



Руководство пользователя (CLI)

Серия DMS-3130

Управляемые стекируемые коммутаторы 3 уровня

Версия 1.01

Содержание

1. Введение.....	6
2. Базовые команды интерфейса командной строки.....	16
3. Команды 802.1X	35
4. Команды ACL (Список управления доступом).....	51
5. Команды управления доступом	87
6. Команды предотвращения атак ARP Spoofing	114
7. Команды Asymmetric VLAN	117
8. Команды Authentication, Authorization и Accounting (AAA).....	118
9. Базовые команды настройки IPv4.....	149
10. Базовые команды настройки IPv6.....	160
11. Команды BPDU Protection	179
12. Команды Cable Diagnostics.....	183
13. Команды логирования выполненных команд	187
14. Команды Connectivity Fault Management (CFM)	188
15. Команды CPU Access Control List (ACL)	235
16. Команды Debug	240
17. Команды DHCP Auto-Configuration	251
18. Команды DHCP Client	253
19. Команды DHCP Relay	257
20. Команды DHCP Server	284
21. Команды DHCP Server Screening	316
22. Команды DHCP Snooping	322
23. Команды DHCPv6 Client.....	338
24. Команды DHCPv6 Guard.....	340
25. Команды DHCPv6 Relay.....	345
26. Команды DHCPv6 Server	365
27. Команды Digital Diagnostics Monitoring (DDM)	379
28. Команды клиента D-Link Discovery Protocol (DDP)	391
29. Команды Domain Name System (DNS).....	394
30. Команды предотвращения атак DoS	402
31. Команды Dynamic ARP Inspection	406
32. Команды Error Recovery.....	423
33. Команды Ethernet OAM	426
34. Команды Ethernet Ring Protection Switching (ERPS)	448

35. Команды File System	472
36. Команды Filter Database (FDB)	480
37. Команды GARP VLAN Registration Protocol (GVRP).....	496
38. Команды Gratuitous ARP	506
39. Команды управления интерфейсом	510
40. Команды Internet Group Management Protocol (IGMP)	536
41. Команды Internet Group Management Protocol (IGMP) Snooping	551
42. IP Multicast (IPMC)	578
43. Команды IP Source Guard	583
44. Команды IP Utility.....	589
45. Команды IP-MAC-Port Binding (IMPB)	599
46. Команды IPv6 Snooping	603
47. Команды IPv6 Source Guard	611
48. Команды Jumbo Frame.....	619
49. Команды Layer 2 Protocol Tunnel (L2PT)	620
50. Команды Link Aggregation Control Protocol (LACP).....	630
51. Команды Link Layer Discovery Protocol (LLDP)	638
52. Команды Loopback Detection (LBD).....	672
53. Команды аутентификации MAC	680
54. Команды Mirror	684
55. Команды Multicast Listener Discovery (MLD) Snooping	694
56. Команды Multicast VLAN	715
57. Команды Neighbor Discovery (ND) Inspection.....	727
58. Команды Network Access Authentication.....	732
59. Команды Network Protocol Port Protection.....	748
60. Команды Open Shortest Path First Version 2 (OSPFv2).....	750
61. Команды Open Shortest Path First Version 3 (OSPFv3).....	801
62. Команды Power over Ethernet (PoE)	843
63. Команды Policy-Based Routing (PBR).....	855
64. Команды Port Security	859
65. Команды энергосбережения.....	867
66. Команды PPPoE Circuit-ID Tag Insertion.....	874
67. Команды Private VLAN	878
68. Команды Protocol Independent.....	885
69. Команды Protocol Independent Multicast (PIM).....	898

70. Команды качества обслуживания (QOS).....	912
71. Команды перезагрузки (Reboot)	953
72. Команды Remote Network MONitoring (RMON).....	956
73. Команды Route Map	965
74. Команды Router Advertisement (RA) Guard	982
75. Команды Routing Information Protocol (RIP)	986
76. Команды Routing Information Protocol Next Generation (RIPng)	1000
77. Команды Safeguard Engine	1014
78. Команды управления картой Secure Digital (SD)	1023
79. Команды сервера Secure File Transfer Protocol (SFTP)	1032
80. Команды Secure Shell (SSH).....	1035
81. Команды Secure Sockets Layer (SSL).....	1044
82. Команды sFlow	1053
83. Команды Simple Mail Transfer Protocol (SMTP).....	1060
84. Команды Simple Network Management Protocol (SNMP)	1066
85. Команды Single IP Management (SIM).....	1090
86. Команды Spanning Tree Protocol (STP).....	1102
87. Команды стекирования	1129
88. Команды Storm Control.....	1135
89. Команды Super VLAN.....	1141
90. Команды Surveillance VLAN.....	1145
91. Команды портов коммутатора	1152
92. Команды управления системными файлами	1158
93. Команды System Log	1172
94. Команды времени и SNTP.....	1185
95. Команды временного диапазона.....	1192
96. Команды Traffic Segmentation	1195
97. Команды Virtual LAN (VLAN)	1198
98. Команды Virtual LAN (VLAN) Tunnel	1214
99. Команды Virtual Router Redundancy Protocol (VRRP)	1230
100. Команды Virtual Router Redundancy Protocol Version 3 (VRRPv3).....	1239
101. Команды Voice VLAN.....	1247
102. Команды Web-аутентификации.....	1256
103. Команды Weighted Random Early Detection (WRED).....	1262
104. Команды CPU Port Statistics	1268

105. Команды Virtual LAN (VLAN) Counter	1271
Приложение А. Восстановление пароля (Password Recovery)	1275
Приложение Б. Записи системного журнала	1277
Приложение В. Записи trap-сообщений	1310
Приложение Г. Назначение атрибутов RADIUS	1326
Приложение Д. Поддержка атрибутов IETF RADIUS	1330

1. Введение

Описание команд в данном руководстве основаны на программном обеспечении версии **1.01.006**. Представленный здесь список команд является подгруппой команд, поддерживаемых коммутаторами серии DMS-3130.

Целевая аудитория

Руководство пользователя предназначено для сетевых администраторов и других IT-специалистов, использующих для управления коммутатором интерфейс командной строки (CLI). Это основной интерфейс управления коммутаторами серии DMS-3130. Настоящее руководство рассчитано на пользователей, знакомых с основными принципами работы Ethernet и организации сетей LAN.

Условные обозначения

Условное обозначение	Описание
Полужирный шрифт	Команды, опции команд и ключевые слова. Ключевые слова в командной строке необходимо вводить именно так, как они представлены в данном документе.
<i>КУРСИВ ЗАГЛАВНЫМИ</i>	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.

Предупреждения и примечания

При использовании данного руководства для управления коммутатором обращайтесь 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.

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 пять уровней привилегий учетной записи пользователя:

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

В интерфейсе командной строки (CLI) доступно три 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**.

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

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

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

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

Доступные командные режимы и уровни привилегий:

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

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

User EXEC Mode с базовым уровнем доступа Basic User

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

Privileged EXEC Mode с расширенным уровнем доступа Advanced User

Режим предназначен для просмотра базовых настроек системы, изменения настроек сеансов локального терминала и базовой проверки сетевых подключений. Пользователь не может получить доступ к информации, относящейся к безопасности. В данный режим можно войти при уровне доступа Advanced User.

Privileged EXEC Mode с уровнем доступа Power User

В этом режиме доступно меньше команд, чем пользователю Operator. Поддерживаются команды 'config', за исключением команд уровня Operator и Administrator. Вход в данный режим можно получить при наличии 8-ого уровня привилегий.

Privileged EXEC Mode с уровнем доступа Operator

Данный режим позволяет получить доступ к глобальным настройкам и настройкам локального терминала, контролировать и решать задачи администрирования, за исключением настроек безопасности. Вход в данный режим можно получить 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 Advanced User, Power User, Operator или Administrator. Настройки безопасности доступны только пользователям с учетной записью уровня Administrator. Помимо применения глобальных настроек для всей системы, данный режим также используется для перехода в специальные режимы конфигурирования. Для доступа к режиму глобальной конфигурации пользователь должен войти в систему с соответствующим уровнем учетной записи и ввести команду **configure terminal** в привилегированном режиме Privileged EXEC.

В следующем примере выполняется вход в систему с учетной записью уровня Administrator в режиме

Privileged EXEC 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 к режиму Privileged EXEC Mode.

```
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.

VLAN Interface Configuration Mode (Режим конфигурирования VLAN-интерфейса)

Режим конфигурирования VLAN-интерфейса используется для настройки параметров VLAN-интерфейсов.

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

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

Создание пользовательской учетной записи

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

Рассмотрим следующий пример.

```
Switch# enable
Switch# configure terminal
Switch(config)# username
username admin password password_specified
Switch(config)# username admin 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 admin password *password_specified*** создается учетная запись пользователя с именем *admin* и указанным паролем.
- Команда **username admin privilege 15** назначает 15-й уровень привилегий для учетной записи *admin*.
- 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.



Примечание: имена пользователей и пароли чувствительны к регистру. Длина имени пользователя не должна превышать 32 символов. Пароль должен содержать 8-30 символов и включать, по крайней мере, одну заглавную и строчную букву, одну цифру и один символ, например, *@!&**. Пароль не должен совпадать с именем пользователя и не должен содержать соседние одинаковые символы или цифры или IP-адрес коммутатора по умолчанию.

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

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

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

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

Switch#
```

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

```
DMS-3130-30PS Gigabit Ethernet Switch

Command Line Interface
Firmware: 1.01.003
Copyright(C) 2018 D-Link Corporation. All rights reserved.

User Verification Access

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 изменить скорость на 1 Гбит/с, используя команду **speed 1000**.

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

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

- Unit ID / Slot ID / ID порта

Unit ID интерфейса указывает на номер коммутатора в стеке. Если стекирование отключено или настраиваемый коммутатор не включен в стек, то данный параметр не имеет значения. Slot ID интерфейса – это идентификатор модуля, подключенного к слоту расширения. Коммутаторы серии DMS-3130 не поддерживают 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 старый текст автоматически будет 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.

Для включения фильтрации данных нужно ввести вертикальную черту (|) после команды **show**, а затем – параметр фильтрации:

- **show** XXX | **begin** *STRING*, или
- **show** XXX | **include** *STRING*, или
- **show** XXX | **exclude** *STRING*

Фильтр интерпретирует фильтрующую строку с использованием языка шаблонов командной оболочки Linux.

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

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

# AAA

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

Switch#
```

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

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

Switch#
```

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

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

Current configuration : 30689 bytes

#-----
#                               DMS-3130-30TS Gigabit Ethernet Switch
#                               Configuration
#
#                               Firmware: Build 1.01.006
#                               Copyright(C) 2018 D-Link Corporation. All rights reserved.
#-----

# STACK

end

# AAA

configure terminal
# AAA START
no aaa new-model
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

В языке шаблонов командной оболочки Linux символу «*» соответствует любая строка, а строке «*» соответствует символ «*».

В следующем примере показано отображение строк с параметром **include** «S*» и «S*». Символ «*» соответствует любой строке.

```
Switch#show ip route | include S\*  
  
S*   >0.0.0.0/0 [1/1] via 10.90.90.101, vlan1
```

В следующем примере показано отображение строк с параметром **include** «S» и любым символом, следующим за «S». Символ «*» соответствует любой строке.

```
Switch#show ip route | include S*  
  
Code: C - Connected, S - Static , R - RIP  
      O - OSPF Derived, IA - OSPF Inter Area  
      E1 - OSPF External Type 1, E2 - OSPF External Type 2  
      N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2  
      * - candidate default, > - Selected route  
  
Gateway of last resort is 10.90.90.101 to network 0.0.0.0  
S*   >0.0.0.0/0 [1/1] via 10.90.90.101, vlan1  
C    >10.0.0.0/8 is directly connected, vlan1  
Total Entries: 2  
  
Switch#
```

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#
```

Следующий пример показывает использование справки **по слову** для отображения команд режима Privileged EXEC, начинающихся с «ге». 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 ?
<1-9>          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

<i>PRIVILEGE-LEVEL</i>	(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

<i>PRIVILEGE-LEVEL</i>	(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: xxxxxxxx

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** учетные данные не заданы.

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

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

Режим ввода команды

Line Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

- При выключении авторизации пользователь войдет в систему с уровнем привилегий 1.
- При выборе опции **by password** после ввода того же пароля, что в команде **password**, пользователь войдет в строку на уровне 1. Если пароль не был сконфигурирован, 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 login-password
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 указанным паролем и уровнем привилегий 12.

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



Примечание: пароль должен содержать 8-30 символов и включать, по крайней мере, одну заглавную и строчную букву, одну цифру и один символ, например, @!&*. Пароль не должен совпадать с именем пользователя и не должен содержать соседние одинаковые символы или цифры или IP-адрес коммутатора по умолчанию.

В нижеприведенном 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# disable  
Switch# logout
```

2.8 end

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

end

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим 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 ethernet 1/1  
Switch(config-if)#end  
Switch#
```

2.9 exit

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

exit

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда 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 ethernet 1/0/1
Switch(config-if)#exit
Switch(config)#
```

2.10 show history

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

show history

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Навигация по командам в истории выполняется следующими комбинациями клавиш:

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

Пример

В данном примере показан процесс вызова буфера истории.

```
Switch# show history

help
history

Switch#
```

2.11 password-recovery

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

password-recovery

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Reset Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

В некоторых ситуациях администратору необходимо обновить учетные данные пользователя, 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.

Любой режим конфигурирования.

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
-----
2         Central Temperature/1         48C/0~76C
2         Central Temperature/2         54C/0~76C
Status code: * temperature is out of threshold range

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

Detail Power Status:
Unit      Power Module      Power Status
-----
2         Power 1             in-operation
2         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 используется для отображения общей информации об устройствах в стеке.

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.

Любой режим конфигурирования.

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  Model Descr                                     Model Name
-----
  2    16*2.5GE PoE AT , 8*5GE PoE BT + 2*10GBASE-T + 4*25G SFP28  DMS-3130-30PS

Unit  Serial-Number      Status      Up Time
-----
  2    TMCAM18000002      OK          0DT1H4M47S

Unit  Memory      Total      Used      Free
-----
  2    DRAM        2023532 K  791428 K  1232104 K
  2    FLASH        92160 K   58151 K   34009 K

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 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.

Любой режим конфигурирования.

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 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 получить информацию о загрузке процессора.

```
Switch#show cpu utilization

CPU Utilization

Five seconds - 21 %           One minute - 22 %           Five minutes - 22 %

Switch#
```

2.15 show version

Данная команда используется для отображения информации о версии коммутатора.

show version

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о версии коммутатора.

Пример

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

```
Switch#show version

Device MAC Address: 00:AD:24:A2:D6:00
System MAC Address: 00:AD:24:A2:D6:00

Unit ID  Module Name          Versions
-----  -
2         DMS-3130-30PS              H/W:A1
                                           Bootloader:1.00.003
                                           Runtime: 1.01.006

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 отставку 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). Данный тип trap-сообщений можно отправлять только через порты 10G.
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 отработку 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 <i>UNIT-ID</i>	Укажите Unit ID.
thermal <i>THERMAL-ID</i>	Укажите идентификатор термодатчика.
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 privilege

Данная команда используется для отображения текущего уровня привилегии.

show privilege

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения текущего уровня привилегии.

Пример

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

```
Switch#show privilege

Current privilege level is 15

Switch#
```

2.19 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 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 об использовании памяти.

```
Switch#show memory utilization
```

Unit	Memory	Total	Used	Free
1	DRAM	1006928 K	676848 K	330080 K
1	FLASH	92160 K	52885 K	39275 K

```
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 ethernet 1/0/1
Switch#
```

3.2 dot1x control-direction

Данная команда используется для настройки типа трафика на порту как однонаправленного (in) или

двунаправленного (both). 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.

Пример

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

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

3.3 dot1x default

Данная команда 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 ethernet 1/0/1
Switch(config-if)# dot1x default
Switch(config-if)#
```

3.4 dot1x port-control

Данная команда используется для управления состоянием авторизации порта. 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 для включения аутентификации IEEE 802.1X для порта.
-------------	---

force-authorized	Укажите, чтобы порт считался принудительно авторизованным.
force-unauthorized	Укажите, чтобы порт считался принудительно неавторизованным.

По умолчанию

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

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

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

3.5 dot1x forward-pdu

Данная команда используется для включения функции продвижения кадров dot1x PDU. 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 ethernet 1/0/1
Switch(config-if)# dot1x forward-pdu
Switch(config-if)#
```

3.6 dot1x initialize

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

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

Параметры

interface <i>INTERFACE-ID</i>	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 <i>MAC-ADDRESS</i>	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 ethernet 1/0/1
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

<i>TIMES</i>	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. Используйте команду, чтобы задать количество повторных попыток для передачи запроса. Если клиент не отвечает на запрос аутентификации в течение периода, заданного командой **dot1x timeout tx-period** *SECONDS*, коммутатор отправит повторный запрос.

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

3.9 dot1x re-authenticate

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

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

Параметры

interface <i>INTERFACE-ID</i>	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 <i>MAC-ADDRESS</i>	Указание MAC-адреса для повторной аутентификации.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

3.12 show dot1x

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

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

Параметры

interface INTERFACE-ID	(Опционально.) Укажите 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.

Любой режим конфигурирования.

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 ethernet 1/0/1

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

Switch#
```

3.13 show dot1x diagnostics

Данная команда используется для просмотра результатов диагностики IEEE 802.1X.

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

Параметры

interface INTERFACE-ID	(Опционально.) 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.

Любой режим конфигурирования.

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 ethernet 1/0/1

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

Switch#
```

3.14 show dot1x statistics

Данная команда используется для просмотра статистики IEEE 802.1X.

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

Параметры

interface INTERFACE-ID	(Опционально.) 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.

Любой режим конфигурирования.

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 ethernet 1/0/1

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

Switch#
```

3.15 show dot1x session-statistics

Данная команда используется для отображения статистики сессий IEEE 802.1X.

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

Параметры

interface 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.

Любой режим конфигурирования.

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 ethernet 1/0/1

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

Switch#
```

3.16 snmp-server enable traps dot1x

Данная команда используется, 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} STARTING-SEQUENCE-NUMBER INCREMENT
no access-list resequence
```

Параметры

NAME	Имя конфигурируемого списка доступа. Может содержать максимум 32 символа.
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# configure terminal
Switch(config)# show access-list ip R&D

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

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

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

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

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

Switch(config)#
```

4.2 acl-hardware-counter

Данная команда используется, чтобы включить аппаратный счетчик ACL указанного списка управления доступом (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 vlan-filter ACCESS-MAP-NAME
no acl-hardware-counter vlan-filter ACCESS-MAP-NAME

Параметры

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

Пример

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

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

4.4 clear acl-hardware-counter

Данная команда используется для сброса аппаратных счетчиков ACL.

clear acl-hardware-counter vlan-filter [ACCESS-MAP-NAME]

Параметры

vlan-filter ACCESS-MAP-NAME	Укажите имя удаляемой access map.
------------------------------------	-----------------------------------

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

```
Switch#clear acl-hardware-counter vlan-filter vlan-map  
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, 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 ethernet 1/0/2
Switch(config-if)# expert access-group exp_acl in

PROMPT: The remaining applicable EXPERT access entries are 768, remaining range entries are 32.

Switch(config-if)# end
Switch# show access-group interface ethernet 1/0/2
eth1/0/2:
  Inbound expert access-list : exp_acl(ID: 9999)
Switch#
```

4.6 expert access-list

Данная команда используется для создания или изменения расширенного списка управления доступом expert (extended expert ACL). Использование данной команды осуществляет вход в режим Extended Expert Access-List Configuration Mode. 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 ethernet 1/0/2
Switch(config-if)#ip access-group Strict-Control

PROMPT: The remaining applicable IP access entries are 767, 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. Для стандартных списков доступа IP диапазон значений составляет 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 под 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 ethernet 1/0/3
Switch(config-if)#ipv6 access-group ip6-control in

PROMPT: The remaining applicable IPv6 access entries are 383, 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. Для стандартных списков доступа IPv6 диапазон значений составляет 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 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 доступа 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 ethernet 1/0/4
Switch(config-if)#mac access-group daily-profile in

PROMPT: The remaining applicable MAC access entries are 1536, remaining range entries are 32.
Switch(config-if)#
```

4.12 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)#
```

4.13 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 spl
Switch(config-access-map)# end
Switch# show vlan access-map

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

Switch#
```

4.14 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 spl
Switch(config-access-map)# end
Switch# show vlan access-map

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

Switch#
```

4.15 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 address:  spl(ID: 3999)
  action: forward
VLAN access-map vlan-map 30
  match mac address:  ext_mac(ID: 7999)
  action: forward

Switch#
```

4.16 permit | deny (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} 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] } [inner INNER-VLAN [MASK]]] [fragments] [[precedence PRECEDENCE [MASK]] [tos TOS [MASK]] | dscp DSCP [MASK]] [time-range PROFILE-NAME]

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

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

no SEQUENCE-NUMBER

Параметры

<i>SEQUENCE-NUMBER</i>	Укажите порядковый номер. Диапазон значений: от 1 до 65535. Чем меньше номер, тем выше приоритет правила permit/deny.
<i>PROTOCOL</i>	(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 <i>MASK</i> (0x0-0xff) является опциональным. Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
cos <i>OUTER-COS</i>	(Опционально.) Укажите значение внешнего приоритета (outer priority). Диапазон значений: от 0 до 7.
<i>MASK</i>	(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 <i>INNER-COS</i>	(Опционально.) Укажите значение внутреннего приоритета (inner priority). Диапазон значений: от 0 до 7.
<i>MASK</i>	(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 <i>OUTER-VLAN</i>	(Опционально.) Укажите outer VLAN ID.
<i>MASK</i>	(Опционально.) Укажите маску outer VLAN ID (0x0-0xffff). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
inner <i>INNER-VLAN</i>	(Опционально.) Укажите inner VLAN ID.
<i>MASK</i>	(Опционально.) Укажите маску inner VLAN ID (0x0-0xffff). 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 <i>SRC-MAC-ADDR</i>	Укажите определенный MAC-адрес узла источника.
<i>SRC-MAC-ADDR SRC-MAC-WILDCARD</i>	Укажите группу MAC-адресов источника, используя значение битовой маски (wildcard). Бит, соответствующий значению бита 1, не будет учитываться. Бит, соответствующий значению бита 0, будет проверяться.
host <i>DST-MAC-ADDR</i>	Укажите определенный MAC-адрес узла назначения.

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 <i>PORT</i>	(Опционально.) Укажите для сопоставления, если значение порта не равно указанному.
range <i>MIN-PORT MAX-PORT</i>	(Опционально.) Укажите для сопоставления, если значение попадает в указанный диапазон портов.
mask <i>PORT MASK</i>	(Опционально.) Укажите для сопоставления портов, определенных маской. Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
<i>TCP-FLAG</i>	(Опционально.) Укажите поля TCP flag и указанные биты заголовка TCP с именем ack (acknowledge), fin (finish), psh (push), rst (reset), syn (synchronize) или urg (urgent).
fragments	(Опционально.) Укажите для фильтрации фрагментов пакета.
time-range <i>PROFILE-NAME</i>	(Опционально.) Укажите имя профиля временного интервала, связанного со списком доступа и определяющего период его активации.
<i>ICMP-TYPE</i>	(Опционально.) Укажите тип сообщения ICMP. Доступны номера типа сообщений от 0 до 255.
<i>ICMP-CODE</i>	(Опционально.) Укажите код сообщения ICMP. Доступны номера кода сообщений от 0 до 255.
<i>ICMP-MESSAGE</i>	(Опционально.) Укажите сообщение ICMP. Для выбора доступны следующие предустановленные параметры: beyond-scope , destination-unreachable , echo-reply , echo-request , 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 (expert access-list)** удалить параметр **fragment** для параметров **tcp**, **udp** или **icmp**, пользователь все равно может использовать опцию **PROTOCOL** в команде **permit | deny (expert access-list)** для настройки параметра **fragment**.

Пример

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

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

4.17 permit | deny (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} 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} 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} 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} {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} {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} {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). 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.
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.
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.
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, связанного со списком доступа и определяющего период его активации.
tcp, udp, 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.
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.

<i>ICMP-CODE</i>	(Опционально) Укажите код сообщения ICMP. Доступны номера кода сообщений от 0 до 255.
<i>ICMP-MESSAGE</i>	(Опционально.) Укажите сообщение ICMP. Для выбора доступны следующие предустановленные параметры: administratively-prohibited, alternate-address, conversion-error, host-prohibited, net-prohibited, echo, echo-reply, pointer-indicates-error, host-isolated, host-precedence-violation, host-redirect, host-tos-redirect, host-tos-unreachable, host-unknown, host-unreachable, information-reply, information-request, mask-reply, mask-request, mobile-redirect, net-redirect, net-tos-redirect, net-tos-unreachable, net-unreachable, net-unknown, bad-length, option-missing, packet-fragment, parameter-problem, port-unreachable, precedence-cutoff, protocol-unreachable, reassembly-timeout, redirect-message, router-advertisement, router-solicitation, source-quench, source-route-failed, time-exceeded, timestamp-reply, timestamp-request, traceroute, ttl-expired, unreachable.

По умолчанию

Нет.

Режим ввода команды

IP Access-list Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

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

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

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

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

Пример

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

```
Switch# configure terminal
Switch(config)# ip 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 примере ниже показано, как создать 2 записи для стандартного списка доступа IP с именем «std-acl». Это следующие записи: разрешить IP-пакеты для сети 10.20.0.0, разрешить IP-пакеты для узла 10.100.1.2.

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

4.18 permit | deny (ipv6 access-list)

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

Расширенный список доступа IPv6 (Extended IPv6 Access List):

[SEQUENCE-NUMBER] {permit | deny | 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 <i>PORT</i>	(Опционально.) Укажите для сопоставления, если значение порта равно указанному.
neq <i>PORT</i>	(Опционально.) Укажите для сопоставления, если значение порта не равно указанному.
range <i>MIN-PORT MAX-PORT</i>	(Опционально.) Укажите для сопоставления, если значение попадает в указанный диапазон портов.
mask <i>PORT MASK</i>	(Опционально.) Укажите для сопоставления с портами, определенными маской. Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
<i>PROTOCOL-ID</i>	(Опционально.) Укажите Protocol ID. Диапазон значений: от 0 до 255.
<i>MASK</i>	(Опционально.) Укажите маску Protocol ID (0x0-0xff). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться.
<i>ICMP-TYPE</i>	(Опционально.) Укажите тип сообщения ICMP. Доступны номера типа сообщений от 0 до 255.
<i>ICMP-CODE</i>	(Опционально.) Укажите код сообщения ICMP. Доступны номера кода сообщений от 0 до 255.
<i>ICMP-MESSAGE</i>	(Опционально.) Укажите сообщение ICMP. Для выбора доступны следующие предустановленные параметры: <i>beyond-scope</i> , <i>destination-unreachable</i> , <i>echo-reply</i> , <i>echo-request</i> , <i>erroneous_header</i> , <i>hop-limit</i> , <i>multicast-listener-query</i> , <i>multicast-listener-done</i> , <i>multicast-listener-report</i> , <i>nd-na</i> , <i>nd-ns</i> , <i>next-header</i> , <i>no-admin</i> , <i>no-route</i> , <i>packet-too-big</i> , <i>parameter-option</i> , <i>parameter-problem</i> , <i>port-unreachable</i> , <i>reassembly-timeout</i> , <i>redirect</i> , <i>renum-command</i> , <i>renum-result</i> , <i>renum-seq-number</i> , <i>router-advertisement</i> , <i>router-renumbering</i> , <i>router-solicitation</i> , <i>time-exceeded</i> , <i>unreachable</i> .
<i>TCP-FLAG</i>	(Опционально.) Укажите поля TCP flag и указанные биты заголовка TCP с именем ack (acknowledge), fin (finish), psh (push), rst (reset), syn (synchronize) или urg (urgent).
flow-label <i>FLOW-LABEL</i>	(Опционально.) Укажите значение flow label. Диапазон значений: от 0 до 1048575.
<i>MASK</i>	(Опционально.) Укажите маску flow label (0x0-0xffff). Бит, соответствующий значению бита 0, не будет учитываться. Бит, соответствующий значению бита 1, будет проверяться. Если значение не указано, используется 0xffff.
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)#
```

4.19 permit | deny (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]} [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 <i>INNER-COS</i>	(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. Если значение не указано, используется 0x7.
vlan <i>VLAN-ID</i>	(Опционально.) Укажите VLAN ID.
MASK	(Опционально.) Укажите маску outer VLAN ID (0x0-0x0fff). Если значение не указано, используется 0x0fff.
inner <i>INNER-VLAN</i>	(Опционально.) Укажите inner VLAN ID.
MASK	(Опционально.) Укажите маску inner VLAN ID (0x0-0x0fff). Если значение не указано, используется 0x0fff.
time-range <i>PROFILE-NAME</i>	(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)#
```

4.20 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, отображаться будет 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#
```

4.21 show access-list

Данная команда используется для отображения информации о настройках списка доступа.

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

Параметры

ip	(Опционально.) Укажите для отображения всех списков доступа IP.
mac	(Опционально.) Укажите для отображения всех списков доступа MAC.
ipv6	(Опционально.) Укажите для отображения всех списков доступа IPv6.
expert	(Опционально.) Укажите для отображения всех списков доступа expert.
NAME	(Опционально.) Укажите имя 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#
```

4.22 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#
```

4.23 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#
```

4.24 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)#
```

4.25 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-access-map)# end
Switch# show vlan filter

VLAN Map vlan-map
  Configured on VLANs: 5

Switch#
```

5. Команды управления доступом

5.1 access class

Данная команда используется для указания списка, которому необходимо ограничить доступ к сессии. 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 #
LINE c banner-text c, where 'c' is a delimiting character
Enter Command Line Interface
#
Switch(config)#
```

5.3 prompt

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

prompt *STRING*
no prompt

Параметры

<i>STRING</i>	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)#
```

5.4 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. Допустимо использование пробелов. Для этого необходимо использовать символ «'», например, 'password 1234'. Если невозможно указать синтаксис пароля, остается незашифрованный текст.
7	(Опционально.) Укажите зашифрованный пароль на основе SHA-1. Длина пароля ограничена 35 байтами, и он должен начинаться с символов *@&. 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, и он должен начинаться с символов *@&. 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 «MyEnable_Password» для уровня привилегий 15.

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

5.5 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)#
```

5.6 ip http secure-server

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

ip http secure-server

no ip http secure-server

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 позволяет включить сервер HTTPS и использовать встроенный локальный сертификат для HTTPS. При выполнении данной команды HTTP-сервер будет автоматически отключен.

Пример

В данном примере показано, как включить HTTPS-сервер.

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

5.7 ip http access-class

Данная команда используется для назначения списка, которому необходимо ограничить доступ к HTTP-серверу. Чтобы отменить проверку указанного списка доступа, воспользуйтесь формой **no** этой команды.

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

Параметры

<i>IP-ACL</i>	Укажите стандартный список доступа IP-адресов. Поле адреса источника в правиле определяет, является ли узел доверенным или нет.
---------------	---

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

5.8 ip http service-port

Данная команда используется, чтобы 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

<i>TCP-PORT</i>	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

Используйте данную команду, чтобы указать TCP-порт для сервера HTTP.

Пример

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

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

5.9 ip http timeout-policy idle

Данная команда используется, чтобы 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

<i>INT</i>	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)#
```

5.10 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. Интерфейс доступа SSH отдельно управляется командами SSH.

Пример

В данном примере показано, как включить сервер Telnet.

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

5.11 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

<i>TCP-PORT</i>	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)#
```

5.12 ip telnet source-interface

Данная команда позволяет задать IP-адрес интерфейса, который будет использоваться в качестве адреса источника Telnet-пакетов при установке Telnet-соединения. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

В данном примере показано, как настроить VLAN 100 в качестве исходного интерфейса для Telnet-пакетов для инициирования подключения по Telnet.

```
Switch# configure terminal
Switch(config)# ip telnet source-interface vlan 100
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 используется для входа 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 используется, чтобы 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.
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.

Любой режим конфигурирования.

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: 9600 bps

Switch#
```

5.17 show ip http server

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

show ip http server

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда 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 : enable  
  
Switch#
```

5.18 show ip http secure-server

Данная команда используется для отображения информации о состоянии SSL.

show ip http secure-server

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения информации о состоянии SSL.

Пример

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

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

5.19 show users

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

show users

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда 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#
```

5.20 telnet

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

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

Параметры

<i>IP-ADDRESS</i>	Укажите IPv4-адрес узла.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес узла.
<i>TCP-PORT</i>	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.

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

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

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

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

Пример

В данном примере показано, как подключиться к IP-адресу 10.90.90.91 с помощью порта 23. IP-адрес 10.90.90.91 является интерфейсом управления DMS-3130-30TS, позволяющим пользователю войти в учетную запись.

```
Switch# telnet 10.90.90.91

DMS-3130-30TS Gigabit Ethernet Switch

Command Line Interface
Firmware: 1.01.006
Copyright(C) 2018 D-Link Corporation. All rights reserved.

Password required, but none set

Switch#
```

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

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

Switch# telnet 10.90.90.91 3500

DMS-3130-30TS Gigabit Ethernet Switch

Command Line Interface
Firmware: 1.01.006
Copyright(C) 2018 D-Link Corporation. All rights reserved.

Password required, but none set

Switch#
```

5.21 terminal length

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

5.22 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

<i>BPS</i>	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)#
```

5.23 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

<i>MINUTES</i>	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)#
```

5.24 terminal width

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

<i>NUMBER</i>	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 действовать 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# show terminal

Terminal Settings:
Length: 24 lines
Width: 80 columns
Default Length: 24 lines
Default Width: 80 columns
Baud rate: 115200 bps

Switch# terminal width 120
Switch# show terminal

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

Switch #
```

5.25 username

Данная команда 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. Имена пользователей чувствительны к регистру.
privilege LEVEL	(Опционально.) Укажите уровень привилегий для каждого пользователя. Диапазон значений: от 1 до 15.
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 должен содержать 8-30 символов и включать, по крайней мере, одну заглавную и строчную букву, одну цифру и один символ, например, @!&*. Пароль не должен совпадать с именем пользователя и не должен содержать соседние одинаковые символы или цифры или IP-адрес коммутатора по умолчанию. Пароль чувствителен к регистру. Если синтаксис пароля не может быть указан, используется обычный текст.
7	(Опционально.) Укажите пароль, зашифрованный на основе SHA-1. Длина пароля ограничена 35 байтами, и он должен начинаться с символов *@&. 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, и он должен начинаться с символов *@\$*. 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, система аутентификации на основе имени пользователя не установлена.

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 паролем.

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

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

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

5.26 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 должен содержать 8-30 символов и включать, по крайней мере, одну заглавную и строчную букву, одну цифру и один символ, например, @!&*. Пароль не должен совпадать с именем пользователя и не должен содержать соседние одинаковые символы или цифры или IP-адрес коммутатора по умолчанию. 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, и он должен начинаться с символов *@&. 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, и он должен начинаться с символов *@\$\$. 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 xxxxxxxx
Switch(config-line)#
```

5.27 clear line

Данная команда используется для завершения сессии подключения.

clear line *LINE-ID*

Параметры

<i>LINE-ID</i>	Укажите 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. 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#
```

5.28 banner exec

Данная команда используется для настройки отображения баннера при запуске процесса 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 ввода имени пользователя и пароля, но до появления приглашения на вход в режим User EXEC Mode.

По умолчанию

По умолчанию баннер EXEC не настроен.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить текст баннера, отображаемый после успешной аутентификации пользователя, но до появления приглашения на вход в режим EXEC Mode.

При настройке текста баннера разрешается использовать определенные маркеры (token) с символом «\$» в форме \$(token) для отображения текущей конфигурации или информации о системе. Существующие маркеры (token) представлены в таблице ниже:

Token	Информация, отображаемая в баннере.
\$(hostname)	Укажите для отображения имени узла.
\$(line)	Укажите для отображения Line ID (идентификатор сессии подключения).

Пример

В данном примере показано, как настроить баннер EXEC с использованием маркеров, которые будут заменены соответствующей конфигурацией или информацией.

```
Switch#configure terminal
Switch(config)#banner exec #
Enter a banner message. End with the '#' symbol.

Session established on $(hostname)#
Switch(config)#

-----
When a user logs in to the system, the output is displayed as follows
-----

          DMS-3130-30TS Gigabit Ethernet Switch

                Command Line Interface
                Firmware: 1.01.006
        Copyright(C) 2018 D-Link Corporation. All rights reserved.

User Access Verification
Username:RDuser
Password:*****

Session established on Switch

Switch#
```

5.29 exec-banner

Данная команда позволяет включить отображение баннера EXEC при установлении определенной сессии или сессий. Чтобы отключить отображение баннера EXEC, воспользуйтесь формой **no** этой команды.

exec-banner

no exec-banner

Параметры

Нет.

По умолчанию

По умолчанию баннер EXEC отображается при установлении каждой сессии.

Режим ввода команды

Line Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить/отключить отображение баннера EXEC при установлении сессий.

Пример

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

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

6. Команды предотвращения атак ARP Spoofing

6.1 ip arp spoofing-prevention

Данная команда применяется, чтобы настроить запись ARP Spoofing Prevention (ASP), используемую для предотвращения атак ARP. 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

<i>GATEWAY-IP</i>	Укажите IP-адрес шлюза.
<i>GATEWAY-MAC</i>	Укажите MAC-адрес шлюза. Настройки MAC-адреса заменят последнюю конфигурацию для того же IP-адреса шлюза.
<i>INTERFACE-ID</i>	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.
<i>,</i>	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
<i>-</i>	(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 предназначена для настройки 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.

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

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 интерфейса Ethernet 1/0/1.

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

6.2 show ip arp spoofing-prevention

Данная команда используется для отображения настроек ARP Spoofing Prevention.

show ip arp spoofing-prevention

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения всех записей ARP Spoofing Prevention.

Пример

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

```
Switch# show ip arp spoofing-prevention

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

Total Entries: 1

Switch#
```

Отображаемые параметры

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

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

7. Команды Asymmetric VLAN

7.1 asymmetric-vlan

Данная команда используется для включения функции Asymmetric VLAN. Чтобы отключить данную функцию, 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 включить 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. Чтобы удалить список методов аккаунтинга, воспользуйтесь формой **no** этой команды.

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

Параметры

<i>LEVEL</i>	Укажите уровень привилегий, на котором необходимо активировать аккаунтинг для всех команд configure . Диапазон значений: от 1 до 15.
default	Укажите для использования списка методов аккаунтинга по умолчанию.
<i>LIST-NAME</i>	Укажите имя списка методов (не более 32 символов).
<i>METHOD1 [METHOD2...]</i>	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. Чтобы отключить аккаунтинг EXEC, воспользуйтесь формой **no** этой команды.

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

Параметры

default	Укажите для использования списка методов аккаунтинга EXEC по умолчанию.
LIST-NAME	Укажите имя списка методов (не более 32 символов).
METHOD1 [METHOD2...]	Укажите список методов, который необходимо выполнить алгоритму аккаунтинга в 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 используется для аккаунтинга действий пользователей при получении доступа к сети. Чтобы удалить список методов аккаунтинга, воспользуйтесь формой **no** этой команды.

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

Параметры

network	Укажите для выполнения аккаунтинга сервисных запросов, касающихся сети.
start-stop	Укажите для отправки accounting-сообщений как при входе, так и при выходе из системы. Пользователям разрешен доступ к сети независимо от того, успешно ли активирован аккаунтинг при отправке начального accounting-сообщения.
default	Укажите для настройки списка методов аккаунтинга сетевых ресурсов по умолчанию.
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 – указывает на использование групп серверов, определенных 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 платы за обеспечение доступа к сети. 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 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 событий системы. Чтобы удалить список методов аккаунтинга, воспользуйтесь формой **no** этой команды.

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

Параметры

system	Укажите для выполнения аккаунтинга событий системного уровня.
start-stop	Укажите для отправки accounting-сообщений как при входе, так и при выходе из системы. Пользователям разрешен доступ к сети независимо от того, успешно ли активирован аккаунтинг при отправке начального accounting-сообщения.
default	Укажите для настройки списка методов аккаунтинга системных ресурсов по умолчанию.
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 событий системы, 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 событий системы, используя RADIUS, который будет отправлять accounting-сообщения.

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

8.5 aaa authentication enable

Данная команда используется, чтобы настроить список методов 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. Чтобы удалить список 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 dot1x default group radius
Switch(config)#
```

8.7 aaa authentication igmp-auth

Данная команда позволяет настроить список методов по умолчанию, используемый для аутентификации IGMP. Чтобы удалить список 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. Чтобы удалить список 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.
<i>LIST-NAME</i>	Укажите имя списка методов, отличного от списка методов по умолчанию. Максимальное количество символов – 32.
<i>METHOD1</i> [<i>METHOD2</i>...]	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 <i>GROUP-NAME</i> – 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. Чтобы удалить список 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. Чтобы удалить список методов по умолчанию, воспользуйтесь формой **no** этой команды.

aaa authentication web-auth defaultMETHOD1 [METHOD2...]
no aaa authentication web-auth default

Параметры

METHOD1 [METHOD2...] Укажите список методов, которые 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. Чтобы удалить группу серверов RADIUS, воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

Группа серверов AAA не настроена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда позволяет назначить 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. Вторая запись узла выступает в качестве резервной для первой записи.

```
Switch#configure terminal
Switch(config)#aaa group server radius group1
Switch(config-sg-radius)# server 172.19.10.100 (or X:X:X:X::X for IPv6 address)
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. Чтобы удалить группу серверов TACACS+, воспользуйтесь формой **no** этой команды.

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

Параметры

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

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+. Команда **server** применяется для привязки серверов TACACS+ к группе. Заданная группа серверов может быть указана в качестве списка методов для аутентификации или аккаунтинга с помощью команд **aaa authentication** и **aaa accounting**.

Пример

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

```
Switch#configure terminal
Switch(config)#aaa group server tacacs+ group1
Switch(config-sg-tacacs+)# server 172.19.10.100 (or X:X:X:X::X for IPv6 address)
Switch(config-sg-tacacs+)# server 172.19.11.20 (or X:X:X:X::X for IPv6 address)
Switch(config-sg-tacacs+)#
```

8.13 aaa server radius dynamic-author

Данная команда используется для настройки динамической авторизации сервера RADIUS. Чтобы удалить настройки динамической авторизации сервера RADIUS, воспользуйтесь формой **no** этой команды.

aaa server radius dynamic-author
no aaa server radius dynamic-author

Параметры

<i>client</i>	Укажите, чтобы настроить клиент динамической авторизации с IPv4-адресом или именем хоста.
<i>port</i>	Укажите, чтобы настроить порт, на котором устройство будет слушать запросы от клиентов динамической авторизации сервера RADIUS. Диапазон значений: 1025 – 65535.
<i>server-key</i>	Укажите, чтобы настроить общий секретный ключ для проверки CoA-запросов клиентов сервера: 0 – необходимо ввести незашифрованный ключ; 7 – необходимо ввести зашифрованный ключ; <key-string> – если тип ключа не указан, необходимо ввести незашифрованный ключ.
<i>ignore</i>	Укажите, чтобы настроить устройство на игнорирование определенных параметров аутентификации от RADIUS-клиентов: server-key – игнорирует ключ сервера; session-key – игнорирует ключ сессии.

По умолчанию

Динамическая авторизация AAA RADIUS-сервера не настроена.

Режим ввода команды

Radius Dynamic-author Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду для входа в режим конфигурации динамической авторизации RADIUS-сервера (Radius Dynamic-author Mode) и настройки порта динамической авторизации,

IP-адреса клиента, имени хоста и ключа сервера.

Пример

В данном примере показано, как указать IP-адрес клиента, который принимает CoA-запросы.

```
Switch#configure terminal
Switch(config)#aaa server radius dynamic-author
Switch(config-radius-da)#client 192.168.66.7
```

8.14 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)#
```

8.15 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

<i>LEVEL</i>	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.
<i>METHOD-LIST</i>	Укажите имя списка методов для использования.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Line Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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, то команда не вступает в силу. Доступно использование разных списков методов для аккаунтинга команд на разных уровнях. Для одного уровня может быть указан только один список методов.

Пример

В данном примере показано, как включить аккаунтинг команд, вводимых через консоль, на 15-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 имя списка методов для использования.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Line Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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 с именем «list-1», использующий сервер RADIUS. Если сервер безопасности не отвечает, аккаунтинг не выполняется. После настройки аккаунтинг EXEC применяется к консоли.

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

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 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 ip radius source-interface

Данная команда позволяет указать интерфейс, IP-адрес которого будет использоваться в качестве IP-адреса источника для отправки пакетов RADIUS. Чтобы вернуться 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 установить VLAN 100, IP-адрес которого будет использоваться в качестве IP-адреса источника для отправки пакетов RADIUS.

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

8.19 ip tacacs source-interface

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

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

Параметры

<i>INTERFACE-ID</i>	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.

Когда 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 установить VLAN 100, IP-адрес которого будет использоваться в качестве IP-адреса источника для отправки пакетов TACACS.

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

8.20 ipv6 radius source-interface

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

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

Параметры

<i>INTERFACE-ID</i>	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 установить VLAN 100, IPv6-адрес которого будет использоваться в качестве IPv6-адреса источника для отправки пакетов RADIUS.

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

8.21 ipv6 tacacs source-interface

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

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

Параметры

<i>INTERFACE-ID</i>	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 установить VLAN 100, IPv6-адрес которого будет использоваться в качестве IPv6-адреса источника для отправки пакетов TACACS.

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

8.22 login authentication

Данная команда позволяет настроить список методов, используемый для аутентификации при входе для конкретной сессии. Чтобы вернуться 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 имя списка методов для использования.

По умолчанию

По умолчанию используется список методов по умолчанию.

Режим ввода команды

Line Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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 установить локальную сессию консоли, чтобы использовать список 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)#
```

8.23 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

<i>MINUTES</i>	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)#
```

8.24 radius-server attribute

Данная команда используется для настройки атрибутов RADIUS-сервера. Чтобы удалить определенную настройку атрибута, воспользуйтесь формой **no** этой команды.

radius-server attribute *code and value*

no radius-server attribute *code and value*

Параметры

<i>attribute type code</i>	Укажите код атрибута: 4 – атрибут IP-адреса NAS (NAS-IP Address); 55 – атрибут временной метки события (Event-Timestamp).
----------------------------	---

По умолчанию

По умолчанию атрибут не настроен.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду для настройки определенного атрибута RADIUS-сервера.

Пример

В данном примере показано, как настроить атрибут IP-адреса NAS для RADIUS-сервера.

```
Switch#configure terminal
Switch(config)# radius-server attribute 4 192.168.3.8
Switch(config)#
```

8.25 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

<i>IP-ADDRESS</i>	Укажите IP-адрес RADIUS-сервера.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес RADIUS-сервера.
auth-port <i>PORT-NUMBER</i>	(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 <i>PORT-NUMBER</i>	(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 <i>SECONDS</i>	Укажите значение тайм-аута сервера. Диапазон значений: от 1 до 255 секунд. Если значение не указано, по умолчанию используется 5 секунд.
retransmit <i>COUNT</i>	(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.
0	(Опционально.) Укажите пароль в форме обычного незашифрованного текста. Данный параметр используется по умолчанию.
7	(Опционально.) Укажите пароль в зашифрованной форме.
key <i>KEY-STRING</i>	Укажите ключ, используемый для связи с сервером. Незашифрованный ключ может содержать от 1 до 32 символов незашифрованного текста, а зашифрованный ключ должен содержать 44 символа.

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)#
```

8.26 server (RADIUS)

Данная команда используется для привязки RADIUS-сервера к группе RADIUS-серверов. Чтобы удалить сервер 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

Используйте команду **aaa group server radius** для входа в режим настройки группы серверов RADIUS (RADIUS Group Server Configuration Mode). 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)#
```

8.27 server (TACACS+)

Данная команда используется для привязки сервера TACACS+ к группе серверов. Чтобы удалить сервер 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

Используйте команду **aaa group server tacacs+** для входа в режим настройки группы серверов TACACS+ (TACACS+ Group Server Configuration Mode). 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+)#
```

8.28 show aaa

Данная команда используется для отображения глобального состояния AAA.

```
show aaa
```

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду для отображения глобального состояния AAA.

Пример

В данном примере показано, как отобразить глобальное состояние AAA.

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

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

Параметры

<i>IP-ADDRESS</i>	Укажите IPv4-адрес сервера TACACS+.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес сервера TACACS+.
port <i>PORT-NUMBER</i>	(Опционально.) Укажите номер UDP-порта назначения для отправки request-пакетов. Номер порта по умолчанию – 49. Диапазон значений: от 1 до 65535.
timeout <i>SECONDS</i>	Укажите значение тайм-аута сервера. Диапазон значений: от 1 до 255 секунд. Значение по умолчанию – 5 секунд.
0	(Опционально.) Укажите пароль в форме обычного незашифрованного текста. Данный параметр используется по умолчанию.
7	(Опционально.) Укажите пароль в зашифрованной форме.

key KEY-STRING

Укажите ключ, используемый для связи с сервером. Ключ может содержать от 1 до 254 символов незашифрованного текста.

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)#
```

8.30 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

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

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

Отображаемые параметры

Auth.	Статистика для пакетов аутентификации.
Acct.	Статистика для пакетов аккаунтинга.
Round Trip Time	Интервал времени (в сотых долях секунды) между последним ответом и запросом, который соответствует ему, с этого сервера RADIUS.
Access Requests	Количество пакетов RADIUS Access-Request, отправленных на данный сервер. Не включает повторные передачи.
Access Accepts	Количество пакетов RADIUS Access-Accept (действительных или недействительных), полученных с данного сервера.
Access Rejects	Количество пакетов RADIUS Access-Reject (действительных или недействительных), полученных с данного сервера.
Access Challenges	Количество пакетов RADIUS Access-Challenge (действительных или недействительных), полученных с данного сервера.
Acct Request	Количество отправленных пакетов RADIUS Accounting-Request. Не включает повторные передачи.
Acct Response	Количество пакетов RADIUS, полученных на accounting-порту от данного сервера.
Retransmissions	Количество пакетов RADIUS Request, повторно 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, так же как и тайм-аут. Попытка подключиться к другому серверу рассматривается как запрос, точно так же как и тайм-аут.
Unknown Types	Количество пакетов RADIUS неизвестного типа, полученных от данного сервера.
Packets Dropped	Количество пакетов RADIUS, полученных от данного сервера и отброшенных по какой-либо причине.

8.31 show tacacs statistics

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

show tacacs statistics

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

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

Отображаемые параметры

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

9. Базовые команды настройки IPv4

9.1 arp

Данная команда используется для добавления статической записи в кэш ARP (Address Resolution Protocol). Чтобы удалить статическую запись из кэша ARP (Address Resolution Protocol), 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 традиционного Ethernet-узла.

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

9.2 arp timeout

Данная команда используется для настройки времени устаревания (Aging Time) ARP-записей в таблице ARP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

По умолчанию установлено 240 минут.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для настройки времени устаревания ARP-записей в таблице ARP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

Пример

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

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

9.3 clear arp-cache

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

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

9.4 ip address

Данная команда используется для назначения интерфейсу 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.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

9.5 ip proxy-arp

Данная команда используется для включения опции Proxy ARP на интерфейсе. Чтобы вернуться 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)#
```

9.6 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 второстепенными 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)#
```

9.7 ip arp elevation

Данная команда используется для назначения более высокого приоритета всем ARP-пакетам этого коммутатора по сравнению с остальными ARP-пакетами.

ip arp elevation
no ip arp elevation

Параметры

Нет.

По умолчанию

По умолчанию у всех ARP-пакетов одинаковый приоритет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для назначения всем ARP-пакетам этого коммутатора более высокого приоритета по сравнению с остальными ARP-пакетами.

Пример

В данном примере показано, как включить повышение приоритета IP ARP.

```
Switch# configure terminal
Switch(config)# ip arp elevation
Switch(config)#
```

9.8 ip mtu

Данная команда используется для настройки значения MTU. 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 определенной сетью.
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.

Любой режим конфигурирования.

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.

Любой режим конфигурирования.

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.

Любой режим конфигурирования.

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.

