust point на коммутаторе. Чтобы удалить все сертификаты и пары ключей, ассоциированные с определенной trust point, воспользуйтесь формой **no** этой команды.

crypto pki trustpoint *NAME*
no crypto pki trustpoint *NAME*

Параметры

NAME	Укажите имя доверенной точки (trust point).

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы настроить доверенную точку (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)#
```

110.4 crypto pki certificate chain

Данная команда используется для входа в режим Certificate Chain Configuration Mode.

crypto pki certificate chain *NAME*

Параметры

NAME	Укажите имя доверенной точки (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 Certificate Chain Configuration Mode. Если указанного имени доверенной точки (trust point) не существует, будет отображено сообщение об ошибке.

Пример

В данном примере показано, как войти в режим Certificate Chain Configuration Mode.

```
Switch#configure terminal
Switch(config)#crypto pki certificate chain TP1
Switch(trustpoint)#
```

110.5 crypto pki certificate generate

Данная команда используется для генерирования нового самоподписанного сертификата.

crypto pki certificate generate

Параметры

Нет.

По умолчанию

По умолчанию коммутатор автоматически генерирует случайный встроенный сертификат.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы сгенерировать новый самоподписанный сертификат. Данная

команда применяется независимо от того, сгенерирован ли встроенный самоподписанный сертификат или нет. Коммутатор сгенерирует новый самоподписанный сертификат автоматически, если после загрузки коммутатора сертификат не был обнаружен.

Сертификат, который был сгенерирован с помощью данной команды, не влияет на сертификаты, загруженные пользователем.



Примечание: в данной команде поддерживается только самоподписанный сертификат RSA с длиной ключа 2048.

Пример

В данном примере показано, как сгенерировать новый самоподписанный сертификат.

```
Switch#configure terminal
Switch(config)#crypto pki certificate generate

Start generating key ...
Start generating self-signed certificate ...
Done.
Switch(config)#
```

110.6 primary

Данная команда используется для назначения указанной доверенной точки (trust point) в качестве основной trust point коммутатора. Для отмены назначения воспользуйтесь формой **no** этой команды.

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 доверенную точку (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)#
```

110.7 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 для отображения.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если параметры не указаны, будут отображены 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#
```

110.8 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.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если имя политики SSL service policy не указано, будут отображены все SSL service policy.

Пример

В данном примере показано, как отобразить все SSL service policy.

```
Switch#show ssl-service-policy

SSL Policy Name        : test
  Enabled Versions     :
    TLS 1.0
    TLS 1.1
    TLS 1.2
  Enabled CipherSuites :
    DHE_DSS_WITH_3DES_EDE_CBC_SHA,
    RSA_WITH_3DES_EDE_CBC_SHA,
    RSA_WITH_AES_128_CBC_SHA,
    RSA_WITH_AES_256_CBC_SHA,
    RSA_WITH_AES_128_CBC_SHA256,
    RSA_WITH_AES_256_CBC_SHA256,
    DHE_DSS_WITH_AES_256_CBC_SHA,
    DHE_RSA_WITH_AES_256_CBC_SHA
  Session Cache Timeout: 600
  Secure Trustpoint    :
Switch#
```

110.9 ssl-service-policy

Данная команда используется для настройки политики SSL service policy. Для удаления политики SSL service policy воспользуйтесь формой **no** этой команды.

ssl-service-policy *POLICY-NAME* **[version [tls1.0] [tls1.1] [tls1.2]] | 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] [rsa-aes-128-cbc-sha] [rsa-aes-256-cbc-sha] [rsa-aes-128-cbc-sha256] [rsa-aes-256-cbc-sha256] [dhe-dss-aes-256-cbc-sha] [dhe-rsa-aes-256-cbc-sha] | secure-trustpoint** *TRUSTPOINT* **| session-cache-timeout** *TIME-OUT***]**

no ssl-service-policy *POLICY-NAME* **[version [tls1.0] [tls1.1] [tls1.2]] | 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] [rsa-aes-128-cbc-sha] [rsa-aes-256-cbc-sha] [rsa-aes-128-cbc-sha256] [rsa-aes-256-cbc-sha256] [dhe-dss-aes-256-cbc-sha] [dhe-rsa-aes-256-cbc-sha] | secure-trustpoint | session-cache-timeout]**

Параметры

POLICY-NAME	Укажите имя политики SSL service policy.
version	(Опционально.) Укажите версию TLS. **tls1.0** – укажите, чтобы устройство поддерживало TLS версии 1.0. **tls1.1** – укажите, чтобы устройство поддерживало TLS версии 1.1. **tls1.2** – укажите, чтобы устройство поддерживало TLS версии 1.2.
ciphersuite	(Опционально.) Укажите шифрование cipher suite, которое будет использовать служба безопасности при установлении соединения с удаленным узлом. Чтобы использовать обмен ключами DH с шифрованием 3DES-EDE-CBC и SHA для дайджеста сообщений, укажите **dhe-dss-3des-ede-**

cbc-sha.

Чтобы использовать обмен ключами RSA с шифрованием 3DES и DES-EDE3-CBC и Secure Hash Algorithm (SHA) для дайджеста сообщений, укажите **rsa-3des-ede-cbc-sha**.

Чтобы использовать обмен ключами RSA с 128-битным шифрованием RC4 и SHA для дайджеста сообщений, укажите **rsa-rc4-128-sha**.

Чтобы использовать обмен ключами RSA с 128-битным шифрованием RC4 и Message Digest 5 (MD5) для дайджеста сообщений, укажите **rsa-rc4-128-md5**.

Чтобы использовать обмен ключами RSA EXPORT с 40-битным шифрованием RC4 и MD5 для дайджеста сообщений, укажите **rsa-export-rc4-40-md5**.

Чтобы использовать обмен ключами RSA с 128-битным шифрованием AES и SHA для дайджеста сообщений, укажите **rsa-aes-128-cbc-sha**.

Чтобы использовать обмен ключами RSA с 256-битным шифрованием AES и SHA для дайджеста сообщений, укажите **rsa-aes-256-cbc-sha**.

Чтобы использовать обмен ключами RSA с 128-битным шифрованием AES и 256-битным SHA для дайджеста сообщений, укажите **rsa-aes-128-cbc-sha256**.

Чтобы использовать обмен ключами RSA с 256-битным шифрованием AES и 256-битным SHA для дайджеста сообщений, укажите **rsa-aes-256-cbc-sha256**.

Чтобы использовать обмен ключами DH с 256-битным шифрованием AES и SHA для дайджеста сообщений по методу DSS, укажите **dhe-dss-aes-256-cbc-sha**.

Чтобы использовать обмен ключами DH с 256-битным шифрованием AES и SHA для дайджеста сообщений по методу RSA, укажите **dhe-rsa-aes-256-cbc-sha**.

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** этой команды, чтобы отключить выбранные cipher suite.

secure-trustpoint *TRUSTPOINT*	(Опционально.) Укажите имя доверенной точки (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** этой команды, чтобы отменить указанные trust point и использовать встроенный сертификат/пары ключей.
session-cache-timeout *TIME-OUT*	(Опционально.) Укажите значение тайм-аута в секундах для информации, хранящейся в кэше SSL-сессий. Диапазон значений: от 60 до 86400 секунд. Если данный параметр не указан, тайм-аут кэша сессий по умолчанию составляет 600 секунд. Используйте форму **no** этой команды, чтобы вернуть настройки по умолчанию для тайм-аута кэша SSL-сессий.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы настроить политику SSL service policy. Если параметры не указаны и имя указанной политики не существует, будет создана новая политика SSL service policy со всеми связанными с ней опциональными параметрами, для которых будут настроены значения по умолчанию.

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)#
```

111. Команды Unicast Reverse Path Forwarding (URPF)

111.1 ip urpf

Данная команда используется для включения URPF-проверки глобально. Чтобы отключить функцию, воспользуйтесь формой **no** этой команды.

ip urpf
no ip urpf

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Одним из распространенных методов начала атаки является использование подмены IPv4/IPv6-адреса источника (IPv4/IPv6 source address spoofing). При использовании этого метода хакер пытается отправить трафик в сеть с адресом источника, который известен или которому доверяет целевая система. Если защита отсутствует, то сеть организации будет пропускать трафик и станет уязвимой для различных типов атак. URPF помогает устранить проблемы, вызванные неправильно сформированными или поддельными IPv4/IPv6-адресами источника, проходящими через маршрутизатор.

Команда **ip urpf** используется для глобального включения URPF, а команда **ip verify unicast source** применяется для включения URPF на интерфейсе. Чтобы включить URPF на интерфейсе, включите функцию как глобально, так и на интерфейсе.

Если данная функция включена, сначала необходимо выполнить поиск в аппаратной таблице маршрутизации с использованием протокола инициирования сеанса (Session Initiation Protocol, SIP), а затем с помощью протокола динамической проверки (Dynamic Inspection Protocol, DIP). Это достигается путем разделения таблицы на две половины, так что размер таблицы IP-маршрутизации будет уменьшен вдвое. Чтобы применить настройки, необходимо сохранить конфигурацию и перезагрузить коммутатор.

Пример

В данном примере показано, как включить URPF-проверку глобально.

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

 WARNING: The command does not take effect until after the next reboot.
Switch(config)#
```

111.2 ip verify unicast source

Данная команда используется для настройки URPF на интерфейсах. Чтобы отключить проверку URPF на интерфейсе или вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip verify unicast source [reachable-via any] [access-group *IP-ACCESS-LIST-NAME***] [ipv6-access-group** *IPV6-ACCESS-LIST-NAME***]**

no ip verify unicast source [reachable-via] [access-group] [ipv6-access-group]

Параметры

reachable-via any	(Опционально.) Укажите, чтобы URPF проверил, присутствует ли адрес источника в таблице маршрутизации входящих пакетов (иногда называется Loose Mode).
access-group *IP-ACCESS-LIST-NAME*	(Опционально.) Укажите имя IPv4 ACL, которое будет использовано для проверки.
ipv6-access-group *IPV6-ACCESS-LIST-NAME*	(Опционально.) Укажите имя IPV6 ACL, которое будет использовано для проверки.

По умолчанию

Проверка URPF по умолчанию не выполняется.

По умолчанию список доступа IPv4/IPv6 не указан.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта.

Unicast RPF помогает устранить проблемы, причиной которых являются неправильно сформированные или поддельные IPv4/IPv6-адреса источника, путем отбрасывания пакетов IPv4/IPv6, у которых отсутствует проверяемый IPv4/IPv6-адрес источника.

Когда Unicast RPF включен на интерфейсе, коммутатор проверяет все пакеты IPv4 и IPv6, полученные в качестве входных данных на этом интерфейсе, чтобы убедиться, что адрес источника и интерфейс

источника отображаются в таблице маршрутизации и соответствуют интерфейсу, на котором был получен пакет.

Проверка обратного пути не будет выполняться в следующих случаях:

- IPv4/IPv6-адрес назначения не является индивидуальным (unicast) адресом.
- IP-адрес источника является адресом IPv6 и адресом Link-Local.
- Полученный пакет является пакетом BOOTP/DHCP (IP-адрес источника 0.0.0.0, а IP-адрес назначения 255.255.255.255).

Пример

В данном примере показано, как включить проверку Unicast RPF на интерфейсе Ethernet 1/0/8.

```
Switch#configure terminal
Switch(config)#interface eth1/0/8
Switch(config-if)#ip verify unicast source
Switch(config-if)#
```

В примере ниже показано, как настроить режим функции Unicast RPF для любого порта на интерфейе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip verify unicast source reachable-via any
Switch(config-if)#
```

111.3 show ip urpf

Данная команда используется для отображения настроек URPF.

show ip urpf [*INTERFACE-ID* **[, | -]]**

Параметры

INTERFACE-ID	(Опционально.) Укажите физический интерфейс, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения текущих настроек URPF. Если данная команда выполняется без указания ID интерфейса, будут отображены только общие настройки Unicast RPF.

Пример

В данном примере показано, как отобразить настройки URPF на интерфейсах Ethernet 1/0/7 и Ethernet 1/0/8.

```
Switch#show ip urpf 1/0/7-8

URPF Global State      : Enabled

Port      State     Reachable-  IP Access List Name
                    Via         IPv6 Access List Name
--------  --------  ----------  --------------------------------
1/0/7     Disabled  Any

1/0/8     Enabled   Any

Switch#
```

Параметры

URPF Global State	Общее состояние проверки Unicast RPF.
Save And Reboot Required	Указывает, что настроенное общее состояние Unicast RPF будет действовать только после перезагрузки.
State	Состояние Unicast RPF.
Port	Номер порта.
Reachable-Via	Режим, в котором Unicast RPF проверяет входящие пакеты.
IP Access List Name	Указывает имя IP ACL, которое необходимо проверить. Пустая строка указывает, что имя IP Access List не задано.
IPv6 Access List Name	Указывает имя IPv6 ACL, которое необходимо проверить. Пустая строка указывает, что имя IPv6 Access List не задано.

112. Команды Virtual LAN (VLAN)

112.1 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 интерфейс Ethernet 1/0/1 на прием только тегированных кадров **tagged-only**.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#acceptable-frame tagged-only
Switch(config-if)#
```

112.2 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, если принимающий порт не является участником VLAN, классифицированной для получаемого пакета.

Пример

В данном примере показано, как настроить проверку входящего трафика для включенного интерфейса Ethernet 1/0/1.

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

112.3 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

MAC-ADDRESS	MAC-адрес для привязки.
vlan *VLAN-ID*	VLAN ID для привязки VLAN на основе MAC-адреса.
priority *COS-VALUE*	(Опционально.) Значение приоритета CoS. Если параметр не указан, то значением CoS по умолчанию является 0.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для создания привязки VLAN на основе MAC-адреса. Классификация привязки будет применена к пакетам, получаемым коммутатором. По умолчанию приоритет классификации VLAN для нетегированного пакета следующий: 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)#
```

112.4 protocol-vlan profile

Данная команда используется для создания группы протоколов. Используйте форму **no** для удаления указанной группы протоколов.

protocol-vlan profile *PROFILE-ID* **frame-type {ethernet2 | snap | llc} ether-type** *TYPE-VALUE*
no protocol-vlan profile *PROFILE-ID*

Параметры

PROFILE-ID	Группа протоколов, которую необходимо добавить или удалить.
frame-type	Тип кадров.
ethernet2	Значение для типа кадров Ethernet II.
snap	Значение для типа кадров SNAP.
llc	Значение для типа кадров LLC.
ether-type *TYPE-VALUE*	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, чтобы настроить классификацию 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)#
```

112.5 protocol-vlan profile (Interface)

Данная команда используется, чтобы настроить привязку VLAN для группы протоколов на порту. Используйте форму **no** для удаления привязки VLAN на порту.

protocol-vlan profile *PROFILE-ID* **vlan** *VLAN-ID* **[priority** *COS-VALUE***]**

no protocol-vlan profile *PROFILE-ID*

Параметры

PROFILE-ID	Идентификатор группы протоколов, который должен классифицироваться.
vlan *VLAN-ID*	VLAN ID для protocol VLAN. Для каждой группы привязки может быть указан только один VLAN ID.
priority *COS-VALUE*	(Опционально.) Значение приоритета CoS. Если параметр не указан, то значением CoS по умолчанию является 0.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы указать VLAN для группы протоколов на порту. В результате пакет, полученный на порту, который соответствует указанной группе протоколов, будет определен в указанную VLAN. Для настройки команды VLAN не должна обязательно существовать. По умолчанию классификация VLAN для нетегированного пакета выполняется в следующей последовательности: MAC-based > Subnet-based > Protocol VLAN.

Пример

В данном примере показано, как создать привязку VLAN на интерфейсе Ethernet 1/0/1 для классификации пакетов в группе протоколов 10 в VLAN 3000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#protocol-vlan profile 10 vlan 3000
Switch(config-if)#
```

112.6 subnet-vlan

Команда **subnet-vlan ipv4** используется для настройки привязки VLAN для подсети IPv4. Команда **subnet-vlan ipv6** применяется, чтобы настроить привязку VLAN для подсети IPv6. Используйте форму **no** для удаления привязки VLAN на основе подсети.

subnet-vlan {ipv4 *NETWORK-PREFIX NETWORK-MASK* **| ipv6** *IPV6-NETWORK-PREFIX/PREFIX-LENGTH***} vlan** *VLAN-ID* **[priority** *COS-VALUE***]**

no subnet-vlan {ipv4 *NETWORK-PREFIX NETWORK-MASK* **| ipv6** *IPV6-NETWORK-PREFIX/PREFIX-LENGTH***}**

Параметры

ipv4 *NETWORK-PREFIX NETWORK-MASK*	Укажите сетевой префикс IPv4 и сетевую маску.
ipv6 *IPV6-NETWORK-PREFIX/PREFIX-LENGTH*	Укажите сетевой префикс IPv6 и длину префикса. Длина префикса IPv6 не может превышать 64 бита.
vlan *VLAN-ID*	Укажите VLAN ID для подсети VLAN (subnet VLAN).
priority *COS-VALUE*	(Опционально.) Укажите значение приоритета CoS. Если параметр не указан, значение CoS по умолчанию – 0.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду **subnet-vlan ipv4**, чтобы настроить привязку VLAN для подсети IPv4.

Используйте команду **subnet-vlan ipv6**, чтобы настроить привязку VLAN для подсети IPv6. Привязка применяется к пакетам, полученным коммутатором. Для нетегированного пакета по умолчанию приоритет для привязки следующий: MAC-based > Subnet-based > Protocol VLAN.

Пример

В данном примере показано, как настроить привязки VLAN для определения того, что пакеты принадлежат подсетям 20.0.0.0/8, 192.0.0.0/8 и 3ffe:22:33:44::/64 в VLAN 100.

```
Switch#configure terminal
Switch(config)#subnet-vlan ipv4 20.0.0.0/8 vlan 100 vlan 100
Switch(config)#subnet-vlan ipv4 192.0.0.0/8 vlan 100 priority 4
Switch(config)#subnet-vlan ipv6 3ffe:22:33:44::/64 vlan 100
Switch(config)#
```

112.7 show protocol-vlan profile

Данная команда используется для отображения параметров настройки, касающихся protocol VLAN.

show protocol-vlan {profile [*PROFILE-ID* **[, | -]] | interface [***INTERFACE-ID* **[, | -]]}**

Параметры

profile	Укажите группу протоколов.
PROFILE-ID	(Опционально.) Укажите группу протоколов для отображения.
,	(Опционально.) Используется для перечисления нескольких ID профиля или отделения одного диапазона ID от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона ID профиля. Пробелы до и после дефиса недопустимы.
interface	Укажите интерфейсы для отображения.
INTERFACE-ID	(Опционально.) Укажите порт для отображения настроек классификации protocol VLAN.