```
Switch#show ip interface brief

Interface      IP Address      Link Status
-----
vlan 1         10.90.90.90     up
mgmt_ipif      192.168.0.1     down
Total Entries: 2

Switch#
```

В 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 10.90.90.90/255.0.0.0 (Manual)
  ARP timeout is 240 minutes
  IP MTU is 1500 bytes
  Helper Address is not set
  IP Directed Broadcast is disabled
  Proxy ARP is disabled
  IP Local Proxy ARP is disabled
  gratuitous-send is disabled, interval is 0 seconds
  ICMP Redirects is enabled

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#
```

9.12 ip directed-broadcast

Данная команда используется для включения преобразования направленных широковещательных рассылок, получаемых интерфейсом, в рассылки канального уровня, когда сеть назначения подключена непосредственно к коммутатору. Чтобы отключить преобразование, воспользуйтесь формой **no** этой команды.

ip directed-broadcast
no ip directed-broadcast

Параметры

Нет.

По умолчанию

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для настройки направленной широковещательной рассылки на интерфейсе. Команда не влияет на маршрутизацию одноадресных пакетов, передачу пакетов направленной широковещательной рассылки за пределы локальной сети.

Данная команда влияет только на передачу пакетов направленной широковещательной рассылки, для которых сетями назначения являются локальные подсети коммутатора. При включении опции направленной широковещательной рассылки пакеты будут преобразованы в широковещательные и направлены всем узлам сети назначения. В качестве интерфейса отправки может использоваться интерфейс получения или другие интерфейсы коммутатора.

Пример

В данном примере показано, как включить направленную широковещательную рассылку для интерфейса VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip directed-broadcast
Switch(config-if)#
```

10. Базовые команды настройки IPv6

10.1 clear ipv6 neighbors

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

clear ipv6 neighbors {all | interface INTERFACE-ID}

Параметры

all	Укажите, чтобы удалить динамические записи из IPv6 neighbor cache для всех интерфейсов.
interface 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.
---------------------	--

<i>PREFIX-LENGTH</i>	Укажите длину префикса. Префикс IPv6-адреса также является локальной подсетью на интерфейсе.
<i>PREFIX-NAME</i>	Укажите имя префикса, используя не более 12 символов без пробелов.
<i>SUB-BITS</i>	Укажите сетевую и узловую части IPv6-адреса.
link-local	Укажите адрес Link-Local.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

<i>IPv6-PREFIX</i>	Укажите IPv6-префикс для конфигурируемого IPv6-адреса.
<i>PREFIX-LENGTH</i>	Укажите длину префикса. Префикс IPv6-адреса также является локальной подсетью на интерфейсе. Максимальная длина префикса – 64.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если данная команда сконфигурирована в туннеле ISATAP (IPv6), то последние 32 бита идентификатора интерфейса (Interface ID) формируются с использованием IPv4-адреса источника туннеля.

Пример

В данном примере показано, как добавить IPv6-адрес.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 address 3ffe:501:ffff:0::/64 eui-64
Switch(config-if)#
```

10.4 ipv6 address dhcp

Данная команда используется для настройки интерфейса на получение IPv6-адреса с помощью DHCPv6. 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	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 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.

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
no ipv6 address autoconfig

Параметры

Нет.

По умолчанию

Данная опция по умолчанию отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда доступна только для IPv6-адреса VLAN-интерфейса. Опция автоконфигурации по умолчанию отключена.

При включении автоконфигурации интерфейс включает обработку IPv6 и получает анонс от маршрутизатора IPv6 с назначенным префиксом глобального адреса. Далее итоговый адрес, состоящий из префикса и идентификатора интерфейса, назначается данному интерфейсу.

В случае отключения этой опции полученный Global Unicast-адрес будет удален из интерфейса.

Пример

В данном примере показано, как автоматически сконфигурировать IPv6-адрес, используя механизм Stateless Auto-Configuration.

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

10.6 ipv6 enable

Данная команда используется для включения обработки IPv6 на интерфейсах, у которых нет явно настроенного IPv6-адреса. 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 диапазон значений для параметра IPv6 hop limit. Если задан 0, 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 это значение в качестве начального значения параметра hop limit.

Пример

В данном примере показано, как задать значение hop limit для IPv6.

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

10.8 ipv6 mtu

Данная команда используется, 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 исключительно для настройки интерфейсов L3. Используйте 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, заданное по умолчанию.

```
Switch# configure terminal
Switch(config)# interface vlan 4
Switch(config-if)# no ipv6 mtu
Switch(config-if)#
```

10.9 ipv6 nd managed-config-flag

Данная команда используется для включения флага Managed 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 для получения других параметров конфигурации.

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

10.11 ipv6 nd prefix

Данная команда используется для настройки IPv6-префикса, который будет анонсироваться в сообщениях RA. 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

<i>IPv6-PREFIX/PREFIX-LENGTH</i>	Укажите IPv6-префикс, который будет сгенерирован или анонсирован в сообщении RA на интерфейсе.
<i>VALID-LIFETIME</i>	(Опционально.) Укажите период времени в секундах, в течение которого префикс будет действителен. Диапазон значений: от 0 до 4294967295. Если значение не задано, устанавливается значение по умолчанию – 2592000 секунд (30 дней).
<i>PREFERRED-LIFETIME</i>	(Опционально.) Укажите предпочтительное время жизни префикса в секундах. 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. Чтобы вернуться 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. Чтобы вернуться 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.

Анонсирование RA на интерфейсе туннеля отключено.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду **ipv6 nd suppress-ra**, чтобы отключить отправку сообщений RA на интерфейс. Воспользуйтесь командой **no ipv6 nd suppress-ra** для включения отправки сообщений RA на интерфейс 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. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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

Параметры

<i>MILLI-SECONDS</i>	Укажите время доступности для отправляемых анонсов маршрутизатора (в миллисекундах). 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

<i>MILLI-SECONDS</i>	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. Чтобы удалить статическую запись из таблицы, воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для создания статической записи в таблице IPv6 neighbor cache на интерфейсе. Отслеживание достижимости 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 show ipv6 general-prefix

Данная команда используется для отображения информации по основному IPv6-префиксу.

show ipv6 general-prefix [PREFIX-NAME]

Параметры

<i>PREFIX-NAME</i>	(Опционально.) Укажите имя основного префикса, для которого необходимо отобразить информацию. Если имя основного префикса не указано, будет отображаться информация по всем основным префиксам. Максимальное количество символов – 12.
--------------------	--

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для просмотра информации по основным IPv6-префиксам.

Пример

В данном примере показано, как отобразить информацию по всем основным IPv6-префиксам.

```
Switch# show ipv6 general-prefix

IPv6 prefix yy
  Acquired via DHCPv6 PD
    vlan 1: 200::/48
      Valid lifetime 2592000, preferred lifetime 604800
    Apply to interfaces
      vlan 2: ::2/64

Total Entries: 1

Switch#
```

10.19 show ipv6 interface

Данная команда используется для отображения информации по IPv6-интерфейсу.

show ipv6 interface [INTERFACE-ID] [brief]

Параметры

<i>INTERFACE-ID</i>	(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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки конфигурации IPv6-интерфейса. Для интерфейса IPv6-туннеля будет отображаться только туннель ISATAP.

Пример

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

```
Switch# show ipv6 interface vlan 2

vlan 2 is up, Link status is down
  IPv6 is enabled,
  link-local address:
    FE80::201:1FF:FE02:305
  Global unicast address:
    200::2/64 (DHCPv6 PD)
  IPv6 MTU is 1500 bytes
  RA messages are sent between 66 to 200 seconds
  RA advertised reachable time is 1200000 milliseconds
  RA advertised retransmit interval is 0 milliseconds
  RA advertised life time is 1800 seconds
  RA advertised O flag is OFF, M flag is OFF
  RA advertised prefixes
200::/64
valid lifetime is 2592000, preferred lifetime is 604800

Switch#
```

В 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#
```

10.20 show ipv6 neighbors

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

show ipv6 neighbors [*INTERFACE-ID*] [*IPv6-ADDRESS*]

Параметры

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

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

```
Switch# show ipv6 neighbors

IPv6 Address                               Link-Layer Addr  Interface Type State
-----
FE80::200:11FF:FE22:3344                  00-00-11-22-33-44 vlan 1      D    REACH

Total Entries: 1

Switch#
```

Отображаемые параметры

Type	D – динамическая изученная запись. S – статическая neighbor-запись.
State	INCOMP (неполное) – состояние, когда запрос на получение адреса для записи отправлен, но ответное сообщение neighbor advertisement еще не получено. REACH (достижимое) – состояние, когда сообщение neighbor advertisement уже получено, а время таймера Reachable Time (в миллисекундах) еще не истекло. Это означает, что соседнее устройство работает корректно. STALE – состояние, в которое переходит запись, если с момента получения последнего подтверждения прошло больше заданного таймером Reachable Time времени (в миллисекундах). PROBE – состояние записи, при котором устройство отправляет сообщение neighbor solicitation, чтобы подтвердить достижимость.

11. Команды BPDU Protection

11.1 spanning-tree bpduprotection (global)

Данная команда используется для глобального включения функции BPDU Protection. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree bpduprotection
no spanning-tree bpduprotection

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для экономии ресурсов системы можно предотвратить получение пакетов STP BPDU некоторыми из портов устройства.

Функция BPDU Protection предотвращает получение пакетов BPDU на указанных портах.

При обнаружении коммутатором BPDU-атак есть три варианта защиты порта:

- **Drop** – коммутатор отбрасывает только полученные пакеты STP BPDU, порт остается в рабочем состоянии.
- **Block** – коммутатор отбрасывает все полученные BPDU-пакеты и блокирует все данные, порт остается в рабочем состоянии.
- **Shutdown** – коммутатор отключает порт, после чего порт переходит в состояние error-disabled.

Пример

В данном примере показано, как глобально включить функцию BPDU Protection.

```
Switch# configure terminal
Switch(config)# spanning-tree bpduprotection
Switch(config)#
```

11.2 spanning-tree bpduprotection (Interface)

Данная команда используется для включения функции BPDU Protection на порту. Чтобы отключить функцию BPDU Protection на порту, воспользуйтесь формой **no** этой команды.

spanning-tree bpduprotection {drop | block | shutdown}
no spanning-tree bpduprotection

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

Используйте данную команду, чтобы включить и настроить режим работы BPDU Protection (BPDU Protection Operational Mode). Команда применима исключительно для настройки интерфейсов физического порта и port-channel.

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 ethernet 1/0/1
Switch(config-if)# spanning-tree bpdu-protection block
Switch(config-if)#
```

11.3 show spanning-tree bpdu-protection

Данная команда используется для отображения информации о 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 интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона

интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о BPDU Protection. Если ID интерфейса не указан, будет отображена информация по всем интерфейсам.

Пример

В данном примере показано, как отобразить информацию о BPDU Protection и статусах 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
--More-- or (q)uit (a)ll
```

В примере ниже показано, как отобразить статус BPDU Protection для интерфейса Ethernet 1/0/1.

```
Switch#show spanning-tree bpdu-protection interface ethernet 1/0/1
```

Interface	State	Mode	Status
eth1/0/1	Enabled	Shutdown	Normal

```
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

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

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для диагностики кабеля на физическом порту. Диагностика кабеля позволяет выявить проблемы с подключением на медных портах. Чтобы запустить диагностику, используйте команду **test cable-diagnostics**. Медный порт может находиться в одном из следующих состояний:

- **Shutdown:** удаленное устройство отключено;
- **Unknown:** состояние неизвестно. Результат диагностики содержит информацию о наличии обрыва, короткого замыкания или помех в кабеле. Если обнаружен хотя бы один из этих статусов, коммутатор выведет сообщение о неизвестной ошибке;
- **OK:** неисправностей пары/кабеля не выявлено;
- **No cable:** кабель не подключен к порту.



Примечание: при запуске диагностики кабеля проверка длины кабеля применима исключительно на интерфейсах физического порта.



Примечание: максимально разрешенная длина кабеля при диагностике составляет 120 метров.



Примечание: погрешность обнаружения длины кабеля для портов GE составляет около 10 метров.

Пример

В данном примере показано, как запустить диагностику для проверки статуса и длины медного кабеля.

```
Switch# test cable-diagnostics interface ethernet 1/0/1
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. Допустимым интерфейсом является физический порт.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения результатов диагностики кабеля.

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)
-----
eth2/0/1  2.5GBase-T Link Down    -                -
eth2/0/2  2.5GBase-T Link Down    -                -
eth2/0/3  2.5GBase-T Link Down    -                -
eth2/0/4  2.5GBase-T Link Down    -                -
eth2/0/5  2.5GBase-T Link Down    -                -
eth2/0/6  2.5GBase-T Link Down    -                -
eth2/0/7  2.5GBase-T Link Down    -                -
eth2/0/8  2.5GBase-T Link Down    -                -
eth2/0/9  2.5GBase-T Link Down    -                -
eth2/0/10 2.5GBase-T Link Down    -                -
eth2/0/11 2.5GBase-T Link Down    -                -
eth2/0/12 2.5GBase-T Link Down    -                -
--More--  or (q)uit (a)ll
Switch#
```

12.3 clear cable-diagnostics

Данная команда используется для удаления результатов 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. Допустимым интерфейсом является физический порт.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для удаления результатов 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 ethernet 1/0/1  
Switch#
```

13. Команды логирования выполненных команд

13.1 command logging enable

Данная команда используется для включения функции логирования выполненных команд. Чтобы отключить функцию логирования, воспользуйтесь формой **no** этой команды.

command logging enable
no command logging enable

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команды логирования используются для записи 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 показано, как включить функцию логирования.

```
Switch# configure terminal
Switch(config)# command logging enable
Switch(config)#
```

14. Команды Connectivity Fault Management (CFM)

14.1 cfm global enable

Данная команда используется для глобального включения функции CFM. Чтобы глобально отключить данную функцию, воспользуйтесь формой **no** этой команды.

cfm global enable
no cfm global enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применяется для глобального включения/отключения CFM.

Пример

В данном примере показано, как включить функцию CFM глобально.

```
Switch# configure terminal
Switch(config)# cfm global enable
Switch(config)#
```

14.2 cfm domain

Данная команда используется для определения MD (Maintenance Domain – домена технического обслуживания). Чтобы удалить MD, воспользуйтесь формой **no** этой команды.

cfm domain DOMAIN-NAME level LEVEL
no cfm domain DOMAIN-NAME

Параметры

<i>DOMAIN-NAME</i>	Укажите имя MD. Максимальное количество символов – 22. Использование пробелов недопустимо.
level LEVEL	Укажите уровень MD: от 0 до 7.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для назначения MD или входа в режим конфигурации CFM MD. Для лучшей идентификации административной ответственности каждому MD присваивается уникальное имя, отличное от уже используемых или доступных провайдеру/оператору. Для определения иерархической структуры каждому MD присваивается уникальный уровень обслуживания (от 0 до 7). Чем больше диапазон MD, тем выше уровень обслуживания.

Если имя MD введено некорректно или такое имя уже существует, в регистрации нового MD будет отказано. При удалении MD удаляются все сопутствующие настройки.

Пример

В данном примере показано, как назначить MD под именем «op-domain». Указанный уровень MD – 2.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)#
```

14.3 cfm ma

Данная команда используется для назначения МА (ассоциации технического обслуживания), а также входа в режим CFM MA Configuration. Чтобы удалить МА, воспользуйтесь формой **no** этой команды.

cfm ma name MA-NAME [vlan VLAN-ID]
no cfm ma name MA-NAME

Параметры

name MA-NAME	Укажите МА с именем в качестве идентификатора.					
vlan VLAN-ID	(Опционально.)	Укажите	ID	первичной	VLAN	под управлением МА.

По умолчанию

Нет.

Режим ввода команды

CFM MD Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для назначения/удаления МА, а также входа в режим конфигурации CFM МА. У каждой ассоциации технического обслуживания в MD должно быть уникальное имя. У МА, настроенных в разных MD, могут совпадать идентификаторы МА. При создании МА необходимо указать ID первичной VLAN или войти в режим CFM MD Configuration для уже созданных МА. При удалении МА удаляются все сопутствующие настройки.

Пример

В данном примере показано, как создать МА под именем «ор1», закрепленную за ор-доменом под именем MD.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# cfm ma name opl vlan 2
Switch(config-cfm-ma)#
```

14.4 mip creation (cfm md configuration)

Данная команда используется для настройки правила создания MIP (Maintenance Intermediate Points – промежуточные точки обслуживания) в MD. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

mip creation {none | auto | explicit}
no mip creation

Параметры

none	Укажите, чтобы отказаться от создания MIP для МА в данном MD.
auto	Укажите, чтобы создать MIP на порту для МА в данном MD, если: • на порту отсутствуют MEP (Maintenance End Points – конечные точки обслуживания) для МА с таким же VID на данном уровне MD или активных уровнях MD выше; • на порту настроены MEP для МА с таким же VID на следующем активном уровне MD ниже; • отсутствует МА с таким же VID на активных уровнях MD ниже. Укажите параметр auto, чтобы создать MIP на промежуточном коммутаторе в МА.
explicit	Укажите, чтобы создать MIP на порту для МА в данном MD, если: • на порту отсутствуют MEP для МА с таким же VID на

- данном уровне MD или активных уровнях MD выше;
- на порту настроены MEП для МА с таким же VID на следующем активном уровне MD ниже.

По умолчанию

Параметр по умолчанию – **none**.

Режим ввода команды

CFM MD Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется, чтобы настроить правило создания MIP для домена технического обслуживания.

MIP на MD помогают отслеживать ссылки, MIP by MIP, а также позволяют пользователю выполнять закольцовывание от MEП к MIP. Чтобы узнать, может ли управляющий объект создать MHF (MIP Half Functions) для домена технического обслуживания, обратитесь к списку создания MIP.

Настройки данной команды являются настройками по умолчанию для МА в данном MD при создании MIP. Используйте команду **mip creation** в режиме CFM MA Configuration Mode, чтобы применить настройки по умолчанию.

Пример

В данном примере показано, как настроить правило создания MIP при помощи параметра **auto**.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# mip creation auto
Switch(config-cfm-md)#
```

14.5 mip creation (cfm ma configuration)

Данная команда используется, чтобы настроить правило создания MIP для МА. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

mip creation {none | auto | explicit | defer}
no mip creation

Параметры

none	Укажите, чтобы отказаться от создания MIP на портах в МА.
auto	Укажите, чтобы создать MIP на порту для данной МА, если: на порту отсутствуют MEП для МА с таким же VID на данном уровне MD или активных уровнях MD выше;

- на порту настроены MEP для МА с таким же VID на следующем активном уровне MD ниже;
- отсутствует МА с таким же VID на активных уровнях MD ниже.

Укажите параметр **auto**, чтобы создать MIP на промежуточном коммутаторе в МА.

explicit

Укажите, чтобы создать MIP на порту для данной МА, если:

- на порту отсутствуют MEP для МА с таким же VID на данном уровне MD или активных уровнях MD выше;
- на порту настроены MEP для МА с таким же VID на следующем активном уровне MD ниже.

defer

Укажите, чтобы применить настройки создания MIP для MD, в котором находится МА.

По умолчанию

Параметр по умолчанию – **defer**.

Режим ввода команды

CFM MA Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить правило создания MIP для МА. По умолчанию правило подчиняется команде **mip creation** в режиме CFM MD Configuration.

MIP на МА помогают отслеживать ссылки, MIP by MIP, а также позволяют пользователю выполнять закольцовывание от MEP к MIP. Чтобы узнать, может ли управляющий объект создать MHF для МА, обратитесь к списку создания MIP.

Пример

В данном примере показано, как создать ассоциацию технического обслуживания MIP при помощи параметра **auto**.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# cfm ma name op-ma1 vlan 2
Switch(config-cfm-ma)# mip creation auto
Switch(config-cfm-ma)#
```

14.6 sender-id (cfm md configuration)

Данная команда используется для настройки передачи ID TLV отправителя при помощи MP (Maintenance Points – точки обслуживания) в домене технического обслуживания. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

sender-id {none | chassis | manage | chassis-manage}
no sender-id

Параметры

none	Укажите, чтобы отказаться от передачи ID TLV отправителя.
chassis	Укажите для передачи ID TLV отправителя с информацией об ID шасси.
manage	Укажите для передачи ID TLV отправителя с информацией об управляемом адресе.
chassis-manage	Укажите для передачи ID TLV отправителя с информацией об ID шасси и управляемом адресе.

По умолчанию

ID отправителя по умолчанию – **none**.

Режим ввода команды

CFM MD Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для настройки передачи ID TLV отправителя при помощи MP в MD. В списке ID отправителя указано то, что именно необходимо включить (если требуется) в ID TLV отправителя, передаваемого при помощи MP, настроенных в данном MD.

Настройки данной команды являются настройками по умолчанию для передачи ID TLV отправителя MP для MA в данном MD. Используйте команду **sender-id** в режиме CFM MA Configuration Mode, чтобы применить настройки по умолчанию.

Пример

В данном примере показано, как настроить передачу ID TLV отправителя в режиме CFM MD Configuration Mode, чтобы MP передавали ID TLV отправителя с информацией об ID шасси.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# sender-id chassis
Switch(config-cfm-md)#
```

14.7 sender-id (cfm ma configuration)

Данная команда используется, чтобы настроить передачу ID TLV отправителя при помощи MP для MA. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

sender-id {none | chassis | manage | chassis-manage | defer}

no sender-id

Параметры

none	Укажите, чтобы отказаться от передачи ID TLV отправителя.
chassis	Укажите для передачи ID TLV отправителя с информацией об ID шасси.
manage	Укажите для передачи ID TLV отправителя с информацией об управляемом адресе.
chassis-manage	Укажите для передачи ID TLV отправителя с информацией об ID шасси и управляемом адресе.
defer	Укажите, чтобы применить настройки передачи ID отправителя для MD, в котором находится MA.

По умолчанию

Параметр по умолчанию – **defer**.

Режим ввода команды

CFM MA Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить передачу ID TLV отправителя при помощи MP для MA. В списке ID отправителя указано, что именно необходимо включить (если требуется) в ID TLV отправителя, передаваемого при помощи MP, настроенных в данной MA.

Пример

В данном примере показано, как настроить передачу ID TLV отправителя в режиме CFM MA Configuration Mode, чтобы MP передавали ID TLV отправителя с информацией об ID шасси.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# cfm ma name op-ma1 vlan 2
Switch(config-cfm-ma)# sender-id chassis
Switch(config-cfm-ma)#
```

14.8 mepid-list

Данная команда используется для создания/удаления списка MEP ID.

mepid-list {add | delete} MEPID-LIST

Параметры

add	Укажите, чтобы добавить MEP ID в список MEP ID указанных MA.
delete	Укажите, чтобы удалить MEP ID из списка MEP ID указанных MA.
MEPID-LIST	Укажите MEP ID, который необходимо добавить/удалить в/из списка MEP ID указанных MA. Диапазон значений: от 1 до 8191.

По умолчанию

Нет.

Режим ввода команды

CFM MA Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для добавления MEP ID в список MEP ID или удаления MEP ID из списка MEP ID указанной MA. Для добавления MEP ID в список используйте команду **mepid-list add**. Чтобы удалить MEP ID из списка, воспользуйтесь командой **mepid-list delete**. Перед тем, как указать MEP, необходимо добавить его ID в список MEP ID.

Пример

В данном примере показано, как добавить MEP ID 1 и MEP ID 2 в список MEP ID MA под именем op1.

```
Switch#configure terminal
Switch(config)#cfm domain op-domain level 2
Switch(config-cfm-md)#cfm ma name op1
Switch(config-cfm-ma)#mepid-list add 1,2
Switch(config-cfm-ma)#
```

14.9 mode

Данная команда используется для настройки режима CFM MA.

mode {software | hardware}

Параметры

software	Укажите, чтобы включить режим CFM software для MA.
hardware	Укажите, чтобы включить режим CFM hardware для MA.

По умолчанию

Параметр по умолчанию – **software**.

Режим ввода команды

CFM MA Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Режим CFM hardware предназначен для улучшения производительности CCM (Continuity Check Message). В режиме CFM hardware CCM-пакет обрабатывается при помощи аппаратного оборудования, и использование CPU не является обязательным. В данном режиме также можно установить минимальное значение интервала CCM – 3,3 мс, что невозможно в режиме CFM software ввиду ограниченных возможностей CPU.

Режимы CFM hardware и CFM software можно использовать одновременно. Если применить режим CFM hardware для МА, все MEP в МА будут работать в данном режиме. При необходимости задать конкретные значения для CCM в некоторых МА (например, интервал CCM от 3,3 до 10 мс или наличие Down MEP), пользователь может использовать режим CFM hardware. Если значения процесса CCM не критичны / необходимо установить up MEP или up MIP / требуется наличие функции Full CFM, предпочтительнее выбрать режим CFM software.

Пример

В данном примере показано, как настроить режим CFM МА.

```
Switch#configure terminal
Switch(config)#cfm domain op-domain level 2
Switch(config-cfm-md)#cfm ma name opl
Switch(config-cfm-ma)#mode hardware
Switch(config-cfm-ma)#
```

14.10 ccm interval

Данная команда используется, чтобы настроить интервал CCM для МА. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ccm interval *INTERVAL*

no ccm interval

Параметры

INTERVAL

Укажите интервал CCM:

3.3 ms: 3,3 миллисекунды. Применим только в режиме CFM hardware.

10 ms: 10 миллисекунд. Применим только в режиме CFM hardware.

100 ms: 100 миллисекунд. Не рекомендуется применять в

режиме CFM software, т. к. это может привести к загрузженности CPU.

1sec: 1 секунда.

10sec: 10 секунд.

1min: 1 минута.

10min: 10 минут.

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

CFM MA Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить интервал CCM для МА – периода времени, в течение которого МЕР в МА отправляет CCM.

Пример

В данном примере показано, как настроить интервал CCM для МА.

```
Switch#configure terminal
Switch(config)#cfm domain op-domain level 2
Switch(config-cfm-md)#cfm ma name op1 vlan 2
Switch(config-cfm-ma)#ccm interval 10sec
Switch(config-cfm-ma)#
```

14.11 cfm mep

Данная команда используется для назначения конечной точки ассоциации технического обслуживания и входа в режим CFM МЕР Configuration Mode. Чтобы удалить МЕР, воспользуйтесь формой **no** этой команды.

cfm mep mepid *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* [**direction {up | down}**]
no cfm mep mepid *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*

Параметры

mepid <i>MEP-ID</i>	Укажите МЕР ID. Диапазон значений: от 1 до 8191.
name <i>MA-NAME</i>	Укажите имя МА.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальное количество символов – 22.

direction	(Опционально.) Укажите направление MEP.
up	Укажите, чтобы передавать PDU (CFM Protocol Data Units) по направлению к Bridge Relay Entity и получать их от направления Bridge Relay Entity, которое также называется inward facing (up) MEP.
down	Укажите, чтобы передавать CFM PDU по направлению к LAN и получать их от направления LAN, которое также называется outward facing MEP.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для назначения конечной точки ассоциации технического обслуживания. У MEP, настроенных в одной МА, должны быть уникальные MEP ID. У MEP в разных МА могут быть идентичные MEP ID. Перед тем как создать MEP, их ID необходимо добавить в список MEP ID MA.

Пример

В данном примере показано, как настроить MEP на указанном физическом интерфейсе. Указанное направление MEP – up.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain direction up
Switch(config-cfm-mep)#
```

14.12 cfm enable

Данная команда используется для запуска функции CFM на указанном физическом интерфейсе. Чтобы отключить функцию CFM на указанном физическом интерфейсе, воспользуйтесь формой **no** этой команды.

cfm enable
no cfm enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для включения или отключения функции CFM на указанном физическом интерфейсе.

Пример

В данном примере показано, как включить функцию CFM на указанном физическом интерфейсе.

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

14.13 mep enable

Данная команда используется для запуска статуса MEP. Чтобы отключить статус MEP, воспользуйтесь формой **no** этой команды.

mep enable
no mep enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

CFM MEP Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для запуска/отключения статуса MEP.

Пример

В данном примере показано, как запустить статус MEP.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)#mep enable
Switch(config-cfm-mep)#
```

14.14 pdu-priority

Данная команда используется для назначения приоритета 802.1p в CCM и других CFM PDU, передаваемых при помощи MEP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

pdu-priority COS-VALUE
no pdu-priority

Параметры

COS-VALUE	Укажите приоритет 802.1p в CCM и других CFM PDU, передаваемых при помощи MEP. Диапазон значений: от 0 до 7.
-----------	---

По умолчанию

Приоритет PDU по умолчанию – 7.

Режим ввода команды

CFM MEP Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для назначения приоритета 802.1p в CCM и других CFM PDU, передаваемых при помощи MEP.

Пример

В данном примере показано, как назначить приоритет PDU MEP.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)# pdu-priority 2
Switch(config-cfm-mep)#
```

14.15 fault-alarm

Данная команда используется для получения оповещений о неисправностях и их типах при помощи MEP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

fault-alarm {none | all | mac-status | remote-ccm | error-ccm | xcon-ccm}

no fault-alarm

Параметры

none	Укажите, чтобы отказаться от получения оповещений о неисправностях.
all	Укажите, чтобы получать оповещения обо всех типах неисправностей.
mac-status	Укажите, чтобы получать оповещения о неисправностях, чей приоритет выше или равен DefMAC status.
remote-ccm	Укажите, чтобы получать оповещения о неисправностях, чей приоритет выше или равен DefRemoteCCM.
error-ccm	Укажите, чтобы получать оповещения о неисправностях, чей приоритет выше или равен DefErrorCCM.
xcon-ccm	Укажите, чтобы получать оповещения только о неисправностях DefXconCCM.

По умолчанию

Параметр по умолчанию – **none**.

Режим ввода команды

CFM MEP Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы указать типы неисправностей, о наличии которых будут оповещать уведомления при помощи MEP. Для мониторинга доступны следующие типы неисправностей: DefRDICCM, DefMAC status, DefRemoteCCM, DefErrorCCM и DefXconCCM. Приоритетность возрастает от первого указанного типа к последнему.

- **DefRDICCM:** последний CCM, полученный при помощи данных MEP от удаленных MEP, содержал бит RDI.
- **DefMACstatus:** согласно последнему CCM, полученному при помощи данных MEP от удаленных MEP, передача MAC, связанного с MEP, сообщает о состоянии ошибки при помощи Port Status TLV или Interface Status TLV.
- **DefRemoteCCM:** данные MEP не получают CCM от других MEP, указанных в списке конфигурации.
- **DefErrorCCM:** данные MEP получают неверные CCM.
- **DefXconCCM:** CCM, которые получают данные MEP, предположительно принадлежат другим MA.

Пример

В данном примере показано, как настроить MEP для отправки оповещений обо всех типах неисправностей.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# cfm mep mepid 1 ma name opl domain op-domain
Switch(config-cfm-mep)# fault-alarm all
Switch(config-cfm-mep)#
```

14.16 alarm-time

Данная команда используется для установки интервала отправки оповещений о неисправностях и сброса системы оповещений. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

alarm-time {delay CENTISECOND | reset CENTISECOND}
no alarm-time {delay | reset}

Параметры

delay CENTISECOND	Укажите интервал между обнаружением неисправности на MEP и отправкой оповещения. Единица измерения – сантисекунда. Диапазон значений: от 250 до 1000.
reset CENTISECOND	Укажите интервал между устранением неисправностей, обнаруженных на MEP, и сбросом оповещений. Единица измерения – сантисекунда. Диапазон значений: от 250 до 1000.

По умолчанию

Интервал для отправки оповещений MEP по умолчанию – 250.

Интервал для сброса оповещений MEP по умолчанию – 1000.

Режим ввода команды

CFM MEP Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для установки интервала отправки оповещений о неисправностях с момента их обнаружения. Соответствующее оповещение будет отправлено, если по истечении заданного периода времени неисправность не устранена.

После устранения всех неисправностей, обнаруженных на MEP, запускается таймер обратного отсчета. Если по истечении заданного периода неисправностей не обнаружено, будет выполнен сброс системы оповещений.

Пример

В данном примере показано, как настроить интервал отправки оповещений MEP. Заданное значение – 250 сантисекунд.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)# alarm-time delay 250
Switch(config-cfm-mep)#
```

В примере ниже показано, как настроить интервал сброса оповещений MEP. Заданное значение – 1000 сантисекунд.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)# alarm-time reset 1000
Switch(config-cfm-mep)#
```

14.17 ccm enable

Данная команда используется для включения функции CFM CCM (Continuity Check Message). Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ccm enable

no ccm enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

CFM MEP Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для включения или отключения функции CFM CCM MEP.

Пример

В данном примере показано, как включить функцию CFM CCM MEP.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# cfm mep mepid 1 ma name opl domain op-domain
Switch(config-cfm-mep)# ccm enable
Switch(config-cfm-mep)#
```

14.18 show cfm counter ccm

Данная команда используется для отображения счетчиков CFM CCM всех MEP.

show cfm counter ccm

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1

Использование команды

Данная команда применяется для отображения счетчиков пакета CCM RX всех MEP.

Пример

В данном примере показано, как отобразить счетчики пакета CCM всех MEP.

```
Switch#show cfm counter ccm
CCM counters:
MEPID: 1 VID: 2 Level: 2 Direction: Up Port: 1/0/1
  XCON: 9 Error: 8 Normal: 100
MEPID: 2 VID: 1 Level: 2 Direction: up Port: 1/0/11
  XCON: 9 Error: 8 Normal: 100
Total:
  XCON: 18 Error: 16 Normal: 200
Switch#
```

Отображаемые параметры

XCON	Укажите для отображения количества полученных CCM с кросс-соединением.
Error	Укажите для отображения количества полученных CCM, которые являются недействительными.
Normal	Укажите для отображения количества полученных CCM, которые

являются нормальными.

14.19 clear cfm counter ccm

Данная команда используется для сброса счетчиков CCM всех MEP.

clear cfm counter ccm

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для сброса счетчиков пакетов CCM MEP.

Пример

В данном примере показано, как сбросить счетчики пакетов CCM всех MEP.

```
Switch# clear cfm counter ccm
Switch#
```

14.20 cfm loopback test

Данная команда используется для запуска теста Loopback CFM.

cfm loopback test {MAC-ADDR | remote-mepid REMOTE-MEPID} mepid MEP-ID ma name MA-NAME

domain DOMAIN-NAME [num NUMBER] [length LENGTH | pattern STRING] [pdu-priority COS-VALUE]

Параметры

MAC-ADDR	Укажите MAC-адрес назначения.
remote-mepid REMOTE-MEPID	Укажите MEP ID назначения.
mepid MEP-ID	Укажите MEP ID, на котором необходимо запустить функцию Loopback.

name <i>MA-NAME</i>	Укажите имя MA.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальное количество символов – 22.
num <i>NUMBER</i>	(Опционально.) Укажите количество LBM для отправки. Значение по умолчанию – 4.
length <i>LENGTH</i>	(Опционально.) Укажите длину полезной нагрузки LBM для отправки. Диапазон значений: от 0 до 1500. Значение по умолчанию – 0.
pattern <i>STRING</i>	(Опционально.) Укажите, нужно ли использовать Data TLV. Если использование Data TLV необходимо, задайте нужное значение. Максимальное количество символов – 1500. Использование пробелов недопустимо.
pdu-priority <i>COS-VALUE</i>	(Опционально.) Установите приоритет 802.1p в передаваемых LBM. Если значение не задано, используется приоритет, идентичный приоритету CCM, отправленных при помощи MEP.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте сочетание клавиш CTRL+C, чтобы завершить тест Loopback. В MAC-адресе отображаются MEP или MIP получателя, доступные данному MAC-адресу. Адрес может быть индивидуальным или групповым. На групповых адресах поддерживается функция Multicast Loopback. В MEP ID отображаются исходные MEP, используемые для запуска сообщения loopback.

Пример

В данном примере показан процесс передачи LBM на MAC-адрес получателя 00-01-02-03-04-05.

```
Switch# cfm loopback test 00-01-02-03-04-05 mepid 1 ma name op-mal domain op-domain1

Request timed out.
Request timed out.
Request timed out.
Request timed out.
CFM loopback statistics for 00-01-02-03-04-05:
Packets: Sent=4, Received=0, Lost=4(100% loss).

Switch# cfm loopback test remote-mepid 2 mepid 1 ma name op-mal domain op-domain1

Reply from 00-01-02-03-04-05: bytes=0 time=10ms
Reply from 00-01-02-03-04-05: bytes=0 time=10ms
Reply from 00-01-02-03-04-05: bytes=0 time=10ms
Reply from 00-01-02-03-04-05: bytes=0 time=10ms
CFM loopback statistics for 00-01-02-03-04-05:
    Packets: Sent=4, Received=4, Lost=0(0% loss).

Switch#
```

14.21 cfm linktrace

Данная команда используется для создания сообщения link trace.

cfm linktrace *MAC-ADDR* **mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* [**ttl** *TTL*]
[**pdu-priority** *COS-VALUE*]

Параметры

MAC-ADDR	Укажите MAC-адрес получателя.
mepid <i>MEP-ID</i>	Укажите MEP ID, на котором необходимо запустить функцию Link Trace.
name <i>MA-NAME</i>	Укажите имя MA.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальное количество символов – 22.
ttl <i>TTL</i>	(Опционально.) Укажите значение TTL сообщения link trace. Диапазон значений: от 2 до 255. Значение по умолчанию – 64.
pdu-priority <i>COS-VALUE</i>	(Опционально.) Укажите приоритет 802.1p в передаваемых LTM. Если значение не задано, используется приоритет, идентичный приоритету CCM, отправленных при помощи MEP.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для создания сообщения CFM link trace.

Пример

В данном примере показан процесс передачи LTM на MAC-адрес получателя 00-01-02-03-04-05.

```
Switch# cfm linktrace 00-01-02-03-04-05 mepid 1 ma name op-mal domain op-domain1  
  
Transaction ID: 26  
  
Switch#
```

14.22 show cfm linktrace

Данная команда используется для отображения ответов link trace.

show cfm linktrace [mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME [trans-id ID]]

Параметры

mepid MEP-ID	(Опционально.) Укажите MEP ID. Если значение не задано, будут отображены ответы link trace всех MEP.
name MA-NAME	(Опционально.) Укажите имя МА.
domain DOMAIN-NAME	(Опционально.) Укажите имя MD. Максимальное количество символов – 22.
trans-id ID	(Опционально.) Укажите для отображения идентификатора транзакции. Если значение не задано, будут отображены все транзакции MEP, на которых запущена функция Link Trace.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения ответов link trace. Максимальное количество ответов link trace на устройство – 128.

Пример

В данном примере показано, как отобразить ответы link trace.

```
Switch# show cfm linktrace mepid 1 ma name op-ma domain op-domain trans-id 0
Transaction ID: 0
From MEPID 1 to 00-07-00-00-00-1C
Start Time: 2013-11-02 11:35:11
Hop: 1
    Ingress MAC Address: 00-00-00-00-00-00
    Egress MAC Address: 00-09-5A-B9-AC-1B
    Forwarded: Yes           Relay Action: FDB

Hop: 2
    MEPID: 2
    Ingress MAC Address: 00-07-00-00-00-1C
    Egress MAC Address: 00-00-00-00-00-00
    Forwarded: No           Relay Action: Hit

Switch#
```

Отображаемые параметры

Relay Action	Hit: LTM достиг MP, MAC-адрес которых соответствует MAC-адресу назначения. FDB: выходной порт выбран в соответствии с информацией базы данных о фильтрации. MPDB: выходной порт выбран в соответствии с информацией базы данных MIP CCM.
---------------------	---

14.23 clear cfm linktrace

Данная команда используется для удаления полученных ответов link trace.

```
clear cfm linktrace {mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME | all}
```

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID.
name <i>MA-NAME</i>	Укажите имя MA.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальное количество символов – 22.
all	Укажите, чтобы удалить всю информацию link trace для всех MEP.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для удаления из хранилища данных ответов link trace, запущенных при помощи указанных MEP.

Пример

В данном примере показано, как удалить полученные ответы link trace.

```
Switch# clear cfm linktrace mepid 1 ma name op-mal domain op-domain1  
Switch#
```

14.24 ais

Данная команда используется для запуска и настройки параметров функции AIS (Alarm Indication Signal). Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ais [period *PERIOD*] [level *LEVEL*]
no ais [period | level]

Параметры

period <i>PERIOD</i>	(Опционально.) Укажите интервал передачи AIS PDU: 1 секунда или 1 минута.
level <i>LEVEL</i>	(Опционально.) Укажите уровень MD клиента, которому MEP отправляет AIS PDU. Диапазон значений: от 0 до 7.

По умолчанию

По умолчанию данная функция отключена.

Интервал по умолчанию – 1 секунда.

Режим ввода команды

CFM MEP Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для запуска на MEP функции AIS и настройки ее параметров. Если не указаны дополнительные параметры, функция AIS будет запущена автоматически. Если не указан уровень клиента, будет использован уровень MD, на котором существуют MIP и MEP слоя ближайшего клиента. Уровень домена технического обслуживания клиента по умолчанию может меняться в процессе создания или удаления домена технического обслуживания уровня выше или МА на устройстве.

При выявлении неисправности MEP может начать циклическую передачу кадров, содержащих

информацию об ETH-AIS на уровне клиента. MEP продолжит передачу кадров с информацией об ETH-AIS, пока не будет устранена неисправность. После получения кадра с информацией об ETH-AIS от слоя/sub-слоя соответствующего сервера, MEP слоя/sub-слоя клиента обнаружит статус AIS и отключат оповещения, связанные со всеми равными MEP. MEP возобновит отправку оповещений при обнаружении неисправностей, когда статус AIS будет отключен.

При отсутствии MIP и MEP слоя ближайшего клиента вычислить уровень MD клиента невозможно. Если уровень клиента не задан пользователем, а вычислить уровень MD клиента нельзя, передача AIS PDU невозможна.

Пример

В данном примере показан процесс настройки функции AIS с уровнем клиента 5.

```
Switch# clear cfm linktrace mepid 1 ma name op-mal domain op-domain1
Switch#
```

14.25 lck

Данная команда используется для включения функции LCK и настройки ее параметров. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

lck [period PERIOD] [level LEVEL]
no lck [period | level]

Параметры

period PERIOD	(Опционально.) Укажите интервал передачи LCK PDU: 1 секунда или 1 минута. Интервал по умолчанию – 1 секунда.
level LEVEL	(Опционально.) Укажите уровень MD клиента, которому MEP отправляет LCK PDU. Диапазон значений: от 0 до 7.

По умолчанию

По умолчанию данная функция отключена.

Интервал по умолчанию – 1 секунда.

Режим ввода команды

CFM MEP Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для включения на MEP функции LCK и настройки ее параметров. Если параметры не заданы, функция CFM LCK будет запущена автоматически. Если не указан уровень клиента, будет использован уровень MD, на котором существуют MIP и MEP слоя ближайшего клиента. Уровень домена технического обслуживания клиента по умолчанию может меняться в процессе создания или удаления домена технического обслуживания уровня выше, а также MA на устройстве.

При отсутствии MIP и MEP слоя ближайшего клиента вычислить уровень MD клиента по умолчанию невозможно. Если уровень клиента не задан пользователем, а вычислить уровень MD клиента по умолчанию нельзя, передача LCK PDU невозможна.

Пример

В данном примере показан процесс настройки функции LCK с уровнем клиента 5.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# cfm mep mepid 1 ma name opl domain op-domain
Switch(config-cfm-mep)# lck level 5
```

14.26 cfm lck start

Данная команда используется для включения блокировки от имени администратора. Чтобы отключить блокировку, воспользуйтесь формой **no** этой команды.

cfm lck start mepid *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*

cfm lck stop mepid *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID.
name <i>MA-NAME</i>	Укажите имя MA.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальное количество символов – 22.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для включения/отключения блокировки. При включении блокировки MEP отправляет LCK PDU на MEP уровня клиента. Проверить статус блокировки можно при помощи команды **show cfm mep**. Пункт LCK Action в команде **show cfm mep** отображает текущий статус блокировки – start (запущен) или stop (отключен).

Пример

В данном примере показано, как включить блокировку.

```
Switch# cfm lck start mepid 1 ma name op-ma domain op-domain
Switch#
```


14.27 snmp-server enable traps cfm

Данная команда используется для запуска статуса trap ITU Y.1731 AIS и функции LCK. Чтобы отключить статус trap AIS и LCK, воспользуйтесь формой **no** этой команды.

snmp-server enable traps cfm [ais] [lck]
no snmp-server enable traps cfm [ais] [lck]

Параметры

ais	(Опционально.) Укажите статус trap AIS, который необходимо настроить. Если статус trap AIS запущен, при появлении или удалении события ETH-AIS будет отправлено trap-сообщение.
lck	(Опционально.) Укажите статус trap LCK, который необходимо настроить. Если статус trap LCK запущен, при появлении или удалении события ETH-LCK будет отправлено trap-сообщение.

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 глобальной настройки статуса trap функции ITU Y.1731. Если значение не задано, будут установлены статусы trap AIS и LCK. Используйте команду **show cfm**, чтобы отобразить статус trap ITU Y.1731.

Пример

В данном примере показано, как запустить статус trap AIS.

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

14.28 lm enable

Данная команда используется для запуска функции LM (Loss Measurement) ITU Y.1731. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

lm enable
no lm enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

CFM MEP Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для включения/отключения функции LM. Когда функция Frame Loss Measurement запущена на MEP от имени администратора, MEP поддерживает счетчики функции Frame Loss Measurement и может отвечать на сообщения LMR, получая сообщения LMM.

Пример

В данном примере показано, как запустить функцию LM.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)#lm enable
Switch(config-cfm-mep)#
```

14.29 cfm lm test

Данная команда используется для запуска теста LM на MEP.

cfm lm test *MAC-ADDR* **mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* [**period** *PERIOD*] [**pdu-priority** *COS-VALUE*]

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID.
name <i>MA-NAME</i>	Укажите имя MA.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальное количество символов – 22.
period <i>PERIOD</i>	(Опционально.) Укажите интервал передачи LM PDU: 100 мс, 1 с или 10 с. Интервал по умолчанию – 1 с.
pdu-priority <i>COS-VALUE</i>	(Опционально.) Установите приоритет 802.1p в сообщениях LMM, передаваемых при помощи MEP. Значение по умолчанию – приоритет PDU MEP.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для запуска теста LM на MEP. MEP будет периодически отправлять сообщения LMM на удаленную MEP. Система рассчитывает дальний и ближний FLR (Frame Loss Ratio – коэффициент потери кадров), основанный на полученных сообщениях LMR.

Пользователь может прервать тест Frame Loss Measurement, отключив функцию Frame Loss Measurement на MEP.

При использовании функции Frame Loss Measurement необходимо учитывать ограничения счетчиков.

- Подсчет невозможен в общем (MP-t-MP) Ethernet-соединении устройств, неизвестных одноадресных кадров, широковещательных и многоадресных кадров, передаваемых от удаленной MEP на up MEP, или от down MEP на удаленную MEP.
- Невозможно подсчитать PDU протокола, обрабатываемого при помощи ПО устройства.
- Использование функций ETH-LM/ETH-DM провоцирует расход ресурсов ACL устройства, что необходимо учитывать при запуске функций ETH-LM/ETH-DM, когда количество MEP слишком велико.

Пример

В данном примере показано, как запустить тест LM.

```
Switch# cfm lm test 00-01-02-03-04-05 mepid 1 ma name opl domain op-domain period 1sec pdu-  
priority 7  
Switch#
```

14.30 show cfm lm

Данная команда используется для отображения информации об LM.

show cfm lm [mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME]

Параметры

mepid MEP-ID	(Опционально.) Укажите MEP ID.
name MA-NAME	(Опционально.) Укажите имя MA.
domain DOMAIN-NAME	(Опционально.) Укажите имя MD. Максимальное количество символов – 22.

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 LM. Если параметры не заданы, будет отображена вся информация.

Пример

В данном примере показано, как отобразить информацию об LM.

```
S Switch#show cfm lm mepid 1 ma name op1 domain op-domain
MEP ID: 1
MA Name: op1
Domain Name: op-domain
State: Enabled
LMM Transmitted : 61
LMR Received    : 0
LMM Received    : 0
LMR Transmitted : 0

ID  MAC Address      Status  Period  Pri  Far-End  Near-End  Start Time
---  -
1   00-01-02-03-04-05 Failed  1sec    2    0        0        2000-02-02 23:23:06

Switch#
```

14.31 clear cfm lm

Данная команда используется для удаления информации о функции LM.

clear cfm lm {mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME [result | statistics] | all}

Параметры

mepid MEP-ID	Укажите MEP ID.
name MA-NAME	Укажите имя MA.
domain DOMAIN-NAME	Укажите имя MD. Максимальное количество символов – 22.
result	(Опционально.) Укажите, чтобы удалить результаты LM.

statistics	(Опционально.) Укажите, чтобы очистить статистику кадров ETH-LM (LMM и LMR).
all	Укажите, чтобы удалить информацию о CFM LM для всех MEP.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для удаления информации о функции LM.

Пример

В данном примере показано, как удалить информацию о функции LM.

```
Switch#clear cfm lm mepid 1 ma name op1 domain op-domain
Switch#
```

14.32 dm enable

Данная команда используется для запуска функции DM (Delay Measurement) кадра ITU Y.1731. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

dm enable
no dm enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

CFM MEP Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для включения/отключения функции DM. Когда функция Frame Delay

Measurement запущена на MEP от имени администратора, MEP может генерировать информацию по временным меткам, а также отвечать на сообщения DMR, получая сообщения DMM.

Пример

В данном примере показано, как запустить функцию DM.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#cfm mep mepid 1 ma name opl domain op-domain
Switch(config-cfm-mep)#dm enable
Switch(config-cfm-mep)#
```

14.33 cfm dm test

Данная команда используется для запуска теста DM.

cfm dm test *MAC-ADDR mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME*
[period-interval SELECTION] [percentile NUMBER] [pdu-priority COS-VALUE]

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID.
name <i>MA-NAME</i>	Укажите имя MA.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальное количество символов – 22.
period-interval <i>SELECTION</i>	(Опционально.) Укажите интервал отправки сообщений DDM и интервал диагностики: 100ms-1sec: интервал отправки – 100 миллисекунд, интервал диагностики – 1 секунда. 1sec-10sec: интервал отправки – 1 секунда, интервал диагностики – 10 секунд (значения по умолчанию). 10sec-1min: интервал передачи – 10 секунд, интервал диагностики – 1 минута.
percentile <i>NUMBER</i>	(Опционально.) Укажите процентиль измерений FD (Frame Delay) и FDV (Frame Delay Variation). Диапазон значений: от 0 до 100. Значение по умолчанию – 75.
pdu-priority <i>COS-VALUE</i>	(Опционально.) Установите приоритет 802.1p в сообщениях DMM, передаваемых при помощи MEP. Значение по умолчанию – приоритет PDU MEP.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для запуска теста DM на MEP. MEP периодически будет отправлять сообщения DMM на удаленную MEP в пределах диагностического интервала. Система вычислит FD и FDV на основе полученных сообщений DMR и процентиля теста DM. Чтобы рассчитать FDV, необходимы непрерывно получаемые кадры DMR. Пользователь может прервать тест Frame Delay Measurement, отключив функцию Frame Delay Measurement на MEP.

Пример

В данном примере показан процесс запуска теста LM.

```
Switch# cfm dm test 00-84-57-00-00-00 mepid 1 ma name opl domain op-domain period-interval  
1sec-10sec percentile 75 pdu-priority 7  
Switch#
```

14.34 show cfm dm

Данная команда используется для отображения информации о DM.

show cfm dm [mepid MEP-ID ma name MA-NAME domain DOMAIN-NAME]

Параметры

mepid MEP-ID	(Опционально.) Укажите MEP ID.
name MA-NAME	(Опционально.) Укажите имя MA.
domain DOMAIN-NAME	(Опционально.) Укажите имя MD. Максимальное количество символов – 22.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о DM на MEP. Если параметры не заданы, будет отображена вся информация.

Максимальное количество результатов Frame Delay Measurement, которое может храниться на устройстве – 128.

Пример

В данном примере показано, как отобразить информацию о DM.

```
Switch#show cfm dm mepid 1 ma name opl domain op-domain

MEP ID: 1
MA Name: opl
Domain Name: op-domain
State: Enabled
DMM Transmitted : 11
DMR Received    : 0
DMM Received    : 0
DMR Transmitted : 0

ID  MAC Address      Status  Period Pri Far-End Near-End Start Time
---  -
1   00-84-57-00-00-00 RUNNING 1s:10s 75 7 0 0 2000-11-03
                                10:44

Switch#
```

14.35 clear cfm dm

Данная команда используется для удаления информации о функции DM.

clear cfm dm {mepid *MEP-ID* ma name *MA-NAME* domain *DOMAIN-NAME* [result | statistics] | all}

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID.
name <i>MA-NAME</i>	Укажите имя MA.
domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальное количество символов – 22.
result	(Опционально.) Укажите, чтобы удалить результаты DM.
statistics	(Опционально.) Укажите, чтобы очистить статистику кадров ETH-DM (DMM и DMR).
all	(Опционально.) Укажите, чтобы удалить информацию CFM DM для всех MEP.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для удаления информации о функции DM.

Пример

В данном примере показано, как удалить информацию о функции DM.

```
Switch#clear cfm dm mepid 1 ma name op1 domain op-domain
Switch#
Switch#show cfm dm mepid 1 ma name op1 domain op-domain
```

14.36 show cfm

Данная команда используется для отображения общего состояния CFM.

show cfm

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения общего состояния CFM.

Пример

В данном примере показано, как отобразить общее состояние CFM.

```
Switch#show cfm

CFM State: Enabled
AIS Trap State: Disabled
LCK Trap State: Disabled
Domain Name: op-domain Level: 2

Switch#
```

14.37 show cfm domain

Данная команда используется для отображения информации о домене технического обслуживания CFM.

show cfm domain *DOMAIN-NAME*

Параметры

<i>DOMAIN-NAME</i>	Укажите имя домена технического обслуживания. Максимальное количество символов – 22.
--------------------	--

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о домене технического обслуживания CFM.

Пример

В данном примере показано, как отобразить информацию о домене технического обслуживания CFM.

```
Switch#show cfm domain op-domain

Domain Name: op-domain
Domain Level: 2
MIP Creation: Auto
SenderID TLV: Chassis
MA Name: op1

Switch#
```

14.38 show cfm ma

Данная команда используется для отображения информации о CFM MA.

show cfm ma name *MA-NAME* **domain** *DOMAIN-NAME*

Параметры

name <i>MA-NAME</i>	Укажите имя MA.
----------------------------	-----------------

domain <i>DOMAIN-NAME</i>	Укажите имя MD. Максимальное количество символов – 22.
----------------------------------	--

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 ассоциации технического обслуживания CFM.

Пример

В данном примере показано, как отобразить информацию об ассоциации технического обслуживания CFM.

```
Switch#show cfm ma name op1 domain op-domain

MA Name: op1
MA Mode: Software
MA VID: 2
MIP Creation: Auto
CCM Interval: 10 seconds
SenderID TLV: Chassis
MEPID List  : 1-2
    MEPID: 1 Port: 1/0/1 Direction: Up

Switch#
```

Отображаемые параметры

MEPID	MEP, уже созданная в МА.
Port	Порт MEP.
Direction	Направление MEP (Up или Down).

14.39 show cfm mep

Данная команда используется для отображения информации о MEP.

show cfm mepid *MEP-ID* ma name *MA-NAME* domain *DOMAIN-NAME*

Параметры

mepid <i>MEP-ID</i>	Укажите MEP ID. Диапазон значений: от 1 до 8191.
name <i>MA-NAME</i>	Укажите имя МА.

domain DOMAIN-NAME Укажите имя MD. Максимальное количество символов – 22.

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 MEP.

Пример

В данном примере показано, как отобразить информацию о MEP.

```
Switch#show cfm mepid 1 ma name op1 domain op-domain

MA Mode: Hardware
Port: 2/0/2
Direction: Up
CFM Port Status: Disabled
MAC Address: 00-11-22-33-44-68
MEP State: Disabled
CCM State: Enabled
PDU Priority: 2
Fault Alarm: All
Alarm Time: 250 centisecond((1/100)s)
Alarm Reset Time: 1000 centisecond((1/100)s)
AIS State: Disabled
AIS Period: 1 Second
AIS Client Level: Invalid
AIS Status: Not Detected
LCK State: Disabled
LCK Period: 1 Second
LCK Client Level: Invalid
LCK Status: Not Detected
LCK Action: Stop
Out-of-Sequence CCMs Received: 0
Cross-connect CCMs: 0
Error CCMs Received: 0
Port Status CCMs Received: 0
CCMs transmitted: 0
Out-of-order LBRs Received: 0
Unexpected LTRs Received: 0
AIS PDUs Received: 0
LCK PDUs Received: 0
Normal CCMs Received: 0
If Status CCMs Received: 0
In-order LBRs Received: 0
Next LTM Trans ID: 1
LBMs Transmitted: 0
AIS PDUs Transmitted: 0
LCK PDUs Transmitted: 0
Switch#
```

Отображаемые параметры

Highest Fault	На данной MEP обнаружена неисправность высокого приоритета. Будет отображен один из нижеперечисленных параметров: None: неисправности отсутствуют с момента последнего состояния FNG_RESET. Some Remote MEP Defect Indication: согласно последнему CCM, полученному данной MEP от одной из удаленных MEP, удаленная MEP обнаружила неисправность. Some Remote MEP MAC Status Error: согласно последнему CCM, полученному данной MEP, ассоциированный MAC удаленной MEP сообщает о наличии ошибки. Some Remote MEP Down: данная MEP не получает CCM от других MEP из списка конфигурации. Error CCM Received: данная MEP получает неверные CCM, что может быть вызвано ошибкой конфигурации. Cross-connect CCM Received: CCM, которые получает MEP, могут принадлежать другой MA.
Fault Alarm	На данной MEP настроена система оповещения о неисправностях. Будет отображен один из нижеперечисленных параметров: All: в настройках системы оповещения о неисправностях выбран режим «all». MAC Status: в настройках системы оповещения о неисправностях выбран режим «mac-status». Remote CCM: в настройках системы оповещения о неисправностях выбран режим «remote-ccm». Error CCM: в настройках системы оповещения о неисправностях выбран режим «error-ccm». Xcon CCM: в настройках системы оповещения о неисправностях выбран режим «xcon-ccm». None: в настройках системы оповещения о неисправностях выбран режим «none».

14.40 show cfm interface

Данная команда используется для отображения информации о CFM на указанном физическом интерфейсе.

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

Параметры

interface INTERFACE-ID	(Опционально.) Укажите ID интерфейса для отображения. Применимо только для физических интерфейсов.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы

до и после запятой недопустимы.

- (Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о CFM на указанных физических портах.

Пример

В данном примере показано, как отобразить информацию о CFM на указанных физических портах.

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

eth1/0/1
CFM is enabled
MAC Address: F0-7D-68-10-21-30

Domain Name: op-domain
Level: 2
MA Name: op1
VID: 2
MEPID: 1
Direction: Up

Switch#
```

14.41 show cfm remote-mep

Данная команда используется для отображения информации об удаленных MEP.

show cfm remote-mep mepid LOCAL-MEP-ID ma name MA-NAME domain DOMAIN-NAME
[remote-mepid REMOTE-MEPID]

Параметры

mepid LOCAL-MEP-ID	Укажите MEP ID.
name MA-NAME	Укажите имя MA.
domain DOMAIN-NAME	Укажите имя MD. Максимальное количество символов – 22 символа.

remote-mepid *REMOTE-* (Опционально.) Укажите ID удаленной MEP. Диапазон значений: от 1 до 8191. Если значение не задано, будут отображены все удаленные MEP.

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 удаленных MEP.

Пример

В данном примере показано, как отобразить информацию об удаленной MEP, доступную локальной MEP 1.

```
Switch#show cfm remote-mep mepid 1 ma name op1 domain op-domain

Remote MEPID: 2
MAC Address: FF-FF-FF-FF-FF-FF
Status: OK                      RDI: Yes
Port State: Up                  Interface Status: No
Last CCM Serial Number: 1000
Sender Chassis ID: None
Sender Management Address: SNMP-UDP-IPv4 10.90.90.90:161
Detect Time: 2000-02-02 23:21:38

Remote MEPID: 3
MAC Address: 11-22-33-44-02-05
Status: OK                      RDI: Yes
Port State: Up                  Interface Status: No
Last CCM Serial Number: 200
Sender Chassis ID: None
Sender Management Address: SNMP-UDP-IPv4 10.90.90.90:161
Detect Time: 2010-11-01 17:00:00

Switch#
```

В примере ниже показано, как отобразить информацию об удаленной MEP.

```
Switch# show cfm remote-mep mepid 1 ma name op-ma domain op-domain remote-mepid 2
Remote MEPID: 2
MAC Address: FF-FF-FF-FF-FF-FF
Status: OK RDI: Yes
Port State: Up Interface Status: No
Last CCM Serial Number: 1000
Sender Chassis ID: None
Sender Management Address: SNMP-UDP-IPv4 10.90.90.90:161
Detect Time: 2000-02-02 23:21:38
Switch#
```

Отображаемые параметры

Status	Отображает режим работы диаграммы состояний удаленной MEP: IDLE : выполняется перезапуск. START : таймер не истек с момента перезапуска диаграммы состояний и теперь является недействительным. CCM получен. FAILED : таймер истек с момента получения действительного CCM или с момента перезапуска диаграммы состояний. OK : действительный CCM получен до момента истечения таймера.
RDI	Отображает наличие/отсутствие бита RDI в последнем полученном CCM: Yes : бит RDI установлен. No : бит RDI удален / действительные CCM не получены.
Port State	Указывает, может ли порт моста, на котором находится удаленная MEP, пропускать простые данные независимо от статуса MAC: None : CCM не получен / в последнем полученном CCM отсутствует TLV статуса порта. Blocked : простые данные не могут свободно поступать через порт, на котором присутствует удаленная MEP. Up : простые данные могут свободно поступать через порт, на котором присутствует удаленная MEP.

14.42 show cfm mep fault

Данная команда используется для отображения MEP, у которых обнаружены неисправности.

show cfm mep fault

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для получения сведений о состоянии отказа MEP. Команда отображает все неисправности, обнаруженные на MEP.

Пример

В данном примере показано, как отобразить MEP, имеющие неисправности.

```
Switch# show cfm mep fault

Domain Name: md5
MA Name: ma5
MEPID: 2
AIS Status: Normal
LCK Status: Normal

Domain Name: md6
MA Name: ma6
MEPID: 3
AIS Status: Normal
LCK Status: Normal

Switch#
```

Отображаемые параметры

Status	На MEP обнаружена неисправность высокого приоритета, будет отображен один из нижеперечисленных параметров: None: неисправности отсутствуют с момента последнего состояния FNG_RESET. Some Remote MEP Defect Indication: согласно последнему CCM, полученному данной MEP от одной из удаленных MEP, удаленная MEP обнаружила неисправность. Some Remote MEP MAC Status Error: согласно последнему CCM, полученному данной MEP, ассоциированный MAC удаленной MEP сообщает о состоянии отказа. Some Remote MEP Down: данная MEP не получает CCM от других MEP из списка конфигурации. Error CCM Received: данная MEP получает неисправные CCM, что может быть вызвано ошибкой конфигурации. Cross-connect CCM Received: CCM, которые получает MEP, могут принадлежать другой MA.
AIS Status	AIS Detected: AIS PDU получены. Normal: AIS PDU не получены.
LCK Status	LCK Detected: LCK PDU получены. Normal: LCK PDU не получены.

14.43 show cfm mip ccm

Данная команда используется для отображения записей базы данных MIP CCM.

show cfm mip ccm

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения записей базы данных MIP CCM.

Пример

В данном примере показано, как отобразить записи базы данных MIP CCM.

```
Switch# show cfm mip ccm

VID: 10
MAC Address: 00-07-00-00-00-1C
Port: eth1/0/12

VID: 10
MAC Address: 00-07-00-00-00-1E
Port: eth1/0/14
Total: 2

Switch#
```

14.44 show cfm pkt-cnt interface

Данная команда используется для отображения счетчиков RX/TX пакетов CFM указанного физического интерфейса.

show cfm pkt-cnt interface [INTERFACE-ID [, | -]] [rx] [tx]

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса для отображения. Применимо только для физических интерфейсов.
--------------	--

,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
rx	(Опционально.) Используется для обозначения счетчиков RX указанного физического интерфейса.
tx	(Опционально.) Используется для обозначения счетчиков TX указанного физического интерфейса.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения счетчиков пакета физического интерфейса. Если интерфейсы не указаны, будут отображены счетчики всех интерфейсов. Если указан только физический интерфейс, будут отображены счетчики пакетов RX и TX. Если указан только тип RX или TX, будут отображены счетчики пакета RX или TX всех физических интерфейсов.

Пример

В данном примере показано, как отобразить счетчики пакета на интерфейсе Ethernet 1/0/1.

```
Switch#show cfm pkt-cnt interface ethernet eth1/0/1

eth1/0/1
  CFM RX Statistics
    AllPkt:0 CCM:0
    LBR:0 LBM:0
    LTR:0 LTM:0
    VidDrop:0 OpcoDrop:0

  CFM TX Statistics
    AllPkt:0 CCM:0
    LBR:0 LBM:0
    LTR:0 LTM:0

Switch#
```

В примере ниже показано, как отобразить счетчики пакета RX на интерфейсе Ethernet 2/0/1.

```
Switch#show cfm pkt-cnt interface ethernet eth2/0/1 rx

eth2/0/1
  CFM RX Statistics
    AllPkt:0          CCM:0
    LBR:0             LBM:0
    LTR:0             LTM:0
    VidDrop:0         OpcoDrop:0

Switch#
```

В следующем примере показано, как отобразить счетчики пакета TX на интерфейсе Ethernet 2/0/1.

```
Switch#show cfm pkt-cnt interface ethernet eth2/0/1 tx

eth2/0/1
  CFM TX Statistics
    AllPkt:0          CCM:0
    LBR:0             LBM:0
    LTR:0             LTM:0

Switch#
```

Отображаемые параметры

VidDrop	Пакеты отбрасываются из VLAN.
OpcoDrop	Пакеты отбрасываются при несоответствии нормальному op-code.

14.45 clear cfm pkt-cnt interface

Данная команда используется для сброса счетчиков RX/TX пакета CFM указанного физического интерфейса.

clear cfm pkt-cnt interface {*INTERFACE-ID* [, | -] | all} [rx] [tx]

Параметры

<i>INTERFACE-ID</i>	Укажите ID интерфейса, который необходимо удалить. Применимо только для физических интерфейсов.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
all	Укажите, чтобы сбросить все счетчики CFM интерфейса.
rx	(Опционально.) Используется для обозначения счетчиков RX указанного физического интерфейса.

tx (Опционально.) Используется для обозначения счетчиков TX указанного физического интерфейса.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для сброса счетчиков пакета физического интерфейса. Если указан только физический интерфейс, будут сброшены счетчики пакетов RX и TX указанного физического интерфейса. Если указаны физический интерфейс и тип RX/TX, будут сброшены счетчики пакета RX или TX указанного физического интерфейса.

Пример

В данном примере показано, как сбросить счетчики пакета TX на интерфейсе Ethernet 1/0/1.

```
Switch# clear cfm pkt-cnt interface ethernet eth1/0/1 tx
Switch#
```

14.46 cfm mp-ltr-all

Данная команда используется для настройки всех MP таким образом, чтобы они отвечали сообщением LTR. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

cfm mp-ltr-all
no cfm mp-ltr-all

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

В соответствии с IEEE 802.1ag мост отправляет LTR в ответ на LTM. Используйте данную команду, чтобы все MP на канале перенаправления LTM отправляли LTR, вне зависимости от того, находятся ли они на том же мосту.

Пример

В данном примере показано, как запустить данную функцию.

```
Switch# configure terminal
Switch(config)# cfm mp-ltr-all
Switch(config)#
```

14.47 show cfm mp-ltr-all

Данная команда используется для отображения конфигурации ответов MP на LTR.

show cfm mp-ltr-all

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения конфигурации ответов MP на LTR.

Пример

В данном примере показано, как отобразить конфигурацию ответов MP на LTR.

```
Switch# show cfm mp-ltr-all

All MPs reply LTRs: Disabled

Switch#
```

15. Команды CPU Access Control List (ACL)

15.1 soft-acl filter-map

Данная команда позволяет создать или изменить программные списки 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). 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 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 управления доступом (software ACL filter map) под именем «cpu_filter».

```
Switch# configure terminal
Switch(config)# soft-acl filter-map cpu_filter
Switch(config-soft-acl)#
```

15.2 match access-group

Данная команда используется для привязки списка доступа к программному списку управления доступом (software ACL filter map). Чтобы удалить привязку, 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} 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	Указывает имя списка доступа ACL, которое должно совпадать.

По умолчанию

Нет.

Режим ввода команды

Software ACL Filter Map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для привязки списка доступа к программному списку управления доступом (software ACL filter map). К одному программному списку могут быть привязаны несколько списков доступа, при условии что они относятся к разным типам (expert, MAC, IP и IPv6). В случае привязки списков доступа одинакового типа каждая последующая команда перезаписывает предыдущую.

Порядковые номера определяют приоритет обработки связанного списка доступа в filter map. Список доступа с меньшим порядковым номером обладает более высоким приоритетом. Связанные списки доступа с одинаковым порядковым номером обрабатываются в следующем порядке: список доступа expert, список доступа MAC, список доступа IP, список доступа IPv6.

Пример

В данном примере показано, как привязать список доступа IP с именем «cpu-acl» и список доступа MAC с именем mac4001 к программному списку управления доступом (software ACL filter map) «cpu_filter».

```
Switch# configure terminal
Switch(config)# ip access-list cpu-acl
Switch(config-ip-acl)# permit 10.20.0.0 255.255.0.0
Switch(config-ip-acl)# exit
Switch(config)# mac access-list extended mac4001
Switch(config-mac-ext-acl)# 25 deny host 0013.0049.8272 any
Switch(config-mac-ext-acl)# exit
Switch(config)# soft-acl filter-map cpu_filter
Switch(config-soft-acl)# 2 match ip access-group cpu-acl
Switch(config-soft-acl)# 3 match mac access-group mac4001
Switch(config-soft-acl)#
```


15.3 match interface

Данная команда используется для настройки соответствующих входных интерфейсов (ingress interface). Чтобы удалить соответствующие входные интерфейсы, воспользуйтесь формой **no** этой команды.

```
match interface INTERFACE-ID [, | -]  
no match interface {all | INTERFACE-ID [, | -]}
```

Параметры

INTERFACE-ID	Укажите соответствующий идентификатор интерфейса (Interface ID). Допустимы 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.
all	Укажите 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. Другими словами, если совместимый интерфейс не настроен, программный список не вступит в силу.

Когда пакет принимается ЦПУ, а 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. Когда совпадение будет обнаружено, другие списки доступа будут проигнорированы. В противном случае, будет выполняться поиск списка доступа со следующим наивысшим приоритетом и так далее.

Внутри списка доступа используется похожая проверка номеров. Правило с меньшим порядковым номером получает более высокий приоритет. 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. Когда интерфейс настраивается для нового программного списка, он будет удален из предыдущего списка.

Пример

В данном примере показано, как настроить совместимый интерфейс Ethernet 1/0/1 для программного списка управления доступом (software ACL filter map) «cpu_filter».

```
Switch# configure terminal
Switch(config)# ip access-list cpu-acl
Switch(config-ip-acl)# permit 10.20.0.0 0.0.255.255
Switch(config-ip-acl)# exit
Switch(config)# mac access-list extended mac4001
Switch(config-mac-ext-acl)# 25 deny host 0013.0049.8272 any
Switch(config-mac-ext-acl)# exit
Switch(config)# soft-acl filter-map cpu_filter
Switch(config-soft-acl)# 2 match ip access-group cpu-acl
Switch(config-soft-acl)# 3 match mac access-group mac4001
Switch(config-soft-acl)# match interface ethernet 1/0/1
Switch(config-soft-acl)#
```

15.4 show soft-acl

Данная команда используется для отображения информации о 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.

```
Switch# show soft-acl filter-map

Software ACL Filter Map
  cpu_filter:
Match Access-list(s):
  IP(2): Ext-ip
  MAC(3):mac4001
Match Ingress Interface(s):
  eth1/0/1

Switch#
```

Отображаемые параметры

IP(N)	Тип списка доступа. Число в скобках означает порядковый номер связанного списка доступа.
--------------	--

16. Команды Debug

16.1 debug enable

Данная команда используется для включения функции вывода сообщения отладки (Debug). Чтобы отключить данную функцию, 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 для включения функции вывода сообщения отладки (Debug).

Пример

В данном примере показано, как включить/отключить функцию вывода сообщения отладки (Debug).

```
Switch#configure terminal
Switch(config)#debug enable
Switch(config)#no debug enable
Switch(config)#
```

16.2 debug output

Используйте данную команду, чтобы обозначить индивидуальные модули, для которых необходимо вывести сообщение отладки (Debug). Для отключения данной функции воспользуйтесь формой **no** этой команды.

debug output {module MODULE-LIST | all} {buffer | console}
no debug output {module MODULE-LIST | all}

Параметры

MODULE-LIST	Укажите список модулей, для которых необходимо вывести сообщение отладки (Debug). Для отделения названий модулей используйте пробелы.
-------------	---

all	Укажите, чтобы вывести сообщение отладки (Debug) всех модулей в указанный пункт назначения.
buffer	Укажите, чтобы вывести сообщение отладки (Debug) в буфер отладки.
console	Укажите, чтобы вывести сообщение отладки (Debug) на локальную консоль.

По умолчанию

По умолчанию сообщение отладки (Debug) выводится в буфер.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду для вывода сообщения отладки (Debug) указанного модуля в буфер или на локальную консоль. Используйте команду **debug show output** для отображения информации о строке модуля. По умолчанию сообщение отладки (Debug) модуля выводится в буфер отладки. Для вывода сообщения отладки (Debug) модуля необходимо запустить настройки отладки модуля, а также запустить команду отладки (Debug) в общем режиме.

Пример

В данном примере показано, как вывести все сообщения отладки (Debug) модуля в буфер отладки.

```
Switch# debug output all buffer
Switch#
```

16.3 debug 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.
-------------------	--

LOCATION	Укажите адрес IPv4 или IPv6 TFTP-сервера.
----------	---

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

Пример

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

```
Switch# debug copy buffer tftp: //10.90.90.99/abc.txt

Address of remote host [10.90.90.99]?
Destination filename [abc.txt]?
  Accessing tftp://10.90.90.99/abc.txt...
Transmission starts...
Finished network upload(65739) bytes.

Switch#
```

16.4 debug clear buffer

Данная команда используется для очистки буфера отладки.

debug clear buffer

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду для очистки буфера отладки.

Пример

В данном примере показано, как очистить буфер отладки.

```
Switch# debug clear buffer
Switch#
```

16.5 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#
```

16.6 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 параметры не указаны, будет отображено содержимое буфера.

Пример

В данном примере показано, как отобразить данные буфера отладки.

```
Switch# debug show buffer

Debug buffer is empty

Switch#
```

В примере ниже 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#
```

16.7 debug show output

Данная команда используется для отображения статуса отладки и вывода информации о модулях.

debug show output

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду для отображения информации о выводе статуса отладки и сообщения отладки (Debug) модулей.

Пример

В данном примере показано, как отобразить информацию о выводе сообщения отладки (Debug) модулей.

```
Switch#debug show output

Debug Global State : Disabled

Module name      Output      Enabled
-----
MSTP             buffer      No
VRRP             buffer      No
RIPNG            buffer      No

Switch#
```

16.8 debug show error-log

Данная команда используется для отображения данных журнала регистрации ошибок.

debug show error-log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Любой режим конфигурирования.

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 : 2022/03/11 13:00:00
===== SOFTWARE FATAL ERROR =====
Invalid mutex handle : 806D6480

Current TASK : bcmARL.0
----- TASK STACKTRACE -----
->802ACE98
->8018C814
->8028FF44
->8028352C
->801D703C
->8013B8A4
->802AE754
->802A5E0C
->802A5D6C

*****
# debug log: 2
# level: fatal
# clock: 10000ms
# time : 2022/03/11 15:00:00
===== SOFTWARE FATAL ERROR =====
CLI_UTL_AllocateMemory Fail!

Current TASK : CLI
----- TASK STACKTRACE -----
->802ACE98
->802B4498
->802B4B00
->802BD140
->802BCB08

Total Log : 2

Switch#
```

16.9 debug show tech-support

Данная команда используется для отображения информации, запрашиваемой техническим персоналом.

debug show tech-support

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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

Пример

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

```
Switch#debug show tech-support

***** show version *****

Device MAC Address: 00:11:22:33:44:55
System MAC Address: 00:11:22:33:44:55

Unit ID  Module Name          Versions
-----  -
2        DMS-3130-30PS              H/W:A1
                                           Bootloader:1.00.003
                                           Runtime:1.01.006

***** show fpsysinfo *****
System Description..... DMS-3130-30PS - 16*2.5GE PoE AT , 8*5GE PoE BT
+ 2*10GBASE-T + 4*25G SFP28
System Name..... Switch
System Location.....
System Contact.....
System Object ID..... 1.3.6.1.4.1.171.10.176.2.1
System Up Time..... 0 days 0 hrs 13 mins 32 secs
Current SNTP Synchronized Time..... SNTP Client Mode Is Disabled
```

16.10 debug show cpu

Данная команда используется для отображения информации о загрузке ЦПУ.

debug show cpu [utilization | counter | port | tasks]

Параметры

<i>counter</i>	Укажите, чтобы отобразить счетчики Tx/Rx ЦПУ.
<i>port</i>	Укажите, чтобы отобразить статистику порта ЦПУ.
<i>tasks</i>	Укажите, чтобы сбросить все задачи.
<i>utilization</i>	Укажите, чтобы отобразить информацию о загрузке ЦПУ.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду для отображения информации о загрузке ЦПУ и связанных с ним задачах или информации о порте.

Пример

В данном примере показано, как отобразить информацию о загрузке ЦПУ.

```
Switch#debug show cpu utilization
```

CPU Utilization:

PID	Name	5 Secs	60 Secs	300 Secs
929	LOG	0.00%	0.00%	0.00%
930	attackLog	0.00%	0.00%	0.00%
931	procLOG	0.00%	0.00%	0.00%
932	EmailAlert	0.00%	0.00%	0.00%
933	LogUSB	0.00%	0.00%	0.00%
934	osapiTimer	0.58%	0.50%	0.50%
935	bcmDPC	0.00%	0.00%	0.00%
936	bcmINTR	0.00%	0.01%	0.02%
937	socdmadesc.0	0.19%	0.22%	0.22%
939	bcmL2X.0	7.73%	7.57%	7.62%
940	bcmCNTR.0	1.35%	1.63%	1.66%
941	bcmTX	0.00%	0.00%	0.00%
942	bcmXGS3AsyncTX	0.00%	0.00%	0.00%

--More-- or (q)uit (a)ll

16.11 debug show temperature

Данная команда используется для отображения информации о температуре ЦПУ/СНК.

debug show temperature

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Любой режим конфигурирования.

Использование команды

Используйте данную команду для отображения информации о температуре ЦПУ/СНК.

Функция Prompt

Нет.

Пример

В данном примере показано, как отобразить информацию о температуре ЦПУ/СНК.

```
switch#debug show temperature
```

Unit	Descr	Current
Temperature		

1	SOC0	83C

17. Команды DHCP Auto-Configuration

17.1 autoconfig enable

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

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 12.

Использование команды

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

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

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

Пример

В данном примере показано, как включить автоконфигурацию.

```
Switch#configure terminal
Switch(config)#autoconfig enable
Warning:Autoconfig enabled on VLAN 1 now, but won't take effect until reboot.
Switch(config)#
```

17.2 show autoconfig

Данная команда используется для отображения статуса автоконфигурации.

show autoconfig

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статус автоконфигурации.

Пример

В данном примере показано, как отобразить статус автоконфигурации.

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


18. Команды DHCP Client

18.1 ip dhcp client class-id

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

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

Параметры

<i>STRING</i>	Укажите Vendor Class Identifier в формате строки. Максимальное количество символов – 32.
hex <i>HEX-STRING</i>	Укажите Vendor Class Identifier в шестнадцатеричном формате. Максимальное количество символов – 64.

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 указания 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. Настроенное значение – VOIP-Device для VLAN 100.

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

18.2 ip dhcp client client-id

Данная команда используется для указания VLAN-интерфейса, шестнадцатеричный MAC-адрес которого будет использован в качестве ID клиента и отправлен в сообщении Discover. Чтобы вернуться 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 VLAN-интерфейс, 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 указанного 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 DHCP-клиент, который может получить IP-адрес от DHCP-сервера. Идентификатором клиента может быть назначен один интерфейс.

Пример

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

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

18.3 ip dhcp client hostname

Данная команда используется, 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. Максимальное количество символов – 64. 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. Функция работает, когда на интерфейсе включен DHCP-клиент, который может получить IP адрес от DHCP-сервера. Если данная функция не настроена, коммутатор будет отправлять сообщения без Option 12.

Пример

В данном примере показано, как установить значение опции имени узла (host name). Указанное значение – Site-A-Switch.

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

18.4 ip dhcp client lease

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

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

Параметры

<i>DAYS</i>	Укажите продолжительность аренды в днях. Диапазон значений: от 0 до 10000 дней.
<i>HOURS</i>	(Опционально) Укажите продолжительность аренды в часах. Диапазон значений: от 0 до 23 часов.
<i>MINUTES</i>	(Опционально) Укажите продолжительность аренды в минутах. Диапазон значений: от 0 до 59 минут.

По умолчанию

Время аренды не запрашивается.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

19. Команды DHCP Relay

19.1 ip dhcp pool (DHCP Relay)

Данная команда используется для настройки пула DHCP Relay на DHCP Relay Agent, а также для входа в режим DHCP Pool Configuration Mode. Чтобы удалить пул DHCP Relay, воспользуйтесь формой **no** этой 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 при помощи 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.

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

Пример

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

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

19.2 ip dhcp relay information check

Данная команда используется, чтобы 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, как включить функцию Check DHCP Relay Agent глобально.

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

19.3 ip dhcp relay information check-reply

Данная команда используется для настройки в DHCP Relay Agent проверки информации Relay Agent Information Option (Option 82) в полученном пакете DHCP-ответа. Чтобы удалить данные настройки для интерфейса, воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима, если включен сервис DHCP.

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

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

Если проверка отключена, пакет будет передан напрямую.

Пример

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

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

19.4 ip dhcp relay information option

Данная команда используется, 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 {format | mac-format}
no ip dhcp relay information option {format | mac-format}

Параметры

format	Укажите формат строки DHCP relay information option.
mac-format	Укажите формат MAC-адреса, заданного пользователем в профиле Option 82.

По умолчанию

По умолчанию Option 82 не встроена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима, если включен сервис 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.

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

Пример

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

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

19.5 ip dhcp relay information option-insert

Данная команда используется для включения/отключения встраивания Option 82 для интерфейса в ретранслируемые пакеты DHCP-запроса. Чтобы удалить настройки данной функции для интерфейса, воспользуйтесь формой **no** этой команды.

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12

Использование команды

Данная команда применима, если включен сервис DHCP.

Пример

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

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

19.6 ip dhcp relay information policy

Данная команда используется, чтобы настроить алгоритм 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 применима, если включен сервис DHCP. Используйте команду для настройки общего алгоритма встраивания Option 82 в пакеты, у которых уже есть Option 82.

Пример

В данном примере показано, как настроить алгоритм перенаправления Relay Agent Option (Option 82) с помощью параметра **keep**. Если команда **ip dhcp relay information relay** сконфигурирована в режиме Global Configuration Mode, но не сконфигурирована в режиме Interface Configuration Mode, для всех интерфейсов применим режим Global Configuration Mode.

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

19.7 ip dhcp relay information policy-action

Данная команда используется, 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.

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 свидетельствует о том, что тип данного ID – Remote ID.

b. Длина: длина значения.

c. Значение: строка символов. Системное имя коммутатора.

expert-udf

Укажите, чтобы использовать expert-udf. Оригинальный формат Remote ID представлен ниже:

a.	b.	c.
2	n	User Defined
1 byte	1 byte	Max. 251 bytes

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

b. Длина: общая длина строки, задаваемой пользователем. По умолчанию длина равна 0, поле значений отсутствует.

c. Значение: универсальная задаваемая пользователем строка, настраиваемая при помощи данной команды, а также команды **ip dhcp relay information profile**. Максимальное количество символов – 251.

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 применяется 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)#
```

19.9 ip dhcp relay information option format-type remote-id

Данная команда используется для настройки sub-опции Remote ID DHCP как строки формата vendor в режиме Interface Configuration Mode. Чтобы удалить sub-опцию Remote ID как строку формата vendor, воспользуйтесь формой **no** этой команды.

ip dhcp relay information option format-type remote-id expert-udf NAME

no ip dhcp relay information option format-type remote-id

Параметры

expert-udf	Укажите Remote ID для конкретных портов, которые необходимо связать с указанным профилем Option 82. Максимально допустимое количество символов – 32.
NAME	Укажите имя профиля.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel. Используйте команду, чтобы настроить строку, определенную как vendor для sub-опции Remote ID Option 82 на интерфейсе.

Пример

В данном примере показано, как настроить строку формата expert UDF Remote ID для интерфейса Ethernet 1/0/1. В примере используется строка «switch1».

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ip dhcp relay information option format-type remote-id expert-udf switch1
Switch(config-if)#
```

19.10 ip dhcp relay information option format circuit-id

Данная команда используется для настройки sub-опции Circuit ID DHCP. Чтобы применить настройки по умолчанию, воспользуйтесь формой **no** этой команды.

ip dhcp relay information option format circuit-id {default | string SENTENCE | vendor1 | expert-udf}

no ip dhcp relay information option format circuit-id

Параметры

default

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

a.	b.	c.	d.	e.	f.	g.

1	0x6	0	4	VLAN	Module	Port
					ID	ID

1 byte	1 byte	1 byte	1 byte	2 bytes	1 byte	1 byte

a. 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.

SENTENCE

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

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

vendor1

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

a.	b.	c.	d.	e.	f.
1	0x10	0	6	VLAN	Slot ID
1 byte	1 byte	1 byte	1 byte	2 bytes	2 bytes

g.	h.	i.	j.
Port ID	1	6	MAC
2 bytes	1 byte	1 byte	6 bytes

a. 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.

expert-udf

Укажите, чтобы использовать expert-udf. Circuit ID задается пользователем в следующем формате:

a.	b.	c.

1	n	User defined

1 byte	1 byte	Max. 251 bytes

a. 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 данной команды, а также команды **ip dhcp relay information profile**. Максимальное количество символов – 251.

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 применяется для выбора различных vendor-ов или заданной пользователем строки ASCII в качестве Circuit ID.

Пример

В данном примере показано, как использовать vendor1 в качестве Circuit ID.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format circuit-id vendor1
Switch(config)#
```

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

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


19.11 ip dhcp relay information option format-type circuit-id

Данная команда используется для настройки sub-опции Circuit ID DHCP. Чтобы удалить sub-опцию Circuit ID, воспользуйтесь формой **no** этой команды.

ip dhcp relay information option format-type circuit-id expert-udf NAME
no ip dhcp relay information option format-type circuit-id

Параметры

expert-udf	Укажите Circuit ID для конкретных портов, которые необходимо связать с указанным профилем Option 82. Максимальное количество символов – 32.
NAME	Укажите имя профиля.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel. Используйте команду, чтобы настроить строку, определенную как vendor для sub-опции Circuit ID Option 82 на интерфейсе.

Пример

В данном примере показано, как настроить expert UDF Circuit ID для интерфейса Ethernet 1/0/1. В примере использован expert UDF Circuit ID «abc».

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ip dhcp relay information option format-type circuit-id expert-udf abc
Switch(config-if)#
```

19.12 ip dhcp relay information trust-all

Данная команда позволяет назначить на DHCP Relay Agent все интерфейсы, отправляющие информацию об IP DHCP Relay, доверенными. Чтобы отключить функцию 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. Информация Relay считается доверенной со всех интерфейсов, вне зависимости от настроек команды **ip dhcp relay information trusted**.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information trust-all
Switch(config)#
```

19.13 ip dhcp relay information trusted

Данная команда позволяет назначить на DHCP Relay Agent определенный интерфейс, отправляющий информацию об IP DHCP Relay, в качестве доверенного. Чтобы отключить функцию Trust для интерфейса, 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)#
```

19.14 ip dhcp local-relay vlan

Данная команда используется для включения Local Relay на одной из VLAN или группе VLAN. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

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

Параметры

<i>VLAN-ID</i>	Укажите используемую VLAN.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Local Relay обеспечивает передачу сообщения DHCP на все локальные 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)#
```

19.15 relay destination

Данная команда используется для указания IP-адреса назначения DHCP Relay, ассоциированного с Relay-пулом. Чтобы удалить Relay Destination из пула DHCP-Relay, воспользуйтесь формой **no** этой команды.

relay destination *IP-ADDRESS*
no relay destination *IP-ADDRESS*

Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес DHCP Relay Destination Server.
-------------------	---

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Наряду с пакетами DHCP Relay, подчиняющимися команде **ip helper-address**, Relay Destination

DHCP-сервера можно указать в пуле DHCP Relay. Для этого войдите в режим настройки пула DHCP при помощи команды **ip dhcp pool**, затем при помощи команды **relay source** укажите подсеть-источник (source) запросов клиента, после чего 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)#
```

19.16 relay source

Данная команда используется для указания подсети-источника (source) пакетов клиента. Чтобы удалить подсеть-источник (source), 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

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Наряду с пакетами DHCP relay, подчиняющимися команде **ip helper-address**, Relay Destination DHCP-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.

В пуле DHCP Relay администратор может далее использовать команды **class** и **relay target**, чтобы связать список адресов Relay Target с классом DHCP. DHCP-пакет не будет ретранслирован, если на интерфейсе, принимающем пакет, не настроен IP-адрес.

Пример

В данном примере показано, как создать пул DHCP Relay «pool2». В Relay-пуле подсеть 172.19.18.0/255.255.255.0 указана в качестве подсети-источника (source), а 10.2.1.10 указан в качестве адреса Relay Destination.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool2
Switch(config-dhcp-pool)# relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)# relay destination 10.2.1.10
Switch(config-dhcp-pool)#
```

19.17 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

В пуле DHCP Relay администратор может далее использовать команды **class** и **relay target**, чтобы связать список адресов Relay Target с классом DHCP. Если запрос клиента соответствует Relay-пулу, а пул DHCP Relay настроен с классами, для ретрансляции запрос клиента должен соответствовать классу, указанному в пуле. Если пакет не соответствует ни одному из классов пула, он не будет повторно ретранслирован. Если класс соответствующего Relay-пула не определен, запрос будет ретранслирован в Relay Destination соответствующего Relay-пула. Для класса можно указать несколько команд Relay Target. Если пакет соответствует классу, он будет направлен во все Relay Targets (Destination).

Если для класса не настроена команда **relay target**, за Relay Target будет принято Relay Destination, указанное для пула. DHCP-пакет не будет ретранслирован, если на интерфейсе, принимающем пакет, не настроен IP-адрес.

Пример

В данном примере показано, как настроить DHCP Relay Target для ретрансляции пакетов, которая соответствует образцу значений опции, установленной в классе.

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

19.18 show ip dhcp relay information trusted-sources

Данная команда используется для отображения всех интерфейсов, настроенных в качестве доверенных источников для опции DHCP Relay.

show ip dhcp relay information trusted-sources

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.
Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения рабочих настроек функции Trust Relay Option.

Пример

В данном примере показано, как отобразить список доверенных интерфейсов.

```
Switch# show ip dhcp relay information trusted-sources

List of trusted sources of relay agent information option:
vlan 100   vlan 200   vlan 300   vlan 400   vlan 500

Total Entries: 5

Switch#
```

В 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#
```

19.19 show ip dhcp relay information option format-type

Данная команда используется для отображения настроек формата опций интерфейса.

show ip dhcp relay information option format-type [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите для отображения информации об интерфейсе. Введите ID интерфейса после ключевого слова. Если ID интерфейса не указан, будет отображена информация обо всех интерфейсах.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона

интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения настроек формата опций интерфейса.

Пример

В данном примере показано, как отобразить настройки формата опций интерфейса.

```
Switch#show ip dhcp relay information option format-type

eth1/0/1
Remote ID vendor string: string1
eth1/0/2
Circuit ID vendor string: string1
eth1/0/3
Remote ID vendor string: string3
Circuit ID vendor string: string4

Total Entries: 3

Switch#
```

19.20 show ip dhcp relay information option-insert

Данная команда используется для отображения настройки встраивания Relay Option.

show ip dhcp relay information option-insert [vlan VLAN-ID [, | -]]

Параметры

vlan VLAN-ID	(Опционально.) Укажите, чтобы отобразить информацию на основе VLAN ID.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.

- (Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.
Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения Relay Information Option и информации о настройке встраивания.

Пример

В данном примере показано, как отобразить информацию об Option 82 и информацию о настройке встраивания этой опции для всех VLAN.

```
Switch# show ip dhcp relay information option-insert

Interface      Option-Insert
-----
vlan 1         Enabled
vlan 2         Disabled
vlan 3         Not Configured

Total Entries: 3

Switch#
```

19.21 show ip dhcp relay information policy-action

Данная команда используется, чтобы отобразить информацию об алгоритме перенаправления Relay Option для интерфейса.

show ip dhcp relay information policy-action [vlan VLAN-ID [, | -]]

Параметры

vlan VLAN-ID	(Опционально.) Укажите, чтобы отобразить информацию на основе VLAN ID.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от

предыдущего. Пробелы до и после запятой недопустимы.

-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
---	---

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения информации об алгоритме перенаправления Relay Option.

Пример

В данном примере показано, как отобразить информацию об алгоритме перенаправления Option 82 для всех VLAN.

```
Switch# show ip dhcp relay information policy-action
```

Interface	Policy
-----	-----
vlan 1	Keep
vlan 2	Drop
vlan 3	Replace
vlan 4	Not configured

```
Total Entries: 3
```

```
Switch#
```

19.22 ip dhcp relay unicast

Данная команда используется, чтобы 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, статус **unicast** должен быть идентичным. В ходе DHCPRelayне будет выявлено, какую именно роль выполняет VRRP при ретрансляции пакета – Master или Slave. Пакеты всегда будут передаваться от первого Relay Agent, т. к. при обнаружении DHCP невозможно определить VRRP Master.

Пример

В данном примере показано, как запустить обработку одноадресных пакетов DHCP-клиента.

```
Switch# configure terminal
Switch(config)# ip dhcp relay unicast
Switch(config)#
```

19.23 ip dhcp relay information option mac-format case

Данная команда используется для настройки формата MAC-адреса, задаваемого пользователем в профиле Option 82. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip dhcp relay information option mac-format case {lowercase | uppercase} delimiter{hyphen | colon | dot | none } number {1 | 2 | 5}
no ip dhcp relay information option mac-format case

Параметры

lowercase	Укажите, чтобы использовать нижний регистр при записи MAC-адреса Option 82 для задаваемого пользователем профиля: aa-bb-cc-dd-ee-ff.
uppercase	Укажите, чтобы использовать верхний регистр при записи MAC-адреса Option 82 для задаваемого пользователем профиля: AA-BB-CC-DD-EE-FF.

hyphen	Укажите, чтобы использовать «-» в качестве разделителя данных: AA-BB-CC-DD-EE-FF.
colon	Укажите, чтобы использовать «:» в качестве разделителя данных: AA:BB:CC:DD:EE:FF.
dot	Укажите, чтобы использовать «.» в качестве разделителя данных: AA.BB.CC.DD.EE.FF.
none	Укажите для ввода данных без разделителя: AABCCDDEEFF.
number	Укажите количество разделителей: 1: один разделитель: AABCC.DDEEFF. 2: два разделителя: AAB.CCDD.EEFF. 5: несколько разделителей: AA.BB.CC.DD.EE.FF. Если указан параметр none , параметр number будет недействителен.

По умолчанию

Параметр регистра MAC-адреса аутентификации по умолчанию – **uppercase**.

Параметр разделителя MAC-адреса аутентификации по умолчанию – **none**.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для настройки формата MAC-адреса, заданного пользователем в профиле Option 82.

Пример

В данном примере показано, как настроить формат MAC-адреса, заданного пользователем в профиле Option 82.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information option mac-format case uppercase delimiter hyphen
number 5
Switch(config)#
```

19.24 show ip dhcp relay information option mac-format

Данная команда используется для отображения формата MAC-адреса в профиле Option 82.

show ip dhcp relay information option mac-format

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения формата MAC-адреса в профиле Option 82.

Пример

В данном примере показано, как отобразить формат MAC-адреса в профиле Option 82.

```
Switch#show ip dhcp relay information option mac-format

Case           : Uppercase
Delimiter      : Hyphen
Delimiter Number : 5
Example        : AA-BB-CC-DD-EE-FF

Switch#
```

19.25 ip dhcp relay

Данная команда используется для включения DHCP Relay на интерфейсе. Чтобы отключить данную функцию, 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 применяется для включения/отключения DHCP Relay на интерфейсах физического порта и port-channel.

Пример

В данном примере показано, как включить обработку одноадресных пакетов DHCP-клиента на коммутаторе.

```
Switch#configure terminal
Switch(config)#service dhcp
Switch(config)#interface ethernet 1/0/2
Switch(config-if)#ip dhcp relay
Switch(config-if)#
```

20. Команды DHCP Server

20.1 address range

Данная команда используется для обозначения диапазона IP-адресов, которые необходимо ассоциировать с DHCP-классом в пуле DHCP-адресов. 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

<i>START-IP-ADDRESS</i>	Укажите адрес или первый адрес в диапазоне адресов.
<i>END-IP-ADDRESS</i>	Укажите последний адрес в диапазоне адресов.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Class Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команды **address range** и **class** в конфигурации пула DHCP используются для того, чтобы ограничить выделение IP-адресов из подсети. Сеть разбивается на разделы на основе значения опции DHCP-запроса. Если в пуле адресов определены классы, то назначение адреса будет основано на классе этого адресного пула.

Когда сервер пытается выделить адрес из пула адресов, и если у пула определены классы, то сервер сначала проверит, содержит ли пул запрашиваемую подсеть. Если подсеть пула адресов содержит GIADDR (не равно нулю) или подсеть принимаемого интерфейса, то сервер будет выделять из пула адрес, соответствующий определенному классу.

Для удаления диапазона адресов можно указать только точный диапазон адресов, который уже был ранее настроен.

Пример

В данном примере показано, как создать DHCP-класс «Customer-A» с шаблоном, соответствующим Relay Information Option (Option 82). Он ассоциирован с диапазоном адресов DHCP «pool1».


```
Switch# configure terminal
Switch(config)# ip dhcp class Customer-A
Switch(config-dhcp-class)# option 82 hex 1234 *
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# network 172.28.5.0/24
Switch(config-dhcp-pool)# class Customer-A
Switch(config-dhcp-pool-class)# address range 172.28.5.1 172.28.5.12
Switch(config-dhcp-pool-class)#
```

20.2 bootfile

Используйте данную команду, чтобы указать файл конфигурации или файл образа для загрузки на устройство DHCP-клиента. Для удаления загрузочного файла воспользуйтесь формой **no** этой команды.

bootfile *URL*
no bootfile

Параметры

<i>URL</i>	Укажите ссылку на файл 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 или файл образа для загрузки на устройство DHCP-клиента. Команда **next-server** указывает местоположение сервера, на котором находится загрузочный файл.

Пример

В данном примере показано, как указать файл «mdubootfile.bin» для DHCP-пула «pool1» в качестве загрузочного.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# bootfile \bootimage\mdubootfile.bin
Switch(config-dhcp-pool)#
```

20.3 clear ip dhcp binding

Данная команда используется для удаления записи привязки адресов из базы данных DHCP-сервера.

clear ip dhcp {all | pool NAME} binding {* | IP-ADDRESS}

Параметры

all	Укажите, чтобы очистить записи привязки всех пулов.
pool NAME	Укажите имя DHCP-пула.
*	Укажите, чтобы очистить все записи привязки, ассоциированные с указанным пулом.
IP-ADDRESS	Укажите IP-адрес записи привязки, которую необходимо удалить.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для удаления привязок адресов. Если задан параметр **pool**, а значение IP-адреса – «*», то все автоматические записи привязок, ассоциированные с пулом, будут удалены. Если значение параметра **pool** – **all**, и IP-адрес указан, то автоматическая запись привязки, относящаяся к IP-адресу, будет удалена независимо от пула, в котором содержится запись привязки. Если указаны и параметр **pool**, и IP-адрес, автоматическая запись указанного IP-адреса в обозначенном пуле будет удалена.

Пример

В данном примере показано, как удалить привязку адреса 10.12.1.99 из базы данных DHCP-сервера.

```
Switch# clear ip dhcp all binding 10.12.1.99
Switch#
```

В примере ниже показано, как удалить все привязки из 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#
```

20.4 clear ip dhcp conflict

Данная команда используется для удаления записи конфликта DHCP из базы данных DHCP-сервера.

clear ip dhcp {all | pool NAME} conflict {* | IP-ADDRESS}

Параметры

all	Укажите, чтобы удалить записи конфликтов для всех пулов.
pool NAME	Укажите имя DHCP-пула.
*	Укажите, чтобы удалить все записи конфликтов, ассоциированные с указанным пулом.
IP-ADDRESS	Укажите IP-адрес записи конфликта, которую необходимо 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 IP-адрес указан, то указанная запись конфликта будет удалена независимо от пула, в котором содержится запись конфликта. Если указаны и параметр **pool**, и IP-адрес, то обозначенная запись конфликта в соответствующем пуле будет удалена.

Пример

В данном примере показано, как удалить конфликт с адресом 10.12.1.99 из базы данных DHCP-сервера.

```
Switch# clear ip dhcp all conflict 10.12.1.99
Switch#
```

В 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#
```

20.5 clear ip dhcp server statistics

Данная команда используется для сброса всех счетчиков DHCP-сервера.

clear ip dhcp server statistics

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для сброса всех счетчиков статистики DHCP.

Пример

В данном примере показано, как сбросить все счетчики DHCP.

```
Switch# clear ip dhcp server statistics  
Switch#
```

20.6 class (DHCP Relay & Server)

Данная команда используется для входа в режим DHCP Pool Configuration Mode и привязки диапазона IP-адресов к DHCP-классу. 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.

В пуле DHCP Relay пользователь может далее использовать команду **class** для привязки класса к DHCP-пулу, а затем использовать Relay Target, чтобы указать список адресов для перенаправления DHCP-пакетов. Если запрос DHCP-клиента совпадает с Relay-пулом, настроенным с классами, то для выполнения ретрансляции клиент должен соответствовать классу, настроенному в пуле. При отсутствии настроенных DHCP-классов запрос будет сопоставлен с Relay-пулом и ретранслирован на сервер назначения Relay, указанный для соответствующего Relay-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
Switch(config-dhcp-pool-class)# exit
Switch(config-dhcp-pool)# class Customer-B
Switch(config-dhcp-pool-class)# address-range 172.28.5.18 172.28.5.32
Switch(config-dhcp-pool-class)#
```

В примере ниже показано, как настроить DHCP-класс «Service-A» и задать шаблоны соответствия Option 60 DHCP 0x112233 и 0x102030. Другой класс «Service-B» настроен и задан с шаблонами соответствия Option 60 DHCP 0x556677 и 0x506070. Класс «Default-class» настроен без опции. Эти заданные классы применяются в Relay-пуле «pool1». Класс «Service-A» ассоциирован с Relay Target 10.2.1.2, а класс «Service-B» ассоциирован с Relay Target 10.2.1.5. Класс «Default-class» ассоциирован с Relay Target 10.2.1.32.

```
Switch# configure terminal
Switch(config)# ip dhcp class Service-A
Switch(config-dhcp-class)# option 60 hex 112233
Switch(config-dhcp-class)# option 60 hex 102030
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Service-B
Switch(config-dhcp-class)# option 60 hex 556677
Switch(config-dhcp-class)# option 60 hex 506070
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Default-class
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# relay source 172.19.18.3 255.255.255.0
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)#
```

20.7 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 0x01524153203124.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# client-identifier ee:ee:ee:ee:ee:ee(in xx:xx:xx:xx:xx:xx format)
Switch(config-dhcp-pool)# host 10.1.2.3/24
Switch(config-dhcp-pool)#
```

20.8 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 перечислены в порядке приоритетности. Если шлюзы по умолчанию уже настроены, то шлюзы, настраиваемые позже, будут добавлены в список шлюзов по умолчанию.

Пример

В данном примере показано, как указать IP-адрес шлюза по умолчанию в пуле DHCP-адресов. 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
```

20.9 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

<i>NAME</i>	Укажите доменное имя. Максимально допустимое количество символов – 64.
-------------	--

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда 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
```

20.10 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 DNS-серверов.

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
```

20.11 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

<i>HARDWARE-ADDRESS</i>	Укажите MAC-адрес клиента.
-------------------------	----------------------------

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Запись привязки – это сопоставление IP-адреса с аппаратным адресом оборудования или ID клиента. При создании записи привязки IP-адрес присваивается клиенту вручную.