,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки для классификации VLAN на порту на основе группы протоколов.

Пример

В данном примере показано, как отобразить настройки для классификации VLAN на основе группы протоколов на интерфейсах с Ethernet 1/0/1 по 1/0/3.

```
Switch#show protocol-vlan interface eth1/0/1-3

 Interface       Protocol Group ID  VLAN  Priority
 --------------  -----------------  ----  --------
 eth1/0/1        1                  1     5
 eth1/0/2        10                 3     0
 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)

Switch#
```

112.8 show vlan

Данная команда используется для отображения параметров для всех настроенных VLAN или одной VLAN на коммутаторе.

show vlan [*VLAN-ID* **[, | -] | interface [***INTERFACE-ID* **[, | -]] | mac-vlan | subnet-vlan]**

Параметры

VLAN-ID	(Опционально.) Укажите список VLAN для отображения информации о портах-участниках. Если VLAN не указана, то отображаются все VLAN. Допустимый диапазон: 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.
interface *INTERFACE-ID*	(Опционально.) Укажите порт для отображения настроек VLAN.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
mac-vlan	(Опционально.) Укажите для отображения информации о VLAN на основе MAC-адресов.
subnet-vlan	(Опционально.) Укажите для отображения информации о VLAN на основе подсетей (subnet).

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения параметров одной или всех настроенных на коммутаторе VLAN.

Пример

В данном примере показано, как отобразить все текущие записи VLAN.

```
Switch#show vlan

 VLAN 1
   Name : default
   Description :
   Tagged Member Ports   :
   Untagged Member Ports : eth1/0/1-1/0/26

 Total Entries : 1

Switch#
```

В данном примере показано, как отобразить информацию о PVID, проверке входящих пакетов и допустимых типах кадров для интерфейсов Ethernet 1/0/1-1/0/4.

```
Switch#show vlan interface eth1/0/1-4

eth1/0/1
VLAN mode              : Trunk
Native VLAN            : 5 (Untagged)
Trunk allowed VLAN     : 2,4,5,6
Ingress checking       : Enabled
Acceptable frame type  : Admit-all
Dynamic Tagged VLAN    : 100

eth1/0/2
VLAN mode              : Access
Access VLAN            : 2
Ingress checking       : Enabled
Acceptable frame type  : Untagged-only

eth1/0/3
VLAN mode              : Hybrid
Native VLAN            : 5
Hybrid untagged VLAN   : 2,4,5,6
```

```
Hybrid tagged VLAN      : 8,9,10
Ingress checking        : Enabled
Acceptable frame type   : Admit-All
Dynamic tagged VLAN     :
VLAN Precedence         : MAC-VLAN

eth1/0/4
VLAN mode               : Dot1q-tunnel
Access VLAN             : 800
Hybrid untagged VLAN    : 200, 600
Ingress checking        : Enabled
Acceptable frame type   : Admit-all
VLAN Precedence         : MAC-VLAN

Switch#
```

В данном примере показано, как отобразить все привязки VLAN на основе MAC-адресов.

```
Switch#show vlan mac-vlan

MAC Address          VLAN ID   Priority  Status
 ------------------  --------  --------  ----------
 00-80-cc-00-00-11   101         4       Active
 00-11-22-00-00-05   200         5       Active

Total Entries: 2

Switch#
```

В данном примере показано, как отобразить все привязки VLAN на основе подсетей.

```
Switch#show vlan subnet-vlan

 Subnet                    VLAN ID  Priority
 ------------------------  -------  ---------
 20.0.0.0/8                100      0
 192.0.0.0/8               100      4
 3FFE:22:33:44::/64        100      0

Total Entries: 3

Switch#
```

112.9 switchport access vlan

Данная команда используется для указания access VLAN для интерфейса. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

switchport access vlan *VLAN-ID*

no switchport access vlan

Параметры

VLAN-ID	Access VLAN интерфейса.

По умолчанию

По умолчанию access VLAN является VLAN 1.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда вступает в силу, когда интерфейс настроен в режиме доступа (access mode) или режиме dot1q-tunnel mode. VLAN, указанная в качестве access VLAN, не должна обязательно существовать для настройки команды.

Можно указать только одну access VLAN. Следующая команда перезаписывает предыдущую.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в режиме доступа (access mode) с access VLAN 1000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1000
Switch(config-if)#
```

112.10 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.) Укажите порт, который будет добавлен в указанную(-ые) VLAN.
tagged	Укажите порт в качестве тегированного для указанной(-ых) VLAN.
untagged	Укажите порт в качестве нетегированного для указанной(-ых) VLAN.

remove	Укажите порт, который будет удален из указанной(-ых) VLAN.
VLAN-ID	(Опционально.) Укажите список разрешенных VLAN или список VLAN, который будет добавлен или удален из списка разрешенных VLAN. Если опция не задана, указанный список VLAN перезапишет список разрешенных VLAN.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию гибридный порт является нетегированным членом VLAN 1.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При многократном использовании команды hybrid VLAN с разными VLAN ID порт может стать тегированным или нетегированным участником нескольких VLAN.

Когда разрешенная VLAN указана только как VLAN ID, следующая команда перезапишет предыдущую команду. Если новый нетегированный разрешенный список VLAN частично совпадает с текущим списком тегированных разрешенных VLAN, то совпадающая часть будет изменена на нетегированную разрешенную VLAN. С другой стороны, если новый список тегированных разрешенных VLAN частично совпадает с текущим списком нетегированных разрешенных VLAN, то совпадающая часть будет изменена на тегированную разрешенную VLAN. В силу вступает последняя заданная команда. Необязательно создавать VLAN, чтобы настроить данную команду.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве тегированного порта VLAN 1000 и нетегированного порта VLAN 2000 и 3000.

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

112.11 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 список разрешенных VLAN. Указанная VLAN не должна обязательно существовать для применения этой команды. Команда вступает в силу, если интерфейс настроен в гибридном режиме.

Пример

В данном примере показано, как настроить Ethernet 1/0/1 в качестве гибридного интерфейса и задать PVID со значением 20.

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

112.12 switchport mode

Данная команда используется для настройки режима работы порта в VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

switchport mode {access | hybrid | trunk | dot1q-tunnel}
no switchport mode

Параметры

access	Укажите порт в качестве порта доступа.
hybrid	Укажите порт в качестве гибридного порта.
trunk	Укажите порт в качестве trunk-порта.
dot1q-tunnel	Укажите порт в качестве порта dot1q-tunnel.

По умолчанию

По умолчанию установлена опция hybrid.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

В режиме **access** порт выступает в качестве нетегированного участника access VLAN, заданной для данного порта. В режиме **hybrid** порт может быть нетегированным или тегированным участником всех настроенных VLAN. Цель этого режима VLAN - поддержка protocol VLAN, VLAN на основе подсетей (subnet-based VLAN) и VLAN на основе MAC-адресов (MAC-based VLAN).

В режиме **trunk** этот порт является либо тегированным, либо нетегированным участником его native VLAN и может быть тегированным участником других настроенных VLAN. Цель trunk-порта – поддержка соединения switch-to-switch. В режиме **dot1q-tunnnel mode** порт действует как порт UNI в service VLAN.

При изменении режима работы порта настройки, связанные с VLAN и ассоциированные с предыдущим режимом, будут утеряны.



Примечание: В режиме **access** только нетегированные пакеты могут быть перенаправлены через MPLS Virtual Circuit (VC). Для перенаправления через MPLS VC и тегированных, и нетегированных пакетов необходимо установить режим порта **trunk**.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве trunk-порта.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
```

112.13 switchport trunk allowed vlan

Данная команда используется для настройки VLAN, которым разрешено получать и отправлять трафик на указанный интерфейс в тегированном формате. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

switchport trunk allowed vlan {all | [add | remove | except] *VLAN-ID* **[, | -]}**
no switchport trunk allowed vlan

Параметры

all	Указывает, что на интерфейсе разрешены все VLAN.
add	(Опционально.) Укажите, чтобы добавить указанный список VLAN в список разрешенных VLAN.
remove	(Опционально.) Укажите, чтобы удалить указанный список VLAN из списка разрешенных VLAN.
except	(Опционально.) Указывает, что разрешены все VLAN, за исключением VLAN, находящихся в списке исключений.
VLAN-ID	Укажите список разрешенных VLAN или список VLAN, которые должны быть добавлены в список разрешенных VLAN или удалены из него.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию все VLAN разрешены.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда вступает в силу, только когда интерфейс настроен в режиме trunk. Если VLAN разрешена на trunk-порту, то порт станет тегированным участником VLAN. Когда для разрешенной VLAN установлена опция **all**, то порт будет автоматически добавлен во все VLAN, созданные системой.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве тегированного участника VLAN 1000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 1000
Switch(config-if)#
```

112.14 switchport trunk native vlan

Данная команда используется для указания native VLAN ID интерфейса в режиме trunk. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

switchport trunk native vlan {*VLAN-ID* **| tag}**
no switchport trunk native vlan [tag]

Параметры

VLAN-ID	Native VLAN для trunk-порта.
tag	Включение режима тегирования (tagging mode) native VLAN.

По умолчанию

По умолчанию задана native VLAN 1, режим – нетегированный.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда вступает в силу, только когда интерфейс настроен в режиме trunk. Если 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. Если trunk-порт работает в нетегированном режиме (untagged mode) для native VLAN, передавая нетегированный пакет для native VLAN и тегированные пакеты для всех остальных VLAN, допустимые типы кадров порта должны быть настроены как «admit-all» для корректной работы.

Указанная VLAN не должна обязательно существовать для настройки команды.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве интерфейса trunk и native VLAN 20.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 20
Switch(config-if)#
```

112.15 vlan

Данная команда используется для добавления VLAN и входа в режим VLAN configuration mode. Используйте форму **no** для удаления VLAN.

vlan *VLAN-ID* **[, | -]**
no vlan *VLAN-ID* **[, | -]**

Параметры

VLAN-ID	Идентификатор VLAN, которая должны быть добавлена, удалена или настроена. Корректный диапазон VLAN ID: от 1 до 4094. VLAN ID 1 не может быть удален.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

VLAN ID 1 существует в системе в качестве VLAN по умолчанию.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду глобальной настройки **vlan** для создания VLAN. Ввод команды **vlan** с VLAN ID обеспечивает вход в режим настройки VLAN (VLAN configuration mode). Ввод VLAN ID существующей VLAN не создает новую VLAN, но разрешает пользователю изменить параметры VLAN для указанной VLAN. Когда пользователь вводит VLAN ID новой VLAN, VLAN будет создана автоматически.

Используйте команду **no vlan** для удаления VLAN. VLAN по умолчанию не может быть удалена. Если удаленная VLAN является access VLAN порта, то access VLAN порта будет сброшена в VLAN 1.

Пример

В данном примере показано, как добавить новые VLAN, назначив новые VLAN с VLAN ID от 1000 до 1005.

```
Switch#configure terminal
Switch(config)#vlan 1000-1005
Switch(config-vlan)#
```

112.15 vlan precedence

Данная команда используется для указания приоритета на порту на основе VLAN. Используйте форму **no** для сброса приоритета на порту на основе VLAN.

vlan precedence {mac-vlan | subnet-vlan}

no vlan precedence

Параметры

mac-vlan	Классификация VLAN на основе MAC-адресов предпочтительней классификации VLAN на основе подсетей.
subnet-vlan	Классификация VLAN на основе подсетей предпочтительней классификации VLAN на основе MAC-адресов.

По умолчанию

По умолчанию задана опция VLAN на основе MAC-адресов.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

По умолчанию приоритет для классификации VLAN для нетегированного пакета является MAC-based > Subnet-based > Protocol VLAN. Используйте команду **vlan precedence** для настройки приоритета классификации VLAN между VLAN на основе MAC-адресов и VLAN на основе подсетей. Команда вступает в силу только для гибридных интерфейсов или интерфейсов dot1q tunnel.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве subnet VLAN, обладающей более высоким приоритетом.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#vlan precedence subnet-vlan
Switch(config-if)#
```

112.17 name

Данная команда используется для указания имени VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

name *VLAN-NAME*
no name

Параметры

VLAN-NAME	Имя VLAN (макс. 32 символа). Имя VLAN должно быть уникальным в административном домене.

По умолчанию

По умолчанию именем VLAN является VLANx, где x – четыре цифры номера VLAN, включая начальные нули.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы задать имя VLAN. Имя VLAN должно быть уникальным в административном домене.

Пример

В данном примере показано, как задать имя «admin-vlan» для VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#name admin-vlan
Switch(config-vlan)#
```

113. Команды Virtual LAN (VLAN) Counter

113.1 counting

Данная команда используется, чтобы создать контрольную запись для сбора статистики трафика на указанных интерфейсах L2 VLAN. Для удаления записей воспользуйтесь формой **no** этой команды.

counting [interface *INTERFACE-ID* **[, | -]] {broadcast | multicast |unicast | any} [rx | tx]**
no counting [interface *INTERFACE-ID* **[, | -]] [broadcast | multicast |unicast | any] [rx | tx]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите один или несколько интерфейсов физического порта для подсчета трафика. Если интерфейс физического порта не указан, статистика учитывается только для каждой 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.
broadcast	Укажите, чтобы подсчитать только широковещательные пакеты.
multicast	Укажите, чтобы подсчитать только многоадресные пакеты.
unicast	Укажите, чтобы подсчитать только одноадресные пакеты.
any	Укажите, чтобы подсчитать все типы пакетов.
rx	(Опционально.) Укажите, чтобы подсчитать входящий трафик.
tx	(Опционально.) Укажите, чтобы подсчитать исходящий трафик.

По умолчанию

По умолчанию контрольные записи не указаны.

Режим ввода команды

Layer 2 VLAN Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если тип кадра не указан, контрольные записи создаются или удаляются в зависимости от интерфейсов и направления трафика. Если направление трафика не указано, будет подсчитываться как входящий, так и исходящий трафик.

Данная команда применима исключительно для интерфейсов L2 VLAN и используется для продуктов без соответствующих ресурсов аппаратной статистики для каждой L2 VLAN. Данная функция может совместно использовать ресурсы ACL.

В параметре **interface** могут быть указаны только интерфейсы физических портов. Если интерфейс не указан, статистика собирается на основе VLAN. В противном случае, статистика будет подсчитываться для указанного физического порта (-ов) в определенной VLAN.

Все контрольные записи для определенных VLAN могут быть удалены без указания каких-либо параметров с помощью команды **no counting**. Все контрольные записи для отдельного физического порта(-ов) в определенной VLAN могут быть удалены с помощью команды **no counting interface** *INTERFACE-ID* **[, | -]** без указания остальных параметров.

Пример

В данном примере показано, как создать контрольную запись для подсчета статистики входящего и исходящего трафика для VLAN 2.

```
Switch#configure terminal
Switch(config)#interface L2vlan 2
Switch(config-if)#counting any
Switch(config-if)#
```

В примере ниже показано, как создать контрольную запись для подсчета статистики входящих и исходящих широковещательных пакетов для VLAN 3.

```
Switch#configure terminal
Switch(config)#interface L2vlan 3
Switch(config-if)#counting broadcast
Switch(config-if)#
```

В следующем примере показано, как создать контрольную запись для подсчета статистики входящих одноадресных пакетов на интерфейсе Ethernet 1/0/1 в VLAN 5.

```
Switch#configure terminal
Switch(config)#interface L2vlan 5
Switch(config-if)#counting interface eth1/0/1 unicast rx
Switch(config-if)#
```

В примере ниже показан процесс удаления всех контрольных записей для подсчета статистики входящего и исходящего трафика для VLAN 2.

```
Switch#configure terminal
Switch(config)#interface L2vlan 2
Switch(config-if)#no counting
Switch(config-if)#
```

В нижеприведенном примере показано, как удалить все контрольные записи для подсчета статистики входящего и исходящего трафика на интерфейсе Ethernet 1/0/2 в VLAN 10.

```
Switch#configure terminal
Switch(config)#interface L2vlan 10
Switch(config-if)#no counting interface eth1/0/2
Switch(config-if)#
```

В нижеследующем примере показано, как удалить контрольные записи для подсчета статистики исходящих многоадресных пакетов на интерфейсе Ethernet 1/0/10 в VLAN 20.

```
Switch#configure terminal
Switch(config)#interface L2vlan 20
Switch(config-if)#no counting interface eth1/0/10 multicast tx
Switch(config-if)#
```

113.2 show vlan counting

Данная команда используется, чтобы отобразить контрольные записи для статистики трафика на указанных интерфейсах L2 VLAN.

show vlan counting [interface *INTERFACE-ID*] **[rx | tx]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите один или несколько интерфейсов L2 VLAN для отображения информации о записях. Если интерфейс L2 VLAN не указан, будут отображены все записи.
rx	(Опционально.) Укажите, чтобы отобразить записи для входящего трафика.
tx	(Опционально.) Укажите, чтобы отобразить записи для исходящего трафика.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда применяется, чтобы отобразить контрольные записи для статистики трафика на указанных интерфейсах L2 VLAN.

Пример

В данном примере показано, как отобразить все контрольные записи статистики на интерфейсах L2 VLAN.

```
Switch#show vlan counting

VLAN  Frame Type    Ports
----  ------------  ------------------------------------------------
2     RX Unicast
3     RX Any
4     RX Multicast  1/0/1
10    RX Broadcast  1/0/1-1/0/5
2     TX Unicast
3     TX Any
4     TX Multicast  1/0/1
100   TX Broadcast  1/0/10-1/0/12

Total Entries: 8

Switch#
```

114. Команды Virtual LAN (VLAN) Tunnel

114.1 dot1q inner ethertype

Данная команда используется для указания внутреннего TPID системы. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

dot1q inner ethertype *VALUE*
no dot1q inner ethertype

Параметры

VALUE	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)#
```

114.2 dot1q tunneling ethertype

Данная команда используется для указания внешнего TPID сервисной VLAN. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

dot1q tunneling ethertype *VALUE*
no dot1q tunneling ethertype

Параметры

VALUE	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 eth1/0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#dot1q tunneling ethertype 0x88a8
Switch(config-if)#
```

114.3 switchport vlan mapping

Данная команда используется для указания записи VLAN Translation на trunk-порту или записи привязки сервисной VLAN на порту dot1q tunnel. Для удаления записи VLAN Translation или записи привязки сервисной VLAN воспользуйтесь формой **no** этой команды.