В пуле DHCP-адресов может быть указано не более одной записи привязки. С помощью записи привязки IP-адрес может быть связан с ID клиента или с аппаратным адресом узла.

Используйте команды **client-identifier** и **host**, чтобы настроить ручную запись привязки на основе ID клиента в DHCP-пакете. Команды **hardware-address** и **host** используются для настройки ручной записи привязки на основе аппаратного адреса.

Пример

В данном примере показано, как создать пул DHCP-адресов с настроенной вручную записью привязки, которая связывает IP-адрес 10.1.2.100/24 с MAC-адресом C2:F3:22:0A:12:F4. Указанное имя пула – pool1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# hardware-address C2F3.220A.12F4
Switch(config-dhcp-pool)# host 10.1.2.100/24
Switch(config-dhcp-pool)#
```

20.12 host

Данная команда используется для указания IP-адреса в настроенной вручную записи привязки пула DHCP-адресов. Чтобы удалить IP-адрес из записи, воспользуйтесь формой **no** этой команды.

host {IP-ADDRESS MASK | IP-ADDRESS/PREFIX-LENGTH}
no host

Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес в настроенной вручную записи привязки.
<i>MASK</i>	Укажите биты, определяющие сетевую маску.
<i>PREFIX-LENGTH</i>	Укажите длину префикса сети. Это альтернативный способ указать сетевую маску.

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

В пуле DHCP-адресов может быть указано не более одной записи привязки. С помощью записи привязки IP-адрес может быть связан с 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)#
```

20.13 ip dhcp class (DHCP Relay & 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 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 установить шаблон соответствия DHCP Option 60 0x112233.

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

20.14 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 шлюза и исключенных адресов, которые обозначены при помощи команды **ip dhcp excluded-address**. Можно отменить распределение нескольких диапазонов адресов. Для удаления диапазона исключенных адресов администратору необходимо указать точный диапазон данных адресов.

Пример

В данном примере показано, как исключить диапазон адресов. Указанный диапазон адресов: с 10.1.1.1 по 10.1.1.255 и с 10.2.1.1 по 10.2.1.255.

```
Switch# configure terminal
Switch(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.255
Switch(config)# ip dhcp excluded-address 10.2.1.1 10.2.1.255
```

20.15 ip dhcp ping packets

Данная команда используется для указания количества пакетов, 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)#
```

20.16 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

<i>MILLI-SECONDS</i>	Укажите период ожидания ответного ping-пакета DHCP-сервером. Максимальный период ожидания – 10000 миллисекунд (10 секунд). Указанное значение должно быть кратным 100.
----------------------	--

По умолчанию

Значение по умолчанию – 500 миллисекунд (0,5 секунды).

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда 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)#
```

20.17 ip dhcp pool (DHCP Server)

Данная команда используется для настройки пула DHCP-адресов DHCP-сервера и входа в режим настройки DHCP Pool Configuration Mode. Чтобы удалить пул DHCP-адресов, воспользуйтесь формой **no** этой команды.

ip dhcp pool *NAME*
no ip dhcp pool *NAME*

Параметры

<i>NAME</i>	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)#
```

20.18 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. Для отключения использования DHCP-классов воспользуйтесь формой **no** этой команды.

Пример

В данном примере показано, как отключить использование DHCP-классов.

```
Switch# configure terminal
Switch(config)# no ip dhcp use class
Switch(config)#
```

20.19 lease

Данная команда используется для настройки периода аренды IP-адреса, назначаемого из пула адресов. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

lease {DAYS [HOURS [MINUTES]] | infinite}
no lease

Параметры

<i>DAYS</i>	Укажите период аренды в днях.
<i>HOURS</i>	(Опционально.) Укажите период аренды в часах.
<i>MINUTES</i>	(Опционально.) Укажите период аренды в минутах.
<i>infinite</i>	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 на 1 день. Указанное имя пула – pool1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# lease 1
```

В примере ниже показано, как установить период аренды для пула адресов на 1 час. Указанное имя пула – pool1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# lease 0 1
```

20.20 netbios-node-type

Данная команда используется, 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

<i>NTYPE</i>	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)#
```

20.21 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

<i>IP-ADDRESS</i>	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)#
```

20.22 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, чтобы обеспечить клиенту загрузку файла образа. 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
```

20.23 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

<i>NETWORK-ADDRESS</i>	Укажите адрес подсети для пула адресов.
<i>MASK</i>	Укажите биты, определяющие сетевую маску.
<i>PREFIX-LENGTH</i>	Укажите длину префикса сети (это альтернативный способ указать сетевую маску).

По умолчанию

Нет.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда 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)#
```

20.24 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

<i>CODE</i>	Укажите номер опции в десятичном виде.
ascii <i>STRING</i>	Укажите формат строки ASCII для DHCP-опции. Максимальное количество байт – 255.
hex	Укажите шестнадцатеричный формат для DHCP-опции. Максимальное количество символов – 254.
<i>HEX-STRING</i>	Укажите шестнадцатеричную строку для DHCP-опции.
none	Укажите шестнадцатеричную строку нулевой длины.
ip <i>IP-ADDRESS</i>	Укажите IP-адрес. 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. DHCP-сервер будет вносить все настраиваемые DHCP-опции во все ответные пакеты. Все настроенные DHCP-опции будут внесены в DHCP-пакеты, которые сервер отправляет в ответ.

Длина настраиваемой шестнадцатеричной строки должна быть выражена при помощи четного числа (так, 001100 – пример верного варианта числа, а 11223 – пример неверного варианта числа). Для одной опции можно указать одну строку.

Общая длина DHCP-опций ограничена. Ограничение по длине может быть установлено клиентом или сервером, если клиент не установил данное ограничение. Если ограничение не установлено, максимальная длина по умолчанию – 312.

Ниже перечислены опции, которые можно настроить при помощи других команд режима DHCP Pool Configuration Mode, но нельзя настроить при помощи команды **option**.

- Option 1 (Subnet Mask, настраивается при помощи команды **network**).
- Option 3 (Router Option, настраивается при помощи команды **default router**).
- Option 6 (Domain Name Server, настраивается при помощи команды **dns-server**).
- Option 15 (Domain Name, настраивается при помощи команды **domain-name**).
- Option 44 (NetBIOS Name Server, настраивается при помощи команды **netbios-name-server**).
- Option 46 (NetBIOS Node Type, настраивается при помощи команды **netbios-node-type**).
- Option 51 (IP Address Lease Time, настраивается при помощи команды **lease**).
- Option 58 (Renewal (T1) Time Value, настраивается при помощи команды **lease**).
- Option 59 (Rebinding (T2) Time Value, настраивается при помощи команды **lease**).

Ниже перечислены опции, которые не могут быть настроены при помощи команды **option**:

- Option 12 (Host Name, опция по умолчанию).
- Option 50 (Requested Address, опция по умолчанию).
- Option 53 (DHCP Message Type, опция по умолчанию).
- Option 54 (Server Identifier, опция по умолчанию).
- Option 55 (Parameter Request List, опция по умолчанию).
- Option 61 (Client Identifier, опция по умолчанию).
- Option 82 (Relay Agent Information Option, опция по умолчанию).

Пример

В данном примере показано, как настроить Option 69 DHCP-сервера (опцию SMTP-сервера) в шестнадцатеричном формате. Указанная шестнадцатеричная строка – c0a800fe (192.168.0.254).

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# option 69 hex c0a800fe
```

В 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
```

20.25 option hex (DHCP Relay & 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.
*	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.

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 0x112233 и 0x102030. Другой класс «Service-B» настроен с установленными шаблонами соответствия DHCP Option 60 0x5566* и 0x5060*.

```
Switch# configure terminal
Switch(config)# ip dhcp class Service-A
Switch(config-dhcp-class)# option 60 hex 112233
Switch(config-dhcp-class)# option 60 hex 102030
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Service-B
Switch(config-dhcp-class)# option 60 hex 5566 *
Switch(config-dhcp-class)# option 60 hex 5060 *
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Service-B
Switch(config-dhcp-class)#
```

20.26 service dhcp

Данная команда используется для включения DHCP-сервера и Relay Service. 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)#
```

20.27 manual-binding

Данная команда используется, чтобы настроить запись привязки DHCP вручную. Для удаления записи воспользуйтесь формой **no** этой команды.

manual-binding {*IP-ADDRESS MASK* | *IP-ADDRESS/PREFIX-LENGTH*} {*HARDWARE-ADDRESS* | *CLIENT-IDENTIFIER*}

no manual-binding {*IP-ADDRESS MASK* | *IP-ADDRESS/PREFIX-LENGTH*}

Параметры

<i>IP-ADDRESS MASK</i>	Укажите IP-адрес и сетевую маску для записи привязки вручную. Разрешен только индивидуальный IP-адрес.		
<i>IP-ADDRESS/PREFIX-LENGTH</i>	Укажите IP-адрес и длину префикса для записи привязки вручную.		
<i>HARDWARE-ADDRESS</i>	Укажите MAC-адрес клиента.		
<i>CLIENT-IDENTIFIER</i>	Укажите идентификатор	DHCP-клиента	в
	шестнадцатеричном виде.		

По умолчанию

По умолчанию настроенные записи отсутствуют.

Режим ввода команды

DHCP Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить несколько записей привязки DHCP в пуле DHCP. Запись привязки назначает клиенту IP-адрес на основе аппаратного адреса или идентификатора клиента. У настроенных записей привязки должен быть уникальный IP-адрес. Все записи привязки вручную, сконфигурированные в одном и том же пуле DHCP, должны принадлежать одной и той же подсети. Максимальное количество записей – 256.

Функция Prompt

Prompt-сообщения на экране	Описание
ERROR: Cannot use the command in relay pool.	Этот пул используется в качестве DHCP Relay-пула.
ERROR: This command cannot be used with network pools.	Этот пул указан как сетевой.
ERROR: IP address of manual binding entries in the same pool must belong to the same subnet.	IP-адрес записей привязки в одном и том же пуле принадлежит другой подсети.
ERROR: Invalid IP address.	Недопустимый IP-адрес.

Пример

В данном примере показано, как настроить две записи привязки вручную в пуле DHCP-адресов «pool1».

```
switch(config)#ip dhcp pool pool1
switch(config-dhcp-pool)# manual-binding 10.1.2.100/24 C2:F3:22:0A:12:F4
switch(config-dhcp-pool)# manual-binding 10.1.2.3/24 01524153203124
switch(config-dhcp-pool)#exit
switch(config)#
```

20.28 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1

Использование команды

Будет отображен IP-адрес, аппаратный адрес, сроки начала и истечения периода аренды записи.

Пример

В данном примере показано, как отобразить статус привязки всех связанных IP-адресов.

```
Switch#show ip dhcp binding

IP address      Client-ID/      Lease expiration   Type
                Hardware address
-----
10.0.0.1        c2-f3-22-0a-12-f4 Feb 25 2018 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        c2-f3-22-0a-12-f3 Feb 25 2018 08:21 AM Automatic
Switch#
```

20.29 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.

Любой режим конфигурирования.

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 устранил 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#
```

20.30 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. Если значение не задано, будет отображена информация обо всех DHCP-пулах.
------	---

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы просмотреть параметры настроек пула. Если значение не задано, будут отображены параметры конфигурации всех пулов.

Пример

В данном примере показано, как отобразить информацию о настройках DHCP-пула «pool1».

```
Switch#show ip dhcp pool pool1

Pool name: pool1
Network: 10.0.0.0/8
Boot file:
Default router:
DNS server:
NetBIOS server:
Domain name:
Lease: 1 days 0 hours 0 minutes
NetBIOS node type:
Next server: 0.0.0.0
Remaining unallocated address number: 1023
Number of leased addresses: 1

Switch#
```

20.31 show ip dhcp server

Данная команда используется для отображения текущего статуса DHCP-сервера.

show ip dhcp server

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статус DHCP-сервера и пул адресов, настроенный пользователем.

Пример

В данном примере показано, как отобразить статус DHCP-сервера.

```
Switch# show ip dhcp server

DHCP Service: Disable
Ping packets number: 3
Ping timeout: 500 ms
Excluded Addresses
10.1.1.1-10.1.1.255

List of DHCP server configured address pool
pool1          pool2          pool3          pool4
pool5          pool6          pool7          pool8
pool9          pool10         pool11         pool12

Switch#
```

20.32 show ip dhcp server statistics

Данная команда используется для отображения статистики DHCP-сервера.

show ip dhcp server statistics

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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.

21. Команды DHCP Server Screening

21.1 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

<i>CLIENT-HARDWARE-ADDRESS</i>	Укажите MAC-адрес клиента.
--------------------------------	----------------------------

По умолчанию

Нет.

Режим ввода команды

Configure DHCP Server Screen Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

В данном примере показано, как настроить профиль DHCP Server Screen «campus-profile», содержащий список MAC-адресов клиентов.

```
Switch# configure terminal
Switch(config)# dhcp-server-screen profile campus-profile
Switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-02-03-04
Switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-03-00-01
Switch(config-dhcp-server-screen)#
```

21.2 clear ip dhcp snooping server-screen log

Используйте данную команду, чтобы очистить буфер журнала событий Server Screen.

clear ip dhcp snooping server-screen log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

21.3 dhcp-server-screen profile

Данная команда используется для настройки профиля Server Screen и входа в режим Server Screen Configure Mode. Чтобы удалить профиль Server Screen, воспользуйтесь формой **no** этой команды.

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

Параметры

<i>PROFILE-NAME</i>	Укажите имя профиля. 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 DHCP Server Screen Configure Mode и настроить профиль Server Screen. Профиль можно использовать для настройки записи DHCP Server Screen.

Пример

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

```
Switch# configure terminal
Switch(config)# service dhcp
Switch(config)# dhcp-server-screen profile campus
Switch(config-dhcp-server-screen)#
```

21.4 ip dhcp snooping server-screen

Данная команда используется для включения DHCP Server Screening. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ip dhcp snooping server-screen [SERVER-IP-ADDRESS **profile** PROFILE-NAME]
no ip dhcp snooping server-screen [SERVER-IP-ADDRESS]

Параметры

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

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

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

Если IP-адрес сервера не указан, на интерфейсе будет включен/отключен DHCP Server Screen. По

умолчанию DHCP Server Screen отключен на всех интерфейсах. Если DHCP Server Screen включен, все пакеты DHCP-сервера на указанном интерфейсе будут отфильтрованы и будут переданы только пакеты от доверенного сервера.

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

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

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

Пример

В данном примере показано, как настроить профиль DHCP Server Screen «campus-profile» и ассоциировать его с записью DHCP Server Screen для интерфейса Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# dhcp-server-screen profile campus-profile
Switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-02-03-04
Switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-03-00-01
Switch(config-dhcp-server-screen)# exit
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ip dhcp snooping server-screen 10.1.1.2 profile campus-profile
Switch(config-if)#
```

21.5 ip dhcp snooping server-screen log-buffer

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

ip dhcp snooping server-screen log-buffer entries *NUMBER*
no ip dhcp snooping server-screen log-buffer entries

Параметры

<i>NUMBER</i>	Укажите количество записей в буфере. Максимальное количество записей – 1024.
---------------	--

По умолчанию

Значение по умолчанию – 32.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для настройки максимального количества записей в буфере журнала событий. Буфер журнала событий DHCP Server Screen хранит информацию о пакетах, которые не прошли screening. Первый пакет, который не прошел проверку, будет отправлен в модуль журнала событий и записан в буфер журнала событий Server Screen. Последующие пакеты из той же сессии не будут отправлены в модуль журнала событий, если его запись в буфере журнала не будет удалена. Если буфер журнала событий полон, но события (нарушения) продолжают поступать, пакеты будут отброшены, а события не будут отправлены в модуль системного журнала. Если пользователь задает размер буфера меньше текущего номера записи, буфер журнала будет очищен автоматически.

Пример

В данном примере показано, как изменить размер буфера на 64.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping server-screen log-buffer entries 64
Switch(config)#
```

21.6 show ip dhcp server-screen log

Данная команда используется для отображения буфера журнала событий Server Screen.

show ip dhcp server-screen log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

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

```
Total log buffer size: 64
```

VLAN	Server IP	Client MAC	Occurrence
100	10.20.1.1	00-20-30-40-50-60	06:30:37, 2013-02-07
100	10.58.2.30	10-22-33-44-50-60	06:31:42, 2013-02-07

```
Total Entries: 2
```

```
Switch#
```

21.7 snmp-server enable traps dhcp-server-screen

Данная команда используется для включения отправки SNMP-уведомлений об атаках, поступающих от ложного DHCP-сервера. Чтобы отключить отставку SNMP-уведомлений, воспользуйтесь формой **no** этой команды.

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 отставку SNMP-уведомлений о подобных событиях.

Пример

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

```
Switch# configure terminal
```

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

```
Switch(config)#
```

22. Команды DHCP Snooping

22.1 ip dhcp snooping

Данная команда используется для глобального включения DHCP Snooping. Чтобы отключить DHCP Snooping, воспользуйтесь формой **no** этой команды.

```
ip dhcp snooping
no ip dhcp snooping
```

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Функция DHCP Snooping отслеживает пакеты DHCP, поступающие на недоверенный интерфейс в VLAN, на которой включена данная функция. С помощью данной функции DHCP-пакеты, приходящие с недоверенного интерфейса, могут получить статус проверенных и будет создана таблица привязки DHCP для DHCP Snooping в VLAN. Таблица привязки содержит информацию о привязке IP и MAC, которая дополнительно может использоваться IP Source Guard и Dynamic ARP Inspection.

Пример

В данном примере показано, как включить DHCP Snooping.

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

22.2 ip dhcp snooping information option allow-untrusted

Данная команда используется для глобального доступа DHCP-пакетов с Relay Option 82 к недоверенным интерфейсам. Чтобы запретить пакеты с Relay Option 82, воспользуйтесь формой **no** этой команды.

```
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, поступающие на порт в VLAN, на котором включена функция DHCP Snooping. По умолчанию при проверке будут отброшены пакеты, если их адрес шлюза не равен 0 или присутствует Option 82.

Используйте данную команду, чтобы разрешить пакетам с Relay Option 82 доступ к недоверенным интерфейсам.

Пример

В данном примере показано, как включить DHCP Snooping для Option 82, чтобы разрешить доступ к недоверенным интерфейсам.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping information option allow-untrusted
Switch(config)#
```

22.3 ip dhcp snooping database

Данная команда используется для настройки хранения записей привязки DHCP Snooping в локальной файловой системе (flash-памяти) или на удаленном узле. Чтобы отключить хранение или вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip dhcp snooping database {URL | write-delay SECONDS}
no ip dhcp snooping database [write-delay]

Параметры

URL	Укажите URL в каком-либо из представленных форматов: • ftp://username:password@location:tcpport/filename • tftp://location/filename • flash:/filename
write-delay SECONDS	Укажите время ожидания перед обновлением записи при обнаружении изменений в таблице привязки. Время по умолчанию составляет 300 секунд. Диапазон 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 применяется для хранения записей привязки DHCP в локальной flash-памяти или на удаленном узле. Используйте следующие методы для хранения записей привязки DHCP:

- **flash:** хранение записей в файле в локальной файловой системе.
- **tftp:** хранение записей на удаленном узле через TFTP.
- **ftp:** хранение записей на удаленном узле через FTP.



Примечание: flash-память включает в себя только внешнюю память, например, USB-накопитель.

Используйте данную команду, чтобы сохранить таблицу привязки DHCP Snooping в коммутаторе стека. Таблица не будет сохранена в отдельных коммутаторах стека.

Время аренды записи (Lease Time) не будет изменено, и время жизни (Live Time) продолжит отсчитываться, пока запись существует.

Пример

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

```
Switch# configure terminal
Switch(config)# ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch(config)#
```

22.4 clear ip dhcp snooping database statistics

Данная команда используется для удаления статистики таблицы привязки DHCP.

clear ip dhcp snooping database statistics

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для удаления статистики таблицы привязки DHCP.

Пример

В данном примере показано, как удалить статистику таблицы привязки DHCP Snooping.

```
Switch# clear ip dhcp snooping database statistics
Switch#
```

22.5 clear ip dhcp snooping binding

Данная команда используется для удаления привязки DHCP.

clear ip dhcp snooping binding [MAC-ADDRESS] [IP-ADDRESS] [vlan VLAN-ID] [interface INTERFACE-ID]

Параметры

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

Используйте данную команду, чтобы удалить запись привязки DHCP, включая заданные вручную записи привязки.

Пример

В данном примере показано, как удалить все записи привязки DHCP Snooping.

```
Switch# clear ip dhcp snooping binding
Switch#
```

22.6 renew ip dhcp snooping database

Данная команда используется для обновления таблицы привязки DHCP.

renew ip dhcp snooping database *URL*

Параметры

<i>URL</i>	Укажите URL-адрес для загрузки таблицы привязки и добавления в нее записей. Укажите URL в любом из представленных форматов: • ftp://username:password@location:tcpport/filename • tftp://location/filename • flash:/filename
------------	---

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для обновления таблицы привязки DHCP с URL-адреса и добавления записей в таблицу привязки DHCP Snooping.

Используйте следующие методы для хранения записей привязки DHCP Snooping:

- **flash**: хранение записей из файла в локальной файловой системе.
- **tftp**: хранение записей на удаленном узле через TFTP.
- **ftp**: хранение записей на удаленном узле через FTP.



Примечание: flash-память включает в себя только внешнюю память, например, USB-накопитель.

Пример

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

```
Switch# renew ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch#
```

22.7 ip dhcp snooping binding

Данная команда используется для настройки привязки DHCP Snooping вручную.

ip dhcp snooping binding *MAC-ADDRESS* **vlan** *VLAN-ID* **ip-address** *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 (физический порт или port-channel), на котором необходимо добавить или удалить запись привязки.
expiry SECONDS	Укажите интервал, по истечении которого привязки станут недействительны. Диапазон значений: от 60 до 4294967295 секунд.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется 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 параметром expiry time, равным 100 секундам.

```
Switch# ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface ethernet 1/0/10  
expiry 100  
Switch#
```

22.8 ip dhcp snooping trust

Данная команда используется для настройки порта в качестве доверенного интерфейса для DHCP Snooping. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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 физического порта и port-channel.

Порты, подключенные к DHCP-серверу или другим коммутаторам, должны быть настроены как доверенные интерфейсы. Порты, подключенные к DHCP-клиентам, должны быть настроены как недоверенные интерфейсы. DHCP Snooping работает в качестве межсетевого экрана между недоверенными интерфейсами и DHCP-серверами.

Если порт настроен как недоверенный интерфейс, сообщение DHCP придет на порт в ту VLAN, в которой включен DHCP Snooping. Коммутатор перенаправит пакеты DHCP за исключением следующих случаев, при которых пакеты будут отбрасываться:

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

В дополнение к процессу проверки DHCP Snooping также создает запись привязки на основе IP-адреса, назначенного клиенту сервером в таблице привязки DHCP Snooping. Запись привязки содержит информацию, включающую MAC-адрес, IP-адрес, VLAN ID и идентификатор порта (Port ID), к которому подключен клиент, а также время истечения срока аренды (Lease Time).

Пример

В данном примере показано, как настроить DHCP Snooping для доверенного интерфейса Ethernet 1/0/3.

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

22.9 ip dhcp snooping limit entries

Данная команда используется для настройки количества записей привязки DHCP Snooping, которые

может изучить интерфейс. Чтобы сбросить заданное ограничение на количество записей DHCP, воспользуйтесь формой **no** этой команды.

ip dhcp snooping limit entries {NUMBER | no-limit}
no ip dhcp snooping limit entries

Параметры

NUMBER	Укажите ограничение на количество записей привязок DHCP Snooping на порт. Диапазон значений: от 0 до 1024.
no-limit	Укажите для снятия ограничения на количество записей.

По умолчанию

По умолчанию ограничения не заданы.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

В данном примере показано, как установить ограничение на количество привязок для интерфейса Ethernet 1/0/1. Настроенное значение – 100.

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

22.10 ip dhcp snooping limit rate

Данная команда используется для настройки количества DHCP-сообщений, получаемых на интерфейсе за секунду. Чтобы сбросить заданное ограничение на получение сообщений DHCP, воспользуйтесь формой **no** этой команды.

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 значений: от 1 до 300.
no-limit	Укажите для снятия ограничения скорости.

По умолчанию

По умолчанию ограничения не заданы.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При превышении заданного ограничения на получение DHCP-пакетов порт будет отключен из-за ошибки.

Пример

В данном примере показано, как настроить количество сообщений DHCP, получаемых на интерфейсе Ethernet 1/0/3 за одну секунду.

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

22.11 ip dhcp snooping station-move deny

Данная команда используется для отключения состояния DHCP Snooping Station Move. Чтобы включить состояние DHCP Snooping Roaming, воспользуйтесь формой **no** этой команды.

ip dhcp snooping station-move deny
no ip dhcp snooping station-move deny

Параметры

Нет.

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При включении DHCP Snooping Station Move динамическая запись привязки DHCP Snooping с теми же VLAN ID и MAC-адресом на определенном порту может переместиться на другой порт, если обнаружится, что новому процессу DHCP принадлежит тот же VLAN ID и MAC-адрес.

Пример

В данном примере показано, как отключить состояние roaming.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping station-move deny
Switch(config)#
```

22.12 ip dhcp snooping verify mac-address

Данная команда используется для включения проверки MAC-адреса источника DHCP-пакета на соответствие аппаратному адресу клиента. Чтобы отключить проверку MAC-адреса, воспользуйтесь формой **no** этой команды.

ip dhcp snooping verify mac-address
no ip dhcp snooping verify mac-address

Параметры

Нет.

По умолчанию

По умолчанию данная функция включена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

В данном примере показано, как включить проверку MAC-адреса источника DHCP-пакета на соответствие 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 определенной VLAN или группе VLAN. Чтобы отключить DHCP Snooping в VLAN или группе VLAN, воспользуйтесь формой **no** этой команды.

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

Параметры

<i>VLAN-ID</i>	Укажите VLAN, в которой необходимо включить или отключить функцию DHCP Snooping.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона номеров VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию функция DHCP Snooping отключена во всех VLAN.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для глобального включения DHCP Snooping. Примените команду **ip dhcp snooping vlan**, чтобы включить DHCP Snooping для VLAN. Функция DHCP Snooping отслеживает пакеты DHCP, приходящие на недоверенный интерфейс в VLAN, на которой включена функция DHCP Snooping. С помощью данной функции DHCP-пакеты, приходящие с недоверенного интерфейса, могут получить статус проверенных, а для VLAN с включенной функцией DHCP Snooping будет создана таблица привязки DHCP. Таблица привязки предоставляет информацию о соответствиях IP и MAC-адресов, которая позже может использоваться 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 примере ниже показано, как включить DHCP Snooping в нескольких VLAN.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 10,15-18
Switch(config)#
```

22.14 show ip dhcp snooping

Данная команда используется для отображения настроек DHCP Snooping.

show ip dhcp snooping

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения параметров настроек DHCP Snooping.

Пример

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

```
Switch# show ip dhcp snooping

DHCP Snooping is enabled
DHCP Snooping is enabled on VLANs:
    10, 15-18
Verification of MAC address is disabled
Station move is permitted.
Information option is not allowed on un-trusted interface

Interface      Trusted    Rate Limit  Entry Limit
-----
eth1/0/1       no        10          no_limit
eth1/0/2       no        50          no_limit
eth1/0/3       yes       no_limit    no_limit

Switch#
```

22.15 show ip dhcp snooping binding

Данная команда используется для отображения привязки DHCP Snooping.

show ip dhcp snooping binding [*IP-ADDRESS*] [*MAC-ADDRESS*] [**vlan** *VLAN-ID*] [**interface** *INTERFACE-ID* [, | -]]

Параметры

<i>IP-ADDRESS</i>	(Опционально.) Укажите, чтобы отобразить привязки на основе IP-адреса.
<i>MAC-ADDRESS</i>	(Опционально.) Укажите, чтобы отобразить привязки на основе MAC-адреса.
vlan <i>VLAN-ID</i>	(Опционально.) Укажите, чтобы отобразить привязки на основе VLAN.
interface <i>INTERFACE-ID</i>	(Опционально.) Укажите, чтобы отобразить 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения привязки DHCP Snooping.

Пример

В данном примере показано, как отобразить привязку 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 примере ниже показано, как отобразить привязку DHCP Snooping по IP-адресу 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 привязку DHCP Snooping по IP-адресу 10.1.1.11 и MAC-адресу 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 нижеприведенном примере показано, как отобразить привязку DHCP Snooping по IP-адресу 10.1.1.1 и MAC-адресу 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 нижеуказанном примере показано, как настроить отображение 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 последнем примере показано, как настроить отображение привязки DHCP Snooping на интерфейсе Ethernet 1/0/5.

```
Switch# show ip dhcp snooping binding interface ethernet 1/0/5
```

MAC Address	IP Address	Lease(seconds)	Type	VLAN	Interface
00-01-02-03-04-05	10.1.1.10	1500	dhcp-snooping	100	eth1/0/5
00-01-02-00-00-05	10.1.1.11	495	dhcp-snooping	100	eth1/0/5

Total Entries: 2

```
Switch#
```

Отображаемые параметры

MAC Address	Аппаратный MAC-адрес клиента.
IP Address	IP-адрес клиента, назначенный DHCP-сервером.
Lease (seconds)	Время аренды IP-адреса (в секундах).
Type	Тип привязки, настроенный через интерфейс командной строки или изученный динамически.
VLAN	VLAN ID.
Interface	Интерфейс, подключающийся к узлу DHCP-клиента.

22.16 show ip dhcp snooping database

Данная команда используется, чтобы отобразить статистику таблицы привязки DHCP Snooping.

show ip dhcp snooping database

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статистику таблицы привязки DHCP Snooping.

Пример

В данном примере показано, как отобразить статистику таблицы привязки DHCP Snooping.

```
Switch#show ip dhcp snooping database

URL:  tftp:  //10.0.0.2/store/dhcp-snp-bind
Write Delay Time:  300 seconds

Last ignored bindings counters:
Binding collisions :  0          Expired lease :  0
Invalid interfaces :  0          Unsupported vlans :  0
Parse failures    :  0          Checksum errors :  0

Switch#
```

Отображаемые параметры

Binding Collisions	Количество записей, создавших коллизии с существующими записями в таблице привязки DHCP Snooping.
Expired leases	Количество записей с истекшим сроком аренды в таблице привязки DHCP Snooping.
Invalid interfaces	Количество интерфейсов, получивших сообщение DHCP, для которых не выполняется DHCP Snooping.
Pase failures	Количество запрещенных пакетов DHCP.
Checksum errors	Количество подсчитанных значений контрольной суммы, не равное сохраненному значению контрольной суммы.
Unsupported vlans	Количество записей, для которых VLAN отключена.

23. Команды DHCPv6 Client

23.1 clear ipv6 dhcp client

Данная команда используется для перезапуска DHCPv6 Client на интерфейсе.

clear ipv6 dhcp client *INTERFACE-ID*

Параметры

<i>INTERFACE-ID</i>	Укажите интерфейс VLAN, на котором необходимо перезапустить DHCPv6 Client.
---------------------	--

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для перезапуска IPv6 DHCP Client на указанном интерфейсе.

Пример

В данном примере показано, как перезапустить DHCPv6 Client на интерфейсе VLAN 1.

```
Switch# clear ipv6 dhcp client vlan1
Switch#
```

23.2 show ipv6 dhcp

Данная команда используется для отображения настроек DHCPv6 на интерфейсе.

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

Параметры

<i>INTERFACE-ID</i>	Укажите интерфейс VLAN, для которого необходимо отобразить настройки DHCPv6.
---------------------	--

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить DHCPv6 DUID устройства, или используйте команду **show ipv6 dhcp interface**, чтобы отобразить настройки DHCPv6 для интерфейсов. Если ID интерфейса не указан, будут отображены все интерфейсы с функцией DHCPv6.

Пример

В данном примере показано, как отобразить DHCPv6 DUID для устройства.

```
Switch# show ipv6 dhcp

This device's DUID is 00:03:00:06:00:11:22:33:44:56.

Switch#
```

В примере ниже показано, как отобразить настройки DHCPv6 для интерфейса VLAN 1, если на VLAN 1 отключена функция DHCPv6.

```
Switch# show ipv6 dhcp interface vlan1

vlan 1 is not in DHCPv6 mode

Switch#
```

В следующем примере показано, как отобразить настройки DHCPv6 для всех VLAN. Отображаются только те VLAN, на которых включена функция DHCPv6.

```
Switch# show ipv6 dhcp interface

vlan 1 is in client mode
  State is OPEN
  List of known servers:
    Reachable via address: FE80::200:11FF:FE22:3344
  Configuration parameters:
    IA PD: IA ID 1, T1 40, T2 64
    Prefix: 2000::/48
           preferred lifetime 80, valid lifetime 100
  Prefix name: yy
  Rapid-Commit: disabled

Switch#
```


24. Команды DHCPv6 Guard

24.1 ipv6 dhcp guard policy

Данная команда используется для создания или изменения политики DHCPv6 Guard. Команда позволяет войти в режим DHCPv6 Guard Configuration Mode. Чтобы удалить политику DHCPv6 Guard, воспользуйтесь формой **no** этой команды.

```
ipv6 dhcp guard policy POLICY-NAME  
no ipv6 dhcp guard policy
```

Параметры

<i>POLICY-NAME</i>	Укажите имя политики DHCPv6 Guard.
--------------------	------------------------------------

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для создания или изменения политики DHCPv6 Guard. Команда позволяет войти в режим DHCPv6 Guard Configuration Mode. Политики DHCPv6 Guard могут использоваться для блокировки ответов DHCPv6 и сообщений, приходящих с неавторизованного сервера. Сообщения клиента не блокируются.

После создания политики DHCPv6 Guard используйте команду **ipv6 dhcp guard attach-policy** для применения политики на определенном интерфейсе.

Пример

В данном примере показано, как создать политику DHCPv6 Guard.

```
Switch# configure terminal  
Switch(config)# ipv6 dhcp guard policy policy1  
Switch(config-dhcp-guard)# device-role server  
Switch(config-dhcp-guard)# match ipv6 access-list acl1  
Switch(config-dhcp-guard)#
```

24.2 device-role

Данная команда используется для указания роли подключенного устройства. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

```
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

Параметр по умолчанию – **client**.

Режим ввода команды

DHCPv6 Guard Policy Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется 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 на данном порту будут разрешены.

Пример

В данном примере показано, как создать политику DHCPv6 Guard и настроить устройство в качестве сервера.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp guard policy dhcpguard1
Switch(config-dhcp-guard)# device-role server
Switch(config-dhcp-guard)#
```

24.3 match ipv6 access-list

Данная команда используется для проверки IPv6-адреса источника в сообщениях сервера. Чтобы отключить проверку, воспользуйтесь формой **no** этой команды.

```
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 данная функция отключена.

Режим ввода команды

DHCPv6 Guard Policy Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для фильтрации DHCPv6-сообщений сервера на основе IP-адреса источника. Если не настроена команда **match ipv6 access-list**, все сообщения сервера будут игнорироваться. Список доступа настраивается с помощью команды **ipv6 access-list**.

Пример

В данном примере показано, как создать политику DHCPv6 Guard и настроить проверку соответствия адресов IPv6 со списком доступа list1.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp guard policy dhcp_filter1
Switch(config-dhcp-guard)# match ipv6 access-list list1
Switch(config-dhcp-guard)#
```

24.4 ipv6 dhcp guard attach-policy

Данная команда используется для применения политики DHCPv6 Guard Policy на определенном интерфейсе. Чтобы удалить привязку, воспользуйтесь формой **no** этой команды.

ipv6 dhcp guard attach-policy [*POLICY-NAME* [vlan {add | remove} *VLAN-ID-LIST*]]
no ipv6 dhcp guard attach-policy

Параметры

<i>POLICY-NAME</i>	(Опционально.) Укажите имя политики DHCPv6 Guard.
vlan add <i>VLAN-ID-LIST</i>	(Опционально.) Укажите VLAN для проверки. Если VLAN не указана, проверяться будут все VLAN.
vlan remove <i>VLAN-ID-LIST</i>	(Опционально.) Укажите VLAN, для которой необходимо отменить проверку.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для применения политики DHCPv6 Guard на интерфейсе. Политики DHCPv6 Guard используются для блокировки DHCPv6-сообщений сервера или фильтрации сообщений сервера на основе IP-адреса источника. Если имя политики не указано, то политика по умолчанию настроит устройство в качестве клиента.

Пример

В данном примере показано, как применить политику DHCPv6 Guard «pol1» для интерфейса Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ipv6 dhcp guard attach-policy pol1
Switch(config-if)#
```

24.5 show ipv6 dhcp guard policy

Данная команда используется для отображения информации 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если имя политики не указано, отображается информация для всех политик.

Пример

В данном примере показано, как включить отображение информации для всех политик.

```
Switch# show ipv6 dhcp guard policy

DHCP guard policy: default
  Device Role: DHCP client
  Target: eth1/0/3

DHCP guard policy: test1
  Device Role: DHCP server
  Source Address Match Access List: acl1
  Target: eth1/0/1

Switch#
```

Отображаемые параметры

Device Role	Роль устройства: клиент или сервер.
Target	Имя интерфейса.
Source Address Match Access List	Список доступа IPv6 указанной политики.

25. Команды DHCPv6 Relay

25.1 ipv6 dhcp relay destination

Данная команда используется, 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

Параметры

IPV6-ADDRESS	Укажите адрес DHCPv6 Relay Destination.
INTERFACE-ID	(Опционально.) Укажите выходной интерфейс для Relay Destination.

По умолчанию

По умолчанию данная функция 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**. Для удаления адреса Relay используйте команду **no ipv6 dhcp relay destination**. При удалении всех адресов Relay функция Relay будет отключена.

Входящие сообщения DHCPv6, поступающие от клиента, могут быть заранее ретранслированы при помощи Relay Agent. Адрес назначения, который необходимо ретранслировать, может принадлежать DHCPv6-серверу или другому DHCPv6 Relay Agent.

В качестве адреса назначения может быть использован индивидуальный или групповой адрес, оба могут быть как Link Scoped, так и Global Scoped. Для адресов Link Scoped необходимо указать интерфейс, в котором расположен адрес назначения. Для адресов Global Scoped можно указать выходной интерфейс (опционально). Если выходной интерфейс не указан, он определяется при помощи таблицы маршрутизации.

Для одного интерфейса можно указать несколько адресов Relay Destination. Если сообщение DHCPv6 ретранслируется на групповой адрес, для поля hop limit в заголовке пакета IPv6 будет установлено значение 32.

Пример

В данном примере показано, как сконфигурировать адрес Relay Destination на VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 vlan1
Switch(config-if)# ipv6 dhcp relay destination FE80::22:33 vlan2
Switch(config-if)#
```

25.2 ipv6 dhcp relay remote-id format

Данная команда используется для настройки sub-опции Remote ID. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay remote-id format {default | cid-with-user-define | user-define | expert-udf}
no ipv6 dhcp relay remote-id format

Параметры

default

Укажите, чтобы использовать системный MAC-адрес коммутатора в качестве Remote ID. Формат Remote ID представлен ниже:

F01	F02	F03	F04	F05
Sub Type	VLAN ID	Module ID	Port ID	MAC Address
1 byte	2 bytes	1 byte	1 byte	6 bytes

F01. Тип sub-опции: число 1 свидетельствует о том, что тип данного ID – Remote ID.

F02. VLAN ID: входящий VLANID в пакете DHCP client.

F03. ID модуля: ID модуля для автономных коммутаторов – 0. ID модуля для стекированных коммутаторов – Unit ID.

F04. ID порта: номер входящего порта в пакете DHCP client. Номера портов начинаются с 1.

F05. MAC-адрес: системный MAC-адрес коммутатора.

cid-with-user-define

Укажите, чтобы использовать CID со строкой, заданной пользователем, в качестве Remote ID. Формат Remote ID представлен ниже:

F01	F02	F03	F04	F05
Sub Type	VLAN ID	Module ID	Port ID	User Defined
1 byte	2 bytes	1 byte	1 byte	Max. 256 bytes

F01. Тип sub-опции: число 2 свидетельствует о том, что тип данного ID – Remote ID.

F02. VLAN ID: входящий VLAN ID в пакете DHCP client.

F03. ID модуля: ID модуля для автономных коммутаторов – 0.
ID модуля для стекированных коммутаторов – Unit ID.

F04. ID порта: номер входящего порта в пакете DHCP client.
Номера портов начинаются с 1.

F05. Задать самостоятельно: заданная пользователем строка, настраиваемая при помощи команды **ipv6 dhcp relay remote-id udf**. По умолчанию данное поле не заполнено.

user-define

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

```
|-----|
| F01          | F02          |
|-----|-----|
| Sub Type      | User Defined  |
|-----|-----|
| 1 byte        | Max. 256 bytes |
|-----|
```

F01. Тип sub-опции: число 3 свидетельствует о том, что тип данного ID – Remote ID.

F02. Задать самостоятельно: заданная пользователем строка, настраиваемая при помощи команды **ipv6 dhcp relay remote-id udf**.

expert-udf

Укажите, чтобы задать Remote ID самостоятельно. Формат удаленного ID представлен ниже:

```
|-----|
| F01          |
|-----|
| User Defined  |
|-----|
| Max. 256 bytes |
|-----|
```

F01. Задать самостоятельно: произвольная заданная пользователем строка, настраиваемая при помощи команд **ipv6 dhcp relay remote-id format-type**, **ipv6 dhcp relay remote-id profile** и **format string**. По умолчанию данное поле не заполнено.

По умолчанию

Формат DHCPv6 Relay Remote ID по умолчанию – **default**.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить sub-опцию Remote ID.

Пример

В данном примере показано, как настроить sub-опцию Remote ID «cid-with-user-define».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id format cid-with-user-define
Switch(config)#
```

25.3 ipv6 dhcp relay remote-id option

Данная команда используется, 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 функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить встраивание функции DHCPv6 Relay Agent Remote ID Option.

Пример

В данном примере показано, как включить встраивание DHCPv6 Relay Agent Remote ID Option.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id option
Switch(config)#
```

25.4 ipv6 dhcp relay remote-id policy

Данная команда используется, чтобы настроить политику 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 напрямую ретранслировать пакет запроса DHCPv6, в котором уже есть Relay Agent Remote ID Option, на сервер DHCPv6 в неизменном виде.

По умолчанию

Параметр по умолчанию – **keep**.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить глобальную политику для пакетов, в которых уже есть Option 37. При выборе политики **drop** полученный от клиента пакет, в котором уже присутствует Relay Agent Remote ID Option, будет отброшен. При выборе политики **keep** коммутатор не будет проверять, присутствует ли в полученном пакете Relay Agent Remote ID Option.

Пример

В данном примере показано, как настроить политику DHCPv6 Relay Agent Remote ID Option так, чтобы пакет был отброшен при наличии в нем Relay Agent Remote ID Option.

```
Switch# configure terminal  
Switch(config)# ipv6 dhcp relay remote-id policy drop  
Switch(config)#
```

25.5 ipv6 dhcp relay remote-id udf

Используйте данную команду, чтобы настроить User Define Field (UDF) для Remote ID. 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 примере ниже показано, как настроить UDF (шестнадцатеричная строка) «010c08».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id udf hex 010c08
Switch(config)#
```

25.6 show ipv6 dhcp

Данная команда используется для отображения настроек DHCPv6 на интерфейсе.

show ipv6 dhcp [interface [INTERFACE-ID]]

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса VLAN для отображения.
--------------	--

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить DHCPv6 DUID устройства. Для отображения настроек DHCPv6 и информации об указанном интерфейсе VLAN используйте команду **show ipv6 dhcp interface**. Если ID интерфейса не указан, будут отображены все интерфейсы, для которых включена функция DHCPv6.

Пример

В данном примере показано, как отобразить настройки DHCPv6 для VLAN 1, если режим DHCPv6 Relay Mode включен.

```
Switch # show ipv6 dhcp interface vlan1

vlan1 is in relay mode
  Relay destinations:
    FE80::20A:BBFF:FECC:102 via vlan 2

Switch #
```

В примере ниже показано, как отобразить информацию о DHCPv6 для интерфейса VLAN 1, если режим DHCPv6 Mode отключен.

```
Switch# show ipv6 dhcp interface vlan1

vlan 1 is not in DHCPv6 mode

Switch#
```

25.7 show ipv6 dhcp relay information option

Данная команда используется для отображения настроек DHCPv6 Relay Information Option.

show ipv6 dhcp relay information option

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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 том, что тип данного ID – Interface ID.

F02. VLAN ID: исходящий VLAN ID в пакете DHCP client.

F03. ID модуля: ID модуля для автономных коммутаторов – 0. ID модуля для стекированных коммутаторов – Unit ID.

F04. ID порта: номер входящего порта в пакете DHCP client. Номера портов начинаются с 1.

vendor1

Укажите, чтобы использовать vendor 1. Формат Interface ID показан ниже:

F01	F02	F03	F04	F05
E	t	h	e	r
(0x45)	(0x74)	(0x68)	(0x65)	(0x72)
1 byte	1 byte	1 byte	1 byte	1 byte

F06	F07	F08	F09	F10
n	e	t	Chassis ID	/
(0x6E)	(0x65)	(0x74)		(0x2F)
1 byte	1 byte	1 byte	1~2 byte	1 byte

F11	F12	F13	F14	F15
0	/	Port	:	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. *Косая черта (/)*: код ASCII – 0x2F.

F11. *0*: Код ASCII – 0x30.

F12. *Косая черта (/)*: код ASCII – 0x2F.

F13. *Номер порта*: номер входящего порта в пакете DHCP client.

F14. *Двоеточие (:)*: код ASCII – 0x3A.

F15. *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. *Косая черта (/)*: код ASCII – 0x2F.

F21. *0*: Код ASCII – 0x30.

F22. *Косая черта (/)*: код ASCII – 0x2F.

F23. *0*: Код ASCII – 0x30.

F24. *Косая черта (/)*: код ASCII – 0x2F.

F25. *ID шасси*: номер шасси. ID шасси для автономных коммутаторов – 0. ID шасси для стекированных коммутаторов – Unit ID.

F26. Косая черта (/): код ASCII – 0x2F.

F27. 0: Код ASCII – 0x30.

F28. Косая черта (/): код ASCII – 0x2F.

F29. Номер порта: номер входящего порта в пакете DHCP client.

expert-udf

Укажите, чтобы задать Interface ID самостоятельно. Формат Interface ID представлен ниже:

```
|-----|
|  F01  |
|-----|
| User Defined |
|-----|
| Max. 255 bytes |
|-----|
```

F01. Задать самостоятельно: заданная пользователем строка, настраиваемая при помощи команд **ipv6 dhcp relay interface-id format-type expert-udf**, **ipv6 dhcp relay interface-id profile** и **format string**. По умолчанию данное поле не заполнено.

По умолчанию

Формат DHCPv6 Relay Interface ID по умолчанию – **default**.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить sub-опцию Interface ID.

Пример

В данном примере показано, как настроить sub-опцию Interface ID «cid».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay interface-id format cid
Switch(config)#
```

25.9 ipv6 dhcp relay interface-id option

Данная команда используется, 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 функция включена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить встраивание функции DHCPv6 Relay Agent Interface ID Option.

Пример

В данном примере показано, как включить встраивание DHCPv6 Relay Agent Interface ID Option.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay interface-id option
Switch(config)#
```

25.10 ipv6 dhcp relay interface-id policy

Данная команда используется, чтобы настроить политику перенаправления Option 18 для DHCPv6 Relay Agent. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** данной 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 напрямую 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 (drop) при наличии в нем Relay Agent Interface ID Option.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay interface-id policy drop
Switch(config)#
```

25.11 ipv6 dhcp local-relay vlan

Данная команда используется для включения DHCPv6 Local Relay на VLAN или группе VLAN. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ipv6 dhcp local-relay vlan *VLAN-ID* [, | -]
no ipv6 dhcp local-relay vlan *VLAN-ID* [, | -]

Параметры

<i>VLAN-ID</i>	Укажите ID VLAN, которую необходимо настроить.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для настройки функции DHCPv6 Local Relay.

Если функция DHCPv6 Local Relay включена, коммутатор добавит Option 37 и Option 18 в пакеты запроса клиента.

Если проверка Option 37 включена, коммутатор проверит пакет запроса, полученный от клиента, при этом пакет, содержащий Option 37, в соответствии с функцией DHCPv6 Relay будет отброшен.

Если проверка Option 37 отключена, функция Local Relay будет добавлять Option 37 в пакет запроса вне зависимости от того, включена Option 37 или выключена.

Функция DHCPv6 Local Relay напрямую передаст пакет от сервера клиенту.



Примечание: если на интерфейсе отключена команда **ipv6 dhcp relay enable**, ретрансляция и локальная ретрансляция полученных пакетов DHCPv6 выполняться не будет.

Пример

В данном примере показано, как включить функцию DHCPv6 Local Relay на VLAN 100.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp local-relay vlan 100
Switch(config)#
```

25.12 ipv6 dhcp relay enable

Данная команда используется для включения функции DHCPv6 Relay на порту. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ipv6 dhcp relay enable
no ipv6 dhcp relay enable

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 настроить функцию DHCPv6 Relay для каждого порта.

Пример

В данном примере показано, как отключить функцию DHCPv6 Relay на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#no ipv6 dhcp relay enable
Switch(config-if)#
```

25.13 ipv6 dhcp relay information option mac-format case

Данная команда используется для настройки формата MAC-адреса, задаваемого пользователем в профиле DHCPv6 Option 18 или Option 37. Чтобы вернуться 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 Option 18 или Option 37 для задаваемого пользователем профиля: aa-bb-cc-dd-ee-ff.
uppercase	Укажите, чтобы использовать верхний регистр при записи MAC-адреса Option 18 или Option 37 для задаваемого пользователем профиля: AA-BB-CC-DD-EE-FF.
hyphen	Укажите, чтобы использовать «-» в качестве разделителя данных: AA-BB-CC-DD-EE-FF.
colon	Укажите, чтобы использовать «:» в качестве разделителя данных: AA:BB:CC:DD:EE:FF.
dot	Укажите, чтобы использовать «.» в качестве разделителя данных: AA.BB.CC.DD.EE.FF.
none	Укажите для ввода данных без разделителя: AABCCDDEEFF.
number	Укажите количество разделителей: 1: один разделитель: AABCC.DDEEFF. 2: два разделителя: AAB.CCDD.EEFF. 5: множество разделителей: AA.BB.CC.DD.EE.FF. Если указан параметр none , параметр number будет недействителен.

По умолчанию

Параметр регистра MAC-адреса аутентификации по умолчанию – **uppercase**.

Параметр разделителя MAC-адреса аутентификации по умолчанию – **none**.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить формат MAC-адреса, задаваемого пользователем в профиле Option 18 или Option 37.

Пример

В данном примере показано, как настроить формат MAC-адреса, задаваемого пользователем в профиле Option 18 или Option 37.

```
Switch#configure terminal
Switch(config)# ipv6 dhcp relay information option mac-format case uppercase delimiter hyphen
number 5
Switch(config)#
```

25.14 show ipv6 dhcp relay information option mac-format

Данная команда используется для отображения формата MAC-адреса в профиле Option 18 и Option 37.

show ipv6 dhcp relay information option mac-format

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить формат MAC-адреса в профиле Option 18 и Option 37.

Пример

В данном примере показано, как отобразить формат MAC-адреса в профиле Option 18 и Option 37.

```
Switch#show ipv6 dhcp relay information option mac-format

Case           : Uppercase
Delimiter      : Hyphen
Delimiter Number : 5
Example        : AA-BB-CC-DD-EE-FF

Switch#
```

25.15 ipv6 dhcp relay remote-id format-type expert-udf

Данная команда используется для настройки строки Option 37 expert UDF на порту. Чтобы вернуться 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

<i>STRING</i>	Укажите имя профиля Option 37.
---------------	--------------------------------

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить строку Option 37 expert UDF на порту.

Пример

В данном примере показано, как настроить Option 37 на интерфейсе Ethernet 1/0/1, выбрав профиль «profile1».

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#ipv6 dhcp relay remote-id format-type expert-udf profile1
Switch(config-if)#
```

25.16 ipv6 dhcp relay interface-id format-type expert-udf

Данная команда используется для настройки строки Option 18 expertUDF на порту. Чтобы вернуться 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 интерфейсе Ethernet 1/0/1, выбрав профиль «profile2».

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#ipv6 dhcp relay interface-id format-type expert-udf profile2
Switch(config-if)#
```

25.17 show ipv6 dhcp relay interface-id profile

Данная команда используется для отображения профилей Option 18.

show ipv6 dhcp relay interface-id profile

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить профили Option 18.

Пример

В данном примере показано, как отобразить профили Option 18.

```
Switch#show ipv6 dhcp relay interface-id profile

Option18 Profile name: profile2
Format string: "Ethernet %unit:/0/ %port:\:%sysname:%05svlan"

Total Entries:1

Switch#
```

25.18 show ipv6 dhcp relay remote-id profile

Данная команда используется для отображения профилей Option 37.

show ipv6 dhcp relay remote-id profile

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить профили Option 37.

Пример

В данном примере показано, как отобразить профили Option 37.

```
Switch#show ipv6 dhcp relay remote-id profile

Option37 Profile name: profile1
Format string: "Ethernet %unit:/0/  %port:\:%sysname:%05svlan"

Total Entries:1

Switch#
```


26. Команды DHCPv6 Server

26.1 address prefix

Данная команда используется для указания префикса адреса, который будет присвоен клиенту. Чтобы удалить префикс адреса, воспользуйтесь формой **no** этой команды.

**address prefix IPV6-PREFIXIPPREFIX-LENGTH [lifetime VALID-LIFETIME
PREFERRED-LIFETIME]**
no address prefix

Параметры

<i>IPV6-PREFIX</i>	Укажите префикс IPv6-адреса, который необходимо присвоить клиенту.
<i>PREFIX-LENGTH</i>	Укажите длину префикса IPv6-адреса.
lifetime <i>VALID-LIFETIME</i>	(Опционально.) Укажите значение допустимого времени жизни (Valid Lifetime) для префикса адреса в секундах. Значение Valid Lifetime должно превышать значение предпочтительного времени жизни (Preferred Lifetime). Диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime не задано, устанавливается значение Valid Lifetime по умолчанию – 2592000 секунд (30 дней).
<i>PREFERRED-LIFETIME</i>	(Опционально.) Укажите значение Preferred Lifetime для префикса адреса в секундах. 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. После получения запроса от клиента сервер выполнит проверку пула IPv6 DHCP, ассоциированного с получающим интерфейсом. Если статические записи привязки адреса настроены так, чтобы присваивать адрес запрашивающему клиенту, то 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 под названием «pool1».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# address prefix 2001:0DB8::0/64 lifetime 200 100
Switch(config-dhcp)#
```

26.2 address-assignment

Данная команда используется для указания адреса, который необходимо присвоить обозначенному клиенту. Чтобы удалить адрес статической привязки, воспользуйтесь формой **no** этой команды.

address-assignment IPV6-ADDRESS/PREFIX-LENGTH CLIENT-DUID [**iaid** IAID] [**lifetime** VALID-LIFETIME PREFERRED-LIFETIME]
no address-assignment IPV6-ADDRESS/PREFIX-LENGTH

Параметры

IPV6-ADDRESS	Укажите IPv6-адрес, который необходимо присвоить обозначенному клиенту.
PREFIX-LENGTH	Укажите длину IPv6-префикса.
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). 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. Диапазон значений: от 60 до 4294967295 или до бесконечности. Если значение Lifetime для адреса не задано, устанавливается значение Preferred Lifetime по умолчанию – значение Preferred Lifetime для пула.

По умолчанию

Нет.

Режим ввода команды

DHCPv6 Pool Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить статическую запись привязки адреса так, чтобы она указывала адрес, который необходимо присвоить обозначенному клиенту.

После получения запроса от клиента сервер выполнит проверку пула IPv6 DHCP, ассоциированного с полученным интерфейсом. Если сообщение request содержит опцию IANA, и имеются свободные статические записи, настроенные с IAID и соответствующие DUID и IAID сообщения, соответствующая запись будет присвоена. Если соответствующая запись отсутствует, но есть свободные статические записи без указанных IAID, которые соответствуют DUID сообщения, на соответствующую запись будет отправлен ответ.

При отсутствии соответствующих записей клиенту будет присвоен адрес из префикса адреса, указанного в пуле IPv6 DHCP.

Пример

В данном примере показано, как настроить статическую запись привязки адреса в пуле IPv6 DHCP «pool1» и ассоциировать пул IPv6 DHCP с VLAN 100.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(dhcpv6-config)# address-assignment 2001:0DB8::1:2 000300010506BBCCDDEE
Switch(dhcpv6-config)# exit
Switch(config)# interface vlan 100
Switch(dhcpv6-config)# ipv6 dhcp server pool1
Switch(dhcpv6-config)#
```

В примере ниже показано, как настроить статическую запись привязки адреса в пуле IPv6 DHCP «pool2» с опцией IAID и ассоциировать пул IPv6 DHCP с VLAN 200.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool2
Switch(dhcpv6-config)# address-assignment 2001:AAB8::2:2 00030001050611223344 iaid 1234
Switch(dhcpv6-config)# exit
Switch(config)# interface vlan 200
Switch(config-if)# ipv6 dhcp server pool2
Switch(config-if)#
```

26.3 clear ipv6 dhcp binding

Данная команда используется для удаления записей привязки DHCPv6-сервера.

clear ipv6 dhcp binding {all | IPV6-PREFIX}

Параметры

all	Укажите, чтобы удалить все записи привязки.
IPv6-PREFIX	Укажите, чтобы удалить запись привязки по префиксу.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы удалить записи привязки DHCPv6-сервера. При указании IPv6-префикса будет удалена запись привязки к обозначенному клиенту. Если IPv6-префикс не указан, будут удалены все записи привязки. IPv6-префикс будет возвращен в пул, которому изначально был назначен.

Пример

В данном примере показано, как удалить все записи привязки в таблице привязок DHCPv6-сервера.

```
Switch# clear ipv6 dhcp binding all
Switch#
```

26.4 domain-name

Данная команда используется для назначения имени домена запрашивающему DHCPv6-клиенту. Чтобы удалить настройки имени домена, воспользуйтесь формой **no** этой команды.

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)#
```

26.5 dns-server

Данная команда используется для назначения списка серверов DNS IPv6 запрашивающему IPv6-клиенту. Чтобы удалить DNS-сервер из списка серверов, воспользуйтесь формой **no** этой команды.

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)#
```

26.6 ipv6 dhcp excluded-address

Данная команда используется для указания IPv6-адресов, которые DHCPv6-сервер не должен присваивать DHCP-клиентам. Чтобы удалить исключенные IPv6-адреса, воспользуйтесь формой **no** этой команды.

ipv6 dhcp excluded-address *LOW-ADDRESS* [*HIGH-ADDRESS*]
no ipv6 dhcp excluded-address *LOW-ADDRESS* [*HIGH-ADDRESS*]

Параметры

<i>LOW-ADDRESS</i>	Укажите исключенный IPv6-адрес или первый IPv6-адрес в диапазоне исключенных адресов.
<i>HIGH-ADDRESS</i>	(Опционально.) Укажите последний IPv6-адрес в диапазоне исключенных адресов.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Сервер DHCPv6 предполагает, что клиенту может быть присвоен любой адрес (кроме IPv6-адреса коммутатора). Используйте данную команду, чтобы исключить присвоение одного IPv6-адреса или диапазона IPv6-адресов. Исключенные адреса могут быть присвоены только пулу/пулам адресов.

Пример

В данном примере показано, как исключить IPv6-адрес 3004:DB8::1:10.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp excluded-address 3004:DB8::1:10
Switch(config)#
```

26.7 ipv6 dhcp pool

Данная команда используется для входа в режим DHCP Pool Configuration Mode и настройки пула IPv6 DHCP. Чтобы удалить пул IPv6 DHCP, воспользуйтесь формой **no** этой команды.

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, чтобы войти в режим IPv6 DHCP Pool Configuration Mode и настроить пул IPv6 DHCP. Команда **ipv6 dhcp server** применяется для включения DHCP IPv6 Server Service на интерфейсе и указания пула IPv6 DHCP, используемого для обслуживания DHCP-запроса, полученного на интерфейсе.

Пример

В данном примере показано, как настроить пул адресов «pool1».

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)#
```

26.8 ipv6 dhcp server

Данная команда используется для включения DHCP IPv6 Server Service на интерфейсе. Чтобы отключить DHCP IPv6 Server Service, воспользуйтесь формой **no** этой команды.

ipv6 dhcp server POOL-NAME [rapid-commit]
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.
---------------------	---

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить DHCP для IPv6 Server Service на указанном интерфейсе.

Один пул IPv6 DHCP можно ассоциировать с несколькими интерфейсами, при этом с одним интерфейсом можно ассоциировать только один пул IPv6 DHCP. Перед ассоциированием пул необходимо настроить. Для IPv6 Client функции DHCP-Server DHCP-Relay несовместимы на одном интерфейсе.

Стандартный обмен сообщениями между маршрутизаторами DR и RR включает в себя четыре типа сообщений: *SOLICIT*, *ADVERTISE*, *REQUEST* и *REPLY*. При использовании параметра **rapid-commit** маршрутизаторы обмениваются двумя сообщениями вместо четырех. В этом случае маршрутизатор RR отправит маршрутизатору DR сообщение *SOLICIT*, в котором уведомит его о возможности пропустить получение сообщения *ADVERTISE* и отправку сообщения *REQUEST* и перейти непосредственно к получению сообщения *REPLY* от маршрутизатора DR. В сообщении *REPLY* содержится информация по сетевым настройкам.

Для корректной работы данного функционала необходимо включить параметр **rapid-commit** и на DR, и на RR.

Пример

В данном примере показано, как создать DHCP-пул «pool1» и использовать его для передачи префиксов, включив DHCP IPv6 Server Service на интерфейсе VLAN 100.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# exit
Switch(config)# interface vlan 100
Switch(config-if)# ipv6 dhcp server pool1
Switch(config-if)#
```

26.9 service ipv6 dhcp

Данная команда используется для включения сервера IPv6 DHCP и Relay Service на коммутаторе. Чтобы отключить сервер IPv6 DHCP и Relay Service, воспользуйтесь формой **no** этой команды.

service ipv6 dhcp

no service ipv6 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, чтобы глобально включить сервер IPv6 DHCP и Relay Service на коммутаторе. Для вступления настроек в силу необходимо сначала отключить, а затем снова включить DHCPv6-сервер.

Пример

В данном примере показано, как включить сервер IPv6 DHCP и Relay Service.

```
Switch# configure terminal
Switch(config)# service ipv6 dhcp
Switch(config)#
```

26.10 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения DHCPv6 DUID устройства. Используйте команду **show ipv6 dhcp interface**, чтобы отобразить настройки DHCPv6 для интерфейсов. Если ID интерфейса не указан, будут отображены все интерфейсы, на которых включена функция DHCPv6.

Пример

В данном примере показано, как отобразить информацию о DHCPv6 для интерфейса VLAN 1, если на VLAN 1 отключен DHCPv6.

```
Switch# show ipv6 dhcp interface vlan1

vlan 1 is not in DHCPv6 mode

Switch#
```

В примере ниже показано, как отобразить DHCPv6 Client для интерфейса VLAN 1, если на VLAN 1 включен DHCPv6-сервер.

```
Switch# show ipv6 dhcp interface vlan1

vlan 1 is in server mode
  IPv6 DHCP pool is test
  Preference value: 0
  Hint from client: ignored
  Rapid-Commit is disabled

Switch#
```

26.11 show ipv6 dhcp binding

Данная команда используется для отображения записи привязки IPv6-префикса.

show ipv6 dhcp binding [IPv6-PREFIX]

Параметры

<i>IPv6-PREFIX</i>	(Опционально.) Укажите, чтобы отобразить запись привязки.
--------------------	---

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

При использовании данной команды без указания параметра *IPv6-PREFIX* будут отображены все привязки префикса DHCPv6 клиента в таблице привязок. При указании параметра *IPv6-PREFIX* будет отображена только привязка префикса указанного клиента.

Пример

В данном примере показано, как отобразить запись привязки IPv6-префикса.

```
Switch# show ipv6 dhcp binding

Client DUID : 00030001aabbcd000001
            address: 1234::2
            preferred lifetime 200 ,valid lifetime 300

Client DUID : 00030001aabbcd000000
            address: 1234::3
            preferred lifetime 200 ,valid lifetime 300

Client DUID : 00030001aabbcd000002
            address: 1234::4
            preferred lifetime 200 ,valid lifetime 300

Total Entries: 3

Switch#
```

26.12 show ipv6 dhcp pool

Данная команда используется для отображения информации о настройках пула DHCPv6-сервера.

show ipv6 dhcp pool [*POOL-NAME*]

Параметры

<i>POOL-NAME</i>	(Опционально.) Укажите, чтобы отобразить пул IPv6 DHCP.
------------------	---

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

При использовании данной команды без указания имени пула будет отображена информация о настройках всех пулов DHCPv6-сервера. При указании параметра *POOL-NAME* будет отображена информация только об указанном пуле.

Пример

В данном примере показано, как отобразить информацию о DHCPv6-пуле.

```
Switch# show ipv6 dhcp pool

DHCPv6 pool: pool1
  Static bindings:
    Binding for client 00030001aabbcd000080
    IA PD: IA ID 0x0001
    Prefix: 3000:0:300::/48
    preferred lifetime 604800, valid lifetime 2592000
  Prefix delegation pool: abc
    preferred lifetime 604800, valid lifetime 2592000
  DNS server: 2345::2
  Domain name: pool1.com
  Active clients: 0

DHCPv6 pool: pool2
  DNS server: 6000::2
  DNS server: 6000::9
  Domain name: pool2.com
  Active clients: 0

DHCPv6 pool: test
  Static bindings:
    Binding for client 00030001aabbcd001234
    IA NA: IA ID not specified
    Address: 1234::1234
    preferred lifetime 604800, valid lifetime 2592000
  Address prefix: 1234::/64
    preferred lifetime 200, valid lifetime 300
  DNS server:
  Domain name:
  Active clients: 3

Switch#
```

Отображаемые параметры

DHCPv6 pool	Имя пула.
Binding for client 000300010002FCA5C01C	Статическая привязка для клиента с DUID 000300010002FCA5C01C.
IAPD	Серия префиксов, присвоенных клиенту.
IAID	Идентификатор данной IAPD.
Prefix	Префиксы, которые необходимо делегировать.
preferred lifetime, valid lifetime	Значения Preferred Lifetime и Valid Lifetime для префикса, присвоенные клиенту.

DNS server	Список адресов DNS-сервера.
Domain name	Список настроенных DNS-доменов.
Active clients	Общее количество активных клиентов.

26.13 show ipv6 excluded-address

Данная команда используется для отображения информации о настройках исключенных IPv6-адресов.

show ipv6 excluded-address

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить диапазон исключенных адресов.

Пример

В данном примере показано, как отобразить исключенные адреса.

```
Switch# show ipv6 excluded-address

IPv6 excluded address:
1.3004:DB8::1:10
2.3004:DBB::1:100 - 3004:DBB::1:105

Total Entries: 2

Switch#
```

26.14 show ipv6 dhcp operation

Данная команда используется, чтобы отобразить информацию о работе для DHCPv6-сервера.

show ipv6 dhcp operation

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о работе для DHCPv6-сервера.

Пример

В данном примере показано, как отобразить информацию о работе для DHCPv6-сервера.

```
switch# show ipv6 dhcp operation

DHCPv6 pool: pool1
  Prefix delegation pool: abc, prefix is 3000::/32 48
  Static bindings:
    Binding for client 00030001aabbcd000080
      IA PD: IA ID 0x0001
      Prefix: 3000:0:300::/48
      preferred lifetime 604800, valid lifetime 2592000
  preferred lifetime 604800, valid lifetime 2592000
  DNS server: 2345::2
  Domain name: pool1.com

DHCPv6 pool: test
  Address prefix: 1234::/64
  Static bindings:
    Binding for client 00030001aabbcd001234
      IA NA: IA ID not specified
      Address: 1234::1234
      preferred lifetime 604800, valid lifetime 2592000
  preferred lifetime 200, valid lifetime 300
  DNS server: 2000::2
  Domain name: test.com

switch#
```

27. Команды Digital Diagnostics Monitoring (DDM)

27.1 show interfaces transceiver

Данная команда используется для отображения текущих операционных параметров оптического модуля.

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

Параметры

<i>INTERFACE-ID</i>	(Опционально.) Укажите интерфейсы, для которых необходимо отобразить статус Transceiver Monitoring. Если Interface ID не указаны, будут отображены статусы Transceiver Monitoring для всех действующих интерфейсов.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
detail	(Опционально.) Укажите, чтобы отобразить подробную информацию.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить текущие операционные параметры Transceiver Monitoring для оптического модуля на указанных портах.

Пример

В данном примере показано, как отобразить текущие операционные параметры для всех портов, поддерживающих функцию Transceiver Monitoring.

```
Switch#show interfaces transceiver

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm
mA: milliamperes, mW: milliwatts

Transceiver Monitoring traps: None

port      Temperature Voltage      Bias Current TX Power      RX Power
(Celsius) (V)          (mA)         (mW/dbm)      (mW/dbm)
-----
eth1/0/27 30.845      3.284        7.895        0.604        0.470
              -2.189        -3.279

Total Entries: 1

Switch#
```

В примере ниже показано, как отобразить подробную информацию Transceiver Monitoring для всех портов, поддерживающих данную функцию.

```
Switch#show interfaces transceiver detail

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm
mA: milliamperes, mW: milliwatts
A: The threshold is administratively configured.

eth1/0/27
Transceiver Monitoring is enabled
Transceiver Monitoring shutdown action: None

Current      High-Alarm   High-Warning Low-Warning  Low-Alarm
Temperature(C) 30.803      78.000       73.000      -8.000      -13.000
Voltage(V)      3.284       3.700       3.600       3.000       2.900
Bias Current(mA) 7.890       11.800      10.800      5.000       4.000
TX Power(mW)    0.604       0.832       0.661       0.316       0.251
              (dbm) -2.191      -0.800      -1.800      -5.000      -6.000
RX Power(mW)    0.470       1.000       0.794       0.016       0.010
              (dbm) -3.283      0.000      -1.000     -18.013     -20.000

Switch#
```

27.2 snmp-server enable traps transceiver-monitoring

Данная команда используется для включения отправки всех или определенных SNMP-уведомлений Optical Transceiver Monitoring. Чтобы отключить отправку уведомлений, воспользуйтесь формой **no** этой команды.

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 параметры не указаны, будут включены/отключены все SNMP-уведомления Transceiver Monitoring.

Пример

В данном примере показано, как включить отправку уведомлений уровня warning.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps transceiver-monitoring warning
Switch(config)#
```

27.3 transceiver-monitoring action shutdown

Данная команда используется для отключения порта при обнаружении события alarm (тревога) или warning (предупреждение). Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

transceiver-monitoring action shutdown {alarm | warning}

no transceiver-monitoring action shutdown



Примечание: команды Transceiver Monitoring применимы только к портам с оптоволоконными модулями (т. е. Ethernet 1/0/27 ~ 1/0/30) и используются только в том случае, если стекирование отключено.

Параметры

alarm	Укажите, чтобы отключить порт при обнаружении события alarm.
warning	Укажите, чтобы отключить порт при обнаружении события warning.

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 настроить интерфейс физического порта.

Данная команда позволяет указать, будет ли отключен порт при обнаружении события alarm / события warning. Если функция Monitoring включена, отслеживаются события alarm и события warning. Событие alarm происходит, если отслеживаемые параметры выходят за пределы верхнего или нижнего порога alarm. Событие warning происходит, если отслеживаемые параметры выходят за пределы верхнего или нижнего порога warning.

Отключение порта контролируется модулем Error Disable без таймера восстановления (recovery). Пользователь может включить порт вручную, применив команду **shutdown**, а затем команду **no shutdown**.

Пример

В данном примере показано, как настроить отключение интерфейса Ethernet 1/0/29 при обнаружении события alarm.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/29
Switch(config-if)# transceiver-monitoring action shutdown alarm
Switch(config-if)#
```

27.4 transceiver-monitoring bias-current

Данная команда используется для настройки порогов тока смещения на указанном порту. Чтобы удалить заданные настройки, воспользуйтесь формой **no** этой команды.

transceiver-monitoring bias-current *INTERFACE-ID* {high | low} {alarm | warning} *VALUE*
no transceiver-monitoring bias-current *INTERFACE-ID* {high | low} {alarm | warning}



Примечание: команды Transceiver Monitoring применимы только к портам с оптоволоконными модулями (т. е. Ethernet 1/0/27 ~ 1/0/30) и используются только в том случае, если стекирование отключено.

Параметры

<i>INTERFACE-ID</i>	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.

low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
VALUE	Укажите порог в диапазоне от 0 до 131 мА.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данный функционал доступен только для интерфейсов портов SFP28 (или опционально SFP+) с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда позволяет настроить пороги тока смещения на указанных портах. Заданные значения сохраняются как в системе, так и в трансиверах SFP28/SFP+, а также будут направлены в оптический модуль в 16-битном формате.

Если конфигурируемый модуль SFP28/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

С помощью формы **no** данной команды можно удалить заданные пороговые значения, сохраненные в системе. При этом пороговые значения, сохраненные в оптических трансиверах, остаются неизменными. Используйте форму **no**, чтобы предотвратить изменения пороговых значений в оптическом трансивере при его первом подключении.

Пример

В данном примере показано, как настроить верхний порог warning для тока смещения на интерфейсе Ethernet 1/0/29. Указанное значение – 10,237 мА.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring bias-current ethernet 1/0/29 high warning 10.237

WARNING: A closest value 10.236 is chosen according to the transceiver-monitoring precision
definition

Switch(config)#
```

27.5 transceiver-monitoring enable

Данная команда используется для включения функции Optical Transceiver Monitoring на

оптоволоконном порту. Чтобы отключить функцию Optical Transceiver Monitoring, воспользуйтесь формой **no** этой команды.

transceiver-monitoring enable
no transceiver-monitoring enable



Примечание: команды Transceiver Monitoring применимы только к портам с оптоволоконными модулями (т. е. Ethernet 1/0/27 ~ 1/0/30) и используются только в том случае, если стекирование отключено.

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 настроить интерфейс физического порта.

Данная команда применяется для включения/отключения функции Optical Transceiver Monitoring на оптоволоконном порту. Если функция Monitoring включена, отслеживаются события alarm и события warning. Событие alarm происходит, если отслеживаемые параметры выходят за пределы верхнего или нижнего порога alarm. Событие warning происходит, если отслеживаемые параметры выходят за пределы верхнего или нижнего порога warning.

Если трансивер SFP28/SFP+ с функцией Transceiver Monitoring подключен к порту, на котором данная функция отключена, система не сможет определить аварийный статус оптического трансивера, однако пользователь может проверить статус при помощи команды **show interfaces transceiver**.

Пример

В данном примере показано, как включить функцию Transceiver Monitoring на интерфейсе Ethernet 1/0/29.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/29
Switch(config-if)# transceiver-monitoring enable
Switch(config-if)#
```

27.6 transceiver-monitoring rx-power

Данная команда используется для настройки порогов входной мощности на указанном порту. Чтобы удалить заданные настройки, воспользуйтесь формой **no** этой команды.

```
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}
```



Примечание: команды Transceiver Monitoring применимы только к портам с оптоволоконными модулями (т. е. Ethernet 1/0/27 ~ 1/0/30) и используются только в том случае, если стекирование отключено.

Параметры

<i>INTERFACE ID</i>	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
mwatt VALUE	Укажите порог входной мощности в диапазоне от 0 до 6,5535 мВт.
dbm VALUE	Укажите порог входной мощности в диапазоне от -40 до 8,1647 дБм.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данный функционал доступен только для интерфейсов портов SFP28 (или опционально SFP+) с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда применяется для настройки порогов входной мощности на указанном порту. Заданные значения сохраняются как в системе, так и в трансиверах SFP28/SFP+, а также будут направлены в оптический модуль в 16-битном формате.

Если конфигурируемый модуль SFP28/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

С помощью формы **no** данной команды можно удалить заданные пороговые значения, сохраненные в

системе. При этом пороговые значения, сохраненные в оптических трансиверах, остаются неизменными. Используйте форму **no**, чтобы предотвратить изменения пороговых значений в оптическом трансивере при его первом подключении.

Пример

В данном примере показано, как настроить нижний порог warning для входной мощности на интерфейсе Ethernet 1/0/29. Указанное значение – 0,135 мВт.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring rx-power ethernet 1/0/29 low warning mwatt 0.135
Switch(config)#
```

27.7 transceiver-monitoring temperature

Данная команда используется для настройки порогов температуры на указанном порту. Чтобы удалить заданные настройки, воспользуйтесь формой **no** этой команды.

transceiver-monitoring temperature *INTERFACE-ID* {high | low} {alarm | warning} *VALUE*
no transceiver-monitoring temperature *INTERFACE-ID* {high | low} {alarm | warning}



Примечание: команды Transceiver Monitoring применимы только к портам с оптоволоконными модулями (т. е. Ethernet 1/0/27 ~ 1/0/30) и используются только в том случае, если стекирование отключено.

Параметры

<i>INTERFACE ID</i>	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
<i>VALUE</i>	Укажите порог 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 SFP28 (или опционально SFP+) с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда применяется для настройки порогов температуры на указанном порту. Заданные значения сохраняются как в системе, так и в трансиверах SFP28/SFP+, а также будут направлены в оптический модуль в 16-битном формате.

Если конфигурируемый модуль SFP28/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

С помощью формы **no** данной команды можно удалить заданные пороговые значения, сохраненные в системе, при этом пороговые значения, сохраненные в оптических трансиверах, остаются неизменными. Используйте форму **no**, чтобы предотвратить изменения пороговых значений в оптическом трансивере при его первом подключении.

Пример

В данном примере показано, как настроить верхний порог alarm для температуры на интерфейсе Ethernet 1/0/29. Указанное значение – 127,994 °C.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring temperature ethernet 1/0/29 high alarm 127.994

WARNING: A closer value of 127.992 is chosen according to the transceiver-monitoring precision
definition

Switch(config)#
```

27.8 transceiver-monitoring tx-power

Данная команда используется для настройки порогов выходной мощности на указанном порту. Чтобы удалить заданные настройки, воспользуйтесь формой **no** этой команды.

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}



Примечание: команды Transceiver Monitoring применимы только к портам с оптоволоконными модулями (т. е. Ethernet 1/0/27 ~ 1/0/30) и используются только в том случае, если стекирование отключено.

Параметры

<i>INTERFACE ID</i>	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.

alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
mwatt VALUE	Укажите порог выходной мощности в диапазоне от 0 до 6,5535 мВт.
dbm VALUE	Укажите порог выходной мощности в диапазоне от -40 до 8,1647 дБм.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данный функционал доступен только для интерфейсов портов SFP28 (или опционально SFP+) с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда применяется для настройки порогов выходной мощности на указанных портах. Заданные значения сохраняются как в системе, так и в трансиверах SFP28/SFP+, а также будут направлены в оптический модуль в 16-битном формате.

Если конфигурируемый модуль SFP28/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

С помощью формы **no** данной команды можно удалить заданные пороговые значения, сохраненные в системе. При этом предельные значения, сохраненные в оптических трансиверах, остаются неизменными. Используйте форму **no**, чтобы предотвратить изменения пороговых значений в оптическом трансивере при его первом подключении.

Пример

В данном примере показано, как настроить нижний порог warning для выходной мощности на интерфейсе Ethernet 1/0/29. Указанное значение – 0,181 мВт.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring tx-power ethernet 1/0/29 low warning mwatt 0.181
Switch(config)#
```

27.9 transceiver-monitoring voltage

Данная команда используется для настройки порогов напряжения на указанном порту. Чтобы удалить заданные настройки, воспользуйтесь формой **no** этой команды.

transceiver-monitoring voltage *INTERFACE-ID* {high | low} {alarm | warning} *VALUE*
no transceiver-monitoring voltage *INTERFACE-ID* {high | low} {alarm | warning}



Примечание: команды Transceiver Monitoring применимы только к портам с оптоволоконными модулями (т. е. Ethernet 1/0/27 ~ 1/0/30) и используются только в том случае, если стекирование отключено.

Параметры

<i>INTERFACE ID</i>	Укажите интерфейс, который необходимо настроить.
high	Укажите верхний порог. Значения выше заданного порога свидетельствуют о возникновении проблем.
low	Укажите нижний порог. Значения ниже заданного порога свидетельствуют о возникновении проблем.
alarm	Укажите верхний/нижний порог alarm.
warning	Укажите верхний/нижний порог warning.
<i>VALUE</i>	Укажите порог напряжения в диапазоне от 0 до 6,5535 В.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данный функционал доступен только для интерфейсов портов SFP28 (или опционально SFP+) с оптическими модулями, поддерживающими функцию Transceiver Monitoring.

Данная команда применяется для настройки порогов напряжения на указанных портах. Заданные значения сохраняются как в системе, так и в трансиверах SFP28/SFP+, а также будут направлены в оптический модуль в 16-битном формате.

Если конфигурируемый модуль SFP28/SFP+ не поддерживает функцию изменения пороговых значений, то заданный пользователем порог будет сохранен в системе и отображен. При отсутствии пороговых значений, заданных пользователем, будут отображены значения, заданные производителем.

С помощью формы **no** данной команды можно удалить заданные пороговые значения, сохраненные в системе. При этом пороговые значения, сохраненные в оптических трансиверах, остаются неизменными. Используйте форму **no**, чтобы предотвратить изменения пороговых значений в оптическом трансивере при его первом подключении.

Пример

В данном примере показано, как настроить нижний порог alarm для напряжения на интерфейсе Ethernet 1/0/29. Указанное значение – 0,005 В.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring voltage ethernet 1/0/29 low alarm 0.005
Switch(config)#
```

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

28.1 ddp

Данная команда используется для включения функции клиента DDP глобально или на указанных портах. Чтобы отключить функцию клиента DDP, воспользуйтесь формой **no** этой команды.

ddp
no ddp

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена глобально, но включена на всех физических портах.

Режим ввода команды

Global Configuration Mode.
Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить/отключить функцию клиента DDP глобально или на физическом порту.

Если на порту отключена функция DDP, данный порт не будет ни обрабатывать, ни генерировать DDP-сообщения. Полученные портом DDP-сообщения распространяются в рамках широковещательного домена.

Пример

В данном примере показано, как включить DDP глобально.

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

В примере ниже показано, как включить DDP на интерфейсе Ethernet 1/0/1.

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

28.2 ddp report-timer

Данная команда используется для настройки интервала между двумя последовательными сообщениями DDP report. Чтобы вернуться 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)#
```

28.3 show ddp

Данная команда используется для отображения настроек DDP на коммутаторе.

show ddp [interfaces {INTERFACE-ID[, | -]}]

Параметры

INTERFACE-ID	Укажите Interface ID.
---------------------	-----------------------

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о DDP на коммутаторе.

Пример

В данном примере показано, как отобразить общую информацию о DDP.

```
Switch#show ddp

D-Link Discovery Protocol state: Enabled
Report timer: 30 seconds

Switch#
```

В примере ниже показано, как отобразить информацию о DDP на интерфейсе Ethernet 1/0/1.

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

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

Switch#
```

29. Команды Domain Name System (DNS)

29.1 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	(Опционально.) Укажите, чтобы удалить указанную динамически изученную запись узла.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы удалить запись узла или все записи узла, которые динамически изучены DNS Resolver или Caching Server.

Пример

В данном примере показано, как удалить динамически изученную запись «www.abc.com» из таблицы узлов.

```
Switch# clear host www.abc.com
Switch#
```

29.2 ip dns server

Данная команда используется для включения функции DNS Caching Name Server. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ip dns server

no ip dns server

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Система поддерживает функцию DNS Caching Name Server. Если данная функция и IP Domain-Lookup включены, система направляет пакет запроса DNS на указанный Name Server. Ответ, отправляемый Name Server, будет кэширован и использован для ответа на последующие запросы.

Пример

В данном примере показано, как включить функцию DNS Caching Name Server.

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

29.3 ip dns lookup

Данная команда используется для включения DNS-поиска динамических кэшированных или статических созданных записей узла. Чтобы отключить DNS-поиск, воспользуйтесь формой **no** этой команды.

ip dns lookup [static] [cache]
no ip dns lookup [static] [cache]

Параметры

static	(Опционально.) Укажите, чтобы включить/отключить поиск статических записей перед отправкой запроса на Name Server.
cache	(Опционально.) Укажите, чтобы включить/отключить поиск динамического кэша перед отправкой запроса на Name Server.

По умолчанию

По умолчанию параметры **static** и **cache** включены.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

В процессе поиска имени домена по умолчанию сначала будет проведена проверка статического и динамического кэша, а затем, если не найдены соответствующие записи, будет отправлен запрос на Name Server. Используйте данную команду, чтобы отключить опцию поиска статических/динамических записей кэша до момента отправки запросов на Name Server. При использовании команды без указания дополнительных параметров, параметры **static** и **cache** включаются/отключаются одновременно.

Пример

В данном примере показано, как включить поиск статического узла для ответа на запрос.

```
Switch# configure terminal
Switch(config)# ip dns lookup static
Switch(config)#
```

29.4 ip domain lookup

Данная команда используется для включения DNS, что позволяет использовать функцию Domain Name Resolution. Чтобы отключить данную функцию, 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)#
```

29.5 ip host

Данная команда используется для настройки статической записи привязки для имени узла, а также IP-адреса в таблице узлов. Чтобы удалить статическую запись узла, воспользуйтесь формой **no** этой команды.

ip host *HOST-NAME* {*IP-ADDRESS* | *IPV6-ADDRESS*}
no ip host *HOST-NAME* {*IP-ADDRESS* | *IPV6-ADDRESS*}

Параметры

<i>HOST-NAME</i>	Укажите имя узла устройства.
<i>IP-ADDRESS</i>	Укажите IPv4-адрес устройства.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес устройства.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Имя узла, указанное в 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)#
```

29.6 ip name-server

Данная команда используется для настройки IP-адреса Domain Name Server. Чтобы удалить сконфигурированный Domain Name Server, 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 через пробел. Можно указать не более 2 серверов.
IPV6-ADDRESS2	Укажите несколько IPv6-адресов через пробел. Можно указать не более 2 серверов.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы сконфигурировать DNS-сервер. Если система не может получить ответ от DNS-сервера, будет отправлен запрос на следующий сервер, и так до тех пор, пока ответ не будет получен. Если Name Servers уже сконфигурированы, то серверы, сконфигурированные позже, будут добавлены в список серверов. Можно сконфигурировать до 4 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)#
```

29.7 ip name-server timeout

Данная команда используется для конфигурации значения тайм-аута для Name Server. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

```
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)#
```

29.8 show hosts

Данная команда используется для отображения настроек DNS.

show hosts

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о настройках DNS.

Пример

В данном примере показано, как отобразить информацию о настройках DNS.

```
Switch#show hosts

Number of Static Entries:   3
Number of Dynamic Entries: 0

Host Name:      www.abc.com
IP Address:     192.168.5.243
Age:            forever

Host Name:      www.yes.com
IP Address:     10.0.0.88
Age:            forever

Host Name:      www.yes.com
IPv6 Address:   2001:1::1
Age:            forever

Switch#
```

29.9 show ip name-server

Данная команда используется для отображения текущих DNS.

show ip name-server

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить DNS.

Пример

В данном примере показано, как отобразить DNS.

```
Switch#show ip name-server  
  
Name servers are: 192.168.5.134  
Name servers are: 5001:5::2  
  
Switch#
```

30. Команды предотвращения атак DoS

30.1 dos-prevention

Данная команда используется для включения и настройки механизма предотвращения атак DoS (DoS Prevention). Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

dos-prevention *DOS-ATTACK-TYPE*
no dos-prevention *DOS-ATTACK-TYPE*

Параметры

<i>DOS-ATTACK-TYPE</i>	Укажите строку, идентифицирующую тип DoS, который необходимо настроить.
------------------------	---

По умолчанию

По умолчанию все поддерживаемые типы DoS отключены.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить и настроить механизм предотвращения атак DoS для определенного типа атак DoS или для всех поддерживаемых типов. Механизмы предотвращения атак DoS (сопоставление и принятие мер) являются функциями аппаратного обеспечения.

При включенном предотвращении атак DoS коммутатор сохранит событие (лог) в журнале, если был получен хотя бы один «атакующий» пакет.

Команда **no dos-prevention** с ключевым словом **all** используется для отключения механизма предотвращения атак DoS для всех поддерживаемых типов. Все настройки будут возвращены к значениям по умолчанию для определенных типов атак.

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

- **Blat:** данный тип атаки включает в себя отправку устройству пакетов с портом источника TCP/UDP, равным порту назначения. Это может послужить причиной того, что устройство будет отвечать самому себе.
- **Land:** атака LAND включает в себя отправку устройству IP-пакетов с адресом источника и назначения, равным адресу устройства. Это может послужить причиной того, что устройство будет непрерывно отвечать самому себе.
- **TCP-NULl-scan:** сканирование порта с использованием определенных пакетов, содержащих последовательность чисел от 0 и не содержащих флаги.
- **TCP-SYN-fin:** сканирование порта с использованием определенных пакетов, содержащих флаги SYN и FIN.
- **TCP-SYN-SRCport-less-1024:** сканирование порта с использованием определенных пакетов, содержащих порт источника 0-1023 и флаг SYN.
- **TCP-xmas-scan:** сканирование порта с использованием определенных пакетов, содержащих

последовательность чисел от 0 и флаги Urgent (URG), Push (PSH) и FIN.

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



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

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

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

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

30.2 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 для отображения.
-----------------	---

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 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 примере ниже 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#
```

30.3 snmp-server enable traps dos-prevention

Данная команда используется для отправки SNMP-уведомлений о DoS-атаках. Чтобы отключить отправку 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) #
```

31. Команды Dynamic ARP Inspection

31.1 arp access-list

Данная команда используется для создания или изменения списка доступа ARP. Команда позволяет войти в режим ARP Access-list Configuration Mode. Чтобы удалить список доступа ARP, воспользуйтесь формой **no** этой команды.

arp access-list *NAME*
no arp access-list *NAME*

Параметры

<i>NAME</i>	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 0.0.255.255 mac any
Switch(config-arp-nacl)# permit ip 10.30.0.0 0.0.255.255 mac any
Switch(config-arp-nacl)#
```

31.2 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 применяется для очистки буфера журнала ARP Inspection.

Пример

В данном примере показано, как очистить журнал ARP Inspection.

```
Switch# clear ip arp inspection log
Switch#
```

31.3 clear ip arp inspection statistics

Данная команда используется для удаления данных статистики Dynamic ARP Inspection.

clear ip arp inspection statistics {all | vlan VLAN-ID [, | -]}

Параметры

all	Укажите для удаления данных статистики Dynamic ARP Inspection для всех VLAN.
vlan VLAN-ID	Укажите VLAN или диапазон VLAN.
,	(Опционально.) 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 применяется 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#
```

31.4 ip arp inspection filter vlan

Данная команда используется, чтобы 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

<i>ARP-ACL-NAME</i>	Укажите имя списка управления доступом. Максимальное количество символов – 32.
vlan <i>VLAN-ID</i>	Укажите VLAN, сопоставленную со списком доступа ARP.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона номеров VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона 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 привязки DHCP Snooping. Проверка будет производиться, если данная команда сконфигурирована.

Списки управления доступом ARP (ARP ACL) имеют более высокий приоритет над таблицей привязки DHCP Snooping. Если пакету явно запрещен доступ списком управления доступа, пакет будет отброшен. Если пакету неявно запрещен доступ, он будет дополнительно сопоставлен с записями привязки DHCP Snooping, если не указано ключевое слово «static». Если пакету неявно запрещен доступ и указано ключевое слово «static», пакет будет отброшен.

Пример

В данном примере показано, как применить список управления доступом ARP (ARP ACL) static ARP list в VLAN 10 для DAI.

```
Switch# configure terminal
Switch(config)# ip arp inspection filter static-arp-list vlan 10
Switch(config)#
```

31.5 ip arp inspection limit

Данная команда используется для ограничения скорости входящих ARP-запросов и ответов на интерфейсе. Чтобы вернуться 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 последующих секунд.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/10
Switch(config-if)# ip arp inspection limit rate 30 burst interval 5
Switch(config-if)#
```

31.6 ip arp inspection log-buffer

Данная команда используется для настройки параметра буфера журнала ARP Inspection.

ip arp inspection log-buffer entries *NUMBER*
no ip arp inspection log-buffer entries

Параметры

<i>NUMBER</i>	Укажите количество записей в буфере. Максимальное значение – 1024.
---------------	--

По умолчанию

Значение по умолчанию – 32.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется 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)#
```

31.7 ip arp inspection trust

Данная команда используется, чтобы назначить доверенный интерфейс 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 опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если интерфейс находится в состоянии trust (доверенный), ARP-пакеты, поступающие на интерфейс, не будут проверяться. Если интерфейс находится в состоянии untrusted (недоверенный), ARP-пакеты, поступающие на порт и принадлежащие VLAN, в которой включена проверка, будут проверяться.

Пример

В данном примере показано, как настроить состояние trust (доверенный) на интерфейсе Ethernet 1/0/3 для DAI.

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

31.8 ip arp inspection validate

Данная команда используется для указания дополнительных проверок при ARP Inspection. Чтобы отключить дополнительные проверки, 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 ARP заголовке.
----------------	--

dst-mac (Опционально.) Укажите для проверки пакетов ARP-ответов, а также согласованности MAC-адреса источника в заголовке Ethernet с MAC-адресом источника в ARP заголовке.

ip (Опционально.) Укажите для проверки содержимого ARP на наличие недопустимых и непредвиденных IP-адресов. Укажите для проверки допустимости IP-адреса в заголовке ARP. Проверяются IP-адреса источника во всех ARP-запросах и ответах, а также IP-адрес назначения в ARP-ответе. Пакеты, отправляемые на IP-адреса 0.0.0.0, 255.255.255.255 и все IP-адреса многоадресной рассылки, отбрасываются. IP-адреса источника проверяются во всех ARP-запросах и ответах, а IP-адреса назначения проверяются только в ARP-ответах.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется 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. Используйте форму **no** этой команды, чтобы отключить дополнительные типы проверок.

Пример

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

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

31.9 ip arp inspection vlan

Данная команда используется для включения Dynamic ARP Inspection для определенных VLAN. Чтобы отключить 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 номеров VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию ARP Inspection отключена для всех VLAN.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если VLAN включена для ARP Inspection, проверяться будут ARP-пакеты, включая пакеты ARP-запроса и ответа, принадлежащие VLAN и отправленные на недоверенный интерфейс. Если пара привязки IP-to-MAC MAC-адреса источника и IP-адреса источника не разрешены ARP ACL, либо таблицей привязки DHCP Snooping, ARP-пакеты будут отброшены. Помимо проверки привязки адреса, осуществляться будет дополнительная проверка, определяемая командой **ip arp inspection validate**.

Пример

В данном примере показано, как включить ARP Inspection в VLAN 2.

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 2
Switch(config)#
```

31.10 ip arp inspection vlan logging

Данная команда используется для управления типом пакетов, которые будут регистрироваться (логироваться). Чтобы вернуться 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 номеров VLAN от предыдущего. Пробелы до и после запятой недопустимы.

-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
acl-match	Укажите критерии логирования для пакетов, отброшенных или разрешенных на основе совпадения со списком управления доступом (ACL).
permit	Укажите для логирования, разрешенного сконфигурированным списком управления доступом (ACL).
all	Укажите для логирования, разрешенного или запрещенного сконфигурированным списком управления доступом (ACL).
none	Укажите, чтобы отменить логирование пакетов на основе совпадения со списком управления доступом (ACL).
dhcp-bindings	Укажите критерии логирования для пакетов, отброшенных или разрешенных на основе совпадения с привязкой DHCP.
permit	Укажите для логирования, разрешенного привязкой DHCP.
all	Укажите для логирования, разрешенного или запрещенного привязкой DHCP.
none	Укажите, чтобы отменить логирование всех пакетов, разрешенных или запрещенных на основе привязки DHCP.

По умолчанию

Все запрещенные и отброшенные пакеты логируются.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте форму **no** для возврата команды к критериям логирования по умолчанию.

Пример

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

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

31.11 permit | deny (arp access-list)

Данная команда применяется для управления доступом ARP-записи. Используйте команду **deny** для создания запрещающей ARP-записи. Чтобы удалить запись, 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)#
```

31.12 show ip arp inspection

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

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

Параметры

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

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, 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 примере ниже показано, как включить отображение параметров статистики пакетов, которые были обработаны DAI для всех активных VLAN.

```
Switch# show ip arp inspection statistics
```

VLAN	Forwarded	Dropped	DHCP Drops	ACL Drops
1	0	0	0	0
2	0	0	0	0
10	21546	145261	145261	0
100	0	0	0	0
200	0	0	0	0
1024	0	0	0	0
VLAN	DHCP Permits	ACL Permits	Source MAC Failures	
1	0	0	0	
2	0	0	0	
10	21546	0	0	
100	0	0	0	
200	0	0	0	
1024	0	0	0	
VLAN	Dest MAC Failures	IP Validation Failures		
1	0	0		
2	0	0		
10	0	0		
100	0	0		
200	0	0		
1024	0	0		

```
Switch#
```

Отображаемые параметры

VLAN	VLAN ID, на которой действует ARP Inspection.
Forwarded	Количество ARP-пакетов, переадресованных ARP Inspection.
Dropped	Количество ARP-пакетов, отброшенных ARP Inspection.
DHCP Drops	Количество ARP-пакетов, отброшенных таблицей DHCP Snooping.
ACL Drops	Количество ARP-пакетов, отброшенных с помощью ARP правил ACL (ARP ACL).
DHCP Permits	Количество ARP-пакетов, разрешенных таблицей привязки DHCP Snooping.
ACL Permits	Количество ARP-пакетов, разрешенных правилом ARPACL.
Source MAC Failures	Количество ARP-пакетов, не прошедших проверку MAC-адреса источника.

Dest MAC Failures	Количество ARP-пакетов, не прошедших проверку MAC-адреса назначения.
IP Validation Failures	Количество ARP-пакетов, не прошедших проверку IP-адреса.

Пример

В данном примере показано, как включить отображение настроек и статуса работы DAI.

```
Switch#show ip arp inspection

Source MAC Validation      : Enabled
Destination MAC Validation: Disabled
IP Address Validation      : Disabled
VLAN State      ACL Match      Static ACL
-----
10  Disabled static-arp-list      No
VLAN ACL Logging DHCP Logging
-----
10  Deny      Deny

Switch#
```

Отображаемые параметры

VLAN	VLAN ID, на которой действует ARP Inspection.
State	Состояние настроек ARP Inspection. Enabled: ARP Inspection работает. Disabled: ARP Inspection не работает.
ACL Match	Имя указанного списка управления доступом ARP (ARP ACL).
Static ACL	Настройки статического списка управления доступом (static ACL). Yes: статический список управления доступом (static ARP ACL) настроен. No: статический список управления доступом (static ARP ACL) не настроен.
ACL logging	Состояние логирования для пакетов, отброшенных или разрешенных на 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 привязки DHCP. None: пакеты, отброшенные или разрешенные таблицей привязки DHCP, не

логируются.

Permit: логирование происходит, если пакеты разрешены таблицей привязки DHCP.

Deny: логирование происходит, если пакеты отброшены таблицей привязки DHCP.

All: пакеты, отброшенные или разрешенные таблицей привязки DHCP, логируются.

Пример

В данном примере показано, как включить отображение состояния для интерфейса Ethernet 1/0/10.

```
Switch#show ip arp inspection interfaces ethernet 1/0/10

Interface          Trust State Rate(pps) Burst Interval
-----
eth1/0/10          trusted    None        1
Total Entries: 1

Switch#
```

В примере ниже 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.

31.13 show ip arp inspection log

Данная команда используется для отображения буфера журнала ARP Inspection.

show ip arp inspection log

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения содержимого буфера журнала ARP Inspection.

Пример

В данном примере показано, как включить отображение буфера журнала ARP Inspection.

```
Switch#show ip arp inspection log
Total log buffer size: 64

Interface      VLAN  Sender IP      Sender MAC      Occurrence
-----
eth1/0/1       100   10.20.1.1      00-20-30-40-50-60 1 (2013-12-28 23:08:66)
eth1/0/2       100   10.5.10.16     55-66-20-30-40-50 2 (2013-12-02 00:11:54)
eth1/0/3       100   10.58.2.30     10-22-33-44-50-60 1 (2013-12-30 12:01:38)

Total Entries: 3

Switch#
```

Отображаемые параметры

Interface	Имя интерфейса, на котором производится логирование.
VLAN	VLAN, на которой производится логирование.
Sender IP	IP-адрес источника у логируемого ARP.
Sender MAC	MAC-адрес источника у логируемого ARP.
Occurence	Счетчик общего числа логирования записей, а также времени последнего случившегося логирования.

32. Команды Error Recovery

32.1 errdisable recovery

Данная команда используется для включения функции Error Recovery (автоматическое восстановление порта при возникновении ошибок), а также для настройки времени восстановления (Recovery Interval). Чтобы отключить данную функцию или вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

errdisable recovery cause {all | psecure-violation | storm-control | bpdu-protect | arp-rate | dhcp-rate | loopback-detect | l2pt-guard | duld} [interval SECONDS]

no errdisable recovery cause {all | psecure-violation | storm-control | bpdu-protect | arp-rate | dhcp-rate | loopback-detect | l2pt-guard | duld} [interval SECONDS]

Параметры

all	Укажите, чтобы включить функцию Auto-Recovery для всех ситуаций.
psecure-violation	Укажите, чтобы включить функцию Auto-Recovery при ошибке на порту, вызванной Port Security Violation.
storm-control	Укажите, чтобы включить функцию Auto-Recovery при ошибке на порту, вызванной Storm Control.
bpdu-protect	Укажите, чтобы включить функцию Auto-Recovery при ошибке на порту, вызванной BPDU Protection.
arp-rate	Укажите, чтобы включить функцию Auto-Recovery при ошибке на порту, вызванной ARP Rate Limiting.
dhcp-rate	Укажите, чтобы включить функцию Auto-Recovery при ошибке на порту, вызванной DHCP Rate Limiting.
loopback-detect	Укажите, чтобы включить функцию Auto-Recovery при ошибке на порту, вызванной Loop Detection.
l2pt-guard	Укажите, чтобы включить функцию Auto-Recovery при ошибке на порту, вызванной L2PT Guard.
duld	Укажите, чтобы включить функцию Auto-Recovery при ошибке на порту, вызванной D-Link Unidirectional.
interval SECONDS	Укажите время, необходимое для восстановления порта при ошибке, вызванной указанным модулем. Диапазон значений: от 5 до 86400 секунд. Значение по умолчанию – 300 секунд.

По умолчанию

По умолчанию функция 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 Violation, Storm Control и т. д. При возникновении ошибки порт отключается, однако для настроек конфигурации будет действовать опция **no shutdown**.

Существует два способа восстановления порта при возникновении ошибки. 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 таймер восстановления (Recovery Timer) 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 примере ниже показано, как включить функцию Auto-Recovery для восстановления порта при ошибке, вызванной Port Security Violation.