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

ORIGINAL-VLAN	Укажите исходный VLAN ID, соответствующий входящим пакетам, в диапазоне 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.
ORIGINAL-INNER-VLAN	(Опционально.) Укажите, чтобы сопоставить исходную внутреннюю (inner) VLAN с внутренним (inner) VID для входящих пакетов на порту в режиме trunk. Доступный диапазон значений: от 1 до 4094.
RESULTANT-VLAN	Укажите Translated ID сервисной VLAN в диапазоне от 1 до 4094, чтобы заменить исходную VLAN для соответствующих пакетов.
RESULTANT-INNER-VLAN	(Опционально.) Укажите новую внутреннюю (inner) VLAN, чтобы заменить исходную внутреннюю (inner) VLAN на порту в режиме trunk.
DOT1Q-TUNNEL-VLAN	Укажите, чтобы добавить ID сервисной VLAN для соответствующих пакетов на порту в режиме dot1q-tunnel mode.
COS-VALUE	(Опционально.) Укажите приоритет правила. Если приоритет тега сервисной VLAN не задан, будет использовано значение по умолчанию – 0.

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 тегированном 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 eth1/0/1
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 примере ниже показано, как настроить записи VLAN Mapping на порту 802.1Q tunnel.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
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)#
```

114.4 dot1q-tunnel insert dot1q-tag

Данная команда используется для вставки тега dot1q VLAN. Для удаления вставки тега dot1q VLAN воспользуйтесь формой **no** этой команды.

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 eth1/0/1
Switch(config-if)#switchport mode dot1q-tunnel
Switch(config-if)#dot1q-tunnel insert dot1q-tag 10
Switch(config-if)#
```

114.5 vlan mapping miss drop

Данная команда используется для включения функции VLAN Mapping Missdrop для отбрасывания несоответствующих пакетов. Для отключения функции VLAN Mapping Missdrop воспользуйтесь формой **no** этой команды.

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 применима для настройки 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 eth1/0/1
Switch(config-if)#switchport mode dot1q-tunnel
Switch(config-if)#vlan mapping miss drop
Switch(config-if)#
```

114.6 dot1q-tunnel trust inner-priority

Данная команда используется для установки доверенного приоритета dot1q. Для удаления настройки воспользуйтесь формой **no** этой команды.

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 eth1/0/1
Switch(config-if)#switchport mode dot1q-tunnel
Switch(config-if)#dot1q-tunnel trust inner-priority
Switch(config-if)#
```

114.7 vlan mapping profile

Данная команда используется для создания профиля VLAN Mapping или входа в режим конфигурации профиля VLAN Mapping. Для удаления профиля VLAN Mapping воспользуйтесь формой **no** этой команды.

vlan mapping profile *ID* **[type [ethernet] [ip] [ipv6]]**
no vlan mapping profile *ID*

Параметры

ID	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)#
```

114.8 vlan mapping rule

Данная команда используется для настройки правил профиля VLAN Mapping. Для удаления ранее настроенных правил воспользуйтесь формой **no** этой команды.

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*	(Опционально.) 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*	(Опционально.) 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 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)#
```

114.9 switchport vlan mapping profile

Данная команда используется для применения правил профиля VLAN Mapping к указанному интерфейсу. Для удаления привязки воспользуйтесь формой **no** этой команды.

switchport vlan mapping profile *PROFILE-ID*
no switchport vlan mapping profile *PROFILE-ID*

Параметры

PROFILE-ID	(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 eth1/0/1
Switch(config-if)#switchport vlan mapping profile 1
Switch(config-if)#
```

114.10 show dot1q ethertype

Данная команда используется для отображения настроек TPID.

show dot1q ethertype [*INTERFACE-ID* **[- | ,]]**

Параметры

INTERFACE-ID	(Опционально.) Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

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#
```

114.11 show dot1q-tunnel

Данная команда используется для отображения настроек туннелирования dot1q VLAN на интерфейсах.

show dot1q-tunnel [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(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 одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки 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#
```

114.12 show vlan mapping

Данная команда используется для отображения настроек VLAN Mapping.

show vlan mapping [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите интерфейсы, которые необходимо отобразить. Если интерфейсы не указаны, будут отображены все VLAN Mapping.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки 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#
```

114.13 show vlan mapping profile

Данная команда используется для отображения информации о настроенном профиле VLAN Mapping.

show vlan mapping profile [*ID*]

Параметры

ID	(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.

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#
```

115. Команды Virtual Router Redundancy Protocol (VRRP)

115.1 snmp-server enable traps vrrp

Данная команда используется для включения отправки VRRP trap в SNMP. Чтобы отключить отправку VRRP trap, воспользуйтесь формой **no** этой команды.

snmp-server enable traps vrrp [auth-fail] [new-master]
no snmp-server enable traps vrrp [new-master] [auth-fail]

Параметры

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.
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.

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 параметры не указаны, оба типа trap-сообщений включаются или отключаются одновременно.

Пример

В данном примере показано, как включить отправку trap для нового основного устройства VRRP.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps vrrp new-master
Switch(config)#
```

115.2 vrrp authentication

Данная команда используется для включения аутентификации VRRP и установки пароля на интерфейсе. Чтобы отменить аутентификацию, воспользуйтесь формой **no** этой команды.

vrrp authentication *STRING*
no vrrp authentication

Параметры

STRING	Укажите пароль для аутентификации в текстовом формате. Максимальное 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)#
```

115.3 vrrp ip

Данная команда используется для создания VRRP-группы на интерфейсе. Чтобы удалить VRRP-группу, воспользуйтесь формой **no** этой команды.

vrrp *VRID* **ip** *IP-ADDRESS*
no vrrp *VRID*

Параметры

VRID	Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать группу VRRP. Диапазон значений: от 1 до 255.
IP-ADDRESS	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 vlan1
Switch(config-if)#vrrp 7 ip 10.1.1.1
Switch(config-if)#
```

115.4 vrrp priority

Данная команда используется для настройки приоритета виртуального маршрутизатора. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

vrrp *VRID* **priority** *PRIORITY*
no vrrp *VRID* **priority**

Параметры

VRID	Укажите идентификатор виртуального маршрутизатора в диапазоне от 1 до 255.
PRIORITY	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. Указанное значение – 200.

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#vrrp 1 priority 200
Switch(config-if)#
```

115.5 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. Чтобы отключить ответ на ping, воспользуйтесь формой **no** этой команды.

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)#
```

115.6 vrrp timers advertise

Данная команда используется для настройки интервала между последовательными VRRP advertisement, отправленными Master-маршрутизатором. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

vrrp *VRID* **timers advertise** *INTERVAL*

no vrrp *VRID* **timers advertise**

Параметры

VRID	Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать группу VRRP. Диапазон значений: от 1 до 255.
INTERVAL	Укажите временной интервал между последовательными VRRP advertisement, отправленными Master-маршрутизатором. 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. Настроенное значение – 10 секунд.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#vrrp 7 timers advertise 10
Switch(config-if)#
```

115.7 vrrp preempt

Данная команда позволяет маршрутизатору взять на себя роль основного устройства (Master), если у него более высокий приоритет, чем у текущего устройства (Master). Чтобы вернуться к режиму Non-Preempt Mode, воспользуйтесь формой **no** этой команды.

vrrp *VRID* **preempt**
no vrrp *VRID* **preempt**

Параметры

VRID	Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать группу VRRP. Диапазон значений: от 1 до 255.

По умолчанию

По умолчанию используется режим Preempt Mode.

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 vlan1
Switch(config-if)#vrrp 7 preempt
Switch(config-if)#
```

115.8 vrrp shutdown

Данная команда используется для отключения виртуального маршрутизатора на интерфейсе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

vrrp *VRID* **shutdown**
no vrrp *VRID* **shutdown**

Параметры

VRID	Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать группу VRRP. 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)#
```

115.9 vrrp track critical-ip

Данная команда используется для настройки критического IP-адреса виртуального маршрутизатора. Чтобы удалить критический IP-адрес, воспользуйтесь формой **no** этой команды.

vrrp *VRID* **track critical-ip** *IP-ADDRESS*
no vrrp *VRID* **track critical-ip**

Параметры

VRID	Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать группу VRRP. Диапазон значений: от 1 до 255.
IP-ADDRESS	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)#
```

115.10 show vrrp

Данная команда используется для отображения настроек VRRP.

show vrrp [interface *INTERFACE-ID* **[***VRID***]]**

Параметры

INTERFACE-ID	(Опционально.) Укажите идентификатор интерфейса (Interface ID).
VRID	(Опционально.) Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать VRRP-группу. Диапазон значений: от 1 до 255.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки VRRP.

Пример

В данном примере показано, как отобразить настройки VRRP.

```
Switch#show vrrp

vlan1 - Group 7 - Version2
  State is Master
  Virtual IP Address is 10.1.1.1
  Virtual MAC Address is 00-00-5E-00-01-07
  Advertisement interval is 10 seconds
  Preemption is enabled
  Priority is 100
  Authentication is enabled
  Authentication Text is test
  No critical IP address
  Master Router is 10.90.90.90(local)

Total Entries: 1
Switch#
```

115.11 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.

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
--------- ---- --- ---- --- ----- --- -----  ---------
vlan1      7    2  NA   100        Y  Master 10.1.1.1

Total Entries: 1
Switch#
```

115.12 debug vrrp

Данная команда используется для включения функции отладки VRRP. Для отключения функции воспользуйтесь формой **no** этой команды.

debug vrrp
no debug vrrp

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Команда применяется для включения или отключения функции отладки VRRP.

Пример

В данном примере показано, как включить функцию отладки VRRP.

```
Switch#debug vrrp
Switch#
```

115.13 debug vrrp errors

Данная команда используется для включения функции отладки ошибок VRRP. Для отключения функции воспользуйтесь формой **no** этой команды.

debug vrrp errors
no debug vrrp errors

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Команда применяется для включения или отключения функции отладки ошибок VRRP.

Пример

В данном примере показано, как включить функцию отладки ошибок VRRP.

```
Switch#debug vrrp errors
Switch#
```

115.14 debug vrrp events

Данная команда используется для включения функции отладки событий VRRP. Для отключения функции воспользуйтесь формой **no** этой команды.

debug vrrp events
no debug vrrp events

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Команда применяется для включения или отключения функции отладки событий VRRP. Если данная функция включена, будут записываться сообщения отладки при аутентификации интерфейса VRRP, изменении виртуального MAC-адреса VRRP или получении коммутатором оповещений VRRP.

Пример

В данном примере показано, как включить функцию отладки событий VRRP.

```
Switch#debug vrrp events
Switch#
```

115.15 debug vrrp packets

Данная команда используется для включения функции отладки пакетов VRRP. Для отключения функции воспользуйтесь формой **no** этой команды.

debug vrrp packets
no debug vrrp packets

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Команда применяется для включения или отключения функции отладки пакетов VRRP. Если данная функция включена, будут записываться сообщения отладки при отправке или получении пакетов VRRP.

Пример

В данном примере показано, как включить функцию отладки пакетов VRRP.

```
Switch#debug vrrp packets
Switch#
```

115.16 debug vrrp state

Данная команда используется для включения функции отладки состояния VRRP. Для отключения функции воспользуйтесь формой **no** этой команды.

debug vrrp state
no debug vrrp state

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Команда применяется для включения или отключения функции отладки состояния VRRP. Если функция включена, будут записываться сообщения отладки при изменении состояния канала, IP-адреса интерфейса или состояния VRRP.

Пример

В данном примере показано, как включить функцию отладки состояния VRRP.

```
Switch#debug vrrp state
Switch#
```

115.17 debug vrrp log

Данная команда используется, чтобы включить отправку сообщений журнала событий VRRP. Для отключения функции воспользуйтесь формой **no** этой команды.

debug vrrp log
no debug vrrp log

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Команда применяется для включения или отключения отправки сообщений журнала событий VRRP.

Пример

В данном примере показано, как включить отправку сообщений журнала событий VRRP.

```
Switch#debug vrrp log
Switch#
```

116. Команды Virtual Router Redundancy Protocol Version 3 (VRRPv3)

116.1 vrrp address-family

Данная команда используется для создания виртуального VRRP-маршрутизатора и входа в режим Address Family Configuration Mode с использованием IPv4 или IPv6. Для удаления группы воспользуйтесь формой **no** этой команды.

vrrp *VRID* **address-family {ipv4 | ipv6}**
no vrrp *VRID* **address-family {ipv4 | ipv6}**

Параметры

VRID	Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать группу VRRP. Доступный диапазон значений: от 1 до 255.
ipv4	Укажите, чтобы создать виртуальный маршрутизатор IPv4.
ipv6	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 vlan3
Switch(config-if)#vrrp 1 address-family ipv4
Switch(config-af-vrrp)#
```

116.2 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. Для отключения ответа на ping воспользуйтесь формой **no** этой команды.

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 vlan3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#non-owner-ping
Switch(config-af-vrrp)#
```

116.3 address

Данная команда используется для настройки виртуального адреса IPv4 или IPv6 для одного виртуального маршрутизатора. Для удаления виртуального адреса воспользуйтесь формой **no** этой команды.

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

Параметры

IP-ADDRESS	Укажите виртуальный IPv4-адрес виртуального маршрутизатора.
IPv6-ADDRESS	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 примере показано, как настроить виртуальный адрес IPv6 для VRRP-группы.

```
Switch#configure terminal
Switch(config)#interface vlan3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#address FE80::2
Switch(config-af-vrrp)#
```

116.4 priority

Данная команда используется для настройки приоритета виртуального маршрутизатора. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

priority *PRIORITY*
no priority

Параметры

PRIORITY	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 vlan3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#priority 200
Switch(config-af-vrrp)#
```

116.5 timers advertise

Данная команда используется для настройки интервала между последовательными VRRP advertisement. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

timers advertise *INTERVAL*
no timers advertise

Параметры

INTERVAL	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 vlan3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#timers advertise 10
Switch(config-af-vrrp)#
```

116.6 preempt

Данная команда позволяет маршрутизатору взять на себя роль основного устройства (Master), если у него более высокий приоритет, чем у текущего устройства (Master). Для возврата к режиму Non-Preempt Mode воспользуйтесь формой **no** этой команды.

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 vlan3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#no preempt
Switch(config-af-vrrp)#
```

116.7 shutdown

Данная команда используется для отключения виртуального маршрутизатора. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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 vlan3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#shutdown
Switch(config-af-vrrp)#
```

116.8 track critical-ip

Данная команда используется для настройки критического IP-адреса виртуального маршрутизатора. Для удаления критического IP-адреса воспользуйтесь формой **no** этой команды.

track critical-ip {*IP-ADDRESS* **| [***INTERFACE-ID***]** *IPV6-ADDRESS***}**
no track critical-ip

Параметры

IP-ADDRESS	Задайте критический IP-адрес.
INTERFACE-ID	(Опционально.) Укажите интерфейс критического IP-адреса, который необходимо использовать.
IPv6-ADDRESS	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 vlan1
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#track critical-ip vlan1 FE80::2
Switch(config-af-vrrp)#
```

116.9 show vrrp

Данная команда используется для отображения настроек и статуса VRRP.

show vrrp [interface *INTERFACE-ID* **[***VRID***]] [ipv4 | ipv6]**

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса.
VRID	(Опционально.) Укажите идентификатор виртуального маршрутизатора, чтобы идентифицировать VRRP-группу. Доступный диапазон значений: от 1 до 255.
ipv4	(Опционально.) Укажите, чтобы отобразить информацию о виртуальных маршрутизаторах IPv4.
ipv6	(Опционально.) Укажите, чтобы отобразить информацию о виртуальных маршрутизаторах IPv6.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки и статус VRRP.

Пример

В данном примере показано, как отобразить статус VRRP для всех интерфейсов.

```
Switch#show vrrp

vlan3 - 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#
```

116.10 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.

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
--------- ---- --- ---- --- ----- --- -----  ---------
vlan3      1    3  IPv6 100        Y  Init   ::

Total Entries: 1


Switch#
```

117. Команды Voice VLAN

117.1 voice vlan

Данная команда используется для глобального включения функции Voice VLAN и её настройки. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

voice vlan *VLAN-ID*
no voice vlan

Параметры

VLAN-ID	Укажите ID Voice VLAN в диапазоне от 2 до 4094.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для глобального включения функции Voice VLAN и ее настройки. На коммутаторе может быть настроена только одна Voice VLAN.

Для включения функции Voice VLAN необходимо применить команду **voice vlan** в режиме Global Configuration Mode и команду **voice vlan enable** в режиме Interface Configuration Mode.

При включении на порту функции Voice VLAN полученные VoIP-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 VoIP-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)#
```

117.2 voice vlan aging

Данная команда используется для настройки времени устаревания (Aging Time) для устаревших динамических member-портов Voice VLAN. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

voice vlan aging *MINUTES*
no voice vlan aging

Параметры

MINUTES	Укажите время устаревания Voice VLAN в диапазоне от 1 до 65535 минут.

По умолчанию

Значение по умолчанию – 720 минут.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для настройки времени устаревания для VoIP-устройства и автоматически изученных member-портов Voice VLAN. Когда последнее VoIP-устройство, подключенное к порту, перестает отправлять трафик и MAC-адрес данного устройства устаревает в FDB, запускается таймер времени устаревания Voice VLAN. По истечении данного времени порт будет удален из Voice VLAN. Если VoIP-трафик возобновляется в течение времени устаревания, таймер будет отменен.

Пример

В данном примере показано, как настроить время устаревания Voice VLAN. Указанное значение – 30 минут.

```
Switch#configure terminal
Switch(config)#voice vlan aging 30
Switch(config)#
```

117.3 voice vlan enable

Данная команда используется для включения функции Voice VLAN на портах. Чтобы отключить данную функцию на портах, воспользуйтесь формой **no** этой команды.

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 интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#voice vlan enable
Switch(config-if)#
```

117.4 voice vlan mac-address

Данная команда используется для добавления определенного пользователем OUI (уникального идентификатора организации) VoIP-устройства. Чтобы удалить определенный пользователем OUI VoIP-устройства, воспользуйтесь формой **no** этой команды.

voice vlan mac-address *MAC-ADDRESS MASK* **[description** *TEXT***]**
no voice vlan mac-address *MAC-ADDRESS MASK*

Параметры

MAC-ADDRESS	Укажите MAC-адрес OUI.
MASK	Укажите соответствующую битовую маску MAC-адреса OUI.
description *TEXT*	(Опционально.) Укажите описание определенного пользователем OUI. Максимальное количество символов – 32.

По умолчанию

OUI по умолчанию указаны в следующей таблице:

OUI	Vendor
00:E0:BB	3COM
00:03:6B	Cisco
00:E0:75	Veritel
00:D0:1E	Pingtel
00:01:E3	Siemens
00:60:B9	NEC/Philips
00:0F:E2	Huawei-3COM
00:09:6E	Avaya

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для добавления определенного пользователем OUI VoIP-устройства. 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.

Определенный пользователем OUI не может совпадать с OUI по умолчанию. OUI по умолчанию не может быть удален.

Пример

В данном примере показано, как добавить определенный пользователем OUI для VoIP-устройства.