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

32.2 show errdisable recovery

Данная команда используется для отображения настроек таймера восстановления (Recovery Timer).

show errdisable recovery

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки Recovery Timer.

Пример

В данном примере показано, как отобразить настройки Recovery Timer.

```
Switch#show errdisable recovery
```

ErrDisable Cause	State	Interval
Port Security	disabled	300 seconds
Storm Control	disabled	300 seconds
BPDU Attack Protection	disabled	300 seconds
Dynamic ARP Inspection	disabled	300 seconds
DHCP Snooping	disabled	300 seconds
Loop Detection	disabled	300 seconds
l2pt-guard	disabled	300 seconds
D-LINK Unidirectional Link Detection	disabled	300 seconds

Interfaces that will be recovered at the next timeout:

Interface	Errdisable Cause	Time left(sec)
eth1/0/7	BPDU Attack Protection	infinite
eth2/0/3	Loop Detection	45
eth2/0/5	Loop Detection	45

```
Switch#
```

33. Команды Ethernet OAM

33.1 ethernet oam

Данная команда используется для включения функции Ethernet OAM на указанном порту. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ethernet oam
no ethernet oam

Параметры

Нет.

По умолчанию

По умолчанию функция Ethernet OAM отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

После запуска данной функции на интерфейсе начнется процесс обнаружения OAM (OAM Discovery). Если на интерфейсе включен активный режим OAM, будет запущено обнаружение. В противном случае порт реагирует на обнаружение, полученное от удаленного узла.

Пример

В данном примере показано, как включить Ethernet OAM на интерфейсе Ethernet 1/0/1.

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

33.2 ethernet oam mode

Данная команда используется для настройки режима Ethernet OAM на указанном порту. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ethernet oam mode {active | passive}
no ethernet oam mode

Параметры

active	Укажите, чтобы включить активный режим Ethernet OAM на порту.
---------------	---

passive	Укажите, чтобы включить пассивный режим Ethernet OAM на порту.
----------------	--

По умолчанию

По умолчанию включен активный режим Ethernet OAM.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Два следующих действия разрешены для портов в активном режиме, но запрещены для портов в пассивном режиме:

- Запуск обнаружения OAM;
- Запуск/остановка опции Remote Loopback.

Пример

В данном примере показано, как включить активный режим Ethernet OAM на интерфейсе Ethernet 1/0/1.

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

33.3 ethernet oam link-monitor error-symbol

Данная команда используется для включения уведомлений о событиях Ethernet OAM error symbol, а также для настройки пороговых значений и периода контроля на указанном порту. Чтобы отключить уведомления и вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ethernet oam link-monitor error-symbol [threshold *NUMBER* | window *DECISECONDS*]
no ethernet oam link-monitor error-symbol [threshold | window]

Параметры

threshold <i>NUMBER</i>	(Опционально.) Укажите пороговое количество ошибок кодировки символов в диапазоне от 0 до 4294967295. Если количество ошибок за период времени превысило указанное пороговое значение, будет создано событие Ethernet OAM error symbol.
window <i>DECISECONDS</i>	(Опционально.) Укажите период контроля, в течение которого будет отслеживаться пороговое количество ошибок

кодировки символов. Если в течение указанного периода пороговое значение было превышено, будет создано уведомление OAM PDU с TLV события error symbol. Диапазон значений: от 10 до 600 децисекунд.

По умолчанию

По умолчанию уведомления о событиях Ethernet OAM error symbol включены.

По умолчанию пороговое значение для контроля событий Ethernet OAM error symbol – 1.

По умолчанию период контроля событий Ethernet OAM error symbol – 10 децисекунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

С помощью функции Link Monitoring можно подсчитать количество ошибок кодировки символов в течение указанного периода. Если количество ошибок равно пороговому значению или превышает его, будет создано событие Ethernet OAM error symbol.

Пример

В данном примере показано, как включить уведомления о событиях Ethernet OAM error symbol на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-symbol
Switch(config-if)#
```

В примере ниже показано, как отключить уведомления о событиях Ethernet OAM error symbol на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-symbol
Switch(config-if)#
```

В следующем примере показано, как настроить пороговое значение для контроля событий Ethernet OAM error symbol на интерфейсе Ethernet 1/0/1. Указанное значение – 100.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-symbol threshold 100
Switch(config-if)#
```

В нижеприведенном примере показано, как настроить период контроля событий Ethernet OAM error symbol на интерфейсе Ethernet 1/0/1. Указанное значение – 100 децисекунд.


```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-symbol window 100
Switch(config-if)#
```

В примере ниже показан процесс настройки порогового значения по умолчанию для контроля событий Ethernet OAM error symbol на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-symbol threshold
Switch(config-if)#
```

33.4 ethernet oam link-monitor error-frame

Данная команда используется для включения уведомлений о событиях Ethernet OAM error frame, а также для настройки пороговых значений и периода контроля на указанном порту. Чтобы отключить уведомления и вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ethernet oam link-monitor error-frame [threshold *NUMBER* | window *DECISECONDS*]
no ethernet oam link-monitor error-frame [threshold | window]

Параметры

threshold <i>NUMBER</i>	(Опционально.) Укажите пороговое количество кадров с ошибками в диапазоне от 0 до 4294967295. Если количество кадров с ошибками за период времени превысило указанное пороговое значение, будет создано событие Ethernet OAM error frame.
window <i>DECISECONDS</i>	(Опционально.) Укажите период контроля, в течение которого будет отслеживаться пороговое количество кадров с ошибками. Если в течение указанного периода пороговое значение было превышено, будет создано уведомление OAM PDU с TLV события error frame. Допустимый диапазон значений: от 10 до 600 децисекунд.

По умолчанию

По умолчанию уведомления о событиях Ethernet OAM error frame включены.

По умолчанию пороговое значение для контроля событий Ethernet OAM error frame – 1.

По умолчанию период контроля событий Ethernet OAM error frame – 10 децисекунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

С помощью функции Link Monitoring можно подсчитать количество кадров с ошибками в течение указанного периода. Если количество кадров с ошибками равно пороговому значению или превышает его, будет создано событие Ethernet OAM error frame.

Пример

В данном примере показано, как включить уведомления о событиях Ethernet OAM error frame на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame
Switch(config-if)#
```

В примере ниже показано, как отключить уведомления о событиях Ethernet OAM error frame на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame
Switch(config-if)#
```

В следующем примере показано, как настроить пороговое значение для контроля событий Ethernet OAM error frame на интерфейсе Ethernet 1/0/1. Указанное значение – 100.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame threshold 100
Switch(config-if)#
```

В нижеприведенном примере показано, как настроить период контроля событий Ethernet OAM error frame на интерфейсе Ethernet 1/0/1. Указанное значение – 100 децисекунд.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame window 100
Switch(config-if)#
```

В примере ниже показан процесс настройки периода контроля событий Ethernet OAM error frame на интерфейсе Ethernet 1/0/1. Указанное значение – значение по умолчанию.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame window
Switch(config-if)#
```

33.5 ethernet oam link-monitor error-frame-seconds

Данная команда используется для включения уведомлений о событиях Ethernet OAM error frame seconds, а также для настройки пороговых значений и периода контроля на указанном порту. Чтобы отключить уведомления и вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

**ethernet oam link-monitor error-frame-seconds [threshold *NUMBER* | window *DECISECONDS*]
no ethernet oam link-monitor error-frame-seconds [threshold | window]**

Параметры

threshold <i>NUMBER</i>	(Опционально.) Укажите пороговое количество кадров с ошибками в диапазоне от 1 до 900 секунд. Если количество кадров с ошибками за период времени превысило указанное пороговое значение, будет создано событие Ethernet OAM error frame seconds.
window <i>DECISECONDS</i>	(Опционально.) Укажите период контроля, в течение которого будет отслеживаться пороговое количество кадров с ошибками. Если в течение указанного периода пороговое значение было превышено, будет создано уведомление OAM PDU с TLV события error frame seconds. Диапазон значений: от 100 до 9000 децисекунд.

По умолчанию

По умолчанию уведомления о событиях Ethernet OAM error frame seconds включены.

По умолчанию пороговое значение для контроля событий Ethernet OAM error frame seconds – 1.

По умолчанию период контроля событий Ethernet OAM error frame seconds – 600 децисекунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

С помощью функции Link Monitoring можно подсчитать количество кадров с ошибками в течение указанного периода. Если количество кадров с ошибками равно пороговому значению или превышает его, будет создано событие Ethernet OAM error frame seconds. Error frame seconds – это интервал в одну секунду, в течение которого был обнаружен как минимум один кадр с ошибкой.

Пример

В данном примере показано, как включить уведомления о событиях Ethernet OAM error frame seconds на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-seconds
Switch(config-if)#
```

В примере ниже показано, как отключить уведомления о событиях Ethernet OAM error frame seconds на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame-seconds
Switch(config-if)#
```

В следующем примере показано, как настроить пороговое значение для контроля событий Ethernet OAM error frame seconds на интерфейсе Ethernet 1/0/1. Указанное значение – 100.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-seconds threshold 100
Switch(config-if)#
```

В нижеприведенном примере показано, как настроить период контроля событий Ethernet OAM error frame seconds на интерфейсе Ethernet 1/0/1. Указанное значение – 100 децисекунд.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-seconds window 100
Switch(config-if)#
```

В примере ниже показан процесс настройки порогового значения по умолчанию для контроля событий Ethernet OAM error frame seconds на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame-seconds threshold
Switch(config-if)#
```

33.6 ethernet oam link-monitor error-frame-period

Данная команда используется для включения уведомлений о событиях Ethernet OAM error frame period, а также для настройки пороговых значений и периода контроля на указанном порту. Чтобы отключить уведомления и вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ethernet oam link-monitor error-frame-period [threshold NUMBER | window NUMBER]
no ethernet oam link-monitor error-frame-period [threshold | window]

Параметры

threshold NUMBER	(Опционально.) Укажите пороговое количество кадров с ошибками в диапазоне от 0 до 4294967295. Если количество ошибок за период времени превысило указанное пороговое значение, будет создано событие Ethernet OAM error frame period.
window NUMBER	(Опционально.) Укажите количество кадров для отслеживания порогового значения. Если в течение указанного периода пороговое значение было превышено, будет создано уведомление о событии OAM PDU с TLV события error frame period. Нижняя граница – количество

кадров минимального размера, которое можно получить в течение 100 миллисекунд на нижнем физическом слое. Верхняя граница – количество кадров минимального размера, которое можно получить в течение 1 минуты на нижнем физическом слое.

По умолчанию

По умолчанию уведомления о событиях Ethernet OAM error frame period включены.

По умолчанию пороговое значение для контроля событий Ethernet OAM error frame period – 1.

По умолчанию период для контроля событий Ethernet OAM error frame period – количество кадров минимального размера, которое можно получить в течение 1 секунды на нижнем физическом слое.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

С помощью функции Link Monitoring можно подсчитать количество кадров с ошибками в течение указанного периода. Период исчисляется количеством полученных кадров. Если количество ошибок равно пороговому значению или превышает его, будет создано событие Ethernet OAM error frame period.

Пример

В данном примере показано, как включить уведомления о событиях Ethernet OAM error frame period на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-period
Switch(config-if)#
```

В примере ниже показано, как отключить уведомления о событиях Ethernet OAM error frame period на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame-period
Switch(config-if)#
```

В следующем примере показано, как настроить пороговое значение для контроля событий Ethernet OAM error frame period на интерфейсе Ethernet 1/0/1. Указанное значение – 100.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-period threshold 100
Switch(config-if)#
```


В нижеприведенном примере показано, как настроить период контроля событий Ethernet OAM error frame period на интерфейсе Ethernet 1/0/1. Указанное значение – 1488100 кадров.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-period window 1488100
Switch(config-if)#
```

В примере ниже показан процесс настройки порогового значения по умолчанию для контроля событий Ethernet OAM error frame period на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame-period threshold
Switch(config-if)#
```

33.7 ethernet oam remote-failure dying-gasp

Данная команда используется для включения уведомлений о событиях Ethernet OAM dying gasp на указанном порту. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ethernet oam remote-failure dying-gasp
no ethernet oam remote-failure dying-gasp

Параметры

Нет.

По умолчанию

По умолчанию уведомления о событиях Ethernet OAM dying gasp включены.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для настройки событий dying gasp. Если данная функция отключена, порт не будет отсылать OAM PDU с набором битов события dying gasp при возникновении необратимой локальной неисправности.

Пример

В данном примере показано, как включить уведомления о событиях dying gasp на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam remote-failure dying-gasp
Switch(config-if)#
```

33.8 ethernet oam remote-failure critical-event

Данная команда используется для включения уведомлений о событиях Ethernet OAM critical на указанном порту. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ethernet oam remote-failure critical-event
no ethernet oam remote-failure critical-event

Параметры

Нет.

По умолчанию

По умолчанию уведомления о событиях Ethernet OAM critical включены.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для настройки событий critical. Если данная функция отключена, порт не будет отсылать OAM PDU с набором битов события critical при возникновении неустановленного события critical.

Пример

В данном примере показано, как включить уведомления о событиях critical на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam remote-failure critical-event
Switch(config-if)#
```

33.9 ethernet oam remote-loopback

Данная команда используется для настройки функции Remote Loopback на указанном порту.

ethernet oam remote-loopback {start | stop} interface *INTERFACE-ID* [, | -]

Параметры

start	Укажите, чтобы запросить переход узла в режим Remote Loopback.
stop	Укажите, чтобы запросить переход узла в режим Normal Operation Mode.
interface INTERFACE-ID	Укажите ID интерфейса, на котором необходимо включить функцию Remote Loopback. Доступны только физические порты.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы запросить переход удаленного узла в режим Ethernet OAM Remote Loopback или выход из данного режима. Используйте команду **ethernet oam remote-loopback start**, чтобы запросить переход удаленного узла в режим Ethernet OAM Remote Loopback. Используйте команду **ethernet oam remote-loopback stop**, чтобы запросить выход удаленного узла из режима Ethernet OAM Remote Loopback.

Если удаленный узел сконфигурирован так, чтобы игнорировать запросы Remote Loopback, при получении запроса узел не будет входить в режим Remote Loopback или выходить из данного режима. Чтобы запустить переход удаленного узла в режим Remote Loopback, администратору необходимо убедиться, что локальный клиент функционирует в активном режиме и установлено соединение OAM. Если локальный клиент уже перешел в режим Remote Loopback, данная команда неприменима.

Пример

В данном примере показано, как запустить Ethernet OAM Remote Loopback на интерфейсе Ethernet 1/0/1.

```
Switch# ethernet oam remote-loopback start interface ethernet 1/0/1
Switch#
```


33.10 ethernet oam received-remote-loopback

Данная команда используется для настройки режима работы требований Remote Loopback, полученных от узла на указанном порту. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ethernet oam received-remote-loopback {process | ignore}

Параметры

process	Укажите, чтобы реагировать на требования Remote Loopback, полученные от узла.
ignore	Укажите, чтобы игнорировать требования Remote Loopback, полученные от узла.

По умолчанию

По умолчанию Ethernet OAM игнорирует требования Remote Loopback.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную функцию, чтобы выбрать, будет ли клиент обрабатывать полученную команду Ethernet OAM Remote Loopback или игнорировать ее. В режиме Remote Loopback Mode весь пользовательский трафик обрабатываться не будет. Если полученная команда Remote Loopback игнорирована, на порту не будет включен режим Remote Loopback Mode.

Пример

В данном примере показано, как включить обработку команды Ethernet OAM Remote Loopback на порту Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ethernet oam received-remote-loopback process
Switch(config-if)#
```

33.11 show ethernet oam configuration

Данная команда используется для отображения настроек функции Ethernet OAM.

show ethernet oam configuration [interface INTERFACE-ID [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите Interface ID физического порта, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения настроек Ethernet OAM на порту.

Пример

В данном примере показано, как отобразить настройки Ethernet OAM на интерфейсе Ethernet 1/0/1.

```
Switch#show ethernet oam configuration interface ethernet 1/0/1

eth1/0/1
  Ethernet oam state      : Disabled
  Mode                   : Active
  Dying gasp             : Enabled
  Critical event         : Enabled
  Remote loopback OAMPDU : Not Processed

  Error symbol period event
    Notify state         : Enabled
    Threshold            : 1 error symbol
    Window              : 10 deciseconds

  Error frame event
    Notify state         : Enabled
    Threshold            : 1 error frame
    Window              : 10 deciseconds

  Error frame period event
    Notify state         : Enabled
    Threshold            : 1 error frame
    Window              : 1488100 frames

  Error frame seconds event

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

33.12 show ethernet oam status

Данная команда используется для отображения статуса функции Ethernet OAM.

show ethernet oam status [interface *INTERFACE-ID* [, | -]]

Параметры	
interface <i>INTERFACE-ID</i>	(Опционально.) Укажите Interface ID физического порта, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.
Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения информации о первичных параметрах и статусе Ethernet OAM на указанных портах.

Пример

В данном примере показано, как отобразить статус Ethernet OAM на интерфейсе Ethernet 2/0/1.

```
Switch#show ethernet oam status interface ethernet 2/0/1

eth2/0/1
  Local client
    Admin state           : Disabled
    Mode                  : Active
    Max OAMPDU size       : 1518 bytes
    Remote loopback       : Supported
    Unidirectional        : Not supported
    Link monitoring        : Supported
    Variable request       : Not supported
    PDU revision           : 0
    Operation status      : Disable
    Loopback status       : No Loopback

  ERROR: There is no peer entry information exist.
Switch#
```

Отображаемые параметры

Max OAMPDU size	Максимальный OAMPDU, поддерживаемый устройством. OAM-устройства обмениваются OAMPDU максимального размера и согласовывают использование меньшего из двух максимальных размеров OAMPDU.
PDU revision	Проверка OAM-конфигурации, отраженной в последнем отправленном OAMPDU. Используется OAM-устройствами для того, чтобы сообщить о произошедших изменениях в конфигурации, которые могут привести к переоценке OAM-узлом вопроса о допуске к установке соединения.
Unidirectional	Указывает, что OAM-устройство поддерживает передачу OAMPDU по каналам связи, действующим в однонаправленном режиме (трафик проходит только в одном направлении).

Remote loopback	Указывает, что OAM-устройство может инициировать команды Loopback и отвечать на них.
Link Monitoring	Указывает, что OAM-устройство может отправлять и получать Event Notification OAMPDU.
Variable request	Указывает, что OAM-устройство может отправлять и получать различные запросы для контроля атрибутов, описанных в IEEE 802.3 Clause 30 MIB.
Operation status	Disable: OAM отключен на данном порту. LinkFault: обнаружена ошибка соединения, передаются уведомляющие пакеты OAMPDU. PassiveWait: порт находится в пассивном режиме и ожидает устройство с поддержкой OAM. ActiveSendLocal: порт находится в активном режиме и отправляет локальную информацию. SendLocalAndRemote: локальный порт обнаружил узел, но еще не принял и не отклонил его настройки. SendLocalAndRemoteOk: локальное устройство принимает OAM-обнаружения. PeeringLocallyRejected: локальное OAM-устройство отклоняет OAM-обнаружения удаленного устройства. PeeringRemotelyRejected: удаленное OAM-устройство отклоняет OAM-обнаружения локального устройства. Operational: локальное OAM-устройство узнает, что локальное и удаленное OAM-устройства установили связь. NonOperHalfDuplex: функции Ethernet OAM не работают полностью через полудуплексный порт. Данное значение показывает, что Ethernet OAM включен, но порт работает в полудуплексном режиме.

33.13 show ethernet oam statistics

Данная команда используется для отображения статистики Ethernet OAM.

show ethernet oam statistics [interface INTERFACE-ID [, | -]]

Параметры

interface INTERFACE-ID	(Опционально.) Укажите Interface ID физического порта 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения статистики Ethernet OAM на порту.

Пример

В данном примере показано, как отобразить статистику Ethernet OAM на интерфейсе Ethernet 1/0/1.

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

eth1/0/1
-----
Information OAMPDU TX           : 0
Information OAMPDU RX           : 0
Unique Event Notification OAMPDU TX : 0
Unique Event Notification OAMPDU RX : 0
Duplicate Event Notification OAMPDU TX: 0
Duplicate Event Notification OAMPDU RX: 0
Loopback Control OAMPDU TX      : 0
Loopback Control OAMPDU RX      : 0
Variable Request OAMPDU TX      : 0
Variable Request OAMPDU RX      : 0
Variable Response OAMPDU TX     : 0
Variable Response OAMPDU RX     : 0
Organization Specific OAMPDUs TX : 0
Organization Specific OAMPDUs RX : 0
Unsupported OAMPDU TX           : 0
Unsupported OAMPDU RX           : 0
Frames Lost Due To OAM          : 0

Switch#
```

33.14 clear ethernet oam statistics

Данная команда используется для удаления статистики Ethernet OAM.

clear ethernet oam statistics [interface INTERFACE-ID [, | -]]

Параметры

interface INTERFACE-ID	(Опционально.) Укажите Interface ID физического порта, который необходимо удалить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для удаления статистики Ethernet OAM на порту.

Пример

В данном примере показано, как удалить статистику Ethernet OAM на интерфейсе Ethernet 1/0/1.

```
Switch# clear ethernet oam statistics interface ethernet 1/0/1
Switch#
```

33.15 show ethernet oam event-log

Данная команда используется для отображения журнала событий Ethernet OAM.

show ethernet oam event-log [interface INTERFACE-ID [, | -]]

Параметры

interface INTERFACE-ID	(Опционально.) Укажите Interface ID физического порта, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.

- (Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения журнала событий Ethernet OAM на порту.

Пример

В данном примере показано, как отобразить журнал событий Ethernet OAM на интерфейсе Ethernet 1/0/1.


```
Switch# show ethernet oam event-log interface ethernet 1/0/1

eth1/0/1
  Local Faults:
  -----
    0 Link Fault records
    0 Dying Gasp records
    0 Critical Event records

  Remote Faults:
  -----
    0 Link Fault records
    2 Dying Gasp records
      Event index           : 2
      Time stamp            : 2013.04.18 10:30
      Event index           : 1
      Time stamp            : 2013.04.18 10:20
    0 Critical Event records

  Local event logs:
  -----
    0 Errored Symbol records
    0 Errored Frame records
    0 Errored Frame Period records
    0 Errored Frame Second records

  Remote event logs:
  -----
    0 Errored Symbol records
    1 Errored Frame records
      Event index           : 3
      Time stamp            : 2013.04.18 10:31
      Error frame           : 5
      Window                : 10 (decisecond)
      Threshold              : 3
      Accumulated errors     : 10
    0 Errored Frame Period records
    0 Errored Frame Second records

Switch#
```

Отображаемые параметры

Event index	Индекс события.
-------------	-----------------

Time stamp	Время создания события.
Error frame	Количество кадров с ошибками, обнаруженных за указанный период.
Window	Продолжительность периода в интервалах 100 миллисекунд.
Threshold	Пороговое значение. Если количество кадров с ошибками, обнаруженных за указанный период, равно пороговому значению или превышает его, будет создано событие.
Accumulated errors	Сумма записей об ошибках, обнаруженных в данном событии с момента сброса подуровня OAM.

33.16 clear ethernet oam event-log

Данная команда используется для очистки журнала событий Ethernet OAM.

clear ethernet oam event-log [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите Interface ID физического порта, который необходимо удалить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для очистки журнала событий Ethernet OAM на порту.

Пример

В данном примере показано, как очистить журнал событий Ethernet OAM на интерфейсе Ethernet 1/0/1.

```
Switch# clear ethernet oam event-log interface ethernet 1/0/1  
Switch#
```

34. Команды Ethernet Ring Protection Switching (ERPS)

34.1 description

Данная команда используется для указания строки, которая служит описанием для кольца G.8032 Ethernet.

description *DESCRIPTION*

Параметры

<i>DESCRIPTION</i>	Укажите описание для кольца G.8032 Ethernet. Максимальное 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)#
```

34.2 ethernet ring g8032

Данная команда используется для создания физического кольца G.8032 и перехода в режим ERPS Configuration Mode. Чтобы удалить физическое кольцо G.8032, воспользуйтесь формой **no** этой команды.

ethernet ring g8032 *RING-NAME*

no ethernet ring g8032 *RING-NAME*

Параметры

<i>RING-NAME</i>	Укажите имя кольца G.8032. 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 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)#
```

34.3 ethernet ring g8032 profile

Данная команда используется для создания профиля G.8032 и входа в режим G.8032 Profile Configuration Mode. Чтобы удалить профиль G.8032, воспользуйтесь формой **no** этой команды.

ethernet ring g8032 profile *PROFILE-NAME*
no ethernet ring g8032 profile *PROFILE-NAME*

Параметры

<i>PROFILE-NAME</i>	Укажите имя профиля G.8032. 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 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)#
```

34.4 tcn-propagation

Данная команда используется для включения передачи уведомлений об изменении топологии (TCN) от экземпляра sub-ERPS к основному экземпляру. Чтобы отключить передачу уведомлений об изменении топологии, воспользуйтесь формой **no** этой команды.

tcn-propagation
no tcn-propagation

Параметры

Нет.

По умолчанию

По умолчанию данная функция 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)#
```

34.5 r-aps channel-vlan

Данная команда используется для настройки ERPS R-APS VLAN. Чтобы удалить настройки, 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. Необходимо создать и назначить R-APS VLAN 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 ethernet 2/0/10
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)#
```

34.6 inclusion-list vlan-ids

Данная команда используется для определения заданных VLAN ID, которые защищены механизмом Ethernet Ring Protection. Чтобы удалить заданные VLAN ID, воспользуйтесь формой **no** этой команды.

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

Параметры

<i>VLAN-ID</i>	Укажите VLAN ID защищенных VLAN экземпляра ERPS. Диапазон значений: от 1 до 4094.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

ERPS Instance Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы сконфигурировать защиту VLAN при помощи экземпляра ERPS.

Пример

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

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 ring2
Switch(config-erps-ring)# port0 interface ethernet 1/0/1
Switch(config-erps-ring)# port1 none
Switch(config-erps-ring)# instance 1
Switch(config-erps-ring-instance)# r-aps channel-vlan 20
Switch(config-erps-ring-instance)# inclusion-list vlan-ids 100-200
Switch(config-erps-ring-instance)#
```

34.7 instance

Данная команда используется для создания экземпляра ERPS и входа в режим ERPS Instance Configuration Mode. Чтобы удалить экземпляр 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 ethernet 1/0/1
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#
```

34.8 level

Данная команда используется для настройки значения MEL кольца экземпляра ERPS. Чтобы вернуться 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 ethernet 1/0/1
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#level 6
Switch(config-erps-ring-instance)#
```

34.9 sub-ring

Данная команда используется, чтобы указать экземпляр 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)#
```

34.10 sub-ring instance

Данная команда используется для указания экземпляра подкольца для экземпляра физического кольца. Чтобы удалить экземпляр подкольца для экземпляра физического кольца, воспользуйтесь формой **no** этой команды.

sub-ring instance *INSTANCE-ID*
no sub-ring instance *INSTANCE-ID*

Параметры

<i>INSTANCE-ID</i>	Укажите идентификатор экземпляра ERPS в диапазоне от 1 до 32.
--------------------	---

По умолчанию

Нет.

Режим ввода команды

ERPS Instance Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить экземпляр подкольца, подключенный к другому экземпляру кольца. Данная команда применяется на связанный узел.

Пример

В данном примере показано, как настроить экземпляр 1 физического кольца «ring2» в качестве подкольца экземпляра 2 «ring1».

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 ring2
Switch(config-erps-ring)# instance 1
Switch(config-erps-ring-instance)# exit
Switch(config-erps-ring)# exit
Switch(config)# ethernet ring g8032 ring1
Switch(config)# port0 interface ethernet 1/0/4
Switch(config-erps-ring)#instance 2
Switch(config-erps-ring-instance)# sub-ring instance 1
Switch(config-erps-ring-instance)#
```

34.11 profile

Данная команда используется для привязки экземпляра ERPS к профилю G.8032. Чтобы удалить привязку, воспользуйтесь формой **no** этой команды.

profile *PROFILE-NAME*
no profile

Параметры

<i>PROFILE-NAME</i>	Укажите имя профиля G.8032, к которому необходимо привязать экземпляр ERPS.
---------------------	---

По умолчанию

Нет.

Режим ввода команды

ERPS Instance Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Перед изменением привязки профиля необходимо отключить экземпляр ERPS.

Пример

В данном примере показано, как настроить значения таймеров для профиля «campus», а затем привязать экземпляр 1 и экземпляр 2 к профилю. Для Guard Timer указано значение 700 миллисекунд, для Hold-Off Timer – 1секунда, 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 ethernet 3/0/1
Switch(config-erps-ring)# port1 interface ethernet 3/0/2
Switch(config-erps-ring)# instance 1
Switch(config-erps-ring-instance)# profile campus
Switch(config-erps-ring-instance)#exit
Switch(config-erps-ring)# exit
Switch(config)# ethernet ring g8032 ring2
Switch(config-erps-ring)# exit
Switch(config)# ethernet ring g8032 ring1
Switch(config-erps-ring)# sub-ring ring2
Switch(config-erps-ring)# exit
Switch(config)# ethernet ring g8032 ring2
Switch(config-erps-ring)# port0 interface eth3/0/3
Switch(config-erps-ring)# port1 none
Switch(config-erps-ring)# instance 2
Switch(config-erps-ring-instance)# profile campus
Switch(config-erps-ring-instance)#
```

34.12 port0

Данная команда используется для указания первого порта физического кольца. Чтобы удалить заданные настройки, воспользуйтесь формой **no** этой команды.

port0 interface *INTERFACE-ID*
no port0

Параметры

<i>INTERFACE-ID</i>	Укажите Interface ID порта кольца. Доступны физические порты и port-channel.
---------------------	--

По умолчанию

Нет.

Режим ввода команды

ERPS Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить первый порт физического кольца.

Пример

В данном примере показано, как настроить 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 ethernet 1/0/1
Switch(config-erps-ring)#
```

34.13 port1

Данная команда используется для указания второго порта физического кольца. Чтобы удалить заданные настройки, 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 промежуточный 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)#
```

34.14 revertive

Данная команда используется для возвращения к действующему средству передачи в случае устранения неисправности. 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)#
```

34.15 rpl

Данная команда используется для настройки узла в качестве RPL Owner или RPL Neighbor, а также для назначения порта RPL. Чтобы удалить 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 eth3/0/1
Switch(config-erps-ring)# port1 interface eth3/0/2
Switch(config-erps-ring)# instance 1
Switch(config-erps-ring-instance)# rpl port0 owner
Switch(config-erps-ring-instance)#
```

34.16 show ethernet ring g8032

Данная команда используется для отображения информации об экземпляре ERPS.

show ethernet ring g8032 status [*RING-NAME*] [*instance* [*INSTANCE-ID*]]
show ethernet ring g8032 brief [*RING-NAME*] [*instance* [*INSTANCE-ID*]]
show ethernet ring g8032 profile [*PROFILE-NAME*]

Параметры

<i>RING-NAME</i>	(Опционально.) Укажите, чтобы отобразить информацию о физическом кольце ERPS.
<i>PROFILE-NAME</i>	(Опционально.) Укажите, чтобы отобразить информацию о профиле ERPS.
<i>INSTANCE-ID</i>	(Опционально.) Укажите, чтобы отобразить информацию об экземпляре ERPS.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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 примере ниже 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 следующем 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 нижеприведенном примере показано, как отобразить подробную информацию об экземпляре 1 основного кольца физического кольца ERPS.

```
Switch# show ethernet ring g8032 status major-ring instance 1
```

```
-----
Ethernet Ring major-ring
Admin Port0: eth2/0/3
Admin Port1: eth2/0/5
Ring Type: Sub ring
Ring ID: 2
-----
Instance: 2
Instance Status: Deactivated
R-APS Channel: 0, Protected VLANs:
Port0: eth2/0/3, Forwarding
Port1: eth2/0/5, Forwarding
Profile:
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
ERPS trap status: Enabled
Ring              InstID  Status      Port-State
-----
ring1              1       Deactivated p0:eth1/0/3,Forwarding
                                   p1:eth1/0/2,Forwarding
Switch#
```

В примере ниже 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
ERPS trap status: Enabled
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	ТС распространяются / не распространяются в кольце.
Revertive / Non-revertive	Реверсивный/нереверсивный режим работы колец.
Instance Status	Текущий статус узла кольца экземпляра ERPS (Deactivated / Init / Idle / Protection / force / manual / pending).
RPL Role	Текущая роль узла экземпляра ERPS (Owner / Neighbor / None).
Port0 / Port1	Текущая роль кольцевого порта (Interface_id / virtual_channel).
RPL Port	Текущие настройки RPL (Port0 / Port1 / None).
Ring port0/port1 state	Статус кольцевых портов экземпляра ERPS (Forwarding / Blocking / SF / SF blocked).
RingType	Тип кольца (основное кольцо / подкольцо).

34.17 activate

Данная команда используется для включения экземпляра ERPS. Чтобы отключить экземпляр 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)#
```

34.18 timer

Данная команда используется для того, 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 <i>MILLI-SECONDS</i>	Укажите значение Guard Timer в диапазоне от 10 до 2000 миллисекунд. Указанное значение должно быть кратным 10.
hold-off <i>SECONDS</i>	Укажите значение Hold-Off Timer в диапазоне от 0 до 10 секунд.
wtr <i>MINUTES</i>	Укажите значение WTR Timer в диапазоне от 1 до 12 минут.

По умолчанию

Значение Guard Timer по умолчанию – 500 миллисекунд.

Значение Hold-Off Timer по умолчанию – 0.

Значение WTR Timer по умолчанию – 5 минут.

Режим ввода команды

G.8032 Profile Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить значения таймеров, используемых экземплярами ERPS, привязанными к профилю. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды. 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)#
```

34.19 ring_id

Данная команда используется для указания ID физического кольца. Чтобы удалить настройки, 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 физическим кольцам должны быть назначены разные 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)#
```

34.20 ring_type

Данная команда используется для указания типа физического кольца. Чтобы вернуться 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).

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)#
```

34.21 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, экземпляра 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)#
```

34.22 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.

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)#
```

34.23 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**.

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.

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. Команды File System

35.1 cd

Данная команда используется для смены текущего каталога.

`cd [DIRECTORY-URL]`

Параметры

<i>DIRECTORY-URL</i>	(Опционально.) Укажите путь к каталогу. Если путь не указан, будет отображен текущий каталог.
----------------------	---

По умолчанию

По умолчанию текущим каталогом является корневой каталог в файловой системе внутренней памяти.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если путь не указан, текущий каталог не будет сменен.

Пример

В данном примере показано, как сменить текущий каталог на каталог «d» в файловой системе.

```
Switch#dir

Directory of /c:/
 1  -rw      12785484 Jan 15 2000 01:41:56 runtime.had
 2  -rw          35856 Jan 20 2000 04:58:06 config.cfg
 3  -rw      12799156 Jan 20 2000 04:57:18 firmware.had
 4  -rw      12481700 Jan 15 2000 23:57:11 fw5.had
 5  -rw      12791928 Jan 05 2000 23:09:30 backup.had
 6  d--              0 Jan 23 2000 03:49:07 system

125304832 bytes total (70426624 bytes free)

Switch#cd d:
Switch#
```

В примере ниже показано, как отобразить текущий каталог.

```
Switch#cd
Current directory is /c:
Switch#
```

35.2 delete

Данная команда используется для удаления файла.

delete *FILE-URL*

Параметры

<i>FILE-URL</i>	Укажите имя файла, который необходимо удалить.
-----------------	--

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Невозможно удалить файл программного обеспечения или файл конфигурации, указанный в качестве загрузочного файла.

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#
```

35.3 dir

Данная команда используется для отображения информации о файле или списке файлов в указанном пути.

dir [*URL*]

Параметры

<i>URL</i>	(Опционально.) Укажите имя файла или каталога для отображения
------------	---

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. Для отображения накопителя, привязанного к файловой системе, примените команду **show storage media**.

Пример

В данном примере показано, как отобразить корневой каталог автономного коммутатора.

```
Switch#dir /  
  
Directory of /  
1  d--          0 Jan 23 2000 03:49:07  c:  
  
0 bytes total (0 bytes free)  
  
Switch#
```

35.4 format

Данная команда используется для форматирования внешнего устройства хранения информации.

format *FILE-SYSTEM* [**fat32** | **fat16**]

Параметры

<i>FILE-SYSTEM</i>	Укажите файловую систему.
fat32	(Опционально.) Укажите, чтобы выбрать форматирование в файловую систему FAT32.
fat16	(Опционально.) Укажите, чтобы выбрать форматирование в файловую систему FAT16.

По умолчанию

Формат по умолчанию – FAT32.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Можно отформатировать только внешнее устройство хранения информации. По умолчанию накопитель будет отформатирован в файловую систему FAT32.

Пример

В данном примере показано, как отформатировать внешнюю карту Compact Flash.

```
Switch# format /d:

All sectors will be erased, proceed? (y/n) [n] y
Enter volume id (up to 11 characters):Profiles
Format completed.

Switch#
```

35.5 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 с именем «newdir» в текущем каталоге.

```
Switch# mkdir newdir
Switch#
```

35.6 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 «usr_def.conf».

```
Switch# more /c:/configuration/usr_def.conf

!DMS-3130
!Firmware Version: 1.01.006
!Slot      Model
!-----
! 1         DMS-3130-30TS
! 2         -
! 3         DMS-3130-30TS
! 4         DMS-3130-30TS
!
ip igmp snooping vlan 1
!
end

Switch#
```

35.7 rename

Данная команда используется для переименования файла.

rename *FILE-URL1 FILE-URL2*

Параметры

<i>FILE-URL1</i>	Укажите путь к файлу, который необходимо переименовать.
<i>FILE-URL2</i>	Укажите путь к переименованному файлу.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Переименованный файл может располагаться в том же или другом каталоге.

Пример

В данном примере показано, как изменить имя файла с «doc.1» на «test.txt».

```
Switch# rename /c:/doc.1 /c:/test.txt  
  
Rename file doc.1 to test.txt? (y/n) [n] y  
  
Switch#
```

35.8 rmdir

Данная команда используется для удаления каталога из файловой системы.

rmdir *DIRECTORY-NAME*

Параметры

<i>DIRECTORY-NAME</i>	Укажите имя каталога, который необходимо удалить.
-----------------------	---

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы удалить каталог из текущего каталога.

Пример

В данном примере показано, как удалить каталог «newdir» из текущего каталога.

```
Switch# rmdir newdir

Remove directory newdir? (y/n) [n] y
The directory is removed

Switch#
```

35.9 show storage media-info

Данная команда используется для отображения информации о накопителе.

show storage media-info [unit *UNIT-ID*]

Параметры

unit <i>UNIT-ID</i>	(Опционально.) Укажите Unit ID устройства в стеке. Если Unit ID не указан, будут отображены все устройства.
----------------------------	---

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о доступных накопителях системы.

Пример

В данном примере показано, как отобразить информацию о доступных накопителях на всех устройствах стека.

```
Switch# show storage media-info

Unit  Drive  Media-Type  Size    FS-Type  Label
----  -
1     c:      FLASH      31M     FFS
2     c:      FLASH      31M     FFS
2     d:      SD Card    256M    FAT32    test
3     c:      FLASH      31M     FFS

Switch#
```

Отображаемые параметры

Media-Type	FLASH: отображает внутреннюю память коммутатора.
	SD Card: отображает съемные носители, включая флэш-накопители USB.

36. Команды Filter Database (FDB)

36.1 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 VLANID 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#
```

36.2 mac-address-table aging-time

Данная команда используется для настройки времени устаревания (Aging Time) MAC-адресов в таблице. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

```
mac-address-table aging-time SECONDS
```

no mac-address-table aging-time

Параметры

<i>SECONDS</i>	Укажите время устаревания в диапазоне от 0 или 10 до 1000000 секунд. Укажите 0, чтобы отключить функцию устаревания MAC-адресов в таблице.
----------------	--

По умолчанию

Значение по умолчанию – 300 секунд.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Укажите время устаревания «0», чтобы отключить функцию устаревания MAC-адресов в таблице.

Пример

В данном примере показано, как установить значение времени устаревания на 200 секунд.

```
Switch# configure terminal
Switch(config)# mac-address-table aging-time 200
Switch(config)#
```

36.3 mac-address-table aging destination-hit

Данная команда используется для включения функции Destination MAC Address Triggered Update. Чтобы отключить данную функцию, 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 функция 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 с помощью команды **mac-address-table aging destination-hit**, hit bit записей MAC-адреса, соответствующего порту, который передает 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)#
```

36.4 mac-address-table learning

Данная команда используется для включения изучения MAC-адресов на физическом порту или VLAN. Чтобы отключить данную функцию, 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 VLANID, который необходимо сконфигурировать.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
INTERFACE-ID	Укажите интерфейс физического порта, который необходимо сконфигурировать.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию данная опция включена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить/отключить изучение MAC-адресов на физическом порту или VLAN.

Ниже описаны правила изучения MAC-адресов на VLAN-интерфейсах:

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 ethernet 1/0/5
Switch(config)#
```

36.5 mac-address-table notification change

Данная команда используется для включения/настройки функции уведомлений о MAC-адресах. Чтобы отключить функцию или вернуться 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. 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.

По умолчанию

Уведомления о MAC-адресах отключены.

Интервал отправки трапов по умолчанию – 1 секунда.

Количество записей в таблице истории уведомлений по умолчанию – 1.

Тип трапа по умолчанию – without-vlanid.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При распознавании или удалении коммутатором MAC-адреса соответствующее уведомление может быть отправлено в таблицу истории уведомлений, а затем на SNMP-сервер, если запущена команда **snmp-server enable traps mac-notification change**. В таблице истории уведомлений хранятся распознанные или удаленные MAC-адреса тех интерфейсов, для которых включены 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 ограничение 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)#
```

36.6 mac-address-table static

Данная команда используется для добавления статического адреса в таблицу MAC-адресов. Чтобы удалить запись 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.
vlan VLAN-ID	Укажите VLAN записи в диапазоне от 1 до 4094.
interface INTERFACE-ID	Укажите порты продвижения кадров.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
drop	Укажите, чтобы отбросить кадры, отправленные с указанного MAC-адреса / на указанный MAC-адрес на обозначенной VLAN.
all	Укажите, чтобы удалить все записи статических MAC-адресов.

По умолчанию

По умолчанию сконфигурированные статические адреса отсутствуют.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для записи индивидуального MAC-адреса можно указать только один интерфейс. Для записи группового MAC-адреса можно указать несколько интерфейсов. Чтобы удалить запись индивидуального MAC-адреса, Interface ID указывать не нужно. При удалении записи группового MAC-адреса будет удален только тот интерфейс, ID которого указан. Если Interface ID не указан, будет удалена вся запись группового MAC-адреса. Параметр **drop** может быть применен только для записи индивидуального MAC-адреса.

Пример

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

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

36.7 multicast filtering-mode (Interface)

Данная команда используется для настройки способа обработки групповых пакетов на интерфейсе. Чтобы вернуться 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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данный режим фильтрации применим только к групповым пакетам, предназначенным для адресов, незарезервированных для групповых адресов.

Пример

В данном примере показано, как установить режим фильтрации групповых пакетов на VLAN 100, чтобы отфильтровать незарегистрированные адреса.

```
Switch# configure terminal
Switch(config)# vlan 100
Switch(config-vlan)# multicast filtering-mode filter-unregistered
Switch(config-vlan)#
```

36.8 show mac-address-table

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

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

Параметры

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

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

В данном примере показано, как отобразить все записи таблицы MAC-адресов для MAC-адреса 00-23-7D-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 примере ниже 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 следующем 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#
```

36.9 show mac-address-table aging-time

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

show mac-address-table aging-time

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить время устаревания MAC-адресов в таблице.

Пример

В данном примере показано, как отобразить время устаревания MAC-адресов в таблице.

```
Switch# show mac-address-table aging-time

Aging Time is 300 seconds

Switch#
```

36.10 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 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если не указаны дополнительные параметры, будут отображены все физические порты.

Пример

В данном примере показано, как отобразить статус изучения MAC-адресов на всех физических портах от 1 до 10.

```
Switch#show mac-address-table learning interface ethernet 1/0/1-10
```

Port	State
eth1/0/1	Enabled
eth1/0/2	Enabled
eth1/0/3	Enabled
eth1/0/4	Enabled
eth1/0/5	Enabled
eth1/0/6	Enabled
eth1/0/7	Enabled
eth1/0/8	Enabled
eth1/0/9	Enabled
eth1/0/10	Enabled

```
Switch#
```

36.11 show mac-address-table notification change

Данная команда используется для отображения настроек уведомлений о MAC-адресах или истории уведомлений.

show mac-address-table notification change [interface [INTERFACE-ID] | history]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите интерфейс, который необходимо отобразить.
history	(Опционально.) Укажите, чтобы отобразить историю уведомлений об изменении MAC-адреса.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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

```
---More--or (q)uit (a)ll
```

В примере ниже 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 следующем 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#
```


36.12 show multicast filtering-mode

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

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

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите VLAN, которую необходимо отобразить.
--------------------------------------	---

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки режима фильтрации групповых пакетов для всех VLAN.

Пример

В данном примере показано, как отобразить настройки режима фильтрации групповых пакетов для всех VLAN.

```
Switch#show multicast filtering-mode

VLAN                               Layer 2 Multicast Filtering Mode
-----
default                           forward-unregistered

Total Entries: 1

Switch#
```

36.13 snmp-server enable traps mac-notification change

Данная команда используется для включения отправки SNMP trap об уведомлениях MAC. Чтобы отключить данную функцию, 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 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)#
```

36.14 snmp trap mac-notification change

Данная команда используется для включения уведомлений об изменении MAC-адреса на указанном интерфейсе. Чтобы вернуться 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 на интерфейсе включена отправка уведомлений с помощью команды **snmp trap mac-notification change**, уведомления будут отправлены в таблицу истории только при использовании команды **mac-address-table notification change**.

Пример

В данном примере показано, как включить уведомления о добавлении MAC-адреса на интерфейсе Ethernet 1/0/2.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# snmp trap mac-notification change added
Switch(config-if)#
```

37. Команды GARP VLAN Registration Protocol (GVRP)

37.1 clear gvrp statistics

Данная команда используется для удаления статистики GVRP на порту.

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

Параметры

all	Укажите, чтобы сбросить счетчики статистики GVRP, ассоциированные со всеми интерфейсами.
interface <i>INTERFACE-ID</i>	Укажите интерфейсы, которые необходимо сконфигурировать.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы сбросить счетчики GVRP.

Пример

В данном примере показано, как удалить статистику для всех интерфейсов.

```
Switch# clear gvrp statistics all
Switch#
```

37.2 gvrp global

Данная команда используется для глобального включения функции GVRP. Чтобы глобально отключить функцию GVRP, воспользуйтесь формой **no** этой команды.

gvrp global
no gvrp global

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

GVRP можно включить как глобально, так и на отдельном порту.

Пример

В данном примере показано, как включить GVRP-протокол глобально.

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

37.3 gvrp enable

Данная команда используется для включения функции GVRP на порту. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

gvrp enable
no gvrp enable

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel в режимах Hybrid 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 ethernet 1/0/1
Switch(config-if)# gvrp enable
Switch(config-if)#
```

37.4 gvrp advertise

Данная команда используется, чтобы указать VLAN, для которых разрешено анонсирование при помощи GVRP-протокола. Для отключения данной 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. 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 Mode и Trunk Mode. Используйте команду **gvrp advertise**, чтобы включить функцию анонсирования GVRP для указанных VLAN на заданном интерфейсе. Предварительно необходимо включить GVRP.

Пример

В данном примере показано, как включить функцию анонсирования для VLAN 1000 на интерфейсе Ethernet 1/0/1.

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

37.5 gvrp vlan create

Данная команда используется, чтобы включить создание Dynamic VLAN. Для отключения данной 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)#
```

37.6 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. 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 Mode и Trunk Mode. Порт, указанный в качестве запрещенного порта

VLAN, не может стать членом VLAN при помощи GVRP. VLAN, обозначенная при помощи данной команды, может не существовать.

Команда влияет только на работу GVRP, при этом необходимо предварительно включить GVRP.

Пример

В данном примере показано, как настроить порт Ethernet 1/0/1 в качестве запрещенного порта для VLAN 1000 при помощи GVRP.

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

37.7 gvrp timer

Данная команда используется для настройки значения таймера GVRP на порту. Чтобы вернуться 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.
<i>TIMER-VALUE</i>	(Опционально.) Установите значение таймера. Доступный диапазон значений: от 10 до 10000 сотых долей секунды.

По умолчанию

Join: 20

Leave: 60

Leave-all: 1000

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить значение таймера GVRP на порту.

Пример

В данном примере показано, как настроить значение таймера для выхода из всех групп на интерфейсе Ethernet 1/0/1. Установленное значение – 500 сотых долей секунды.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# gvrp timer leave-all 500
Switch(config-if)#
```

37.8 gvrp nni-bpdu-address

Данная команда используется для настройки адреса GVRPBPDU на сайте поставщика услуг. Чтобы вернуться 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)#
```

37.9 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 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки GVRP. Если параметры не указаны, 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 примере ниже показано, как отобразить настройки GVRP на интерфейсах Ethernet 1/0/5 и Ethernet 1/0/6.

```
Switch# show gvrp configuration interface ethernet 1/0/5-1/0/6

ethernet 1/0/5
GVRP Status      : Enabled
Join Time        : 20 centiseconds
Leave Time        : 60 centiseconds
Leave-All Time    : 1000 centiseconds
Advertise VLAN   : 1-4094
Forbidden VLAN   : 3-5

ethernet 1/0/6
GVRP Status      : Enabled
Join Time        : 20 centiseconds
Leave Time        : 60 centiseconds
Leave-All Time    : 1000 centiseconds
Advertise VLAN   : 1-3
Forbidden VLAN   : 5-8

Switch#
```

37.10 show gvrp statistics

Данная команда используется для отображения статистики GVRP на порту.

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

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите интерфейсы 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 EXEC Mode.

Любой режим конфигурирования.

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	4294967296	4294967296	4294967296
eth1/0/6	RX 0	0	0	0	0	0
	TX 0	0	0	0	0	0

```
Switch#
```

38. Команды Gratuitous ARP

38.1 ip arp gratuitous

Данная команда используется для включения изучения пакетов Gratuitous ARP в таблице ARP-кэша. Чтобы отключить ARP Control, воспользуйтесь формой **no** этой команды.

ip arp gratuitous
no ip arp gratuitous

Параметры

Нет.

По умолчанию

По умолчанию данная функция 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)#
```

38.2 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.

Примените команду **ip gratuitous-arps dad-reply** для включения передачи запросов Gratuitous ARP. Устройство вышлет пакет при обнаружении дублированного IP-адреса.

Пример

В данном примере показано, как включить отправку сообщений Gratuitous ARP request.

```
Switch# configure terminal
Switch(config)# ip gratuitous-arps dad-reply
Switch(config)#
```

38.3 arp gratuitous-send interval

Данная команда используется для установки интервала отправки сообщений Gratuitous ARP request на интерфейс. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

arp gratuitous-send interval SECONDS

no arp gratuitous-send

Параметры

SECONDS

Укажите временной интервал для отправки сообщений с Gratuitous ARP request. Диапазон значений: от 0 до 3600. Если указан 0, данная опция отключена.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если интерфейс коммутатора используется в качестве шлюза для конечных устройств и у данных устройств наблюдается поведение ложного шлюза, администратор может настроить регулярную отправку сообщений с Gratuitous ARP request на данном интерфейсе для уведомления о том, что коммутатор является подлинным шлюзом.

Пример

В данном примере показано, как включить отправку сообщений Gratuitous ARP.

```
Switch# configure terminal
Switch(config)# ip gratuitous-arps
Switch(config)# interface vlan 100
Switch(config-if)# arp gratuitous-send interval 1
Switch(config-if)#
```

38.4 snmp-server enable traps gratuitous-arp

Данная команда используется для включения отправки SNMP-уведомлений об обнаружении дублированного IP-адреса Gratuitous ARP. Чтобы отключить данную функцию, 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 функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется 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)#
```

39. Команды управления интерфейсом

39.1 clear counters

Данная команда используется для сброса счетчиков на указанных интерфейсах.