```
Switch#configure terminal
Switch(config)#voice vlan mac-address 00-02-03-00-00-00 FF-FF-FF-00-00-00 description User1
Switch(config)#
```

117.5 voice vlan mode

Данная команда используется для включения автоматического изучения порта в качестве member-порта Voice VLAN. Чтобы отключить автоматическое изучение, воспользуйтесь формой **no** этой команды.

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 member-порта Voice VLAN. В дальнейшем членство будет автоматически удалено согласно времени устаревания. Когда порт работает в автотегированном режиме (**Auto Tag Mode**) и фиксирует VoIP-устройство через OUI, он автоматически присоединится к Voice VLAN как тегированный порт. Если VoIP-устройство отправляет тегированные пакеты, коммутатор изменит их приоритет. Нетегированные пакеты отправляются в PVID VLAN порта.

Когда порт работает в автонетегированном режиме (**Auto Untag Mode**) и получает информацию о VoIP-устройстве через OUI, он автоматически присоединится к Voice VLAN как нетегированный порт. Если VoIP-устройство отправляет тегированные пакеты, коммутатор изменит их приоритет. Нетегированные пакеты отправляются в Voice VLAN.

Когда коммутатор принимает пакеты LLDP-MED, он проверяет VLAN ID, флаги тега и приоритета, настройкам которых он должен следовать.

Если автоматическое изучение отключено, используйте команду **switchport hybrid vlan** для настройки порта в качестве тегированного или нетегированного member-порта Voice VLAN.

Пример

В данном примере показано, как настроить автотегированный режим (Auto Tag Mode) на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#voice vlan mode auto tag
Switch(config-if)#
```

117.6 voice vlan qos

Данная команда используется для настройки приоритета CoS для входящего трафика Voice VLAN. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

voice vlan qos *COS-VALUE*
no voice vlan qos

Параметры

COS-VALUE	Укажите приоритет Voice VLAN в диапазоне от 0 до 7.

По умолчанию

Значение по умолчанию – 5.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для маркировки CoS VoIP-пакетов, поступающих на порт, на котором включена Voice VLAN. Маркировка CoS позволяет отделить VoIP-трафик от трафика данных по качеству обслуживания.

Пример

В данном примере показано, как настроить приоритет Voice VLAN. Указанное значение – 7.

```
Switch#configure terminal
Switch(config)#voice vlan qos 7
Switch(config)#
```

117.7 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 *INTERFACE-ID*	(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.

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         : 1/0/1-1/0/5
 Dynamic Member Ports : 1/0/1-1/0/3

 Voice VLAN OUI       :

OUI Address         Mask              Description
 ----------------  ----------------  --------------
 00-01-E3-00-00-00  FF-FF-FF-00-00-00  Siemens
 00-02-03-00-00-00  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 примере ниже показано, как отобразить информацию о портах Voice VLAN.

```
Switch#show voice vlan interface eth1/0/6-10

 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 интерфейсах Ethernet 1/0/1 и 1/0/2.

```
Switch#show voice vlan device interface eth1/0/1-2

 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 примере ниже показано, как отобразить VoIP-устройства, обнаруженные через LLDP-MED, на интерфейсах Ethernet 1/0/1 и 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 10:00:00
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 11:00:00
Remain Time          : 105 Seconds

Total Entries: 2
Switch#
```

118. Команды Web-аутентификации

118.1 web-auth enable

Данная команда используется для включения функции web-аутентификации на порту. Чтобы отключить функцию web-аутентификации, воспользуйтесь формой **no** этой команды.

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 включения аутентификации узлов, подключенных к порту, через браузер.

Пример

В данном примере показано, как включить функцию web-аутентификации на порту 1.

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

118.2 web-auth page-element

Данная команда используется для настройки элементов страницы web-аутентификации. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

web-auth page-element {page-title *STRING* **| login-window-title** *STRING* **| username-title** *STRING* **| password-title** STRING **| logout-window-title** *STRING* **| copyright-line** *LINE-NUMBER* **title** *STRING***}**

no web-auth page-element {page-title | login-window-title | username-title | password-title | logout-window-title | copyright-line}

Параметры

page-title *STRING*	Укажите заголовок страницы web-аутентификации. Максимальное количество символов – 128.
login-window-title *STRING*	Укажите заголовок окна для ввода логина/пароля страницы web-аутентификации. Максимальное количество символов – 64.
username-title *STRING*	Укажите название поля для ввода имени пользователя на странице web-аутентификации. Максимальное количество символов – 32.
password-title STRING	Укажите название поля для ввода пароля на странице web-аутентификации. Максимальное количество символов – 32.
logout-window-title *STRING*	Укажите заголовок окна выхода из системы (logout) на странице web-аутентификации. Максимальное количество символов – 64.
copyright-line *LINE-NUMBER* **title** *STRING*	Укажите информацию об авторских правах построчно на странице web-аутентификации. Максимальное количество строк – 5. Максимальное количество символов в каждой строке – 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 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 кастомизированы администратором.
Существуют две страницы web-аутентификации: (1) страница входа и (2) страница выхода.
На странице входа запрашиваются имя пользователя и пароль пользователя. После успешного входа в сеть пользователь может использовать кнопку **Logout** для выхода.

Пример

В данном примере показано, как изменить информацию об авторских правах в двух строках нижней части страницы аутентификации:
Строка 1: Copyright @ 2020 All Rights Reserved
Строка 2: Site: http://support.website.com

```
Switch#configure terminal
Switch(config)#web-auth page-element copyright-line 1 title Copyright @ 2020 All Rights
Reserved
Switch(config)#web-auth page-element copyright-line 2 title Site: http://support.website.com
Switch(config)#
```

118.3 web-auth success redirect-path

Данная команда используется для настройки URL, на который клиент будет переадресован после успешной аутентификации. Чтобы удалить указанный URL, воспользуйтесь формой **no** этой команды.

web-auth success redirect-path *STRING*

no web-auth success redirect-path

Параметры

STRING	Укажите URL, на который клиент будет переадресован после успешной аутентификации. Если URL не указан, будет отображена страница выхода web-аутентификации. Максимальное количество символов – 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 применяется для указания страницы, которую необходимо отобразить узлам, прошедшим web-аутентификацию.

Пример

В данном примере показано, как настроить URL для переадресации клиентов прохождения web-аутентификации. Указанный путь – http://www.website.com.

```
Switch# configure terminal
Switch(config)# web-auth success redirect-path http://www.website.com
Switch(config)#
```

118.4 web-auth system-auth-control

Данная команда используется для глобального включения функции web-аутентификации на коммутаторе. Чтобы отключить функцию web-аутентификации глобально на коммутаторе, воспользуйтесь формой **no** этой команды.

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

Функция используется для аутентификации пользователей, пытающихся получить доступ в сеть. 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)#
```

118.5 web-auth virtual-ip

Данная команда используется для настройки виртуального IP-адреса web-аутентификации, который используется для приема запросов аутентификации от узла. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

web-auth virtual-ip {ipv4 *IP-ADDRESS* **| ipv6** *IPV6-ADDRESS* **| url** *STRING***}**
no web-auth virtual-ip {ipv4 | ipv6 | url}

Параметры

ipv4 *IP-ADDRESS*	Укажите виртуальный IPv4-адрес web-аутентификации.
url *STRING*	Укажите FQDN URL для web-аутентификации. Максимальное количество символов – 128.
ipv6 *IPV6-ADDRESS*	Укажите виртуальный IPv6-адрес web-аутентификации.

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. С данным адресом взаимодействуют все процессы аутентификации, но виртуальный IP-адрес не отвечает на запросы ICMP или ARP. Поэтому настройка виртуального IP-адреса в той же подсети, что и IP-адреса интерфейса коммутатора или узла, недопустима. В противном случае, функция web-аутентификации будет работать некорректно.

Перед использованием указанного URL необходимо настроить виртуальный IP-адрес. Для получения IP-адреса по FQDN URL используется обращение к DNS-серверу. 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. Указанный IPv4-адрес – 1.1.1.1. Заданный 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 примере ниже показано, как настроить виртуальный IPv6 и FQDN URL для Web-аутентификации. Указанный IPv6-адрес – 2000::2. Заданный 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)#
```

118.6 snmp-server enable traps web-auth

Данная команда используется, чтобы включить отправку SNMP-уведомлений для web-аутентификации. Для отключения отправки SNMP-уведомлений воспользуйтесь формой **no** этой команды.

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

Данная команда используется, чтобы включить/отключить отправку SNMP-уведомлений для web-аутентификации.

Пример

В данном примере показано, как включить отправку SNMP-уведомлений для web-аутентификации.

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

119. Команды Weighted Random Early Detection (WRED)

119.1 random-detect

Данная команда используется для включения функции WRED. Чтобы отключить функцию, воспользуйтесь формой **no** этой команды.

random-detect *COS-VALUE* **[profile** *ID***]**
no random-detect *COS-VALUE*

Параметры

COS-VALUE	Укажите очереди CoS, для которых необходимо включить функцию WRED. Диапазон значений: от 0 до 7.
profile *ID*	(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:

$$Drop\,\Pr obability = \frac{avg_Qsize - MinThreshold}{MaxThreshold - MinThreshold} * MaxDropRate$$

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 WRED 10.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# random-detect 5 profile 10
Switch(config-if)#
```

119.2 random-detect exponential-weight

Данная команда используется для настройки экспоненциального весового коэффициента (exponential weight factor) WRED для расчета среднего размера очереди. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

random-detect exponential-weight *COS-VALUE* **exponent** *VALUE*
no random-detect exponential-weight *COS-VALUE*

Параметры

COS-VALUE	Укажите очереди CoS, на которых необходимо установить экспоненту. Диапазон значений: от 0 до 7.
exponent *VALUE*	Укажите значение экспоненты в диапазоне от 0 до 15.

По умолчанию

Экспоненциальный весовой коэффициент по умолчанию – 9.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить экспоненциальный весовой коэффициент WRED для расчета среднего размера очереди.

Пример

В данном примере показано, как настроить значение экспоненты для очереди 5 на интерфейсе Ethernet 1/0/1. Указанное 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)#
```

119.3 random-detect profile

Данная команда используется для настройки профиля WRED. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

random-detect profile *ID* **[tcp] [green | yellow | red] min-threshold** *VALUE* **max-threshold** *VALUE* **max-drop-rate** *VALUE*

no random-detect profile *ID*

Параметры

ID	Укажите ID профиля WRED.
tcp	(Опционально.) Укажите параметры отбрасывания WRED, которые необходимо установить для пакетов TCP.
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 *VALUE*	Укажите минимальное количество ячеек в очереди, после достижения которого пакеты начнут отбрасываться при помощи WRED.
max-threshold *VALUE*	Укажите максимальное количество ячеек в очереди, после достижения которого все пакеты, предназначенные для данной очереди, будут отброшены при помощи WRED.
max-drop-rate *VALUE*	Укажите вероятность отброса пакетов в случае, если средний размер очереди достигнет максимального порога. Если значение равно нулю, пакет не будет отброшен или отмечен для ECN. Диапазон – от 0 до 14, где значения от 0 до 10 представляют собой вероятности от 0% до 10%, 11 обозначает 25%, 12 - 50%, 13 - 75%, а 14 - 100%.

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 разные листы ожидания (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)#
```

В примере ниже показано, как настроить параметры отбрасывания WRED для желтых пакетов TCP в профиле 10.

```
Switch#configure terminal
Switch(config)#random-detect profile 10 tcp yellow min-threshold 20 max-threshold 40 max-drop-
rate 5
Switch(config)#
```

119.4 show queueing random-detect

Данная команда используется для отображения настроек WRED на указанном интерфейсе.

show queueing random-detect [interface *INTERFACE-ID* **[, | -]]**

Параметры

interface *INTERFACE-ID*	(Опционально.) Укажите ID интерфейса для отображения.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

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 eth1/0/1

 Current WRED configuration:

   eth1/0/1
   CoS  WRED State  Exp-weight-constant  Profile
   ---  ----------  -------------------  -------
   0    Disabled    9                    1
   1    Disabled    9                    1
   2    Disabled    9                    1
   3    Disabled    9                    1
   4    Disabled    9                    1
   5    Disabled    9                    1
   6    Disabled    9                    1
   7    Disabled    9                    1

Switch#
```

119.5 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 для отображения. Если профиль не указан, будут отображены настройки всех профилей WRED.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

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#
```

120. Команды Zone Defense

120.1 zone-defense

Данная команда используется для включения функции Zone defense. Чтобы отключить функцию, воспользуйтесь формой **no** этой команды.

zone-defense
no zone-defense

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 или отключения функции Zone defense. При включении функции ресурсы ACL будут зарезервированы для ее работы. Если ресурсов ACL на коммутаторе недостаточно, включение функции Zone defense невозможно.

Пример

В примере показано, как включить функцию Zone defense.

```
Switch#configure terminal
Switch(config)#zone-defense
Switch(config)#
```

120.2 show zone_defense

Данная команда используется для отображения состояния функции Zone defense.

show zone_defense

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для отображения состояния функции Zone defense.

Пример

В примере показано, как отобразить состояние функции Zone defense.

```
Switch#show zone_defense

Zone Defense Status           : Enabled


Switch#
```

Приложение A. Восстановление пароля (Password Recovery)

В данной главе представлен процесс сброса паролей на коммутаторах D-Link серии DXS-3610.

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                                          1.00.010
-----------------------------------------------------------------------------

  Power On Self Test ....................................  100 %

  MAC Address    : 80-26-89-15-28-00
  H/W Version    : A1

  Please Wait, Loading V1.00.022 Runtime Image ..............  100 %
  UART init .................................................  100 %
```