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

Параметры

all	Укажите, если необходимо сбросить счетчики на всех интерфейсах.
interface <i>INTERFACE-ID</i>	Укажите настраиваемые интерфейсы. Интерфейсами могут считаться физические порты, порт управления OOB, port-channel или VLAN-интерфейсы 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

Данная команда применяется для сброса счетчиков на интерфейсе физического порта.

Пример

В данном примере показано, как сбросить счетчики на интерфейсе Ethernet 1/0/1.

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

39.2 description

Данная команда используется, чтобы добавить описание для интерфейса. Для удаления описания воспользуйтесь формой **no** этой команды.

description *STRING*

no description

Параметры

<i>STRING</i>	Укажите описание для интерфейса. Максимальное количество символов – 64.
---------------	---

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Пример

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

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

39.3 interface

Данная команда используется, чтобы войти в режим Interface Configuration Mode для одного интерфейса. Для удаления интерфейса воспользуйтесь формой **no** этой команды.

```
interface INTERFACE-ID
no interface INTERFACE-ID
```

Параметры

<i>INTERFACE-ID</i>	Укажите ID интерфейса. В качестве ID интерфейса указывается тип и номер интерфейса без пробелов.
---------------------	--

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы войти в режим Interface Configuration Mode для определенного интерфейса. ID интерфейса состоит из типа интерфейса и номера интерфейса без пробелов.

Для обозначения интерфейсов применяются следующие ключевые слова:

- **Ethernet** – физический Ethernet-порт коммутатора;
- **L2vlan** – VLAN-интерфейс 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;
- **Null** – интерфейс null;
- **Port-channel** – агрегированный интерфейс port-channel;
- **Tunnel** – виртуальный интерфейс, используемый для туннелирования;
- **Vlan** – VLAN-интерфейс.

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**.

Воспользуйтесь командой **interface Vlan** для создания интерфейса 3 уровня. Введите команду **vlan** в режиме Global Configuration Mode, чтобы создать VLAN перед созданием интерфейса 3 уровня. Для удаления интерфейса 3 уровня используйте команду **no interface Vlan**.

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

Для интерфейса null поддерживается интерфейс null0, который не может быть удален.

Для интерфейсов loopback или tunnel команда **interface** применяется для создания интерфейса или изменения настроек интерфейса. Чтобы удалить интерфейс, воспользуйтесь формой **no** этой команды.

Режимы интерфейсов **L2vlan** и **L2vc** применяются только для добавления описания к существующим L2VLAN и L2 Virtual circuit. Команды **interface l2vlan** и **interface l2vc** не создают новые интерфейсы, а форма **no** данных команд не используется для удаления существующих интерфейсов.

Пример

В данном примере показано, как войти в режим Interface Configuration Mode для Ethernet 1/0/5.

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

В примере ниже показано, как войти в режим Interface Configuration Mode для VLAN 100.

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

В следующем примере показано, как войти в режим Interface Configuration Mode для port-channel 3.

```
Switch# configure terminal
Switch(config)# interface port-channel 3
Switch(config-if)#
```

В нижеприведенном примере показано, как добавить интерфейс loopback 2 и войти в режим Interface Configuration Mode.

```
Switch# configure terminal
Switch(config)# interface loopback 2
Switch (config-if)#
```

В данном примере показан процесс удаления интерфейса loopback 2.

```
Switch# configure terminal
Switch(config)# no interface loopback 2
Switch (config)#
```

39.4 interface range

Данная команда используется, чтобы войти в режим Interface Range Configuration Mode для нескольких интерфейсов.

interface range *INTERFACE-ID* [, | -]

Параметры

<i>INTERFACE-ID</i>	Укажите ID интерфейса. В качестве ID интерфейса указывается тип и номер интерфейса без пробелов.
,	(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, чтобы войти в режим Interface Configuration Mode для указанного диапазона интерфейсов. Команды, введенные в режиме Interface Range Mode, применяются ко всем интерфейсам диапазона.

Пример

В данном примере показано, как войти в режим Interface Configuration Mode для диапазона интерфейсов от Ethernet 2/0/1 до Ethernet 2/0/5, а также для интерфейса Ethernet 3/0/3.

```
Switch# configure terminal
Switch(config)# interface range Ethernet 2/0/1-5,3/0/3
Switch(config-if-range)#
```

39.5 show counters

Данная команда используется для отображения информации об интерфейсе.

show counters [interface *INTERFACE-ID*]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите необходимый интерфейс: физический порт, port-channel или VLAN. Если интерфейс не указан, будут отображаться счетчики для всех интерфейсов.
--------------------------------------	---

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения счетчиков на интерфейсе.

Следующие пункты предоставляют подробную информацию об отображении параметров данной команды:

- **max-rcv-frame-size**: максимальный размер Ethernet-кадра, определенный в командах **Jumbo Frame**. Диапазон доступных значений – от 64 до 12288 байт.

Пример

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

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

```
eth1/0/1 counters
```

```
rxHCTotalPkts           : 67004
txHCTotalPkts           : 63918
rxHCUnicastPkts         : 66026
txHCUnicastPkts         : 46199
rxHCMulticastPkts       : 383
txHCMulticastPkts       : 9848
rxHCBroadcastPkts       : 595
txHCBroadcastPkts       : 7871
rxHCOctets              : 14339916
txHCOctets              : 13420831
rxHCPkt64Octets         : 45325
rxHCPkt65to127Octets    : 1058
rxHCPkt128to255Octets   : 0
rxHCPkt256to511Octets   : 4705
rxHCPkt512to1023Octets  : 15916
rxHCPkt1024to1518Octets : 0
rxHCPkt1519to1522Octets : 0
rxHCPkt1519to2047Octets : 0
rxHCPkt2048to4095Octets : 0
rxHCPkt4096to9216Octets : 0

txHCPkt64Octets         : 6347
```

```
txHCPkt65to127Octets    : 21566
txHCPkt128to255Octets   : 27683
txHCPkt256to511Octets   : 5822
txHCPkt512to1023Octets  : 270
txHCPkt1024to1518Octets : 2230
txHCPkt1519to1522Octets : 0
txHCPkt1519to2047Octets : 0
txHCPkt2048to4095Octets : 0
txHCPkt4096to9216Octets : 0
```

```
rxCRCAAlignErrors       : 0
rxUndersizedPkts        : 0
rxFragmentPkts          : 0
rxSymbolErrors          : 0
rxBufferFullDropPkts    : 0
rxMulticastDropPkts     : 0
rxVLANIngressCheckDropPkts : 0
rxIpv6DropPkts          : 0
rxSTPDropPkts           : 0
rxStormAndFDBDropPkts   : 0
rxMTUDropPkts           : 0
```

```
txCollisions            : 0
ifInErrors               : 0
ifOutErrors              : 0
ifInDiscards             : 0
```

```
ifOutDiscards           : 0
txDelayExceededDiscards : 0
txCRC                   : 0
txSTPDPkts              : 0
txCoS0DropPkts          : 0
txCoS1DropPkts          : 0
txCoS2DropPkts          : 0
txCoS3DropPkts          : 0
txCoS4DropPkts          : 0
txCoS5DropPkts          : 0
txCoS6DropPkts          : 0
txCoS7DropPkts          : 0

dot3StatsSingleColFrames : 0
dot3StatsMultiColFrames  : 0
dot3StatsDeferredTransmissions : 0
dot3StatsLateCollisions  : 0
dot3StatsExcessiveCollisions : 0
dot3StatsInternalMacTransmitErrors : 0
dot3StatsFrameTooLongs   : 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.

	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-size.
txHCOctets	Счетчик переданных байтов. Увеличивается с подсчетом байтов переданных пакетов, исключая поврежденные пакеты (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, 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-gcv-frame-size (или max-gcv-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).
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).
rxSymbolErrors	Счетчик принятых кадров с ошибкой кода. Увеличивается с каждым принятым кадром, содержащим недопустимый символ данных, но допустимый носитель.
txCollisions	Счетчик общего числа коллизий при передаче. Увеличивается с общим числом коллизий, возникших во время передачи.
ifInErrors	Счетчик принятых пакетов с ошибкой. Увеличивается при приеме пакетов, содержащих ошибки, не допускающие их дальнейшую передачу протоколу на уровень выше. Счетчик является суммой dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsFrameTooLongs и dot3StatsInternalReceiveError.
ifOutErrors	Счетчик пакетов, переданных с ошибкой. Увеличивается 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. Увеличивается при приеме пакетов, которые в дальнейшем отбрасываются по какой-либо причине. Например, MTU drop, Buffer Full Drop, ACL Drop, Multicast Drop, VLAN Ingress Drop, Invalid IPv6, STP Drop, Storm and FDB Discard и т. д.

ifOutDiscards	Счетчик отброшенных переданных пакетов. Увеличивается при передаче пакетов, отброшенных в дальнейшем по какой-либо причине. Например, excessive transit delay discards, HOL drop, STP drop, MTU drop, VLAN drop, и т. д.
txDelayExceededDiscards	Счетчик просроченных переданных пакетов. Увеличивается при передаче пакетов, которые были отброшены из-за превышения времени передачи.
txCRC	Счетчик переданных пакетов с ошибкой FCS. Увеличивается с каждым переданным пакетом, не прошедшим проверку FCS.
dot3StatsSingleColFrames	Счетчик переданных кадров с одиночной коллизией. Доступен только для режима 10/100. Увеличивается с каждым переданным кадром, испытавшим одну коллизию во время передачи.
dot3StatsMultiColFrames	Счетчик переданных кадров многочисленных коллизий. Доступен только в режиме 10/100. Увеличивается с каждым успешно переданным кадром, испытавшим больше одной коллизии во время передачи.
dot3StatsDeferredTransmissions	Счетчик одиночных отложенных при передаче кадров. Доступен только в режиме 10/100. Увеличивается 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.
dot3StatsFrameTooLongs	Счетчик принятых кадров слишком большой длины. Возрастает с каждым принятым кадром, превышающим размер max-rcv-frame-size.

39.6 show interfaces

Данная команда используется для отображения информации об интерфейсе.

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

Параметры

<i>INTERFACE-ID</i>	(Опционально.) Укажите физический порт, VLAN, интерфейс loopback или другой интерфейс.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Укажите диапазон интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если интерфейс не указан, 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

vlan 1 is enabled, Link status is up
  Interface type: VLAN
  Interface description:
  MAC address: F0-7D-68-36-30-B0

Switch#
```

В примере ниже показано, как отобразить информацию об интерфейсе loopback для интерфейса loopback 1.

```
Switch# show interfaces loopback 1

Loopback 1 is up, link status is up
Interface type: Loopback
Interface description: Loopback 1 for MIS

Switch#
```

В следующем примере показано, как отобразить информацию об интерфейсе NULL для интерфейса null0.

```
Switch# show interfaces null 0

Null 0 is enabled, link status is up
Interface type: Null
Interface description: Null0 for MIS

Switch#
```

В нижеприведенном примере показано, как отобразить информацию об интерфейсе для Ethernet 2/0/1.

```
Switch#show interfaces ethernet 2/0/1

Eth2/0/1 is enabled link status is up
  Interface type: 2.5G-BaseFX
  Interface description:
  MAC Address: 00-ad-24-a2-d6-12
  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, 1000Mb/s
  Maximum transmit unit: 1536 bytes
  Last Linkchange  0:2:48:5
  Current Link Duration: 0 day 0 hr 1 min 46 sec
  RX rate: 3968 bits/sec, TX rate: 2080 bits/sec
  RX bytes: 51138, TX bytes: 37730
  RX rate: 6 packets/sec, TX rate: 3 packets/sec
  RX packets: 318, TX packets: 99
  RX multicast: 136, RX broadcast: 47
  RX CRC error: 0, RX undersize: 0
  RX fragment: 0, RX dropped Pkts: 85
  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
--More-- or (q)uit (a)ll
```

В нижеследующем примере показано, как отобразить информацию об интерфейсе для порта управления (management port 0).

```
Switch#show interfaces mgmt 0

mgmt_ipif 0 is enabled, Link status is up
  Interface type: Management port
  Interface description:
Switch#
```

39.7 show interfaces counters

Данная команда используется для отображения счетчиков на определенных интерфейсах.

show interfaces [*INTERFACE-ID* [, | -]] **counters** [errors | history {15_minute [slot 1-5] | 1_day [slot 1-2]]]

Параметры

<i>INTERFACE-ID</i>	(Опционально.) Укажите, является ли интерфейс физическим портом или VLAN-интерфейсом. Если интерфейс не указан, отображаться будут счетчики для всех интерфейсов.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
errors	(Опционально.) Укажите для отображения счетчика ошибок.
history	(Опционально.) Укажите для отображения истории счетчиков. Если параметр не указан, история статистики счетчиков не будет отображена.
15_minute	(Опционально.) Укажите для отображения истории статистики за 15 минут.
1_day	(Опционально.) Укажите для отображения истории статистики за сутки.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить общие счетчики, счетчики ошибок или архивную информацию для указанного или всех интерфейсов.

Пример

В данном примере показано, как отобразить счетчики принятых пакетов (RX) для интерфейсов Ethernet 2/0/1 и Ethernet 2/0/2.

```
Switch#show interfaces ethernet 2/0/1-2 counters
```

Port	InOctets / InUcastPkts	InMcastPkts / InBcastPkts
eth2/0/1	86417 342	174 47
eth2/0/2	0 0	0 0

Port	OutOctets / OutUcastPkts	OutMcastPkts / OutBcastPkts
eth2/0/1	50480 208	0 0
eth2/0/2	0 0	0 0

Total Entries: 2

```
Switch#
```

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

```
Switch#show interfaces ethernet 2/0/1,2/0/3 counters errors

Port          CrcAlign-Err /      Undersize /
              Rcv-Err /      InDiscard /
              Xmit-Err      OutDiscard
-----
eth2/0/1      0              0
              0              157
              0              0
eth2/0/3      0              0
              0              0
              0              0

Port          Single-Col /      Excess-Col /
              Multi-Co /      Runts /
              Late-Col      Symbol-Err
-----
eth2/0/1      0              0
              0              0
              0              0
eth2/0/3      0              0
              0              0
              0              0

Port          DeferredTx      IntMacTx
-----
eth2/0/1      0              0
eth2/0/3      0              0

Total Entries: 2

Switch#
```

Отображаемые параметры

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 .
Symbol-Err	Относится к строке «rxSymbolErrors» 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 .

39.8 show interfaces status

Данная команда используется, чтобы просмотреть состояние подключения портов коммутатора.

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

Параметры

<i>INTERFACE-ID</i>	(Опционально.) Укажите ID интерфейса. Если параметр не указан, будет отображен статус подключения всех портов коммутатора.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы просмотреть состояние подключения портов коммутатора.

Пример

В данном примере показано, как просмотреть состояние подключения портов коммутатора.

```
Switch#show interfaces status

Port          Status      VLAN      Duplex  Speed      Type
-----
eth2/0/1      not-connected 1          auto    auto       2.5GBase-T
eth2/0/2      not-connected 1          auto    auto       2.5GBase-T
eth2/0/3      not-connected trunk       auto    auto       2.5GBase-T
eth2/0/4      not-connected trunk       auto    auto       2.5GBase-T
eth2/0/5      not-connected trunk       auto    auto       2.5GBase-T
eth2/0/6      not-connected trunk       auto    auto       2.5GBase-T
eth2/0/7      not-connected 1          auto    auto       2.5GBase-T
eth2/0/8      not-connected 1          auto    auto       2.5GBase-T
eth2/0/9      not-connected 1          auto    auto       2.5GBase-T
eth2/0/10     not-connected 1          auto    auto       2.5GBase-T
eth2/0/11     not-connected 1          auto    auto       2.5GBase-T
eth2/0/12     not-connected 1          auto    auto       2.5GBase-T
eth2/0/13     not-connected 1          auto    auto       2.5GBase-T
eth2/0/14     not-connected 1          auto    auto       2.5GBase-T
eth2/0/15     not-connected 1          auto    auto       2.5GBase-T
eth2/0/16     not-connected 1          auto    auto       2.5GBase-T
qq
eth2/0/18     not-connected 1          auto    auto       5GBase-T
eth2/0/19     not-connected 1          auto    auto       5GBase-T
eth2/0/20     not-connected 1          auto    auto       5GBase-T
--More-- or (q)uit (a)ll

Switch#
```

39.9 show interfaces utilization

Данная команда используется для отображения информации о загрузке портов коммутатора.

```
show interfaces [INTERFACE-ID [, | -]] utilization[history {15_minute [slot 1-5 ] | 1_day [slot 1-2]]]
```

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса. Если параметр не указан, будет отображена информация о загрузке всех физических портов коммутатора.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
utilization	(Опционально.) Укажите для отображения информации о загрузке.
history	(Опционально.) Укажите для отображения архивной информации о загрузке портов. Если параметр не указан, архивная информация о загрузке портов не будет отображена.

15_minute (Опционально.) Укажите для отображения архивной статистики за 15 минут.

1_day (Опционально.) Укажите для отображения архивной статистики за сутки.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о загрузке всех или указанных интерфейсов, а также архивную информацию об использовании ЦПУ 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 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 отображения 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 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
--More-- or (q)uit (a)ll
```

39.10 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	Укажите, чтобы отобразить информацию о состоянии GBIC.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.
Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о состоянии GBIC.

Пример

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

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

eth1/0/1
Interface Type: 2.5G-BaseFX

Switch#
```

39.11 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 для отображения подробной информации об автосогласовании.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.
Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения детальной информации об автосогласовании.

Пример

В данном примере показано, как отобразить информацию об автосогласовании.

```
Switch#show interfaces ethernet 2/0/1 auto-negotiation

eth2/0/1
  Auto Negotiation: Enabled

  Speed auto downgrade: Disabled
  Remote Signaling: Not detected
  Configure Status: Complete
  Capability Bits: 100M_Half, 100M_Full, 1000M_Full, 2.5G_Full
  Capability Advertised Bits: 100M_Half, 100M_Full, 1000M_Full
  Capability Received Bits: 100M_Half, 100M_Full, 1000M_Full
  RemoteFaultAdvertised: Disabled
  RemoteFaultReceived: NoError

Switch#
```

39.12 show interfaces description

Данная команда используется для просмотра описания и состояния интерфейсов.

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

Параметры

INTERFACE-ID	(Опционально.) Укажите ID интерфейса. Если параметр не указан, 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для просмотра описания и состояния интерфейсов.

Пример

В данном примере показано, как отобразить описание для всех интерфейсов.

```
Switch#show interfaces description
```

Interface	Status	Administrative	Description
-----	-----	-----	-----
eth1/0/1	down	enabled	
eth1/0/2	down	disabled	
eth1/0/3	down	enabled	
eth1/0/4	down	enabled	
eth1/0/5	up	enabled	My_port
eth1/0/6	up	enabled	
eth1/0/7	up	enabled	
eth1/0/8	up	enabled	
eth1/0/9	up	enabled	
eth1/0/10	up	enabled	
eth1/0/11	down	enabled	
eth1/0/12	down	enabled	
eth1/0/13	down	enabled	
eth1/0/14	down	enabled	
eth1/0/15	down	enabled	
eth1/0/16	down	enabled	
eth1/0/17	down	enabled	
eth1/0/18	down	enabled	
eth1/0/19	down	enabled	
eth1/0/20	down	enabled	
eth1/0/21	up	enabled	
eth1/0/22	up	enabled	
eth1/0/23	up	enabled	
eth1/0/24	up	enabled	
eth1/0/25	up	enabled	
eth1/0/26	up	enabled	
eth1/0/27	up	enabled	
eth1/0/28	up	enabled	
eth1/0/29	up	enabled	
eth1/0/30	up	enabled	
Port-channel1	up	enabled	Uplink channel grp
Interface VLAN1	up	enabled	mgmt interface
Loopback1	up	enabled	The loopback intf
mgmt	up	enabled	oob mgmt port
Null0	up	enabled	Null intf
Total Entries: 35			

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

```
Switch#show interfaces vlan 1 description
```

Interface	Status	Administrative	Description
-----	-----	-----	-----
Interface VLAN1	up	enabled	Data VLAN

39.13 shutdown

Данная команда используется для отключения интерфейса. Чтобы включить интерфейс, 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 может применяться для отключения интерфейсов физического порта, loopback, VLAN, tunnel и интерфейсов управления. Команда также может использоваться для портов port-channel.

При выполнении данной команды отключается порт, при этом пакеты не будут приниматься и передаваться. Чтобы снова включить порт, введите команду **no shutdown**. Если порт отключен, соединение и подключение к сети также будет невозможно.

Пример

В данном примере показано, как отключить интерфейс Ethernet 1/0/1.

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

40. Команды Internet Group Management Protocol (IGMP)

40.1 clear ip igmp groups

Данная команда используется для удаления информации в буфере IGMP об участниках динамических групп, полученной из ответных сообщений.

clear ip igmp groups {all | IP-ADDRESS | interface INTERFACE-ID}

Параметры

all	Укажите для удаления записей всех групп.
IP-ADDRESS	Укажите для удаления записи определенной группы.
interface INTERFACE-ID	Укажите для удаления записей групп, изученных на данном 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, к которым присоединяются узлы из данной подсети. Используйте команду для удаления информации о динамических группах. Чтобы удалить все записи о динамических группах из буфера IGMP, воспользуйтесь командой **clear ip igmp groups all**.

Пример

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

```
Switch# clear ip igmp groups all
Switch#
```

В примере ниже показано, как удалить записи из кэша IGMP для многоадресной группы 224.0.255.1.

```
Switch# clear ip igmp groups 224.0.255.1
Switch#
```

В следующем примере показано, как удалить записи из кэша IGMP для определенного интерфейса.

```
Switch# clear ip igmp groups interface vlan 1
Switch#
```

40.2 ip igmp ignore-subscriber-ip-check

Данная команда используется для отключения проверки IP-адреса источника подписчика при получении сообщений IGMP report или leave. Чтобы вернуться 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 сообщения IGMP report и leave, принимаемые на интерфейсе, будут проверяться на то, принадлежит ли IP-адрес источника к той же подсети, 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** для отключения проверки 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 vlan 1
Switch(config-if)# ip igmp ignore-subscriber-ip-check
Switch(config-if)#
```

40.3 ip igmp enable

Данная команда используется для включения протокола IGMP. Чтобы отключить протокол IGMP, воспользуйтесь формой **no** этой команды.

ip igmp enable
no igmp 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 VLAN-интерфейсов и 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 vlan 1
Switch(config-if)# ip igmp enable
Switch(config-if)#
```

40.4 ip igmp last-member-query-interval

Данная команда используется для конфигурации интервала между сообщениями IGMP с запросом принадлежности с указанием группы (group-specific queries) или источника группы/канала (group-source-specific (channel) queries). Чтобы вернуться 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. 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 установить на VLAN 1000 значение IGMP last member query interval на 2 секунды.

```
Switch# configure terminal
Switch(config)# interface vlan 1000
Switch(config-if)# ip igmp enable
Switch(config-if)# ip igmp last-member-query-interval 2
Switch(config-if)#
```

40.5 ip igmp query-interval

Данная команда используется для конфигурации интервала, с которым маршрутизатор периодически отправляет общие запросы. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip igmp query-interval SECONDS
no ip igmp query-interval

Параметры

SECONDS	Укажите интервал, с которым маршрутизатор отправляет общие запросы IGMP. Диапазон значений: от 1 до 31744 секунд.
---------	---

По умолчанию

Значение по умолчанию – 125 секунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применяется для конфигурации 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 сконфигурировать на VLAN 1000 интервал IGMP query в 300 секунд.

```
Switch# configure terminal
Switch(config)# interface vlan 1000
Switch(config-if)# ip igmp enable
Switch(config-if)# ip igmp query-interval 300
Switch(config-if)#
```

40.6 ip igmp query-max-response-time

Данная команда используется для конфигурации максимального времени ответа, анонсируемого в запросах IGMP query. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip igmp query-max-response-time SECONDS

no ip igmp query-max-response-time

Параметры

SECONDS	Укажите максимальное время ответа в секундах, анонсируемое в запросах IGMP query. 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

С помощью команды можно указать период, в течение которого участник группы может ответить на запрос, прежде чем маршрутизатор удалит членство. Время членства вычисляется следующим образом: query interval x robustness + maximum response time.

Пример

В данном примере показано, как указать значение 10 секунд для максимального времени ответа, анонсируемого в запросах IGMP query, на VLAN 1000.


```
Switch# configure terminal
Switch(config)# interface vlan 1000
Switch(config-if)# ip igmp query-max-response-time 10
Switch(config-if)#
```

40.7 ip igmp robustness-variable

Данная команда используется для конфигурации переменной надежности (robustness), используемой в IGMP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip igmp robustness-variable *VALUE*

no ip igmp robustness-variable

Параметры

<i>VALUE</i>	Укажите переменную надежности (robustness) со значением 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 (robustness) обеспечивает точную настройку с учетом ожидаемой потери пакетов на интерфейсе. Значение переменной используется при вычислении следующих интервалов сообщений IGMP:

- **Group member interval** – время, по истечении которого маршрутизатор решает, что в сети больше нет участников группы. Этот интервал вычисляется следующим образом: $(\text{robustness} \times \text{query interval}) + (1 \times \text{query response interval})$.
- **Other querier present interval** – время, по истечении которого маршрутизатор решает, что в сети больше нет другого Querier (маршрутизатора, отвечающего за отправку multicast-трафика). Интервал вычисляется следующим образом: $(\text{robustness} \times \text{query interval}) + (0,5 \times \text{query response interval})$.
- **Last member query count** – количество запросов с указанием группы (group-specific queries), отправляемое до того, как маршрутизатор решит, что больше нет локальных участников группы. По умолчанию значение равно переменной надежности.

Пример

В данном примере показано, как указать значение переменной надежности «3» на интерфейсе VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface vlan 1000
Switch(config-if)# ip igmp robustness-variable 3
Switch(config-if)#
```

40.8 ip igmp ssm-map enable

Данная команда используется, чтобы включить привязку Source Specific Multicast (SSM, многоадресной рассылки с заданным источником) для узлов IGMPv1 или IGMPv2. Для отключения привязки воспользуйтесь формой **no** этой команды.

ip igmp [vrf VRF-NAME] ssm-map enable
no ip igmp ssm-map enable

Параметры

vrf VRF-NAME	(Опционально.) Укажите экземпляр многоадресной VPN-маршрутизации и пересылки (VRF).
---------------------	---

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду для включения/отключения привязки SSM для групп в сконфигурированном диапазоне SSM. Привязка SSM применяется только к принимаемым пакетам membership report IGMPv1 или IGMPv2.

Пример

В данном примере показано, как включить привязку SSM для узлов IGMPv1 или IGMPv2.

```
Switch# configure terminal
Switch(config)# ip igmp ssm-map enable
```

40.9 ip igmp ssm-map static

Данная команда используется, чтобы создать статическую запись SSM для узлов IGMPv1 или IGMPv2. Для удаления записи воспользуйтесь формой **no** этой команды.

ip igmp [vrf VRF-NAME] ssm-map static ACCESS-LIST SOURCE-ADDRESS
no ip igmp ssm-map static ACCESS-LIST SOURCE-ADDRESS

Параметры

vrf VRF-NAME	(Опционально.) Укажите экземпляр многоадресной VPN-маршрутизации и пересылки (VRF).
ACCESS-LIST	Укажите стандартный список доступа IP, который содержит многоадресные группы для привязки. Для того чтобы разрешить группу, укажите «any» в поле адреса источника и групповой адрес в поле адреса назначения в записи списка доступа.
SOURCE-ADDRESS	Укажите адрес источника, который должен быть ассоциирован с группой, определенной в списке доступа.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Внедрение SSM позволяет провайдеру легко управлять IP-адресом многоадресной рассылки.

При включении SSM маршрутизатор, являющийся последним узлом, построит «дерево» на основе источника для канала (S, G) после получения запроса '(S, G) INCLUDE mode' от подключенных узлов IGMPv3, которые попадают в данный диапазон SSM.

Когда подключенные узлы IGMPv1 или IGMPv2 отправляют запросы (*, G), и многоадресная группа находится в диапазоне SSM, коммутатор будет привязывать запросы (*, G) к запросам (S, G) на основе ассоциаций адреса источника с группой, определенных командой **ip igmp ssm-map static**. В результате маршрутизатор построит «дерево» на основе источника для привязанных (S, G).

Команда может быть выполнена несколько раз. Групповой адрес может быть ассоциирован со множеством адресов источника. При наличии нескольких ассоциаций маршрутизатор построит «дерево» (S, G) для каждого источника.

Команда действует при опциях, включенных командами **ip pim ssm** и **ip igmp ssm-map enable**.

Пример

В данном примере показано, как настроить диапазон SSM, включить привязку SSM и сконфигурировать запись привязки SSM.

```
Switch# configure terminal
Switch(config)# ip access-list SSM-GROUP
Switch(config-ip-acl)# permit any 232.0.0.0 0.255.255.255
Switch(config-ip-acl)# exit
Switch(config)# ip pim ssm range SSM-GROUP
Switch(config)# ip igmp ssm-map enable
Switch(config)# ip access-list CHANNEL-1
Switch(config-ip-acl)# permit any 232.1.1.1 0.0.0.0
Switch(config-ip-acl)# exit
Switch(config)# ip access-list CHANNEL-2
Switch(config-ip-acl)# permit any 232.1.1.2 0.0.0.0
Switch(config-ip-acl)# exit
Switch(config)# ip igmp ssm-map static CHANNEL-1 10.1.1.1
Switch(config)# ip igmp ssm-map static CHANNEL-2 10.2.1.1
```

40.10 ip igmp static-group

Данная команда используется, чтобы создать статическое членство 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

<i>GROUP-ADDRESS</i>	Укажите групповой IP-адрес. Допустимый диапазон адресов: 224.0.0.0 – 239.255.255.255.
----------------------	--

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду для создания статической группы IGMP в случае, когда подключенный узел не поддерживает протокол IGMP. При настройке в кэш IGMP добавляется запись группы.

Пример

В данном примере показано, как настроить запись статической группы IGMP на VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface vlan 1000
Switch(config-if)# ip igmp static-group 238.1.1.2
Switch(config-if)#
```

40.11 ip igmp version

Данная команда используется для изменения версии IGMP на указанном интерфейсе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

ip igmp version *NUMBER*
no ip igmp version

Параметры

<i>GROUP-ADDRESS</i>	Укажите версию IGMP. 1: Укажите для запуска IGMP версии 1 на коммутаторе. 2: Укажите для запуска IGMP версии 2 на коммутаторе. 3: Укажите для запуска IGMP версии 3 на коммутаторе.
----------------------	--

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 vlan 1000
Switch(config-if)# ip igmp enable
Switch(config-if)# ip igmp version 3
Switch(config-if)#
```

40.12 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

<i>IP-ADDRESS</i>	(Опционально.) Укажите IP-адрес группы для отображения. Если IP-адрес не указан, будет отображаться информация по всем группам IGMP.
interface <i>INTERFACE-ID</i>	(Опционально.) Укажите интерфейс для отображения. Если интерфейс не указан, будет отображаться информация о группах IGMP для всех интерфейсов, на которых включен IGMP.
detail	(Опционально.) Укажите для отображения подробной информации.
static	(Опционально.) Укажите для отображения статических групп.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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       225.0.1.10         0DT00H00M56S       0DT00H14M13S       20.0.2.36

Total Entries:1

Switch#
```

В примере ниже показано, как отобразить подробную информацию IGMP для группы 224.1.1.1.

```
Switch# show ip igmp groups detail

Interface      : vlan1000
Group          : 224.1.1.1
Uptime        : 0DT00H00M42S
Expires       : Stopped
Group mode     : Include
Last reporter  : 192.168.50.111

Group source List: (M - SSM Mapping)
  Source Address  v3 Exp      Flags
  -----
  192.168.55.55   0DT00H15M08S
  192.168.10.55   0DT00H15M08S

Total Source Entries:2

Interface      : vlan2000
Group          : 224.1.1.1
Uptime        : 0DT00H00M42S
Expires       : 0DT00H03M38S
Group mode     : Exclude
Last reporter  : 192.168.51.111

Group source List: (M - SSM Mapping)
  Source Address  v3 Exp      Flags
  -----
  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.
----------------------	--

40.13 show ip igmp interface

Данная команда используется для отображения конфигурации IGMP на интерфейсе.

show ip igmp interface [INTERFACE-ID]

Параметры

<i>INTERFACE-ID</i>	(Опционально.) Укажите интерфейс. Если интерфейс не указан, коммутатор отображает информацию IGMP для всех интерфейсов, на которых включен IGMP. Разрешены только VLAN-интерфейсы.
---------------------	--

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения конфигурации 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      : 10.90.90.90/255.0.0.0
  IGMP State              : Enabled
  Querier                 : 10.90.90.90
  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, запущенная 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 пакетах IGMP от подписчика. Enabled – указывает, что проверка IP-адреса источника не игнорируется. Disabled – указывает, что проверка IP-адреса источника игнорируется.

40.14 show ip igmp ssm-mapping

Данная команда используется для отображения конфигурации привязки SSM.

```
show ip igmp [vrf VRF-NAME] ssm-mapping [GROUP-ADDRESS]
```

Параметры

vrf VRF-NAME	(Опционально.) Укажите экземпляр многоадресной VPN-маршрутизации и пересылки (VRF).
GROUP-ADDRESS	Укажите многоадресную группу для отображения.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.
Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить привязку SSM для указанной многоадресной группы.

Пример

В данном примере показано, как отобразить конфигурацию привязки SSM.

```
Switch# show ip igmp ssm-mapping
SSM Mapping : Enabled
Switch#
```

В данном примере показано, как отобразить привязку SSM для группового адреса 232.1.1.1.

```
Switch# show ip igmp ssm-mapping 232.1.1.1
SSM Mapping : Enabled
Group address: 232.1.1.1
Source address: 10.1.1.1
Switch#
```

Отображаемые параметры

SSM Mapping	Enabled/Disabled: указывает, включена или отключена функция привязки SSM.
Group address	Групповой адрес SSM.
Source address	Адрес источника, который будет использоваться для преобразования запросов (*, G) в (S, G).

41. Команды Internet Group Management Protocol (IGMP) Snooping

41.1 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 <i>VLAN-ID</i>	Укажите VLAN, для которой необходимо удалить статистику IP IGMP Snooping.
interface <i>INTERFACE-ID</i>	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 groups all
Switch#
```

41.2 ip igmp snooping

Данная команда используется для включения функции IGMP Snooping на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ip igmp snooping
no ip igmp snooping

Параметры

Нет.

По умолчанию

Функция IGMP Snooping отключена на всех интерфейсах VLAN.

Функция IGMP Snooping отключена глобально.

Режим ввода команды

Interface Configuration Mode.

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

В режиме Interface Configuration Mode команда может быть использована только для настройки VLAN-интерфейсов. Для того чтобы предоставить VLAN доступ к IGMP Snooping, необходимо включить данную функцию глобально и для интерфейса. Настройки IGMP Snooping и MLD Snooping являются независимыми и могут быть применены для VLAN одновременно.

Пример

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

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

В примере ниже показано, как включить функцию IGMP Snooping на всех VLAN.

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

В следующем 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)#
```

41.3 ip igmp snooping access-group

Данная команда используется, 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

<code>ACCESS-LIST-NAME</code>	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.
<code>vlan VLAN-ID</code>	(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

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

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.

Пример

В данном примере показано, как выбрать группу 226.1.1.1 в качестве единственной разрешенной обслуживаемой группы IGMP Snooping для интерфейса Ethernet 3/0/1. 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 3/0/1.

```
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(config)# interface eth3/0/1
Switch(config-if)# ip igmp snooping access-group igmp_filter
Switch(config-if)# end
```

В данном примере показано, как выбрать группу 226.1.1.1 в качестве единственной разрешенной обслуживаемой группы IGMP Snooping для интерфейса port-channel 1.

```
Switch# configure terminal
Switch(config)# interface port-channel 1
Switch(config-if)# ip igmp snooping access-group igmp_filter vlan 2
Switch(config-if)# end
```

41.4 ip igmp snooping accounting

Данная команда используется для включения IGMP Accounting при подключении получателя к IGMP-группе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ip igmp snooping accounting
no ip igmp snooping accounting

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 данную команду, чтобы включить/отключить IGMP Accounting при подключении получателя к IGMP-группе. Если данная функция включена, при подключении получателя к группе на RADIUS будет выслано сообщение IGMP accounting.

Пример

В данном примере показано, как включить IGMP Accounting на интерфейсе Ethernet 1/0/1.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#ip igmp snooping accounting
Switch(config-if)#
```

41.5 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 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, 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 3/0/1.

```
Switch#configure terminal
Switch(config)# interface ethernet 3/0/1
Switch(config-if)# ip igmp snooping authentication
Switch(config-if)# end
```

41.6 ip igmp snooping fast-leave

Данная команда используется для настройки функции IGMP Snooping Fast Leave на интерфейсе. Чтобы отключить данную функцию на указанном интерфейсе, 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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. Используйте команду **ip igmp snooping fast-leave**, чтобы удалить членство IGMP на порту после получения сообщения leave, не применяя механизм обработки сообщений group-specific query (с указанием группы) или group-source-specific query (с указанием источника группы).

Пример

В данном примере показано, как включить функцию IGMP Snooping Fast Leave на VLAN 1.

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

41.7 ip igmp snooping ignore-topology-change-notification

Данная команда используется для игнорирования изменений STP и отказа от отправки на интерфейс STP-запроса. Чтобы отключить игнорирование изменений STP и отправку 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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. Коммутатор с включенной функцией IGMP Snooping получает информацию об изменениях топологии Link Layer, вызванных Spanning Tree. Если порт включен/отключен при помощи Spanning Tree, на все активные порты, кроме router-портов, будет отправлено сообщение general query, чтобы сократить интервал сетевой 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)#
```

41.8 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). Чтобы вернуться 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. Диапазон значений: от 1 до 25.
---------	---

По умолчанию

Значение по умолчанию – 1 секунда.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. Получив сообщение IGMP leave, IGMP Snooping Querier будет считать, что на интерфейсе нет локальных участников, если по истечении времени ожидания не будет получено ни одного ответа. Пользователи могут уменьшить данный интервал, чтобы сократить время, которое уходит у коммутатора на обнаружение потери последнего участника группы.

Пример

В данном примере показано, как настроить значение last member query interval. Указанное значение – 3 секунды.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping last-member-query-interval 3
Switch(config-vlan)#
```

41.9 ip igmp snooping limit

Данная команда используется для установки ограничения по количеству записей кэша IGMP, которые можно создать. Чтобы удалить ограничение, 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 создаваемых записей кэша IGMP. Диапазон значений: от 1 до 2048.
exceed-action	(Опционально.) Укажите, чтобы применить действие к изученным группам при превышении установленного ограничения. drop: укажите, чтобы отбросить новую группу. replace: 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 ограничения отсутствуют.

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. При превышении лимита, системное сообщение будет генерироваться и регистрироваться.

Пример

В данном примере показано, как установить ограничение по количеству групп IGMP Snooping с ограничением настройки от ACL, к которому может подключиться интерфейс Ethernet 4/0/38 с VLAN ID 1000.

```
Switch# configure terminal
Switch(config)# interface ethernet 4/0/38
Switch(config-if)# ip igmp snooping limit 80 except igmp_filter vlan 1000
Switch(config-if)# end
```

В примере ниже показано, как сбросить ограничение по количеству групп IGMP Snooping по

умолчанию, к которому может подключиться интерфейс port-channel 4.

```
Switch# configure terminal
Switch(config)# interface port-channel 4
Switch(config-if)# no ip igmp snooping limit vlan 1
Switch(config-if)# end
```

41.10 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. Чтобы удалить интерфейс/интерфейсы 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 multicastrouter-порты IGMP Snooping отсутствуют.

По умолчанию включено автоматическое изучение.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. Multicast router-портом

можно назначить физический порт или port-channel. Указанный multicast router-порт должен являться портом-участником сконфигурированной VLAN. Multicast router-порт может быть изучен динамически или сконфигурирован статически. При помощи динамического изучения устройство IGMP Snooping будет изучать пакеты IGMP, PIM или DVMRP, чтобы идентифицировать multicast router-порт. Если автоматическое изучение отключено, multicast router-порт может быть сконфигурирован только статически.

Пример

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

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping mrouter interface ethernet 1/0/4
Switch(config-vlan)#
```

41.11 ip igmp snooping proxy-reporting

Данная команда используется для включения функции Proxy Reporting. Чтобы отключить данную функцию, 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 составляет 0.
--------------------------	---

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. Если функция Proxy Reporting включена, перед отправкой на router-порт полученные пакеты IGMP report или IGMP leave для указанного канала (S, G) будут объединены в один отчет. В качестве IP-адреса источника отчета будет использован IP-адрес источника Proxy Reporting. Если IP-адрес источника Proxy Reporting не настроен, будет использован нулевой IP-адрес. MAC-адрес интерфейса будет использован в качестве MAC-адреса источника отчета. Если на VLAN нет настроенных IP-адресов, будет использован системный MAC-адрес.

Пример

В данном примере показано, как включить IGMP Snooping Proxy Reporting на VLAN 1 и настроить IP-адрес источника сообщения proxy reporting. Настроенный IP-адрес – 1.2.2.2.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-if)# ip igmp snooping proxy-reporting source 1.2.2.2
Switch(config-if)#
```

41.12 ip igmp snooping querier

Данная команда используется для указания устройства в качестве IGMP Snooping Querier. Чтобы отключить данную функцию, 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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. Чтобы запустить Querier, интерфейсу необходимо присвоить IP-адрес. Если у VLAN отсутствует IP-адрес, система вышет сообщение warning. Если Querier включен, но IP-адрес удален, работа querier будет остановлена. Если система может выполнить роль Querier, устройство будет ожидать пакеты IGMP query, отправленные другими устройствами. При получении сообщения IGMP query устройство с более низким значением IP-адреса становится Querier. Если на интерфейсе также включен IGMP-протокол, IGMP Snooping Querier будет автоматически отключен.

Пример

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

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

41.13 ip igmp snooping query-interval

Данная команда используется для настройки интервала между сообщениями IGMP general query. Чтобы вернуться 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. 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 VLAN-интерфейсов. 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)#
```

41.14 ip igmp snooping query-max-response-time

Данная команда используется для настройки максимального значения времени ожидания, анонсированного в сообщениях IGMP snooping query. Чтобы вернуться 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. Диапазон значений: от 1 до 25 секунд.
---------	--

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. 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)#
```

41.15 ip igmp snooping query-version

Данная команда используется для настройки версии пакетов general query, отправляемых IGMP Snooping Querier. Чтобы вернуться 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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. 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)#
```

41.16 ip igmp snooping rate-limit

Данная команда используется, чтобы установить ограничение скорости передачи входящих управляющих IGMP-пакетов. Чтобы отключить ограничения по скорости, воспользуйтесь формой **no** этой команды.

ip igmp snooping rate-limit *NUMBER*

no ip igmp snooping rate-limit

Параметры

<i>NUMBER</i>	Укажите пропускную способность (количество пакетов в секунду) для управляющих IGMP-пакетов, обработка которых возможна на определенном интерфейсе.
---------------	--

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-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 ограничить скорость передачи пакетов на интерфейсе VLAN 1000. Указанное ограничение – 30 пакетов в секунду.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping rate-limit 30
Switch(config-vlan)#
```

41.17 ip igmp snooping report-suppression

Данная команда используется для включения функции Report Suppression. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

ip igmp snooping report-suppression
no ip igmp snooping report-suppression

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 VLAN-интерфейсов. 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)#
```

41.18 ip igmp snooping robustness-variable

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

ip igmp snooping robustness-variable *VALUE*
no ip igmp snooping robustness-variable

Параметры

<i>VALUE</i>	Укажите значение robustness variable в диапазоне от 1 до 7.
--------------	---

По умолчанию

Значение по умолчанию – 2.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. Robustness variable обеспечивает точную настройку в соответствии с ожидаемой потерей пакетов на интерфейсе. Значение robustness variable используется для расчета следующих интервалов IGMP-сообщений:

- **Group member interval** – промежуток времени, по истечении которого многоадресный маршрутизатор считает, что в группе больше нет активных участников. Данный интервал рассчитывается следующим образом: (robustness variable x query interval) + (1 x query response interval).
- **Other querier present interval** – промежуток времени, по истечении которого многоадресный маршрутизатор считает, что маршрутизатор, являющийся Querier, больше не доступен. Данный интервал рассчитывается следующим образом: (robustness variable x query interval) + (0.5 x query response interval).
- **Last member query count** – количество запросов group-specific queries (с указанием группы), отправленных маршрутизатором до того, как он предполагает, что в группе нет локальных участников. Robustness variable является значением по умолчанию данного счетчика.

Пользователи могут увеличить данное значение, если для сети требуются более свободные условия.

Пример

В данном примере показано, как настроить robustness variable на интерфейсе VLAN 1000. Указанное значение – 3.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping robustness-variable 3
Switch(config-vlan)#
```

41.19 ip igmp snooping static-group

Данная команда используется для настройки статической группы IGMP Snooping. Чтобы удалить статическую группу, 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 диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

По умолчанию статическая группа не настроена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. Используйте данную команду на VLAN-интерфейсе, чтобы добавить запись статической группы и/или источник multicast потока.

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

Пример

В данном примере показано, как добавить запись статической группы и источник multicast потока для IGMP Snooping.

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

41.20 ip igmp snooping suppression-time

Данная команда используется, чтобы указать 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 интервал подавления дублированных сообщений IGMP report. Диапазон значений: от 1 до 300.
---------	--

По умолчанию

Значение по умолчанию – 10 секунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется исключительно для настройки VLAN-интерфейсов. Функция Report Suppression блокирует дублированные сообщения IGMP report или IGMP leave, полученные в течение указанного времени. Чем меньше значение интервала подавления, тем чаще будут отправляться дублированные IGMP-сообщения.

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)#
```

41.21 ip igmp snooping minimum-version

Данная команда используется для настройки минимальной версии IGMP-узлов, разрешенной на интерфейсе. Чтобы удалить ограничение, воспользуйтесь формой **no** этой команды.

ip igmp snooping minimum-version {2 | 3}

no ip igmp snooping minimum-version

Параметры

2	Укажите, чтобы отфильтровать сообщения IGMPv1.
3	Укажите, чтобы отфильтровать сообщения IGMPv1 и IGMPv2.

По умолчанию

По умолчанию ограничения минимальной версии отсутствуют.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. Настройки применяются 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)#
```

41.22 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 для отображения.
---------------------	--

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

В данном примере показано, как отобразить настройки IGMP Snooping.

```
Switch#show ip igmp snooping

IGMP snooping global state: Enabled

VLAN #1 configuration
  IGMP snooping state           : Enabled
  Minimum version               : v1
  Fast leave                    : Enabled (host-based)
  Report suppression            : Disabled
  Suppression time              : 10 seconds
  Querier state                 : Enabled (Non-active)
  Querier                       : -
  Query expiry time             : 0 seconds
  Query version                 : v3
  Query interval                : 125 seconds
  Max response time             : 10 seconds
  Robustness value              : 3
  Last member query interval    : 3 seconds
  Proxy reporting               : Enabled (Source 1.2.2.2)
  Rate limit                    : 0
  Ignore topology change       : Enabled
Total Entries: 1

Switch#
```

41.23 show ip igmp snooping aaa

Данная команда используется для отображения информации об аутентификации IGMP Snooping и конфигурации IGMP Accounting.

show ip igmp snooping aaa [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите интерфейс или список интерфейсов. Может быть использован физический интерфейс или port-channel.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об аутентификации IGMP Snooping и конфигурации IGMP Accounting. Если параметры не указаны, 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#
```

41.24 show ip igmp snooping groups

Данная команда используется для отображения информации о группе IGMP Snooping, изученной на коммутаторе.

show ip igmp snooping groups [vlan VLAN-ID [, | -] | [IP-ADDRESS] [detail]

Параметры

vlan VLAN-ID	(Опционально.) Укажите интерфейс VLAN, который необходимо отобразить. Если VLAN не указаны, будет отображена информация о группе IGMP Snooping для всех VLAN с включенной функцией IGMP Snooping.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
IP-ADDRESS	(Опционально.) Укажите IP-адрес группы для отображения. Если IP-адрес не указан, будет отображена информация обо всех группах IGMP.
detail	(Опционально.) Укажите, чтобы отобразить подробную информацию о группе IGMP.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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


```
Switch# show ip igmp snooping groups

Total Group Entries : 1
Total Source Entries: 2

vlan 1, 230.1.1.1
Learned on port: 1/0/3,1/0/5

Switch#
```

41.25 show ip igmp snooping filter

Данная команда используется для отображения информации о конфигурации IGMP Snooping Filter для всех интерфейсов или указанного интерфейса.

show ip igmp snooping filter [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите физический интерфейс или port-channel. Если интерфейс не указан, будет отображена информация об IGMP Snooping Filter для всех интерфейсов.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.
Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

В данном примере показано, как отобразить информацию об IGMP Snooping Filter, если интерфейс не

указан.

```
Switch#show ip igmp snooping filter

eth2/0/7
  Rate limit: Not Configured
  Access group: igmp_filter
  Groups/Channel Limit: Not Configured
  vlan2:
    Access group: igmp_filter
    Groups/Channel Limit: Not Configured

eth2/0/8
  Rate limit: Not Configured
  Access group: Not Configured
  Groups/Channel Limit: Not Configured
  vlan1:
    Access group: Not Configured
    Groups/Channel Limit: 80 (Exception List: igmp_filter, exceed-action: drop)

Switch#
```

В примере ниже показано, как отобразить информацию об IGMP Snooping Filter для интерфейса Ethernet 1/0/2.

```
Switch#show ip igmp snooping filter interface ethernet 1/0/2

eth1/0/2
  Rate limit: 10pps
  Access group: Not Configured
  Groups/Channel Limit: Not Configured
  vlan 1:
    Access group: Not Configured
    Groups/Channel Limit: 100 (Exception List: ExtendACL, exceed-action: drop)

Switch#
```

41.26 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 диапазона VLAN от предыдущего.

Пробелы до и после запятой недопустимы.

-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
---	--

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.
Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить интерфейсы динамически изученного или настроенного вручную многоадресного маршрутизатора.

Пример

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

```
Switch#show ip igmp snooping mrouter

VLAN    Ports
-----
1       1/0/1-1/0/4 (static)

Total Entries: 1

Switch#
```

41.27 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 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.
vlan	Укажите, чтобы отобразить счетчики статистики VLAN.
<i>VLAN-ID</i>	(Опционально.) Укажите VLAN ID 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

```
Switch#show ip igmp snooping statistics vlan 1
```

```
VLAN 1 Statistics:
```

```
IGMPv1 Rx: Report 0, Query 0
IGMPv2 Rx: Report 0, Query 0, Leave 0
IGMPv3 Rx: Report 3, Query 0
IGMPv1 Tx: Report 0, Query 0
IGMPv2 Tx: Report 0, Query 0, Leave 0
IGMPv3 Tx: Report 1, Query 2
```

```
Total Entries: 1
```

```
Switch#
```

41.28 show ip igmp snooping static-group

Данная команда используется для отображения статически настроенных групп IGMP Snooping на коммутаторе.

show ip igmp snooping static-group [*GROUP-ADDRESS* | **vlan** *VLAN-ID*]

Параметры

<i>GROUP-ADDRESS</i>	(Опционально.) Укажите IP-адрес группы для отображения.
vlan <i>VLAN-ID</i>	(Опционально.) Укажите VLAN ID для отображения.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статически настроенные группы IGMP Snooping на коммутаторе. Если параметры не указаны, 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#
```

42. IP Multicast (IPMC)

42.1 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 функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если функция IP Multicast Routing отключена, система остановит пакеты routing multicast, даже если включен протокол Multicast Routing.