```
Password Recovery Mode

Switch(reset-config)#
```

В режиме восстановления пароля могут быть использованы следующие команды:

Команда	Описание
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 B. Записи системного журнала

В таблице ниже перечислены все записи и их соответствующие значения, появляющиеся в системном журнале коммутатора.

802.1X

Описание записей журнала	Уровень
Описание события: ошибка аутентификации 802.1X. Сообщение в журнале: 802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>). Описание параметров: reason: причина ошибки аутентификации. Возможные причины: (1) Ошибка аутентификации пользователя. (2) Нет ответа от сервера (серверов). (3) Нет настроенных серверов. (4) Нет источников. (5) Время ожидания пользователя истекло. username: пользователь, проходящий аутентификацию. interface-id: имя интерфейса. mac-address: MAC-адрес аутентифицированного устройства.	Критический
Описание события: успешная аутентификация 802.1X. Сообщение в журнале: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>). Описание параметров: username: пользователь, проходящий аутентификацию. interface-id: имя интерфейса. mac-address: MAC-адрес аутентифицированного устройства.	Информационный

AAA

Описание записей журнала	Уровень
Описание события: глобальное включение/отключение AAA. Сообщение в журнале: AAA is <status>. Описание параметров: status: функция AAA включена или отключена.	Информационный

Описание события: успешный вход. Сообщение в журнале: Successful login 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.	Информационный
Описание события: ошибка входа. Сообщение в журнале: Login 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.	Предупреждение
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.	Предупреждение

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.	Информационный
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.	Предупреждение
Описание события: Удаленный сервер не отвечает на запрос аутентификации с применением пароля. Сообщение в журнале: Enable privilege 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.	Предупреждение

Описание события: RADIUS назначил атрибуты допустимого VLAN ID. Сообщение в журнале: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>). Описание параметров: server-ip: IP-адрес RADIUS-сервера. vid: назначенный VLAN ID, авторизованный RADIUS-сервером. interface-id: номер порта аутентифицированного клиента. username: имя пользователя аутентификации.	Информационный
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>). Описание параметров: server-ip: IP-адрес RADIUS-сервера. direction: направление полосы пропускания: ingress (входящая) или egress (исходящая). threshold: назначенный порог полосы пропускания, авторизованный RADIUS-сервером. interface-id: номер порта аутентифицированного клиента. username: имя пользователя аутентификации.	Информационный
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>). Описание параметров: server-ip: IP-адрес RADIUS-сервера. priority: назначенный авторитет, авторизованный RADIUS-сервером. interface-id: номер порта аутентифицированного клиента. username: имя пользователя аутентификации.	Информационный

Описание события: RADIUS назначил ACL Script, который не может быть применен в системе из-за недостаточности ресурса. Сообщение в журнале: RADIUS server <server-ip> assigns <username> ACL failure at port <interface - id> (<acl-script>). Описание параметров: server-ip: IP-адрес RADIUS-сервера. username: имя пользователя аутентификации. interface-id: номер порта аутентифицированного клиента. acl-script: назначенный ACL Script, авторизованный RADIUS-сервером.	Предупреждение
Описание события: RADIUS назначил ACL Script, который применен в системе из-за недостаточности ресурса. Сообщение в журнале: RADIUS server <server-ip> assigns <username> ACL success at port <interface -id> (<acl-script>). Описание параметров: server-ip: IP-адрес RADIUS-сервера. username: имя пользователя аутентификации. interface-id: номер порта аутентифицированного клиента. acl-script: назначенный ACL Script, авторизованный RADIUS-сервером.	Информационный

ARP

Описание записей журнала	**Уровень**
Описание события: добровольный ARP-запрос (Gratuitous ARP) обнаружил, что другой узел уже использует данный IP-адрес. Сообщение в журнале: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>). Описание параметров: ipaddr: заданный IP-адрес, который используется другим узлом. macaddr: заданный MAC-адрес, который используется другим узлом. UnitID: 1. Значение должно быть целым числом. 2. ID модуля в стеке. PortNum: 1. Значение должно быть целым числом. 2. Номер логического порта устройства. ipif_name: имя интерфейса коммутатора, из-за IP-адреса которого возник конфликт.	Предупреждение

ARP Spoofing Prevention

Описание записей журнала	Уровень
Описание события: ложный ARP-пакет обнаружен функцией ARP Spoofing Prevention. Сообщение в журнале: Gateway <ipaddr> is under attack by <macaddr> from <interface-id> Описание параметров: ipaddr: IP-адрес шлюза. macaddr: MAC-адрес хакера. interface-id: интерфейс хакера.	Предупреждение

Auto Image

Описание записей журнала	Уровень
Описание события: обновление ПО через функцию Auto Image выполнено успешно. Сообщение в журнале: The downloaded firmware was successfully executed by DHCP Auto Image update (TFTP Server IP: <ipaddr>). Описание параметров: ipaddr: IP-адрес TFTP-сервера.	Информационный
Описание события: обновление ПО через функцию Auto Image выполнить не удалось. Сообщение в журнале: The downloaded firmware was not successfully executed by DHCP Auto Image update (TFTP Server IP: <ipaddr>). Описание параметров: ipaddr: IP-адрес TFTP-сервера.	Информационный

Auto Save

Описание записей журнала	Уровень
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>). Описание параметров: unit: Box ID. Username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный

Auto Surveillance VLAN

Описание записей журнала	Уровень
Описание события: обнаружение на интерфейсе нового устройства видеонаблюдения. Сообщение в журнале: New surveillance device detected (<interface-id>, MAC: <mac-address>). Описание параметров: interface-id: название интерфейса. mac-address: MAC-адрес устройства видеонаблюдения.	Информационный
Описание события: автоматическое присоединение интерфейса, на котором включена surveillance VLAN, к surveillance VLAN. Сообщение в журнале: <interface-id> add into surveillance VLAN <vid>. Описание параметров: interface-id: название интерфейса. vid: VLAN ID.	Информационный
Описание события: выход интерфейса из surveillance VLAN и одновременное отсутствие на этом интерфейсе устройств видеонаблюдения по истечении интервала устаревания (aging). Сообщение в журнале: <interface-id> remove from surveillance VLAN <vid>. Описание параметров: interface-id: название интерфейса. vid: VLAN ID.	Информационный

BPDU Protection

Описание записей журнала	Уровень
Описание события: атака BPDU. Сообщение в журнале: <interface-id> enter STP BPDU under protection state (mode: <mode>). Описание параметров: interface-id: интерфейс, на котором обнаружена атака STP BPDU. mode: режим защиты BPDU интерфейса. Возможные режимы: drop (отбрасывание), block (блокировка) или shutdown (отключение).	Информационный
Описание события: атака BPDU устранена. Сообщение в журнале: <interface-id> recover from BPDU under protection state. Описание параметров: interface-id: интерфейс, на котором обнаружена атака STP BPDU.	Информационный

Конфигурация/ПО

Описание записей журнала	Уровень
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.	Информационный

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.	Предупреждение
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.	Информационный
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. macaddr: MAC-адрес клиента. serverIP: IP-адрес сервера pathFile: путь и имя файла на сервере.	Предупреждение

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.	Информационный
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.	Предупреждение
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.	Информационный

Описание события: не удалось выгрузить конфигурацию. Сообщение в журнале: [Unit <unitID>,]Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>). Описание параметров: unitID: unit ID. session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. serverIP: IP-адрес сервера. pathFile: путь и имя файла на сервере.	Предупреждение
Описание события: конфигурация сохранена на флэш-память через консоль. Сообщение в журнале: [Unit <unitID>,]Configuration saved to flash by console (Username: <username>). Описание параметров: unitID: unit ID. username: имя текущего пользователя.	Информационный
Описание события: сообщение успешно выгружено. Сообщение в журнале: [Unit <unitID>,] Log message uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Описание параметров: unitID: unit ID. session: сессия пользователя. username: имя текущего пользователя ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента.	Информационный

Описание события: не удалось выгрузить сообщение. Сообщение в журнале: [Unit <unitID>,] Log message uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Описание параметров: unitID: unit ID. session: сессия пользователя. username: имя текущего пользователя ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента.	Предупреждение
Описание события: конфигурация сохранена на флэш-память удаленно. Сообщение в журнале: [Unit <unitID>,]Configuration saved to flash (Username: <username>, IP: <ipaddr>) Описание параметров: unitID: unit ID. username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный
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>) Описание параметров: unitID: unit ID. session: сессия пользователя. username: имя текущего пользователя. ipaddr: IP-адрес клиента. macaddr: MAC-адрес клиента. serverIP: IP-адрес сервера pathFile: путь и имя файла на сервере.	Предупреждение

Примечание:

1. Сессия пользователя указывает на доступ через Console, Web, SNMP, Telnet, SSH или DDP.
2. Если коммутатор находится в автономном (standalone) состоянии, unit ID в журнале указываться не будет.
3. Если обновление конфигурации/ПО выполняется через консоль, информация об IP- и MAC-адресах в журнале указываться не будет.

DAD

Описание записей журнала	Уровень
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. Описание параметров: ipv6address: IPv6-адрес сообщений Neighbor Solicitation. interface-id: ID интерфейса порта.	Предупреждение
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. Описание параметров: ipv6address: IPv6-адрес сообщений Neighbor Advertisement. interface-id: ID интерфейса порта.	Предупреждение

DAI

Описание записей журнала	Уровень
Описание события: обнаружен запрещенный ARP-пакет. Сообщение в журнале: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>). Описание параметров: type: тип ARP-пакета (request или response). Ipaddr: IP-адрес. macaddr: MAC-адрес. vlanid: VLAN ID. interface-id: имя интерфейса.	Предупреждение

Описание события: обнаружен допустимый ARP-пакет. Сообщение в журнале: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>). Описание параметров: type: тип ARP-пакета (request или response). Ipaddr: IP-адрес. macaddr: MAC-адрес. vlanid: VLAN ID. interface-id: имя интерфейса.	Информационный

DDM

Описание записей журнала	**Уровень**
Описание события: какой-либо из параметров SFP превысил порог warning (предупреждение). Сообщение в журнале: Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded. 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.	Предупреждение
Описание события: какой-либо из параметров SFP превысил порог alarm (тревога). Сообщение в журнале: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded. 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.	Критический

Описание события: какой-либо из параметров SFP вернулся к нормальному состоянию после превышения порога warning. 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).	Предупреждение

DHCPv6 Client

Описание записей журнала	**Уровень**
Описание события: состояние DHCPv6-клиента на указанном интерфейсе изменено администратором. Сообщение в журнале: DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled]. Описание параметров: <ipif-name>: имя интерфейса DHCPv6-клиента.	Информационный
Описание события: DHCPv6-клиент получил IPv6-адрес от сервера DHCPv6. Сообщение в журнале: DHCPv6 client obtains an ipv6 address <ipv6address> on interface <ipif-name>. Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.	Информационный
Описание события: IPv6-адрес, полученный от сервера DHCPv6, обновляется. Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> starts renewing. Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.	Информационный

Описание события: IPv6-адрес, полученный от сервера DHCPv6, успешно обновлен. Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> renews success. Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.	Информационный
Описание события: выполняется повторная привязка IPv6-адреса, полученного от сервера DHCPv6. Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding. Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.	Информационный
Описание события: повторная привязка IPv6-адреса, полученного от сервера DHCPv6, выполнена успешно. Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> rebinds success. Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. ipif-name: имя интерфейса DHCPv6-клиента.	Информационный
Описание события: IPv6-адрес, полученный от сервера DHCPv6, удален. Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> was deleted. Описание параметров: ipv6address: IPv6-адрес, полученный от сервера DHCPv6. Ipif-name: имя интерфейса DHCPv6-клиента.	Информационный
Описание события: состояние DHCPv6-клиента PD на указанном интерфейсе изменено администратором. Сообщение в журнале: DHCPv6 client PD on interface <intf-name> changed state to <enabled | disabled>. Описание параметров: intf-name: имя интерфейса DHCPv6-клиента PD.	Информационный

Описание события: DHCPv6-клиент PD получил IPv6-префикс от делегирующего маршрутизатора. Сообщение в журнале: DHCPv6 client PD obtains an ipv6 prefix <ipv6networkaddr> on interface <intf-name>. Описание параметров: ipv6networkaddr: IPv6-префикс, полученный от делегирующего маршрутизатора. intf-name: имя интерфейса DHCPv6-клиента PD.	Информационный
Описание события: IPv6-префикс, полученный от делегирующего маршрутизатора, обновляется. Сообщение в журнале: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> starts renewing. Описание параметров: ipv6networkaddr: IPv6-префикс, полученный от делегирующего маршрутизатора. intf-name: имя интерфейса DHCPv6-клиента PD.	Информационный
Описание события: IPv6-префикс, полученный от делегирующего маршрутизатора, успешно обновлен. Сообщение в журнале: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> renews success. Описание параметров: ipv6anetworkaddr: IPv6-префикс, полученный от делегирующего маршрутизатора. intf-name: имя интерфейса DHCPv6-клиента PD.	Информационный
Описание события: выполняется повторная привязка IPv6-префикса, полученного от сервера DHCPv6. Сообщение в журнале: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> starts rebinding. Описание параметров: ipv6address: IPv6-префикс, полученный от делегирующего маршрутизатора. Intf-name: имя интерфейса DHCPv6-клиента PD.	Информационный

Описание события: повторная привязка IPv6-префикса, полученного от делегирующего маршрутизатора, выполнена успешно. Сообщение в журнале: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> rebinds success. Описание параметров: ipv6address: IPv6-префикс, полученный от делегирующего маршрутизатора. intf-name: имя интерфейса DHCPv6-клиента PD.	Информационный
Описание события: IPv6-префикс, полученный от делегирующего маршрутизатора, удален. Сообщение в журнале: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> was deleted. Описание параметров: ipv6address: IPv6-префикс, полученный от делегирующего маршрутизатора. intf-name: имя интерфейса DHCPv6-клиента PD.	Информационный

DHCPv6 Relay

Описание записей журнала	**Уровень**
Описание события: состояние DHCPv6-клиента 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-клиента.	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

DNS Resolver

Описание записей журнала	Уровень
Описание события: добавлено дублирующееся доменное имя, в результате чего будет удалена запись DNS из динамического кэша. Сообщение в журнале: Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr> Описание параметров: domainname: доменное имя. ipaddr: IP-адрес.	Информационный

DoS Prevention

Описание записей журнала	Уровень
Описание события: обнаружена DoS-атака. Сообщение в журнале: <dos-type> is dropped from (IP: <ip-address> Port <interface-id>). Описание параметров: dos-type: тип DoS-атаки. ip-address: IP-адрес. interface-id: имя интерфейса.	Уведомление

Errdisable

Описание записей журнала	Уровень
Описание события: порт переходит в состояние отключения из-за ошибки (error disable). Сообщение в журнале: Port <interface-id> enters error disable state due to <reason-id>. Описание параметров: interface-id: номер порта. reason-id: Loopback Detection (обнаружение петель на порту коммутатора), Port Security Violation (нарушение безопасности порта), Storm Control, BPDU Protect (защита BPDU), ARP Rate Limit (ограничение скорости ARP), DHCP Rate Limit (ограничение скорости DHCP), L2 Protocol Tunneling (протокол туннелирования второго уровня), Digital Diagnostics Monitoring (цифровой диагностический мониторинг), Scheduled Port-shutdown by Power Saving (запланированное отключение порта за счет энергосбережения), Scheduled Hibernation by Power Saving (запланированный спящий режим за счет энергосбережения).	Предупреждение

Описание события: порт выходит из состояния отключения из-за ошибки (error disable). Сообщение в журнале: Port <interface-id> leaves the error disable state which is previously caused by <reason-id>. Описание параметров: interface-id: номер порта. reason-id: Loopback Detection (обнаружение петель на порту коммутатора), Port Security Violation (нарушение безопасности порта), Storm Control, BPDU Protect (защита BPDU), ARP Rate Limit (ограничение скорости ARP), DHCP Rate Limit (ограничение скорости DHCP), L2 Protocol Tunneling (протокол туннелирования второго уровня), Scheduled Port-shutdown by Power Saving (запланированное отключение порта за счет энергосбережения), Scheduled Hibernation by Power Saving (запланированный спящий режим за счет энергосбережения).	Предупреждение
Описание события: порт переходит в состояние отключения из-за ошибки (error disable). Сообщение в журнале: Port <interface-id> VLAN <vid> enters error disable state due to <reason-id>. Описание параметров: interface-id: номер порта. reason-id: Loopback Detection (обнаружение петель на порту коммутатора), Port Security Violation (нарушение безопасности порта), Storm Control, BPDU Protect (защита BPDU), ARP Rate Limit (ограничение скорости ARP), DHCP Rate Limit (ограничение скорости DHCP), L2 Protocol Tunneling (протокол туннелирования второго уровня), Scheduled Port-shutdown by Power Saving (запланированное отключение порта за счет энергосбережения), Scheduled Hibernation by Power Saving (запланированный спящий режим за счет энергосбережения). vid: VLAN ID.	Предупреждение

Описание события: порт выходит из состояния отключения из-за ошибки (error disable). Сообщение в журнале: Port <interface-id> VLAN <vid> leaves the error disable state which is previously caused by <reason-id> Описание параметров: interface-id: номер порта. reason-id: Loopback Detection (обнаружение петель на порту коммутатора), Port Security Violation (нарушение безопасности порта), Storm Control, BPDU Protect (защита BPDU), ARP Rate Limit (ограничение скорости ARP), DHCP Rate Limit (ограничение скорости DHCP), L2 Protocol Tunneling (протокол туннелирования второго уровня), Scheduled Port-shutdown by Power Saving (запланированное отключение порта за счет энергосбережения), and Scheduled Hibernation by Power Saving (запланированный спящий режим за счет энергосбережения). vid: VLAN ID.	Предупреждение

Interface

Описание записей журнала	**Уровень**
Описание события: соединение на порту прервано. Сообщение в журнале: Port <port-type>< interface-id> link down Описание параметров: port-type: тип порта. interface-id: имя интерфейса.	Информационный
Описание события: соединение на порту установлено. Сообщение в журнале: Port <port-type>< interface-id> link up, <link-speed> port-type: тип порта. interface-id: имя интерфейса. link-speed: скорость канала порта.	Информационный

IP Source Guard

Описание записей журнала	Уровень
Описание события: ошибка создания записи DHCP Snooping в таблице IPSG из-за отсутствия ресурсов аппаратных правил. 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: ipaddr: IP-адрес. macaddr: MAC-адрес. vlanid: VLAN ID interface-id: имя интерфейса.	Предупреждение

IPv6 Snooping

Описание записей журнала	Уровень
Описание события: не удалось получить данные IPv6. Сообщение в журнале: Failed to glean (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Port <INTERFACE-ID>) Описание параметров: IPADDR: IP-адрес записи IPv6 Snooping. MACADDR: MAC-адрес записи IPv6 Snooping. VLANID: VLAN ID записи IPv6 Snooping. INTERFACE_ID: порт записи IPv6 Snooping.	Уведомление
Описание события: данные IPv6 получены успешно. Сообщение в журнале: Glean to recover (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Port <INTERFACE-ID>) Описание параметров: IPADDR: IP-адрес записи IPv6 Snooping. MACADDR: MAC-адрес записи IPv6 Snooping. VLANID: VLAN ID записи IPv6 Snooping. INTERFACE_ID: порт записи IPv6 Snooping.	Информационный

IPv6 Source Guard

Описание записей журнала	Уровень
Описание события: ошибка создания записи IPv6 Snooping в таблице IPv6SG из-за отсутствия ресурсов аппаратных правил. Сообщение в журнале: Failed to set IPv6SG entry due to no hardware rule resource. (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Interface <INTERFACE-ID>). Описание параметров: ipaddr: IPv6-адрес записи IPv6 Snooping. macaddr: MAC-адрес записи IPv6 Snooping. vlanid: VID записи IPv6 Snooping. interface-id: интерфейс записи IPv6 Snooping.	Предупреждение

LACP

Описание записей журнала	Уровень
Описание события: группа агрегирования (Link Aggregation) включена. Сообщение в журнале: Link Aggregation Group <group_id> link up. Описание параметров: group_id: ID включенной группы агрегирования.	Информационный
Описание события: группа агрегирования (Link Aggregation) отключена. Сообщение в журнале: Link Aggregation Group <group_id> link down. Описание параметров: group_id: ID включенной группы агрегирования.	Информационный
Описание события: member-порт присоединился к группе агрегирования. Сообщение в журнале: <ifname> attach to Link Aggregation Group <group_id>. Описание параметров: ifname: имя интерфейса порта, который был присоединен к группе агрегирования. group_id: ID группы агрегирования, к которой был присоединен порт.	Информационный
Описание события: member-порт покинул группу агрегирования. 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.	Информационный

LBD

Описание записей журнала	**Уровень**
Описание события: на интерфейсе обнаружена петля. Сообщение в журнале: <interface-id> LBD loop occurred. Описание параметров: interface-id: интерфейс, на котором обнаружена петля.	Критический
Описание события: на интерфейсе обнаружена петля. Сообщение в журнале: <interface-id> VLAN <vlan-id> LBD loop occurred. Описание параметров: interface-id: интерфейс, на котором обнаружена петля. vlan-id: VLAN, на которой обнаружена петля.	Критический
Описание события: на интерфейсе обнаружена петля. Сообщение в журнале: <interface-id> LBD loop recovered. Описание параметров: interface-id: интерфейс, на котором обнаружена петля.	Критический
Описание события: на интерфейсе обнаружена петля. Сообщение в журнале: <interface-id> VLAN <vlan-id> LBD loop recovered. Описание параметров: interface-id: интерфейс, на котором обнаружена петля. vlan-id: VLAN, на которой обнаружена петля.	Критический
Описание события: число VLAN, на которых была обнаружена петля, превысило указанное число. Сообщение в журнале: Loop VLAN numbers overflow.	Критический

LLDP-MED

Описание записей журнала	Уровень
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: 1. chassisComponent(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.	Уведомление

Описание события: обнаружен конфликт типа устройства LLDP-MED. Сообщение в журнале: Conflict LLDP-MED device type 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: 1. chassisComponent(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.	Уведомление

Описание события: обнаружен несовместимый набор TLV LLDP-MED. Сообщение в журнале: Incompatible LLDP-MED TLV set 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: 1. chassisComponent(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.	Уведомление

Login/Logout

Описание записей журнала	**Уровень**
Описание события: успешный вход через консоль. Сообщение в журнале: [Unit <unitID>,]Successful login through Console (Username: <username>). Описание параметров: unitID: unit ID. username: имя текущего пользователя.	Информационный
Описание события: не удалось выполнить вход через консоль. Сообщение в журнале: [Unit <unitID>,] Login failed through Console (Username: <username>). Описание параметров: unitID: Unit ID. username: имя текущего пользователя.	Предупреждение

Описание события: время сессии в консоли истекло. Сообщение в журнале: [Unit <unitID>,] Console session timed out (Username: <username>). Описание параметров: unitID: Unit ID. username: имя текущего пользователя.	Информационный
Описание события: выполнен выход через консоль. Сообщение в журнале: [Unit <unitID>,] Logout through Console (Username: <username>). Описание параметров: unitID: unit ID. username: имя текущего пользователя.	Информационный
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.	Предупреждение
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 клиента.	Информационный
Описание события: выполнен выход через SSH. Сообщение в журнале: Logout through SSH (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя текущего пользователя. ipaddr: IP-адрес клиента.	Информационный

MAC-based Access Control

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
Описание события: количество авторизованных пользователей на интерфейсе вернулось к значению ниже максимального за заданный интервал времени. Сообщение в журнале: <interface-id> recovers from MAC-based Access Control stop learning state. Описание параметров: interface-id: интерфейс, на котором аутентифицирован хост.	Предупреждение

MSTP Debug

Описание записей журнала	Уровень
Описание события: Spanning Tree Protocol включен. Сообщение в журнале: Spanning Tree Protocol is enabled.	Информационный
Описание события: Spanning Tree Protocol отключен. Сообщение в журнале: Spanning Tree Protocol is disabled.	Информационный
Описание события: изменилась топология экземпляра MSTP. Сообщение в журнале: Topology changed (Instance : <Instance-id>,<interface_id>, MAC:<macaddr>) Описание параметров: Instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. interface_id: номер порта, обнаружевшего или получившего информацию об изменении топологии. macaddr: система MAC-адреса моста.	Уведомление
Описание события: выбран новый корневой мост экземпляра MSTP. Сообщение в журнале: [CIST | CIST Regional | MSTI Regional] New Root bridge selected ([Instance: <Instance-id>] MAC: <macaddr> Priority :<priority>) Описание параметров: Instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. macaddr: система MAC-адресов моста. priority: значение приоритета моста должно быть кратным 4096.	Информационный
Описание события: выбран новый корневй мост экземпляра MSTP. Сообщение в журнале: New root port selected (Instance:<Instance-id>, <interface_id>) Описание параметров: Instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. interface_id: номер порта, обнаружевшего или получившего информацию об изменении топологии.	Уведомление

Описание события: изменился статус порта экземпляра MSTP. Сообщение в журнале: Spanning Tree port status change (Instance :<Instance-id>, <interface_id>) <old_status> -> <new_status> Описание параметров: Instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. interface_id: номер порта, обнаружевшего или получившего информацию об изменении топологии. old status: new status: Порт STP. Возможные значения: Disable, Discarding, Learning, Forwarding.	Уведомление
Описание события: изменилась роль порта экземпляра MSTP. Сообщение в журнале: Spanning Tree port role change (Instance :<Instance-id>, <interface_id>) <old_role> -> <new_role> Описание параметров: Instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. interface_id: номер порта, обнаружевшего или получившего информацию об изменении топологии. old role: new role: Роль порта STP. Возможные значения: DisabledPort, AlternatePort, BackupPort, RootPort, DesignatedPort, MasterPort.	Информационный
Описание события: создан экземпляр MSTP. Сообщение в журнале: Spanning Tree instance created (Instance :<Instance-id>) Описание параметров: Instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST.	Информационный
Описание события: удален экземпляр MSTP. Сообщение в журнале: Spanning Tree instance deleted (Instance :<Instance-id>) Описание параметров: Instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST.	Информационный
Описание события: изменена версия STP. Сообщение в журнале: Spanning Tree version change (new version :<new_version>) Описание параметров: new_version: версия STP.	Информационный

Описание события: имя конфигурации и revision level изменились в MST Configuration Identification. Сообщение в журнале: Spanning Tree MST configuration ID name and revision level change (name: <name>, revision level <revision_level>) Описание параметров: name: имя конкретного региона MST. revision_level: коммутаторы с одинаковым именем, но разными revision level считаются членами разных регионов MST.	Информационный
Описание события: привязка VLAN к экземпляру MST. Сообщение в журнале: Spanning Tree MST configuration ID VLAN mapping table change (instance: <Instance-id> add vlan <startvlanid> [- <endvlanid>]) Parameters Description: Instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. startvlanid: начальный vid для добавления диапазона vlan. endvlanid: конечный vid для добавления диапазона vlan.	Информационный
Описание события: удаление VLAN из экземпляра MST. Сообщение в журнале: Spanning Tree MST configuration ID VLAN mapping table change (instance: <Instance-id> delete vlan <startvlanid> [- <endvlanid>]) Parameters Description: Instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. startvlanid: начальный vid для удаления диапазона vlan. endvlanid: конечный vid для удаления диапазона vlan.	Информационный
Описание события: присвоена роль альтернативного порта (Alternate Port) из-за Root Guard. Сообщение в журнале: Spanning Tree port role change (Instance :<instance-id>, <interface-id>) to alternate port due to the guard root Parameters Description: Instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. Interface_id: номер порта, обнаружевшего событие.	Информационный

Описание события: статус Blocking из-за Loop Guard. Сообщение в журнале: Spanning Tree loop guard blocking (Instance :< instance-id >, <interface-id>) Parameters Description: Instance-id: идентификатор экземпляра MST. Экземпляр 0 используется для экземпляра по умолчанию, CIST. Interface_id: номер порта, обнаружевшего событие.	Информационный

OSPFv2

Описание записей журнала	**Уровень**
Описание события: состояние канала интерфейса OSPF изменилось. Сообщение в журнале: OSPF interface <intf-name> changed state to [Up | Down]. Описание параметров: intf-name: название интерфейса OSPF.	Информационный
Описание события: административное состояние интерфейса OSPF изменилось. Сообщение в журнале: OSPF protocol on interface <intf-name> changed state to [Enabled | Disabled]. Описание параметров: intf-name: название интерфейса OSPF.	Информационный
Описание события: интерфейс OSPF перешел из одной зоны в другую. Сообщение в журнале: OSPF interface <intf-name> changed from area <area-id> to area <area-id>. Описание параметров: intf-name: название интерфейса OSPF. area-id: ID зоны OSPF.	Информационный
Описание события: состояние соседнего устройства OSPF сменилось с Loading на Full. Сообщение в журнале: OSPF nbr <nbr-id> on interface <intf-name> changed state from Loading to Full. Описание параметров: intf-name: название интерфейса OSPF. nbr-id: ID соседнего маршрутизатора.	Уведомление

Описание события: состояние соседнего устройства OSPF сменилось с Full на Down. Сообщение в журнале: OSPF nbr <nbr-id> on interface <intf-name> changed state from Full to Down. Описание параметров: intf-name: название интерфейса OSPF. nbr-id: ID соседнего маршрутизатора.	Уведомление
Описание события: таймер dead соседнего устройства OSPF истек. Сообщение в журнале: OSPF nbr <nbr-id> on interface <intf-name> dead timer expired. Описание параметров: intf-name: название интерфейса OSPF. nbr-id: ID соседнего маршрутизатора.	Уведомление
Описание события: состояние виртуального соседнего устройства OSPF сменилось с Loading на Full. Сообщение в журнале: OSPF nbr <nbr-id> on virtual link changed state from Loading to Full. Описание параметров: nbr-id: ID соседнего маршрутизатора.	Уведомление
Описание события: состояние виртуального соседнего устройства OSPF сменилось с Full на Down. Сообщение в журнале: OSPF nbr <nbr-id> on virtual link changed state from Full to Down. Описание параметров: nbr-id: ID соседнего маршрутизатора.	Уведомление
Описание события: ID маршрутизатора OSPF изменился. Сообщение в журнале: OSPF router ID changed to <router-id>. Описание параметров: router-id: ID маршрутизатора OSPF.	Информационный

Peripheral

Описание записей журнала	**Уровень**
Команда	**Описание**
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.

PoE

Описание записей журнала	**Уровень**
Описание события: превышен предел мощности. Сообщение в журнале: Unit <unit-id> usage threshold <percentage> is exceeded Описание параметров: unit-id: box ID. Percentage: предельное значение.	Предупреждение
Описание события: нет превышения предела мощности. Сообщение в журнале: Unit <unit-id> usage threshold <percentage> is recovered Описание параметров: unit-id: box ID. Percentage: предельное значение.	Предупреждение

Описание события: PD-устройство не отвечает на запрос ping. Сообщение в журнале: PD alive check failed. (Port: <portNum>, PD: <ipaddr>) portNum: номер порта. Ipaddr: IP (IPv4/IPv6) адрес PD.	Предупреждение

Port Security

Описание записей журнала	**Уровень**
Описание события: превышено максимальное количество адресов на порту. Сообщение в журнале: MAC address <macaddr> causes port security violation on <interface-id>. Описание параметров: macaddr: недопустимый MAC-адрес. interface-id: имя интерфейса.	Предупреждение
Описание события: превышено максимальное количество адресов в системе. Сообщение в журнале: Limit on system entry number has been exceeded	Предупреждение

Safeguard

Описание записей журнала	**Уровень**
Описание события: загрузка CPU превысила верхний порог, коммутатор перешел в режим высокой загрузки. Сообщение в журнале: Unit <unit-id>, Safeguard Engine enters EXHAUSTED mode. Описание параметров: unit-id: unit ID.	Предупреждение
Описание события: загрузка CPU снизилась до нижнего порога, коммутатор перешел в нормальный режим. Сообщение в журнале: Unit <unit-id>, Safeguard Engine enters NORMAL mode. Описание параметров: unit-id: unit ID.	Информационный

SNMP

Описание записей журнала	Уровень
Описание события: получен запрос SNMP с неверной строкой сообщества. Сообщение в журнале: SNMP request received from <ipaddr> with invalid community string. Описание параметров: ipaddr: IP-адрес.	Информационный

SSH

Описание записей журнала	Уровень
Описание события: SSH-сервер включен. Сообщение в журнале: SSH server is enabled.	Информационный
Описание события: SSH-сервер отключен. Сообщение в журнале: SSH server is disabled.	Информационный

Stacking

Описание записей журнала	Уровень
Описание события: горячее подключение. Сообщение в журнале: Unit: <unitID>, MAC: <macaddr> Hot insertion. Описание параметров: unitID: Box ID. Macaddr: MAC-адрес.	Информационный
Описание события: горячее отключение. Сообщение в журнале: Unit: <unitID>, MAC: <macaddr> Hot removal. Описание параметров: unitID: Box ID. Macaddr: MAC-адрес.	Информационный
Описание события: изменение топологии стека. Сообщение в журнале: Stacking topology is <Stack_TP_TYPE>. Master (Unit <unitID>, MAC: <macaddr>). Описание параметров: Stack_TP_TYPE: тип топологии стека: 1. кольцо (ring) 2. цепь (chain). unitID: Box ID. Macaddr: MAC-адрес.	Информационный

Описание события: Резервное устройство Master стало устройством Master. Сообщение в журнале: Backup master changed to master. Master (Unit: <unitID>). Описание параметров: unitID: Box ID.	Информационный
Описание события: устройство Slave стало устройством Master. Сообщение в журнале: Slave changed to master. Master (Unit: <unitID>). Описание параметров: unitID: Box ID.	Информационный
Описание события: конфликт Box ID. Сообщение в журнале: Hot insert failed, box ID conflict: Unit <unitID> conflict (MAC: <macaddr> and MAC: <macaddr>). Описание параметров: unitID: Box ID. macaddr: MAC-адрес конфликтующих адресов.	Критический
Описание события: соединение на порту стекирования установлено. Порт стекирования будет работать как интерфейс SIO или член интерфейса SIO (SIO Trunk). Запись журнала доступна только для проектов, в которых у порта стекирования есть ID номера порта на панели устройства. Сообщение в журнале: Stacking port <portID> link up. Описание параметров: port: логический номер порта стекирования.	Критический
Описание события: соединение на порту стекирования прервано. Порт стекирования будет работать как интерфейс SIO или член интерфейса SIO (SIO Trunk). Запись журнала доступна только для проектов, в которых у порта стекирования есть ID номера порта на панели устройства. Сообщение в журнале: Stacking port <portID> link down. Описание параметров: port: логический номер порта стекирования.	Критический
Описание события: соединение на интерфейсе SIO установлено. Установлено первое соединение SIO Trunk на member-порте. Сообщение в журнале: SIO interface Unit <unitID> <SIOn > link up Описание параметров: unitID: Box ID. SIOn: номер интерфейса SIO. Текущий номер поддерживаемого интерфейса SIO – SIO1 и SIO2.	Критический

Описание события: соединение на интерфейсе SIO прервано. Прервано последнее соединение SIO Trunk на member-порте. Сообщение в журнале: SIO interface Unit <unitID> <SIOn > link down Описание параметров: unitID: Box ID. SIOn: номер интерфейса SIO. Текущий номер поддерживаемого интерфейса SIO – SIO1 и SIO2.	Критический

Storm Control

Описание записей журнала	**Уровень**
Описание события: возникновение шторма. Сообщение в журнале: <Broadcast | Multicast | Unicast> storm is occurring on <interface-id> Описание параметров: Broadcast: шторм, возникший из-за широковещательных пакетов (DA = FF:FF:FF:FF:FF:FF). Multicast: шторм, возникший из-за многоадресных пакетов, включая известные и неизвестные пакеты 2 уровня, пакеты с известным и неизвестным IP. Unicast: шторм, возникший из-за одноадресных пакетов, включая известные и неизвестные пакеты. interface-id: ID интерфейса, на котором возник шторм.	Предупреждение
Описание события: шторм устранен. Сообщение в журнале: <Broadcast | Multicast | Unicast> storm is cleared on <interface-id> Описание параметров: Broadcast: устранен шторм широковещательных пакетов (Broadcast Storm). Multicast: устранен шторм многоадресных пакетов (Multicast Storm). Unicast: устранен шторм одноадресных пакетов, включая известные и неизвестные пакеты (Unicast Storm). interface-id: ID интерфейса, на котором шторм устранен.	Информационный
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 Описание параметров: interface-id: ID интерфейса, находящегося в состоянии error-disabled из-за шторма. Broadcast: интерфейс отключен из-за шторма широковещательных пакетов. Multicast: интерфейс отключен из-за шторма многоадресных пакетов. Unicast: интерфейс отключен из-за шторма одноадресных пакетов, включая известные и неизвестные пакеты.	Предупреждение

System

Описание записей журнала	Уровень
Описание события: сообщение генерируется при горячем старте. Сообщение в журнале: [Unit <unitID>,]System warm start. Описание параметров: unitID: ID устройства	Критический
Описание события: сообщение генерируется при холодном старте. Сообщение в журнале: [Unit <unitID>,]System cold start. Описание параметров: unitID: unit ID.	Критический
Описание события: сообщение генерируется при старте системы. Сообщение в журнале: [Unit <unitID>,]System started up. Описание параметров: unitID: unit ID.	Критический

Telnet

Описание записей журнала	Уровень
Описание события: успешный вход через Telnet. Сообщение в журнале: Successful login through Telnet (Username: <username>, IP: <ipaddr>). Описание параметров: ipaddr: IP-адрес Telnet-клиента. username: имя пользователя, используемое для входа на Telnet-сервер.	Информационный
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.	Предупреждение
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.	Информационный

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.	Информационный

Voice VLAN

Описание записей журнала	**Уровень**
Описание события: на интерфейсе обнаружено новое устройство VoIP. Сообщение в журнале: New voice device detected (<interface-id>, MAC: <mac-address>). Описание параметров: interface-id: название интерфейса. mac-address: MAC-адрес устройства VoIP.	Информационный
Описание события: интерфейс, который находится в режиме auto voice VLAN, присоединяется к voice VLAN. Сообщение в журнале: <interface-id> add into voice VLAN <vid>. Описание параметров: interface-id: название интерфейса. vid: VLAN ID.	Информационный
Описание события: сообщение появляется, когда интерфейс покидает voice VLAN, и при этом на интерфейсе не обнаруживаются устройства VoIP за интервал устаревания (aging). Сообщение в журнале: <interface-id> remove from voice VLAN <vid>. Описание параметров: interface-id: название интерфейса. vid: VLAN ID.	Информационный

VRRP Debug

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 interface <intf-name> switch to Init. Описание параметров: vr-id: ID виртуального маршрутизатора VRRP. intf-name: имя интерфейса, на котором настроен виртуальный маршрутизатор.	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>. Описание параметров: vr-id: ID виртуального маршрутизатора VRRP. intf-name: имя интерфейса, на котором настроен виртуальный маршрутизатор. auth-type: тип аутентификации интерфейса VRRP.	Предупреждение
Описание события: получено одно сообщение VRRP advertisement с неверной Checksum. Сообщение в журнале: Received an ADV msg with incorrect checksum 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: получено одно сообщение VRRP advertisement с неверным ID виртуального маршрутизатора. Сообщение в журнале: Received ADV msg virtual router ID mismatch. 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: получено одно сообщения VRRP advertisement, которое не соответствует заданному интервалу. Сообщение в журнале: Received ADV msg adv interval mismatch. 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: в таблицу 2 уровня добавлен виртуальный MAC-адрес. Сообщение в журнале: Added a virtual MAC <vrrp-mac-addr> into L2 table. Описание параметров: vrrp-mac-addr: виртуальный MAC-адрес VRRP.	Уведомление

Описание события: из таблицы 2 уровня удален виртуальный MAC-адрес. Сообщение в журнале: Deleted a virtual MAC <vrrp-mac-addr> from L2 table. Описание параметров: vrrp-mac-addr: виртуальный MAC-адрес VRRP.	Уведомление
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. Описание параметров: vrrp-ip-addr: виртуальный IP-адрес VRRP. vrrp-mac-addr: виртуальный MAC-адрес VRRP.	Уведомление
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. Описание параметров: vrrp-ip-addr: виртуальный IP-адрес VRRP. vrrp-mac-addr: виртуальный MAC-адрес VRRP.	Уведомление
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.	Ошибка
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.	Ошибка
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.	Ошибка

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.	Ошибка
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-intf: номер порта виртуального MAC-адреса VRRP.	Ошибка
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> into L3 table. Box id <mac-box> is invalid. Описание параметров: vrrp-ip-addr: виртуальный IP-адрес VRRP. vrrp-mac-addr: виртуальный MAC-адрес VRRP. mac-box: номер устройства в стеке виртуального MAC-адреса VRRP.	Ошибка
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>. Описание параметров: vrrp-ip-addr: виртуальный IP-адрес VRRP. vrrp-mac-addr: виртуальный MAC-адрес VRRP. vrrp-errcode: errcode протокола VRRP.	Ошибка

Описание события: не удалось удалить виртуальный MAC-адрес из таблицы 3 уровня чипсета. Сообщение в журнале: Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode> Описание параметров: vrrp-ip-addr: виртуальный IP-адрес VRRP. vrrp-mac-addr: виртуальный MAC-адрес VRRP. vrrp-errcode: errcode протокола VRRP.	Ошибка

Web

Описание записей журнала	**Уровень**
Описание события: успешный вход через Web. Сообщение в журнале: Successful login through Web (Username: <username>, IP: <ipaddr>) Описание параметров: username: имя пользователя, используемое для входа на HTTP-сервер. ipaddr: IP-адрес HTTP-клиента.	Информационный
Описание события: не удалось войти через Web. Сообщение в журнале: Login failed through Web (Username: <username>, IP: <ipaddr>) Описание параметров: username: имя пользователя, используемое для входа на HTTP-сервер. ipaddr: IP-адрес HTTP-клиента.	Предупреждение
Описание события: время сессии Web истекло. Сообщение в журнале: Web session timed out (Username: <username>, IP: <ipaddr>) Описание параметров: username: имя пользователя, используемое для входа на HTTP-сервер. ipaddr: IP-адрес HTTP-клиента.	Информационный
Описание события: выполнен выход через Web. 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.	Информационный

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 войти 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

Web-Auth

Описание записей журнала	Уровень
Описание события: узел прошел аутентификацию. Сообщение в журнале: Web-Authentication host login success (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Описание параметров: Username: имя пользователя. IP: IP-адрес узла. mac-address: MAC-адрес узла. interface-id: интерфейс, на котором аутентифицировался узел. vlan-id: VLAN ID, к которому относится узел.	Информационный
Описание события: узлу не удалось пройти аутентификацию. Сообщение в журнале: Web-Authentication host login fail (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Описание параметров: Username: имя пользователя. IP: IP-адрес узла. mac-address: MAC-адрес узла. interface-id: интерфейс, на котором аутентифицировался узел. vlan-id: VLAN ID, к которому относится узел.	Критический
Описание события: число авторизованных пользователей на устройстве достигло максимального значения. Сообщение в журнале: Web-Authentication enters stop learning state.	Предупреждение
Описание события: число авторизованных пользователей стало ниже максимального значения. Сообщение в журнале: Web-Authentication recovers from stop learning state.	Предупреждение

ZTP Table

Описание записей журнала	Уровень
Описание события: сообщение означает, что ZTP Firmware успешно обновлен. Сообщение в журнале: The downloaded firmware was successfully executed by ZTP update (TFTP Server IP: <ipaddr>) Описание параметров: ipaddr: IP-адрес сервера TFTP.	Информационный

Описание события: сообщение означает, что не удалось обновить ZTP Firmware. Сообщение в журнале: The downloaded firmware was not successfully executed by ZTP update (TFTP Server IP: <ipaddr>) Описание параметров: ipaddr: IP-адрес сервера TFTP.	Информационный

Приложение C. 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	Узел 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	Узел 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

Authentication Fail

Сообщение trap	Описание	OID
authenticationFailure	SNMPv2-устройство в роли агента получило сообщение протокола, которое не аутентифицировано должным образом. Данное trap-сообщение генерируется всеми реализациями SNMPv2 и будет отправлено, только если параметр snmpEnableAuthenTraps включен.	1.3.6.1.6.3.1.1 .5.5

BPDU Protection

Сообщение trap	Описание	OID
dBpduProtectionAttackOccur	Атака BPDU на интерфейсе. Вариабельные привязки: (1) ifIndex (2) dBpduProtectionIfCfgMode	1.3.6.1.4.1.17 1.14.47.0.1
dBpduProtectionAttackRecover	Атака BPDU на интерфейсе устранена. Вариабельные привязки: (1) ifIndex	1.3.6.1.4.1.17 1.14.47.0.2

DDM

Сообщение trap	Описание	OID
dDdmAlarmTrap	Возникновение проблем уровня alarm или	1.3.6.1.4.1.17

	возвращение к нормальному состоянию после устранения данных проблем. Trap-сообщение об устранении проблем будет отправлено, если текущее значение выше заданного нижнего порога alarm или ниже заданного верхнего порога alarm. Вариабельные привязки: (1) dDdmNotifyInfoIfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.14.72.0.1
dDdmWarningTrap	Возникновение проблем уровня warning или возвращение к нормальному состоянию после устранения данных проблем. Вариабельные привязки: (1) dDdmNotifyInfoIfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.17 1.14.72.0.2

DHCP Server Screen Prevention

Сообщение trap	**Описание**	**OID**
dDhcpFilterAttackDetected	Если функция DHCP Server Screen включена, trap-сообщения будут отправлены при получении каждого пакета ложного DHCP-сервера. Вариабельные привязки: (1) dDhcpFilterLogBufServerIpAddr (2) dDhcpFilterLogBufClientMacAddr (3) dDhcpFilterLogBufferVlanId (4) dDhcpFilterLogBufferOccurTime	1.3.6.1.4.1.17 1.14.133.0.1

DoS Prevention

Сообщение trap	**Описание**	**OID**
dDosPreveAttackDetectedPacket	Обнаружена DoS-атака. Вариабельные привязки: (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.17 1.14.59.0.2

ErrDisable

Сообщение trap	**Описание**	**OID**
dErrDisNotifyPortDisabledAssert	Порт перешел в состояние Error-Disabled. Вариабельные привязки: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.17 1.14.45.0.1

dErrDisNotifyPortDisabledClear	Порт возвращается в исходное состояние по истечении определенного интервала времени. Вариабельные привязки: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.17 1.14.45.0.2

General Management

Сообщение trap	Описание	OID
dGenMgmtLoginFail	Ошибка авторизации на коммутаторе. Вариабельные привязки: (1) dGenMgmtNotifyInfoLoginType (2) dGenMgmtNotifyInfoUserName	1.3.6.1.4.1.17 1.14.165.0.1

Gratuitous ARP

Сообщение trap	Описание	OID
agentGratuitousARPTrap	Обнаружен конфликт IP-адреса. Вариабельные привязки: (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName	1.3.6.1.4.1.17 1.14.45.0.1

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 истечении 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 истечении определенного интервала времени. Вариабельные привязки: (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	1.3.6.1.4.1.17 1.14.46.0.4

LLDP-MED

Сообщение trap	**Описание**	**OID**
lldpRemTablesChange	Значение lldpStatsRemTableLastChangeTime изменилось. Вариабельные привязки: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2 .0.0.1

lldpXMedTopologyChangeDetected	Обнаружено изменение в топологии: к порту было подключено новое устройство, удаленное устройство было отключено или было отключено с дальнейшим подключением к другому порту. Вариабельные привязки: (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8808.1.1.2 .1.5.4795.0.1

MAC-based Access Control

Сообщение trap	Описание	OID
dMacAuthLoggedSuccess	Узел успешно прошел аутентификацию на основе MAC. Вариабельные привязки: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.1
dMacAuthLoggedFai	Узел не прошел аутентификацию на основе MAC. Вариабельные привязки: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.2
dMacAuthLoggedAgesOut	Время аутентификации узла истекло. (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.3

MAC Notification

Сообщение trap	Описание	OID
dL2FdbMacNotification	Изменение MAC-адресов в таблице коммутации. Вариабельные привязки: (1) dL2FdbMac ChangeNotifyInfo	1.3.6.1.4.1.17 1.14.3.0.1
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-собщение будет отправлено мостом сразу же после его назначения в качестве нового корня. По истечении таймера (Topology Change Timer) мост немедленно будет назначен корнем. Отправка данного trap-собщения является опциональной.	1.3.6.1.2.1.17.0.1
topologyChange	Мост отправляет trap-собщение, когда какой-то из его настроенных портов переходит из состояния learning в состояние forwarding или из состояния forwarding в состояние blocking. Данное trap-собщение 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». Вариабельные привязки: (1) dEntityExtEnvTempUnitId (2) dEntityExtEnvTempIndex (3) dEntityExtEnvTempStatus	1.3.6.1.4.1.17 1.14.5.0.2
dEntityExtPowerStatusChg	Выход из строя, удаление или восстановление модуля питания. Данное trap-сообщение отправляется Commander Switch. Вариабельные привязки: (1) dEntityExtEnvPowerUnitId (2) dEntityExtEnvPowerIndex (3) dEntityExtEnvPowerStatus	1.3.6.1.4.1.17 1.14.5.0.3

dEntityExtFactoryResetButton	Уведомление «Нажмите кнопку возврата к заводским настройкам». Вариабельные привязки: (1) dEntityExtUnitIndex	1.3.6.1.4.1.17 1.14.5.0.5

PIM6-SM

Сообщение trap	**Описание**	**OID**
pimNeighborLoss	Соединение с соседним устройством прервано. Данное уведомление генерируется по истечении таймера соседнего устройства, если у маршрутизатора нет других соседних устройств на одном и том же интерфейсе с одинаковой версией IP и IP-адресом меньше, чем собственный. Данное уведомление генерируется при каждом увеличении счетчика pimNeighborLossCount с учетом ограничения скорости, указанного pimNieghborLossNotificationsPeriod. Вариабельные привязки: (1) pimNeighborUpTime	1.3.6.1.2.1.15 7.0.1
pimInvalidRegister	На устройстве было получено недействительное сообщение PIM register. Данное уведомление генерируется при каждом увеличении счетчика pimInvalidRegisterMsgsRcvd с учетом ограничения, указанного pimInvalidRegisterNotificationPeriod. Вариабельные привязки: (1) pimGroupMappingPimMode (2) pimInvalidRegisterAddressType (3) pimInvalidRegisterOrigin (4) pimInvalidRegisterGroup (5) pimInvalidRegisterRp	1.3.6.1.2.1.15 7.0.2
pimInvalidJoinPrune	На устройстве было получено недействительное сообщение PIM join/prune. Данное уведомление генерируется при каждом увеличении счетчика pimInvalidJoinPruneMsgsRcvd с учетом ограничения, указанного pimInvalidJoinPruneNotificationPeriod. Вариабельные привязки: (1) pimGroupMappingPimMode (2) pimInvalidJoinPruneAddressType (3) pimInvalidJoinPruneOrigin (4) pimInvalidJoinPruneGroup (5) pimInvalidJoinPruneRp (6) pimNeighborUpTime	1.3.6.1.2.1.15 7.0.3

pimRPMappingChage	На устройстве произошло изменение в активном RP Mapping. Данное уведомление генерируется при каждом увеличении счетчика pimRPMappingChangeCount с учетом ограничения, указанного pimRPMappingChangeNotificationPeriod. Вариабельные привязки: (1) pimGroupMappingPimMode (2) pimGroupMappingPrecedence	1.3.6.1.2.1.157.0.4
pimInterfaceElection	В сети был назначен новый DR или DF. Данное уведомление генерируется при каждом увеличении счетчика pimInterfaceElectionWinCount с учетом ограничения, указанного pimInterfaceElectionNotificationPeriod. Вариабельные привязки: (1) pimInterfaceAddressType (2) pimInterfaceAddress	1.3.6.1.2.1.157.0.5

PoE

Сообщение trap	**Описание**	**OID**
pethMainPowerUsageOnNotification	Индикация порога потребления PSE включена. Мощность потребления выше настроенного порога. Между отправкой уведомлений одним и тем же экземпляром параметра должно пройти не менее 500 миллисекунд. Вариабельные привязки: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.2
pethMainPowerUsageOffNotification	Индикация порога потребления PSE отключена. Мощность потребления ниже настроенного порога. Между отправкой уведомлений одним и тем же экземпляром параметра должно пройти не менее 500 миллисекунд. Вариабельные привязки: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.3
dPoeIfPowerDeniedNotification	Состояние диаграммы статуса PSE – POWER_DENIED. Между отправкой уведомлений одним и тем же экземпляром параметра должно пройти не менее 500 миллисекунд. Вариабельные привязки: (1) pethPsePortPowerDeniedCounter	1.3.6.1.4.1.171.14.24.0.1

dPoeIfPowerOverLoadNotification	Состояние диаграммы статуса PSE – ERROR_DELAY_OVER. Между отправкой уведомлений одним и тем же экземпляром параметра должно пройти не менее 500 миллисекунд. Вариабельные привязки: (1) pethPsePortOverLoadCounter	1.3.6.1.4.1.17 1.14.24.0.2
dPoeIfPowerShortCircuitNotification	Состояние диаграммы статуса PSE – ERROR_DELAY_SHORT. Между отправкой уведомлений одним и тем же экземпляром параметра должно пройти не менее 500 миллисекунд. Вариабельные привязки: (1) pethPsePortShortCounter	1.3.6.1.4.1.17 1.14.24.0.3
dPoeIfPdAliveFailOccurNotification	PD-устройство прекратило работу или не отвечает. Между отправкой уведомлений одним и тем же экземпляром параметра должно пройти не менее 500 миллисекунд. Вариабельные привязки: (1) pethMainPseGroupIndex (2) pethPsePortIndex (3) dPoeIfPdAliveCfgPdIpType (4) dPoeIfPdAliveCfgPdIpAddr	1.3.6.1.4.1.17 1.14.24.0.4

Port

Сообщение trap	**Описание**	**OID**
linkUp	Соединение на порту установлено. Вариабельные привязки: (1) ifIndex, (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1 .5.4
linkDown	Соединение на порту прервано. Вариабельные привязки: (1) ifIndex, (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1 .5.3

Port Security

Сообщение trap	Описание	OID
dPortSecMacAddrViolation	Если отправка trap-сообщений Port Security включена, trap-сообщения будут отправлены при обнаружении недопустимых MAC-адресов. Вариабельные привязки: (1) ifIndex, (2) dPortSecIfCurrentStatus (3) dPortSecIfViolationMacAddress	1.3.6.1.4.1.17 1.14.8.0.1

RMON

Сообщение trap	Описание	OID
risingAlarm	Запись уровня alarm превысила заданный верхний порог. Вариабельные привязки: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16. 0.1
fallingAlarm	Запись уровня alarm снизилась до заданного нижнего порога. Вариабельные привязки: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (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 отправлено Commander Switch, если участником его группы было сгенерировано уведомление о «горячем» старте. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.12
swSingleIPMSLinkDown	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление о прерванном соединении. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.17 1.12.8.6.0.13
swSingleIPMSLinkUp	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление об установленном соединении. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.17 1.12.8.6.0.14
swSingleIPMSAuthFail	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление об ошибки аутентификации. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.15
swSingleIPMSnewRoot	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление о новом корне. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.16

swSingleIPMSTopologyChange	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление об изменении топологии. Вариабельные привязки: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.17

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 неизмененной конфигурацией.	1.3.6.1.6.3.1.1 .5.2

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

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-собщения является опциональной. Вариабельные привязки: (1) vrrpTrapPacketSrc (2) vrrpTrapAuthErrorType	1.3.6.1.2.1.68.0.2

Web-Authentication

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

ZTP

Сообщение trap	**Описание**	**OID**
swResetButtonPressedTrap	Функция, выполняемая нажатием Reset_Button: Вариабельные привязки: (1) swResetButtonMode	1.3.6.1.4.1.17 1.12.120.2.0.1

Приложение D. Назначение атрибутов RADIUS

На коммутаторе 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 атрибут уровня привилегии не сконфигурирован и аутентификация проходит успешно, устройство не назначит пользователю уровень привилегии. Если атрибут уровня привилегии установлен на значение ниже минимального поддерживаемого значения или выше максимального, 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 атрибут полосы пропускания не сконфигурирован 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

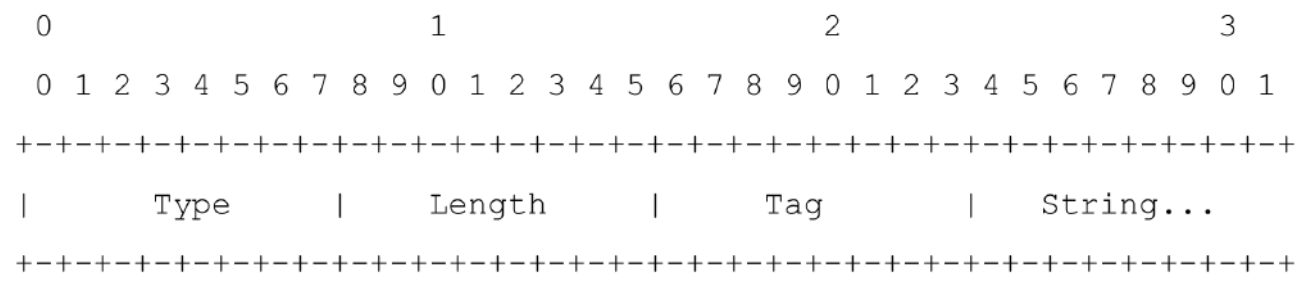
Если пользователь сконфигурировал атрибут приоритета 802.1p на RADIUS-сервере (например, приоритет 7) и аутентификация 802.1X или на основе MAC прошла успешно, устройство назначит порту приоритет по умолчанию в соответствии со значением на RADIUS-сервере. Если атрибут приоритета не сконфигурирован и 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 среду передачи	6 (802)	Обязательно
Tunnel-Private-Group-ID	Атрибут указывает групповой ID для определенной туннельной сессии	Строка (VID)	Обязательно

Ниже показана краткая информация о формате атрибута Tunnel-Private-Group-ID:



В таблице ниже приведено описание поля Tag, которое отличается от RFC 2868:

Значение поля Tag	**Формат строки поля**
0x01	Название VLAN (ASCII)
0x02	VLAN ID (ASCII)
Другие (0x00, 0x03 ~ 0x1F, >0x1F)	При получении строки настройки VLAN коммутатор сначала будет проверять все существующие VLAN ID и выберет подходящий, который станет идентификатором данной VLAN. Если подходящий VLAN ID отсутствует, коммутатор будет проверять доступные имена VLAN.

Примечание: поле тега больше 0x1F распознается как первый октет следующего поля.

Если пользователь сконфигурировал атрибут VLAN на RADIUS-сервере (например, VID 3) и аутентификация 802.1X, WAC или на основе MAC прошла успешно, порт будет назначен в VLAN 3. Однако если пользователь не сконфигурировал атрибуты VLAN, порт, который не является членом Guest VLAN, останется в текущей VLAN аутентификации, а порт, являющийся членом Guest VLAN, будет назначен в исходную VLAN.

Для того чтобы RADIUS-сервер назначил **ACL**, необходимо сконфигурировать соответствующие параметры на сервере. В таблице ниже приведены параметры для ACL.

VSA14 ACL Script

Параметры для производителя (Vendor-Specific Attributes):

RADIUS Tunnel Attribute	**Описание**	**Значение**	**Использование**
Vendor-ID	Определяет производителя	171 (DLINK)	Обязательно
Vendor-Type	Определяет атрибут	14 (для ACL Script)	Обязательно

Attribute-Specific Field	Используется для назначения ACL script. Формат основывается на командах списка управления доступом (ACL)	ACL Script Например: **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;**	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)»**.

NAS-Filter-Rule (92)

В таблице ниже приведены параметры для NAS-Filter-Rule:

RADIUS Tunnel Attribute	**Описание**	**Значение**	**Использование**
NAS-Filter-Rule	Атрибут указывает правила фильтрации, которые должны быть применены к пользователю.	Строка (содержащая отдельные правила фильтрации, разделенные нулевым (0x00) октетом).	Обязательно

Формат правила фильтрации

Используйте команду **permit** для добавления разрешающей записи и команду **deny** для добавления запрещающей записи.

{permit | deny} in tcp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***} [***TCP-PORT-RANGE***]**

{permit | deny} in udp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***} [***UDP-PORT-RANGE***]**

{permit | deny} in icmp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***} [***ICMP-TYPE***]**

{permit | deny} in ip from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***}**

{permit | deny} in *IP-PROT-VALUE* **from any to {any |** *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***}**

tcp, **udp**, **icmp**, **ip**, *IP-PROT-VALUE*	С правилом можно использовать протокол TCP, UDP, ICMP, IP или значение протокола, заданное пользователем. Доступный диапазон значений для *IP-PROT-VALUE:* от 0 до 255.
any	Обозначает любой адрес назначения (destination address).

DST-IP-ADDR	Указывает определенный IP-адрес узла назначения.
DST-IP-NET-ADDR	Указывает IP-адрес сети назначения с маской в формате 1.2.3.4/24.
DST-IPV6-ADDR	Указывает определенный IPv6-адрес узла назначения.
DST-IPV6-NET-ADDR	Указывает IPv6-адрес сети назначения в формате 2000::1/64.
TCP-PORT-RANGE	(Опционально.) Указывает порт или диапазон портов TCP в формате 22-23, 80.
UDP-PORT-RANGE	(Опционально.) Указывает порт или диапазон портов UDP в формате 56, 67-68.
ICMP-TYPE	(Опционально.) Указывает тип сообщения ICMP. Диапазон значений: от 0 до 255.

Пример

В примере показано, как на RADIUS-сервере запретить протокол telnet.

```
Nas-filter-Rule="deny in tcp from any to any 23"
Nas-filter-Rule+="permit in ip from any to any"
```

В следующем примере показано, как на RADIUS-сервере ограничить узлу доступ к группе IP-адресов.

```
Nas-filter-Rule="permit in ip from any to 10.10.10.1/24"
Nas-filter-Rule+="permit in ip from any to fe80::d1:1/64"
```

Параметры для производителя (Vendor-Specific Attributes):

RADIUS Tunnel Attribute	**Описание**	**Значение**	**Использование**
Vendor-ID	Определяет производителя	171 (DLINK)	Обязательно
Vendor-Type	Определяет атрибут	14 (для ACL Script)	Обязательно
Attribute-Specific Field	Правило фильтрации IPv6.	Атрибут указывает один из следующих режимов IP для NAS-Filter-Rule: 1= Передача трафика IPv4 и IPv6 2= Передача только трафика IPv4 (трафик IPv6 отбрасывается) Если данный атрибут не назначен RADIUS-сервером, передается только трафик IPv4, а все пакеты IPv6 будут отбрасываться.	Обязательно



Примечание: если одновременно назначены как проприетарный ACL script (VSA14), так и стандартное NAS-Filter-Rule (92), будет выполняться NAS-Filter-Rule (92), а VSA14 игнорируется.

Приложение E. Поддержка атрибутов IETF RADIUS

Для атрибутов RADIUS существуют определенные параметры 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 призводителям создавать собственные дополнительные атрибуты RADIUS. Для подробной информации о VSA D-Link обратитесь к **Приложению «Назначение атрибутов RADIUS»**.

Атрибуты RADIUS стандарта IETF определены в RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support и RFC 2869 RADIUS Extensions.

Список атрибутов IETF RADIUS, поддерживаемых коммутатором D-Link, приведен в таблице ниже.

Атрибуты аутентификации RADIUS:

Номер	Атрибут IETF
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type

64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval
87	NAS-Port-ID
95	NAS-IPv6-Address

Атрибуты RADIUS Accounting:

Номер	**Атрибут IETF**
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
8	Framed-IP-Address
31	Calling-Station-ID
32	NAS-Identifier
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause

52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
61	NAS-Port-Type
95	NAS-IPv6-Address

Приложение F. Информация ERPS

Только аппаратный ERPS поддерживает функцию Fast Link Drop Interrupt с временем восстановления 50 мс в кольце до 16 узлов. Расстояние должно быть меньше 1200 км.

Модель	ERPS	Порты 1-8	Порты 9-26	• Порты 27-28
DGS-1520-28	Аппаратный	V		V
	Программный		V	

Модель	ERPS	Порты 1-4	Порты 5-26	• Порты 27-28
DGS-1520-28MP	Аппаратный	V		V
	Программный		V	

Модель	ERPS	Порты 1-8	Порты 9-24	• Порты 25-32	• Порты 33-50	• Порты 51-52
DGS-1520-52	Аппаратный	V		V		V
	Программный		V		V	

Модель	ERPS	Порты 1-8	Порты 9-24	• Порты 25-28	• Порты 29-50	• Порты 51-52
DGS-1520-52MP	Аппаратный	V		V		V
	Программный		V		V	

Приложение G. Информация по стекированию

На коммутаторе поддерживаются следующие топологии стекирования:

• **Линейная** – данная топология объединяет коммутаторы в стек в виде цепи. При использовании этого метода передача данных возможна только в одном направлении. При разрыве в цепи передача данных будет нарушена.

• **Кольцевая** – данная топология объединяет коммутаторы в стек в виде кольца, в котором данные могут передаваться в двух направлениях. Эта топология обладает отказоустойчивостью, поскольку при разрыве соединения данные могут предаваться между коммутаторами в стеке по альтернативному пути.

На следующей схеме 4 коммутатора объединены в стек по линейной топологии. Для соединения используются 2 порта 10GBASE-T.

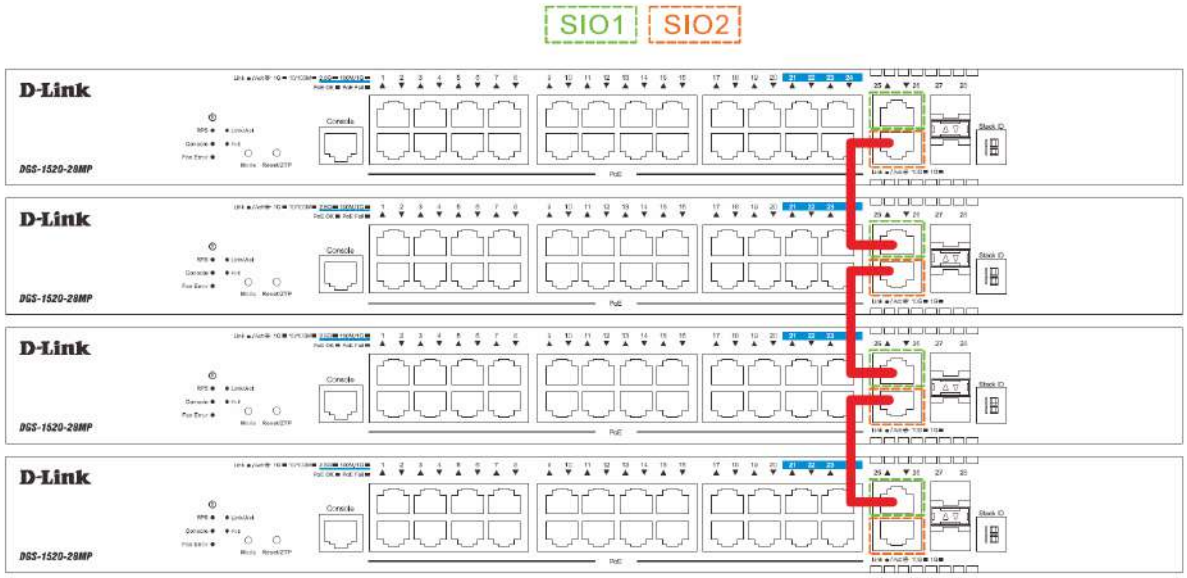


Рис. 1 – Линейная топология (четное количество коммутаторов, с использованием 2 портов).

На схеме ниже 4 коммутатора объединены в стек по кольцевой топологии. Для соединения используются 2 порта 10GBASE-T.

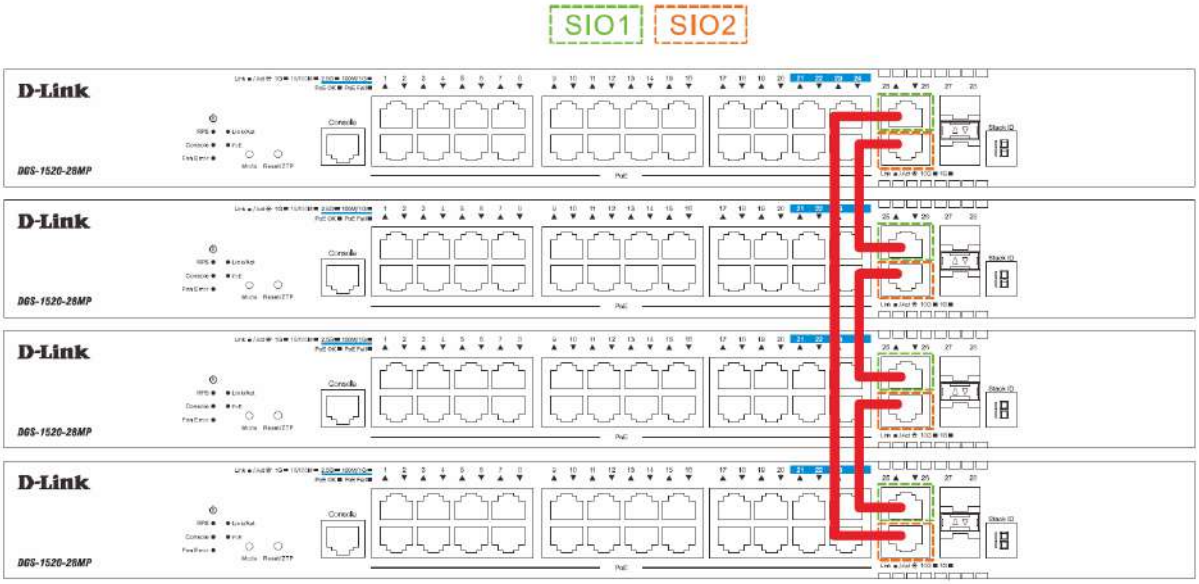


Рис. 2 – Кольцевая топология (четное количество коммутаторов, с использованием 2 портов).

На следующей схеме 4 коммутатора объединены в стек по линейной топологии. Для соединения используются 4 порта.

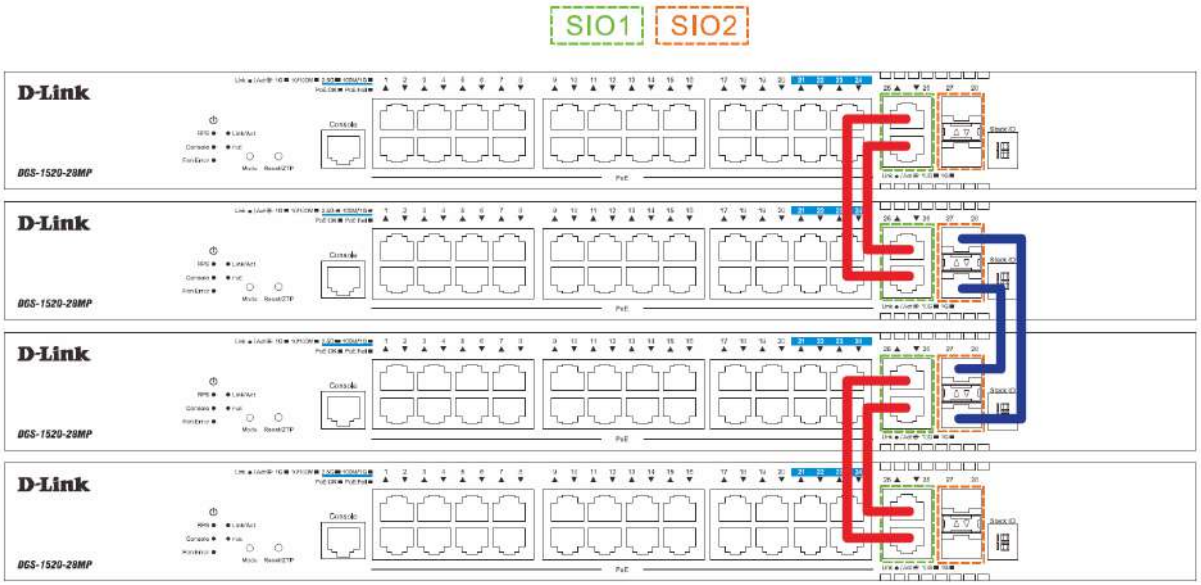


Рис. 3 – Линейная топология (четное количество коммутаторов, с использованием 4 портов).

На схеме ниже 4 коммутатора объединены в стек по кольцевой топологии. Для соединения используются 4 порта.

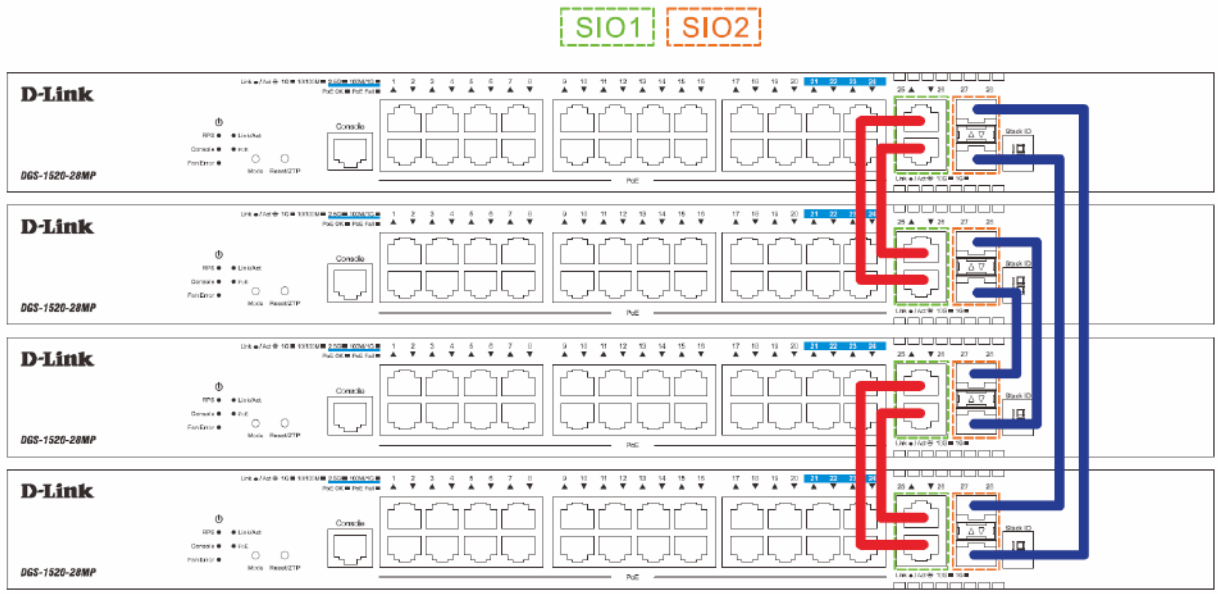


Рис. 4 – Кольцевая топология (четное количество коммутаторов, с использованием 4 портов).

На следующей схеме нечетное количество коммутаторов (в примере – 3) объединены в стек по линейной топологии. Для соединения используются 4 порта.

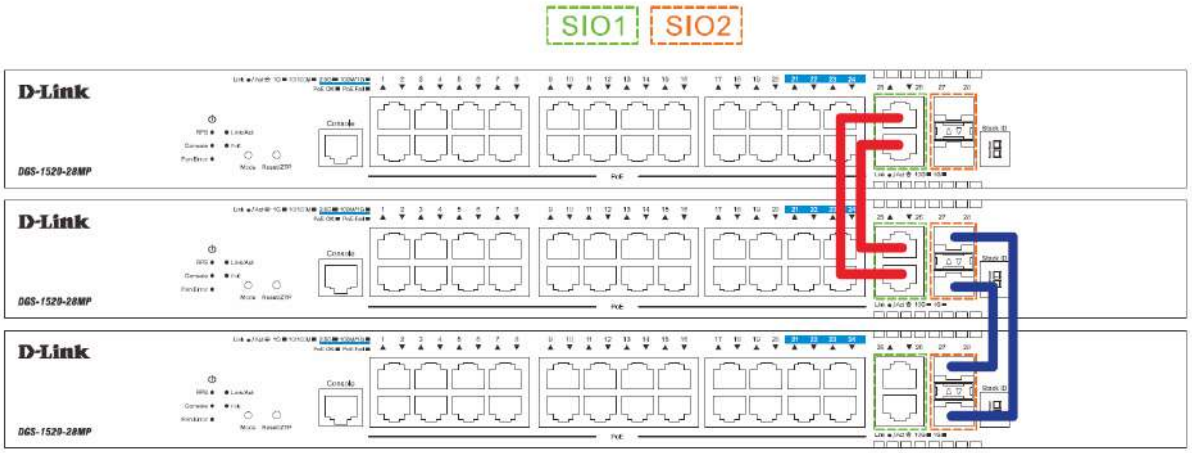


Рис. 5 – Линейная топология (нечетное количество коммутаторов, с использованием 4 портов).

На схеме ниже нечетное количество коммутаторов (в примере – 3) объединены в стек по кольцевой топологии. Для соединения используются 4 порта. Топология не поддерживается на коммутаторах этой серии.

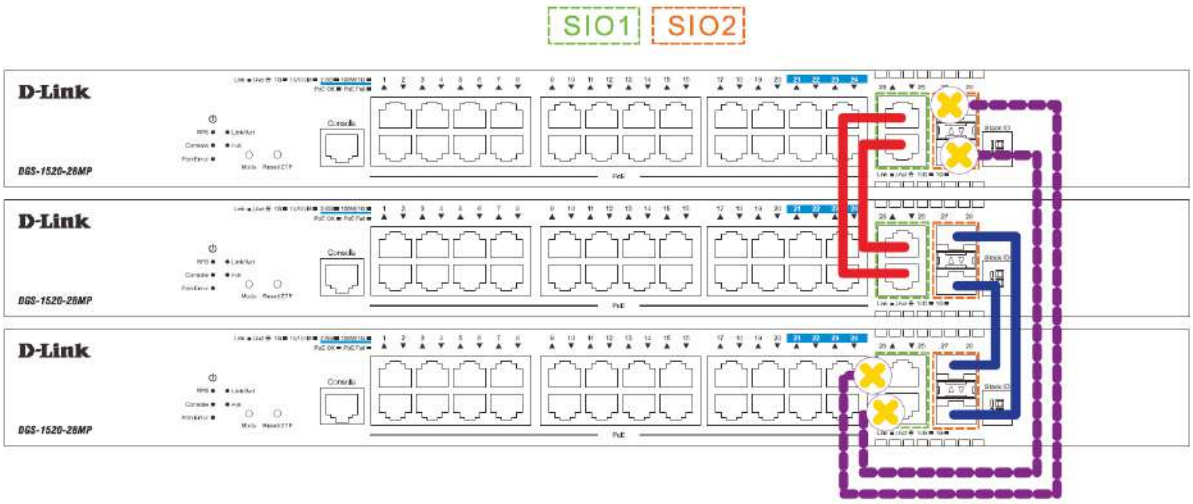


Рис. 6 – Кольцевая топология (нечетное количество коммутаторов, с использованием 4 портов).