Пример

В данном примере показано, как включить IP Multicast Routing.

```
Switch# configure terminal
Switch(config)# ip multicast-routing
Switch(config)#
```

42.2 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 отображения информации об IP multicast.
--------------	---

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения информации об интерфейсе IP multicast. Если параметр **interface** не указан, будет отображен 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 режима поиска (lookup mode) перенаправления IP multicasting.

```
Switch#show ip multicast

IP multicast-routing global state: Enabled
Table lookup mode: IP

Switch#
```

В примере ниже 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#
```

42.3 show ip mroute

Данная команда используется, чтобы отобразить содержимое таблицы IP multicast routing.

show ip mroute *[{GROUP-ADDRESS [SOURCE-ADDRESS] | sparse | summary | static}]*

Параметры

<i>GROUP-ADDRESS</i>	(Опционально.) Укажите IP-адрес группы.
<i>SOURCE-ADDRESS</i>	Укажите IP-адрес multicast-источника.
summary	(Опционально.) Укажите, чтобы отобразить краткую однострочную информацию для каждой записи в таблице IP multicast routing.
sparse	(Опционально.) Укажите для отображения только маршрутов PIM-SM.
static	(Опционально.) Укажите для отображения только статических multicast-маршрутов.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить содержимое 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 групповой рассылки 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
Multicast route table summary
Source IP      Group IP      Protocol    Incoming    Outgoing
Interface      Interface    List
-----
*              225.0.1.10   PIMSM              vlan1100
Switch#
```


В примере ниже 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

( *,225.0.1.10), ODT00H00M01S/ODT00H00M00S, RP is 20.0.1.10, Flags: S
  Incoming interface: NULL, RPF neighbor: NULL
  Outgoing interface list:
    vlan1100, Forwarding ODT00H00M01S/ODT00H04M18S

Total Entries: 1

Switch#
```

В следующем примере показано, как отобразить запись multicast-маршрута в режиме Sparse Mode.

```
Switch# show ip mroute sparse

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

( *,225.0.1.10), ODT00H02M09S/ODT00H00M00S, RP is 20.0.1.10, Flags: S
  Incoming interface: NULL, RPF neighbor: NULL
  Outgoing interface list:
    vlan1100, Forwarding ODT00H02M09S/ODT00H02M10S

Total Entries: 1

Switch#
```

42.4 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-ADDRESS	(Опционально.) Укажите IP-адрес группы.
---------------	---

SOURCE-ADDRESS Укажите IP-адрес multicast-источника.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию 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 кэш 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, T2

(*,225.0.0.0) VLAN0070
  Outgoing interface list: 1/0/1-1/0/2

(10.1.1.1, 239.0.0.1) VLAN0060
  Outgoing interface list: 1/0/1, 2/0/2

Total entries: 3
```

43. Команды IP Source Guard

43.1 ip verify source vlan dhcp-snooping

Данная команда используется для включения на порту функции защиты IP-адреса – IP Source Guard. Чтобы отключить 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 и IP- и MAC-адреса получаемых IP-пакетов.
---------------	---

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки интерфейсов физического порта и port-channel. Используйте данную команду, чтобы включить 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.

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 ethernet 1/0/1
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config-if)#
```

43.2 ip source binding

Данная команда используется, чтобы создать статическую запись 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-ADDRESS	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, чтобы создать статическую привязку, используемую для проверки IP Source Guard. При использовании формы **no** этой 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 ethernet 1/0/10
Switch(config)#
```

В примере ниже показано, как удалить привязку IP Source Guard с IP-адресом 10.1.1.1 и MAC-адресом 00-01-02-03-04-05 в VLAN 2 на интерфейсе Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# no ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface ethernet
1/0/10
Switch(config)#
```

43.3 show ip source binding

Данная команда используется для отображения привязки IP Source Guard.

show ip source binding [*IP-ADDRESS*] [*MAC-ADDRESS*] [*dhcp-snooping* | *static*] [*vlan* *VLAN-ID*] [*interface* *INTERFACE-ID* [, | -]]

Параметры

<i>IP-ADDRESS</i>	(Опционально.) Укажите для отображения привязки IP Source Guard на основе IP-адреса.
<i>MAC-ADDRESS</i>	(Опционально.) Укажите для отображения привязки IP Source Guard на основе MAC-адреса.
dhcp-snooping	(Опционально.) Укажите для отображения привязки IP Source, изученной при помощи DHCP Snooping.
static	(Опционально.) Укажите для отображения привязки IP Source Guard, настроенной вручную.
vlan <i>VLAN-ID</i>	(Опционально.) Укажите для отображения привязки IP Source Guard на основе VLAN.
interface <i>INTERFACE-ID</i>	(Опционально.) Укажите для отображения привязки IP Source Guard на основе порта.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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 записи привязки IP Source Guard без каких-либо параметров.

```
Switch#show ip source binding
```

MAC Address	IP Address	Lease(sec)	Type	VLAN	Interface
00-01-01-01-01-01	10.1.1.10	infinite	static	100	eth1/0/3
00-01-01-01-01-10	10.1.1.11	3120	dhcp-snooping	100	eth1/0/3

```
Total Entries: 2
```

```
Switch#
```

В примере ниже 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 следующем примере показано, как отобразить записи привязки IP Source Guard на основе IP-адреса 10.1.1.11, MAC-адреса 00-01-01-01-01-10 в VLAN 100 на интерфейсе 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 ethernet 1/0/3
```

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.

43.4 show ip verify source

Данная команда используется для отображения записи списка управления доступом (ACL) аппаратного порта на определенном интерфейсе.

show ip verify source [interface *INTERFACE-ID*][, | -]

Параметры

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

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения записей в аппаратной таблице ACL.

Пример

В данном примере показано, как отобразить запись, когда в VLAN 100 – 110 включен DHCP Snooping, интерфейс в режиме IP Source Filter Mode настроен как IP, а существующая привязка произведена на основе IP-адреса 10.1.1.1 в VLAN 100.

```
Switch#show ip verify source interface ethernet 1/0/3
```

Interface	Filter-type	Filter-mode	IP address	MAC address	VLAN
eth1/0/3	ip	active	10.1.1.1	-	100
eth1/0/3	ip	active	deny-all	-	101-120

Total Entries: 2

```
Switch#
```

В примере ниже 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

Total Entries: 2

```
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.

44. Команды IP Utility

44.1 ping

Данная команда используется для диагностики базового сетевого соединения.

```
ping {[ip] IP-ADDRESS | [ipv6] IPV6-ADDRESS | HOST-NAME} [length LENGTH] [count TIMES]  
[timeout SECONDS] [stoptime SECONDS] [tos TOS] [source {IP-ADDRESS | IPV6-ADDRESS}]  
[frequency SECONDS]
```

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.
HOST-NAME	Укажите имя узла системы, которое необходимо обнаружить.
length LENGTH	(Опционально.) Укажите количество байтов данных, которое необходимо отправить. Значение не включает длину тега VLAN или IEEE 802.1Q. Диапазон значений: от 1 до 1420.
count TIMES	(Опционально.) Укажите, чтобы завершить процесс после отправки указанного количества пакетов echo request.
timeout SECONDS	(Опционально.) Укажите время ожидания ответа в секундах.
stoptime SECONDS	(Опционально.) Укажите для прекращения проверки ping по истечении указанного времени. Диапазон значений: от 0 до 99.
tos TOS	(Опционально.) Укажите для настройки QoS в датаграммах ICMP. Диапазон значений: от 0 до 255.
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.
frequency SECONDS	(Опционально.) Укажите частоту проверки ping. Введите интервал времени между каждым ICMP-запросом. Диапазон значений: от 0 до 86400. Значение по умолчанию — 0.

По умолчанию

Значение **length** – 56 байт.

Параметр **count** отключен. Проверка ping будет продолжаться до тех пор, пока пользователь не завершит процесс.

Значение **timeout** – 1 секунда.

Значение **stoptime** – 0.

Значение **tos** – 0.

Значение **frequency** – 0.

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. Обязательно установите значение параметра **count** или **timeout**.

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 примере ниже 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#
```

44.2 ping access-class

Данная команда используется, чтобы указать список 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
```

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 226.1.1.1.

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

44.3 traceroute

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

```
traceroute {[ip] IP-ADDRESS | [ipv6] IPV6-ADDRESS | HOST-NAME} [length LENGTH] [probe NUMBER] [timeout SECONDS] [max-ttl TTL] [port DEST-PORT]
```

```
traceroute [vrf VRF-NAME] {IP-ADDRESS | IPV6-ADDRESS | HOST-NAME} [length LENGTH] [probe NUMBER] [timeout SECONDS] [tos TOS] [initial-ttl TTL] [max-ttl TTL] [port DEST-PORT] [source {IP-ADDRESS | IPV6-ADDRESS}] [frequency SECONDS]
```

Параметры

ip	(Опционально.) Укажите, чтобы использовать IPv4-адрес.
<i>IP-ADDRESS</i>	Укажите IPv4-адрес узла назначения.
ipv6	(Опционально.) Укажите, чтобы использовать IPv6-адрес.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес системы, который необходимо обнаружить.
<i>HOST-NAME</i>	Укажите имя узла системы, которое необходимо обнаружить.
length <i>LENGTH</i>	(Опционально.) Укажите количество байтов исходящих датаграмм. Диапазон значений: от 1 до 1420.
probe <i>NUMBER</i>	(Опционально.) Укажите количество датаграмм, которое необходимо отослать. Диапазон значений: от 1 до 1000.
timeout <i>SECONDS</i>	(Опционально.) Укажите время ожидания ответа в секундах.
tos <i>TOS</i>	(Опционально.) Укажите для настройки ToS в заголовке IP-адреса исходящих датаграмм. Диапазон значений: от 0 до 255.
initial-ttl <i>TTL</i>	(Опционально.) Укажите для отправки датаграмм UDP с определенным значением TTL, равным INITIAL_TTL, вместо TTL по умолчанию, равного 1. Этот параметр позволяет пропускать обработку для узлов, значение которых меньше, чем INITIAL_TTL. Диапазон значений: от 1 до 255.
max-ttl <i>TTL</i>	(Опционально.) Укажите максимальное значение TTL для исходящих UDP-датаграмм. Максимальный доступный диапазон значений: от 1 до 255.
port <i>DEST-PORT</i>	(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.
source { <i>IP-ADDRESS</i> <i>IPV6-ADDRESS</i> }	(Опционально.) Укажите IP-адрес источника, используемый для пакетов ping. Указанный IP-адрес должен быть одним из адресов, настроенных на коммутаторе. IP-адреса источника и назначения должны быть одного и того же типа, либо IPv4, либо IPv6.
frequency <i>SECONDS</i>	(Опционально.) Укажите частоту для трассировки. Диапазон значений: от 0 до 86400.

По умолчанию

По умолчанию отправляются три 40-байтовые UDP-датаграммы, Initial TTL которых равен 1.

Максимальное значение TTL – 30.

Значение **timeout** – 5 секунд.

Значение **tos** – 0.

Номер UDP-порта назначения – 33434.

Количество запросов для каждого TTL – 3.

Значение **frequency** – 0.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Чтобы прервать выполнение данной команды, используйте сочетание клавиш Ctrl+C.

Данная команда использует поле TTL в IP-заголовке, чтобы маршрутизаторы и серверы могли генерировать определенные ответные сообщения (return messages). **Traceroute** запускается при отправке UDP-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 примере ниже показано, как выполнить трассировку маршрута к узлу 172.50.71.123, при этом маршрутизатор не отвечает.

```
Switch# traceroute 172.50.71.123

*      Request timed out.
*      Request timed out.
Switch#
```

В следующем примере показано, как выполнить трассировку маршрута к узлу 172.50.71.123, при этом маршрутизатор отвечает, что назначение недоступно.

```
Switch# traceroute 172.50.71.123

<10 ms  Network Unreachable

Switch#
```

В примере ниже показано выполнение трассировки 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#
```

44.4 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

<i>IP-ADDRESS</i>	Укажите IP-адрес назначения для передачи пакетов UDP broadcast.
-------------------	---

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для настройки VLAN-интерфейса. 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)#
```

44.5 ip forward-protocol

Данная команда используется для включения передачи пакетов UDP определенного типа службы. Чтобы отключить передачу 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)#
```

44.6 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 для отображения. Если Interface ID не указан, будет отображена информация для всех интерфейсов.
--------------	--

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить таблицу адресов UDP Helper.

Пример

В данном примере показано, как отобразить таблицу адресов UDP Helper.

```
Switch#show ip helper-address
```

Interface	Helper-address
vlan 200	10.0.2.15
vlan 400	1.1.1.3
	1.1.1.4
	1.1.1.5
	1.1.1.6
	1.1.1.7
	1.1.1.8
	1.1.1.9
	1.1.1.10
	1.1.1.11
	1.1.1.12
	1.1.1.13
	1.1.1.14
	1.1.1.15
	1.1.1.16
	1.1.1.17
	1.1.1.18
	1.1.1.19
	1.1.1.20
	30.90.90.88

```
Switch#
```

44.7 show ip forward-protocol udp

Данная команда используется для отображения информации обо всех указанных UDP-портах.

show ip forward-protocol udp

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию обо всех указанных UDP-портах.

Пример

В данном примере показано, как отобразить информацию обо всех указанных UDP-портах.

```
Switch#show ip forward-protocol udp
```

Application	UDP Port
-----	-----
Time Service	37
IEN-116 Name Service	42
TACACS	49
TFTP	69
NetBIOS-NS	137
NetBIOS-DS	138

```
Switch#
```

45. Команды IP-MAC-Port Binding (IMPV)

45.1 clear ip ip-mac-port-binding violation

Данная команда используется для удаления заблокированных записей IP-MAC-Port Binding (IMPV).

clear ip ip-mac-port-binding violation {all | interface *INTERFACE-ID* | *MAC-ADDRESS*}

Параметры

all	Укажите для удаления всех неразрешенных записей.
interface <i>INTERFACE-ID</i>	Укажите для удаления неразрешенных записей, созданных определенным интерфейсом.
<i>MAC-ADDRESS</i>	Укажите для удаления неразрешенных записей с определенным MAC-адресом.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применяется для удаления неразрешенных записей IMPV 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 ethernet 1/0/4
Switch#
```

45.2 ip ip-mac-port-binding

Данная команда используется, чтобы включить управление доступом IMPV для интерфейсов порта. Для отключения функции управления доступом IMPV воспользуйтесь формой **no** этой команды.

ip ip-mac-port-binding [*MODE*]
no ip ip-mac-port-binding

Параметры

<i>MODE</i>	Укажите режим управления доступом IMPV. strict-mode: укажите для включения строгого режима управления доступом (strict). loose-mode: укажите для включения режима управления доступом loose.
--------------------	--

Если режим не задан, используется **strict-mode**.

По умолчанию

По умолчанию функция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если на порту назначен режим управления доступом IMPB **strict-mode**, узел может получить доступ к порту только после того, как узел отправит ARP или IP-пакеты, и эти пакеты пройдут проверку привязки. Чтобы пройти проверку привязки, IP и MAC-адрес источника, VLAN ID и номер порта назначения должны совпадать с любой записью, определенной либо статической записью привязки IP Source Guard, либо изученной динамической записью привязки DHCP Snooping.

Если на порту назначен режим управления доступом IMPB **loose-mode**, узлу будет отказано в доступе к порту после отправки узлом ARP или IP-пакетов, а эти пакеты, отправленные узлом, не пройдут проверку привязки. Чтобы пройти проверку привязки, IP и MAC-адрес источника, VLAN ID и номер порта назначения должны совпадать с любой записью, определенной либо статической записью привязки IP Source Guard, либо изученной динамической записью привязки DHCP Snooping.

Пример

В данном примере показано, как включить управление доступом IMPB на Ethernet 1/0/10.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/10
Switch(config-if)# ip ip-mac-port-binding strict
Switch(config-if)#
```

45.3 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения настроек IMPB. Чтобы отобразить записи, заблокированные из-за нарушения проверки IMPB, введите команду **show ip ip-mac-port-binding violation**.

Пример

В данном примере показано, как отобразить все заблокированные записи 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 примере ниже 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#
```

45.4 snmp-server enable traps ip-mac-port-binding

Данная команда используется, чтобы включить SNMP-уведомления для привязки IP-MAC-Port Binding. Для отключения SNMP-уведомлений 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

Коммутатор, на котором включена данная функция, при получении некорректного пакета будет отправлять trap-сообщения, свидетельствующие о нарушении безопасности. 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)#
```

46. Команды IPv6 Snooping

46.1 ipv6 snooping policy

Данная команда используется для создания или изменения политики IPv6 Snooping. Команда позволяет войти в режим IPv6 Snooping Configuration Mode. Чтобы удалить политику 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 настроенные политики IPv6 Snooping отсутствуют.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для создания политики IPv6 Snooping и входа в режим IPv6 Snooping Configuration Mode. После создания политики IPv6 Snooping используйте команду **ipv6 snooping attach-policy**, чтобы применить политику на указанном интерфейсе.

Пример

В данном примере показано, как создать политику IPv6 Snooping под именем «policy1».

```
Switch# configure terminal  
Switch(config)#ipv6 snooping policy policy1  
Switch(config-ipv6-snooping)#
```

46.2 protocol

Данная команда используется, чтобы указать протокол, для которого необходимо применить IPv6 Snooping. Чтобы отключить IPv6 Snooping для указанного протокола, воспользуйтесь формой **no** этой команды.

```
protocol {dhcp | ndp | dhcp-pd}  
no protocol {dhcp | ndp | dhcp-pd}
```

Параметры

dhcp	Укажите для отслеживания адресов DHCPv6-пакетов.
------	--

ndp	Укажите для отслеживания адресов NDP-пакетов.
------------	---

dhcpd	Укажите для отслеживания префикса IPv6 в пакетах DHCPv6 PD.
--------------	---

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 применяется для автоконфигурации IPv6-адресов без сохранения состояния и IPv6-адресов, настроенных вручную. Перед назначением IPv6-адреса узел должен сначала выполнить обнаружение Duplicate Address Detection (DAD), позволяющее определить дублирование адресов узлов локальной сети. ND Snooping обнаруживает сообщения DAD, включающие DAD Neighbor Solicitation (NS) и DAD Neighbor Advertisement (NA), для построения таблицы привязки. NDP-пакет (NS и NA) также используется для определения того, доступен ли узел по-прежнему и можно ли удалить привязку или нет.

DHCPv6 Snooping анализирует DHCPv6-пакеты, отправляемые между DHCPv6-клиентом и сервером во время процедуры назначения адреса. Когда DHCPv6-клиент успешно получает действительный IPv6-адрес, DHCPv6 Snooping создает свою таблицу привязок.

DHCP-PD Snooping анализирует пакеты DHCPv6 Prefix Delegation (PD) между Delegating Router (назначенным IPv6-префиксом) и соответствующим Requesting Router для настройки привязок префикса.

Пример

В данном примере показано, как включить DHCPv6 Snooping.

```
Switch# configure terminal
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# protocol dhcp
Switch(config-ipv6-snooping)#
```

46.3 data-glean

Данная команда используется для включения функции Data Glean. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

data-glean

no data-glean

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

IPv6 Snooping Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Трафик устройств, действительный адрес которых не может быть найден коммутатором в таблице привязок, 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 policyl
Switch(config-ipv6-snooping)#data-glean
Switch(config-ipv6-snooping)#
```

46.4 limit address-count

Данная команда используется для ограничения максимального количества привязок IPv6 Snooping. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

limit address-count *MAXIMUM*

no limit address-count

Параметры

<i>MAXIMUM</i>	Укажите максимальное количество привязок IPv6 Snooping. Диапазон значений: от 0 до 1024.
----------------	---

По умолчанию

По умолчанию ограничений нет.

Режим ввода команды

IPv6 Snooping Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы ограничить количество привязок IPv6 Snooping, для которых

применяется политика IPv6 Snooping. Команда позволяет ограничить размер таблицы привязок.

Пример

В данном примере показано, как задать максимальное количество привязок 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)#
```

46.5 ipv6 snooping attach-policy

Данная команда используется для применения политики IPv6 Snooping к указанной VLAN. Чтобы удалить привязку, воспользуйтесь формой **no** этой команды.

ipv6 snooping policy attach-policy *POLICY-NAME*
no ipv6 snooping policy attach-policy

Параметры

<i>POLICY-NAME</i>	Укажите имя политики IPv6 Snooping.
--------------------	-------------------------------------

По умолчанию

По умолчанию политика IPv6 Snooping не применяется.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

После создания политики IPv6 Snooping используйте данную команду для применения политики к определенной VLAN.

Пример

В данном примере показано, как включить IPv6 Snooping в VLAN 200.

```
Switch#configure terminal
Switch(config)#vlan 200
Switch(config-vlan)#ipv6 snooping attach-policy policy1
Switch(config-vlan)#
```

46.6 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 продвигаться к другому порту, если обнаружены следующие условия:

- Запись привязки DHCPv6 Snooping запускает новый DHCP-процесс на новом интерфейсе.
- Запись привязки ND Snooping запускает новый DAD-процесс на новом интерфейсе.

Пример

В данном примере показано, как запретить функцию Station Move.

```
Switch# configure terminal
Switch(config)# ipv6 snooping station-move deny
Switch(config)#
```

46.7 ipv6 neighbor binding max-entries

Данная команда используется для настройки максимального количества записей IPv6 Snooping. Чтобы вернуться 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 для DHCPv6 Snooping.
ndp	Укажите максимальное количество записей для ND Snooping.
dhcp-pd	Укажите максимальное количество записей для DHCPv6 PD Snooping.

NUMBER	Укажите максимальное количество записей. Диапазон значений: от 0 до 1024. Укажите 0, чтобы отключить изучение на определенном порту.
--------	--

По умолчанию

Значение по умолчанию – 1024.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для интерфейсов физического порта и port channel. Используйте данную команду, чтобы настроить максимальное количество записей IPv6 Snooping. Для каждого протокола Snooping задаются свои собственные настройки.

Пример

В данном примере показано, как настроить максимальное количество записей для 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)#
```

46.8 show ipv6 snooping policy

Данная команда используется для отображения информации о DHCPv6 Guard.

show ipv6 snooping policy [POLICY-NAME]

Параметры

POLICY-NAME	(Опционально.) Укажите имя политики DHCPv6 Guard для отображения.
-------------	---

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о DHCPv6 Guard. Если параметр не указан, будет отображена информация для всех политик.

Пример

В данном примере показано, как отобразить информацию о DHCPv6 Guard.

```
Switch#show ipv6 snooping policy

Snooping policy: policy1
  Protocol: DHCP
  Limit Address Count: 25
  Target VLAN: 200

Switch#
```

Отображаемые параметры

Protocol	Протокол, используемый для Snooping.
Data Glean	Состояние функции Data Glean.
Limit Address Count	Максимально допустимое число записей для данной политики IPv6 Snooping.
Target VLAN	Имя списка VLAN.

46.9 clear ipv6 snooping entries

Данная команда используется для удаления записей IPv6 Snooping на определенных интерфейсах.

```
clear ipv6 snooping entries [protocol {dhcp | ndp | dhcp-pd}] [vlan VLAN-ID] [interface  
INTERFACE-ID[,|-] ] [ipv6 IPV6-ADDRESS ] [mac MAC-ADDRESS]
```

Параметры

Protocol	Укажите Snooping-протокол: dhcp: укажите, чтобы удалить записи DHCPv6 Snooping. ndp: укажите, чтобы удалить записи ND Snooping. dhcp-pd: укажите, чтобы удалить записи DHCPv6 PD Snooping.
vlan VLAN-ID	(Опционально.) Укажите для удаления записей, соответствующих указанной VLAN.
interface INTERFACE-ID	Укажите интерфейсы, на которых необходимо удалить записи.

,	(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.
ipv6 IPV6-ADDRESS	(Опционально.) Укажите для удаления записей, соответствующих указанному IPv6-адресу.
mac MAC-ADDRESS	(Опционально.) Укажите для удаления записей, соответствующих указанному MAC-адресу.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для удаления записей Snooping на интерфейсах.

Пример

В данном примере показано, как удалить записи ND Snooping на интерфейсе Ethernet 1/0/1.

```
Switch# clear ipv6 snooping entries protocol ndp interface ethernet 1/0/1
Switch#
```

47. Команды IPv6 Source Guard

47.1 ipv6 source binding vlan

Данная команда используется для добавления статической записи в таблицу привязки. Чтобы удалить статическую привязку, 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 применяется для добавления статической записи в таблицу привязки вручную. При вводе команды можно указать несуществующую VLAN. Если удалить указанный интерфейс, конфигурация команды будет соответственно также 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 ethernet 1/0/1  
Switch(config)#
```

47.2 ipv6 source-guard policy

Данная команда используется для создания политики IPv6 Source Guard. Команда позволяет войти в режим IPv6 Source-Guard Policy Configuration Mode. Чтобы удалить политику IPv6 Source Guard, воспользуйтесь формой **no** этой команды.

```
ipv6 source-guard policy POLICY-NAME
```

no ipv6 source-guard policy *POLICY-NAME*

Параметры

<i>POLICY-NAME</i>	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 применяется для создания политики IPv6 Source Guard. Команда позволяет войти в режим IPv6 Source-Guard Policy Configuration Mode.

Пример

В данном примере показано, как создать политику IPv6 Source Guard.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)#
```

47.3 deny global-autoconfig

Данная команда используется для запрета автоматически сконфигурированного трафика. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

deny global-autoconfig
no deny global-autoconfig

Параметры

Нет.

По умолчанию

По умолчанию данная функция разрешена.

Режим ввода команды

Source-Guard Policy Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для запрета трафика от автоматически сконфигурированных глобальных адресов. Рекомендуется к применению, когда все глобальные адреса назначены DHCP и администратор хочет заблокировать входящий трафик от узлов с самостоятельно сконфигурированными адресами.

Пример

В данном примере показано, как запретить автоматически сконфигурированный трафик.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)# deny global-autoconfig
Switch(config-source-guard)#
```

47.4 permit link-local

Данная команда используется для аппаратного разрешения трафика данных, отправленного с адреса Link-Local. Чтобы отключить данную функцию, 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, отправленного с адреса Link-Local.

Пример

В данном примере показано, как разрешить весь трафик данных, отправленный с адреса Link-Local.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)# permit link-local
Switch(config-source-guard)#
```

47.5 validate address

Данная команда используется, чтобы включить функцию 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)#
```

47.6 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 SourceGuard 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)#
```

47.7 ipv6 source-guard attach-policy

Данная команда используется для применения IPv6 Source Guard на интерфейсе. Чтобы удалить IPv6 Source Guard с интерфейса, воспользуйтесь формой **no** этой команды.

ipv6 source-guard attach-policy [POLICY-NAME]
no ipv6 source-guard attach-policy

Параметры

<i>POLICY-NAME</i>	(Опционально.) Укажите имя политики Source Guard.
--------------------	---

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Когда команда применена к порту, 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 привязки адресов. Таблица привязки включает в себя динамическую таблицу (созданную с помощью команд IPv6 Snooping) и статическую таблицу (созданную с помощью команды **ipv6 source binding vlan**).

Если имя политики не указано, политика Source Guard, используемая по умолчанию, 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 ethernet 1/0/3
Switch(config-if)# ipv6 source-guard attach-policy pol1
Switch(config-if)#
```

47.8 show ipv6 source-guard policy

Данная команда используется для отображения 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения 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 отобразить настройки для политики IPv6 Source Guard.

```
Switch#show ipv6 source-guard policy

Policy policy1 configuration:
  Target: eth1/0/3

Switch#
```

47.9 show ipv6 neighbor binding

Данная команда используется для отображения таблицы привязок IPv6.

show ipv6 neighbor binding [vlan *VLAN-ID*] [interface *INTERFACE-ID*] [ipv6 *IPv6-ADDRESS*]
[mac *MAC-ADDRESS*] [max-entries *MAXIMUM-LIMITED-ENTRIES*]

Параметры

vlan <i>VLAN-ID</i>	(Опционально.) Укажите для отображения привязок, соответствующих указанной VLAN.
interface <i>INTERFACE-ID</i>	(Опционально.) Укажите для отображения привязок, соответствующих указанному номеру интерфейса.
ipv6 <i>IPv6-ADDRESS</i>	(Опционально.) Укажите для отображения привязок, соответствующих указанному IPv6-адресу.
mac <i>MAC-ADDRESS</i>	(Опционально.) Укажите для отображения привязок, соответствующих указанному MAC-адресу.
max-entries <i>MAXIMUM-LIMITED-ENTRIES</i>	(Опционально.) Укажите для отображения всех привязок NDP/DHCP/DHCP-PD.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда применяется для отображения таблицы привязок.

Пример

В данном примере показано, как отобразить указанные записи 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.

48. Команды Jumbo Frame

48.1 max-rcv-frame-size

Данная команда используется для настройки максимально допустимого размера Ethernet-кадров. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

max-rcv-frame-size *BYTES*

no max-rcv-frame-size

Параметры

<i>BYTES</i>	Укажите максимально допустимый размер Ethernet-кадров. Диапазон значений: от 64 до 12288 байт.
--------------	---

По умолчанию

Значение по умолчанию – 1536 байт.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки физических портов. Кадры избыточного размера будут отброшены, на входных портах будут проведены проверки. Используйте данную команду, чтобы передавать кадры большого размера или jumbo-кадры через коммутатор и оптимизировать передачу от сервера к серверу.

Пример

В данном примере показано, как настроить максимальный размер полученных Ethernet-кадров на интерфейсе Ethernet 1/0/3. Указанное значение – 6000 байт.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/3
Switch(config-if)#max-rcv-frame-size 6000
Switch(config-if)#
```

49. Команды Layer 2 Protocol Tunnel (L2PT)

49.1 clear l2protocol-tunnel counters

Данная команда используется для сброса счетчиков статистики L2PT (Layer 2 Protocol Tunnel).

clear l2protocol-tunnel counters {all | interface INTERFACE-ID}

Параметры

all	Укажите, чтобы сбросить счетчики на всех интерфейсах.
interface INTERFACE-ID	Укажите интерфейс, на котором необходимо сбросить счетчики.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы сбросить счетчики Protocol Tunnel на всех интерфейсах или указанном интерфейсе. Команда применима исключительно для настройки интерфейсов физического порта и port-channel.

Пример

В данном примере показано, как сбросить счетчики L2PT на всех портах L2PT.

```
Switch# clear l2protocol-tunnel counters all
Switch#
```

49.2 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 функция 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 member-порты сервисной VLAN. Обычно пакет инкапсулируется и передается на удаленный сайт через trunk-порт. При передаче пакета на удаленный сайт через trunk-порт туннелированный пакет будет тегирован с сервисной VLAN. Пакет также может быть передан на другие порты локального сайта, на которых включена функция туннелирования протокола.

Обычно туннелирование протокола инкапсулирует пакет протокола, заменяя MAC-адрес назначения пакета на заданный vendor-ом групповой адрес. Однако если на порту передачи включена функция L2PT, MAC-адрес назначения пакета протокола не будет изменен.

На удаленном сайте коммутатор деинкапсулирует туннелированный пакет, восстанавливая заданный vendor-ом групповой адрес до изначального PDU-адреса, и передает пакет на клиентскую сеть через порты, на которых включено туннелирование протокола.

Если порт, на котором включена функция L2PT, получит инкапсулированный пакет, порт перейдет в состояние «отключено из-за ошибки».

Пример

В данном примере показано, как включить функцию L2PT для STP-протокола на интерфейсе.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# l2protocol-tunnel stp

WARNING: STP doesn't run when l2 protocol tunnel is enabled for the port.

Switch(config-if)#
```

49.3 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

<i>COS-VALUE</i>	Укажите значение CoS в диапазоне от 0 до 7. Высший приоритет – 7.
------------------	---

По умолчанию

Значение по умолчанию – 5.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если пакет L2-протокола прибывает на порт, на котором включена функция L2PT, коммутатор инкапсулирует пакет с тегом сервисной VLAN и заменяет значение CoS на значение, указанное при помощи данной команды.

Пример

В данном примере показано, как указать значение CoS для L2PT.

```
Switch# configure terminal
Switch(config)# l2protocol-tunnel cos 7
Switch(config)#
```

49.4 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. Диапазон значений: от 1 до 4096.

По умолчанию

По умолчанию пороговое значение не задано.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При инкапсулировании, декапсулировании и передаче пакетов функцией L2PT расходуется производительность ЦПУ. Используйте данную команду, чтобы ограничить потребление производительности ЦПУ, указав пороговое количество пакетов L2-протокола, которое может быть получено на порту. Пакеты, полученные после превышения заданного значения, будут отброшены.

Если тип протокола не указан, настройки будут применены ко всем типам протоколов.

Используйте команду **l2protocol-tunnel drop-threshold** и команду **l2protocol-tunnel shutdown-threshold**, чтобы ограничить пропускную способность. Если на интерфейсе также сконфигурировано пороговое значение shutdown, пороговое значение drop должно быть меньше или равно указанному пороговому значению shutdown.

Пример

В данном примере показано, как сконфигурировать пороговое значение drop для STP-протокола.

```
Switch# configure terminal  
Switch(config)# interface ethernet 1/0/1  
Switch(config-if)# l2protocol-tunnel drop-threshold stp 2000  
Switch(config-if)#
```

49.5 l2protocol-tunnel global drop-threshold

Данная команда используется для указания максимального количества пакетов L2-протокола, которое может быть обработано системой за 1 секунду. Чтобы вернуться 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. 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)#
```

49.6 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. Диапазон значений: от 1 до 4096.

По умолчанию

Пороговое значение по умолчанию не установлено.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы ограничить потребление производительности ЦПУ, указав пороговое количество пакетов L2-протокола, которое может быть получено на порту. Если заданное пороговое значение превышено, порт перейдет в состояние «отключено из-за ошибки».

Если тип протокола не указан, настройки будут применены ко всем типам протоколов.

Используйте команду **l2protocol-tunnel shutdown-threshold** и команду **l2protocol-tunnel drop-threshold**, чтобы ограничить туннелирование. Если на интерфейсе также сконфигурировано пороговое значение drop, пороговое значение shutdown должно быть больше или равно указанному пороговому значению drop.

Пример

В данном примере показано, как указать максимальное количество STP-пакетов, которое может быть обработано на интерфейсе за 1 секунду.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# l2protocol-tunnel shutdown-threshold stp 200
Switch(config-if)#
```

49.7 l2protocol-tunnel mac-address

Данная команда используется, чтобы указать групповой адрес L2PT для обозначенного протокола. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

```
l2protocol-tunnel mac-address [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc |  
01-00-0c-cc-cc-cd}] MAC-ADDR  
no l2protocol-tunnel mac-address [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc |  
01-00-0c-cc-cc-cd}]
```

Параметры

gvrp	(Опционально.) Укажите GVRP-пакеты, которые необходимо туннелировать на обозначенный адрес.
stp	(Опционально.) Укажите STP-пакеты, которые необходимо туннелировать на обозначенный адрес.
01-00-0c-cc-cc-cc	(Опционально.) Укажите адрес назначения (destination) пакетов протокола, которые необходимо туннелировать на обозначенный адрес.
01-00-0c-cc-cc-cd	(Опционально.) Укажите адрес назначения пакетов протокола, которые необходимо туннелировать на обозначенный адрес.
MAC-ADDR	Укажите MAC-адрес, на который необходимо туннелировать пакеты. Данный адрес не может быть зарезервирован или использован другими протоколами.

По умолчанию

Адрес туннелирования GVRP-пакетов – 01-05-5D-00-00-21.

Адрес туннелирования STP-пакетов – 01-05-5D-00-00-00.

Адрес туннелирования MAC-адреса 01-00-0C-CC-CC-CC протокола – 01-05-5D-00-00-10.

Адрес туннелирования MAC-адреса 01-00-0C-CC-CC-CD протокола – 01-05-5D-00-00-11.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы указать групповой адрес L2PT для обозначенного протокола.

Если тип протокола не указан, настройки будут применены ко всем типам протоколов.

Ниже перечислены зарезервированные или используемые другими протоколами MAC-адреса, которые не могут быть сконфигурированы в команде:

- FF-FF-FF-FF-FF-FF
- 00-00-00-00-00-00
- Unicast MAC address
- 01-00-08-06-0F-0F
- 01-00-0C-CC-CC-CC
- 01-00-0C-CC-CC-CD
- 01-19-A7-00-00-01
- 01-1B-19-00-00-00
- от 01-80-C2-00-00-00 до 01-80-C2-00-00-0F
- 01-80-C2-00-00-10
- от 01-80-C2-00-00-20 до 01-80-C2-00-00-2F
- от 01-00-5E-00-00-00 до 01-00-5E-FF-FF-FF
- 33-33-00-00-00-04
- 33-33-00-00-00-05
- 33-33-00-00-00-06
- 33-33-00-00-00-09
- 33-33-00-00-00-0D
- CF-00-00-00-00-00

Пример

В данном примере показано, как указать групповой адрес L2PT для STP-протокола. Заданный адрес – 01-00-0c-cd-cd-d0.

```
Switch# configure terminal
Switch(config)# l2protocol-tunnel mac-address stp 01-00-0c-cd-cd-d0
Switch(config)#
```

49.8 show l2protocol-tunnel

Данная команда используется для отображения протоколов, которые туннелированы на интерфейсе или на всех интерфейсах.

show l2protocol-tunnel [interface *INTERFACE-ID*]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите интерфейс для отображения.
--------------------------------------	---

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки, статус и счетчики L2PT.

Пример

В данном примере показано, как отобразить туннелированные протоколы на всех интерфейсах.

```
Switch#show l2protocol-tunnel

CoS for Encapsulated Packets      :5
Drop Threshold for Encapsulated Packets :0

Protocol          Drop Counter    Tunneling Address
-----
gvrp              0               01-05-5D-00-00-21
stp              0               01-00-0C-CD-CD-D0
01-00-0c-cc-cc-cc 0               01-05-5D-00-00-10
01-00-0c-cc-cc-cd 0               01-05-5D-00-00-11

Port      Protocol  Shutdown Drop      Encap      Decap      Drop
          Threshold Threshold Counter  Counter  Counter
-----
eth1/0/3  gvrp      -       2000      0          0          0
          stp      -       -          0          0          0
          01000ccccccc -       -          0          0          0
          01000ccccccd -       -          0          0          0
eth1/0/5  gvrp      -       2000      0          0          0
          stp      -       2000      0          0          0
          01000ccccccc -       2000      0          0          0
          01000ccccccd -       2000      0          0          0

Switch#
```

Отображаемые параметры

CoS for Encapsulated Packets	Значение CoS (Class of Service) для туннелированных пакетов L2-протокола.
Drop Threshold for Encapsulated Packets	Ограничение скорости на L2PT.
Protocol	Тип L2-протокола, который необходимо туннелировать.
Drop Counter	Количество отброшенных пакетов L2-протокола.
Tunneling Address	Настройки группового адреса туннелирования протокола.
Port	Порт, на котором включена функция L2PT.

Shutdown Threshold	Пороговое значение shutdown для указанного пакета L2-протокола.
Drop Threshold	Пороговое значение drop для указанного пакета L2-протокола.
Encap Counter	Количество пакетов L2-протокола, полученных и инкапсулированных портом, на котором включена функция L2PT.
Decap Counter	Количество пакетов L2-протокола, декапсулированных и переданных на порт, на котором включена функция L2PT.

50. Команды Link Aggregation Control Protocol (LACP)

50.1 channel-group

Данная команда используется для привязки интерфейса к агрегированной группе (channel group). Чтобы удалить интерфейс из агрегированной группы, воспользуйтесь формой **no** этой команды.

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

Параметры

CHANNEL-NO	Укажите channel group ID. 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 применима исключительно для настройки интерфейсов физического порта. При первом подключении порта к channel group система автоматически создаст port-channel. Интерфейс может подключиться только к одной channel group.

Если в команде указан параметр **on**, тип channel group – статическая. Если в команде указан параметр **active** или **passive**, тип channel group – LACP. Channel group может состоять только или из статических участников, или из участников LACP. После того как тип channel group был определен, интерфейсы других типов не смогут подключиться к channel group.

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

Пример

В данном примере показано, как привязать интерфейсы от Ethernet 1/0/4 до Ethernet 1/0/5 к новой LACP channel group с ID 3 и включить режим LACP Active Mode.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/4-1/0/5
Switch(config-if)# channel-group 3 mode active
Switch(config-if)#
```

50.2 lacp port-priority

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

lacp port-priority *PRIORITY*
no lacp port-priority

Параметры

<i>PRIORITY</i>	Укажите приоритет порта в диапазоне от 1 до 65535.
-----------------	--

По умолчанию

Приоритет порта по умолчанию – 32768.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Приоритет порта LACP определяет, какие порты могут подключиться к port-channel и на каких портах включен режим Standalone Mode. Чем ниже значение, тем выше приоритет. Если у двух и более портов совпадает приоритет, то приоритет будет определяться номером порта.

Пример

В данном примере показано, как сконфигурировать приоритет порта на интерфейсах от Ethernet 1/0/4 до Ethernet 1/0/5. Указанное значение – 20000.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/4-1/0/5
Switch(config-if)# lacp port-priority 20000
Switch(config-if)#
```

50.3 lacp timeout

Данная команда используется для настройки таймера LACP Long или LACP Short. Чтобы вернуться 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

Данная команда применима исключительно для настройки интерфейсов физического порта.

Пример

В данном примере показано, как сконфигурировать режим LACP Timeout Long на интерфейсе Ethernet 1/0/1.

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

50.4 lacp system-priority

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

lacp system-priority *PRIORITY*

no lacp system-priority

Параметры

<i>PRIORITY</i>	Укажите приоритет системы в диапазоне от 1 до 65535.
-----------------	--

По умолчанию

Приоритет системы LACP по умолчанию – 32768.

Режим ввода команды

Global Configuration Mode.

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)#
```

50.5 port-channel load-balance

Данная команда используется для настройки алгоритма Load Balancing (балансировка нагрузки), используемого коммутатором для распределения пакетов на порты одного канала. Чтобы вернуться 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.

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)#
```

50.6 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.
----------------	---

<i>CHANNEL-NO</i>	(Опционально.) Укажите channel group ID.
detail	(Опционально.) Укажите, чтобы отобразить подробную информацию о channel group.
neighbor	(Опционально.) Укажите, чтобы отобразить информацию о соседнем устройстве.
load-balance	(Опционально.) Укажите, чтобы отобразить информацию о балансировке нагрузки.
sys-id	(Опционально.) Укажите, чтобы отобразить system identifier, используемый LACP.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если номер port-channel не указан, будут отображены все port-channel. Если в команде **show channel-group** не указаны параметры **channel**, **load-balance** и **sys-id**, будет отображена только краткая информация о channel group.

Пример

В данном примере показано, как отобразить подробную информацию обо всех port-channel.

```
Switch#show channel-group channel detail
```

Flag:
 S - Port is requesting Slow LACPDU's F - Port is requesting fast LACPDU
 A - Port is in active mode P - Port is in passive mode

LACP state:
 bndl: Port is attached to an aggregator and bundled with other ports.
 hot-sby: Port is in a hot-standby state.
 indep: Port is in an independent state(not bundled but able to switch data traffic)
 down: Port is down.

Channel Group 3
 Member Ports: 2, Maxports = 12, Protocol: LACP
 Description:

Port	Flags	LACP State	Port Priority	Port Number
eth1/0/4	FA	down	20000	4
eth1/0/5	FA	down	20000	5

```
Switch#
```

В примере ниже показано, как отобразить информацию о соседнем устройстве для port-channel 3.

```
Switch#show channel-group channel 3 neighbor
```

Flag:
 S - Port is requesting Slow LACPDU's F - Port is requesting fast LACPDU
 A - Port is in active mode P - Port is in passive mode

Channel Group 3

Port	Partner System ID	Partner PortNo	Partner Flags	Partner Port_Pri
eth1/0/21	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 следующем 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 нижеприведенном 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 нижеследующем примере показано, как отобразить краткую информацию обо всех port-channel.

```
Switch#show channel-group  
  
load-balance algorithm: src-dst-mac  
System-ID: 32768,F0-7D-68-34-00-10  
  
Group          Protocol  
-----  
3              LACP  
  
Switch#
```

51. Команды Link Layer Discovery Protocol (LLDP)

51.1 clear lldp counters

Данная команда используется для удаления статистики LLDP.

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

Параметры

all	(Опционально.) Укажите, чтобы сбросить счетчик LLDP для всех интерфейсов и статистики Global LLDP.
interface <i>INTERFACE-ID</i>	(Опционально.) Укажите интерфейс, на котором необходимо сбросить 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. Введите команду **clear lldp counters**, указав параметр **all**, для удаления статистики LLDP и Global LLDP на всех интерфейсах. Если параметры не указаны, будут сброшены только счетчики Global LLDP.

Пример

В данном примере показано, как удалить всю статистику LLDP.

```
Switch# clear lldp counters all
Switch#
```

51.2 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 не указан параметр **interface**, будет удалена вся информация, полученная от соседних устройств, на всех интерфейсах.

Пример

В данном примере показано, как удалить всю информацию, полученную от соседних устройств, на всех интерфейсах.

```
Switch# clear lldp table all
Switch#
```

51.3 lldp dot1-tlv-select

Данная команда используется для указания дополнительных настроек TLV (type-length-value) в указанном в пределах IEEE 802.1. TLV будет передан и инкапсулирован в LLDPDU, а также отправлен на соседние устройства. Чтобы отключить передачу TLV, воспользуйтесь формой **no** этой команды.

lldp dot1-tlv-select {port-vlan | protocol-vlan VLAN-ID [, | -] | vlan-name [VLAN-ID [, | -]] | protocol-identity [PROTOCOL-NAME]}

no lldp dot1-tlv-select {port-vlan | protocol-vlan [VLAN-ID [, | -]] | vlan-name [VLAN-ID [, | -]] | protocol-identity [PROTOCOL-NAME]}

Параметры

port-vlan	Укажите Port VLAN ID TLV, который необходимо отправить. Port VLAN ID TLV – это дополнительный TLV фиксированной длины, который позволяет порту VLAN bridge анонсировать PVID (Port VLAN Identifier), который будет ассоциирован с нетегированными или тегированными по приоритету кадрами.
protocol-vlan	Укажите PPVID (Port and Protocol VLAN ID) TLV, который необходимо отправить. PPVID TLV – это дополнительный TLV, который позволяет порту bridge анонсировать PPVID.
<i>VLAN-ID</i>	Укажите VLAN ID в PPVID TLV. Диапазон значений: от 1 до 4094. Если VLAN ID не указан, все сконфигурированные PPVID VLAN будут удалены, PPVID TLV отправлен не будет.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
vlan-name	Укажите VLAN Name TLV, который необходимо отправить. VLAN Name TLV – это дополнительный TLV, который позволяет IEEE 802 LAN station, совместимой с IEEE 802.1Q, анонсировать присвоенное имя любой VLAN, с которой она сконфигурирована.
<i>VLAN-ID</i>	(Опционально.) Укажите VLAN ID в VLAN Name TLV. 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.
<i>PROTOCOL-NAME</i>	(Опционально.) Укажите имя протокола. Ниже перечислены допустимые для <i>PROTOCOL-NAME</i> строки: eapol - Extensible Authentication Protocol (EAP) over LAN lACP - Link Aggregation Control Protocol

gvrp - GARP VLAN Registration Protocol
stp - Spanning Tree Protocol

По умолчанию

По умолчанию указанные в пределах IEEE 802.1 TLV не заданы.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки физических портов. Если включено анонсирование дополнительных TLV, они будут инкапсулированы в LLDPDU и отправлены на другие устройства.

Тип Protocol Identity TLV определяет, анонсировать ли соответствующий экземпляр Protocol Identity локальной системы на порту. Protocol Identity TLV позволяет устройствам анонсировать протоколы, которые важны для работы сети. Например, такие протоколы как Spanning Tree Protocol, Link Aggregation Control Protocol и другие протоколы, установленные vendor-ом, отвечают за поддержку топологии и подключения к сети. Если работают обе функции протокола и на порту включено анонсирование Protocol Identity, Protocol Identity TLV будет анонсирован.

PPVID TLV будет отправлен на VLAN только при условии, что сконфигурированный VLAN ID соответствует настройкам Protocol VLAN на данном интерфейсе, а данная VLAN существует. VLAN будет анонсирована в VLAN Name TLV только при условии, что интерфейс является member-портом сконфигурированного VLAN ID.

Пример

В данном примере показано, как включить анонсирование Port VLAN ID TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp dot1-tlv-select port-vlan
Switch(config-if)#
```

В примере ниже показано, как включить анонсирование Port and Protocol VLAN ID TLV. Анонсированные VLAN: от VLAN 1 до VLAN 3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp dot1-tlv-select protocol-vlan 1-3
Switch(config-if)#
```

В следующем примере показано, как включить анонсирование VLAN Name TLV. Анонсированные VLAN: от VLAN 1 до VLAN 3.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#lldp dot1-tlv-select vlan-name 1-3
Switch(config-if)#
```

В нижеприведенном примере показано, как включить анонсирование LACP Protocol Identity TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp dot1-tlv-select protocol-identify lacp
Switch(config-if)#
```

51.4 lldp dot3-tlv-select

Данная команда используется для указания дополнительных настроек TLV (type-length-value) в пределах IEEE 802.3. TLV будет передан и инкапсулирован в LLDPDU, а также отправлен на соседние устройства. Чтобы отключить передачу TLV, воспользуйтесь формой **no** этой команды.

lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | max-frame-size | power]
no lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | max-frame-size | power]

Параметры

mac-phy-cfg	(Опционально.) Укажите MAC/PHY Configuration/Status TLV, который необходимо отправить. MAC/PHY Configuration/Status TLV – это дополнительный TLV, который определяет (1) режим дуплекса и максимальную скорость передачи узла IEEE 802.3 LAN в бит/сек, а также (2) текущий режим дуплекса и настройки скорости передачи узла IEEE 802.3 LAN в бит/сек.
link-aggregation	(Опционально.) Укажите Link Aggregation TLV, который необходимо отправить. Link Aggregation TLV содержит информацию о том, можно ли агрегировать группу, агрегируется ли группа в данный момент, а также информацию об агрегированном port channel ID. Если порт не агрегирован, значение port channel ID – 0.
max-frame-size	(Опционально.) Укажите Maximum Frame Size TLV, который необходимо отправить. Maximum Frame Size TLV указывает максимальный размер фрейма для используемого MAC и PHY.
power	Укажите Power для включения передачи информации TLV питания через MDI.

По умолчанию

По умолчанию указанные в пределах IEEE 802.3 TLV не заданы.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки физических портов. Если при помощи данной команды включено анонсирование дополнительных TLV, указанных в пределах IEEE 802.3, они будут инкапсулированы в LLDPDU и отправлены на другие устройства.

Если параметры не указаны, будут выбраны все поддерживаемые TLV, указанные в пределах IEEE 802.3, или выбор всех TLV, указанных в пределах IEEE 802, будет отменен.

Пример

В данном примере показано, как включить анонсирование MAC/PHY Configuration/Status TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp dot3-tlv-select mac-phy-cfg
Switch(config-if)#
```

51.5 lldp fast-count

Данная команда используется для настройки количества отправляемых пакетов Fast Start (LLDP MED Fast Start Repeat Count Option) на коммутаторе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

lldp fast-count *VALUE*
no lldp fast-count

Параметры

<i>VALUE</i>	Укажите количество отправляемых пакетов Fast Start. 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 настроить количество отправляемых пакетов Fast Start.

```
Switch# configure terminal
Switch(config)# lldp fast-count 10
Switch(config)#
```

51.6 lldp hold-multiplier

Данная команда используется, 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

<i>VALUE</i>	Укажите множитель для интервала передачи LLDPDU, с помощью которого будет вычислено значение TTL для LLDPDU. 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)#
```


51.7 lldp management-address

Данная команда используется для настройки адреса управления (Management Address), который будет анонсирован на физическом интерфейсе. Чтобы удалить заданные настройки, воспользуйтесь формой **no** этой команды.

lldp management-address [*IP-ADDRESS* | *IPV6-ADDRESS*]
no lldp management-address [*IP-ADDRESS* | *IPV6-ADDRESS*]

Параметры

<i>IP-ADDRESS</i>	(Опционально.) Укажите IPv4-адрес, передаваемый в Management Address TLV.
<i>IPV6-ADDRESS</i>	(Опционально.) Укажите IPv6-адрес, передаваемый в Management Address TLV.

По умолчанию

По умолчанию адрес управления LLDP не настроен (Management Address TLV не отправляется).

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки физических портов. Используйте данную команду, чтобы указать IPv4/IPv6-адрес, передаваемый в Management Address TLV на указанном порту. Если IP-адрес указан, но адрес не ассоциирован с одним из интерфейсов системы, адрес не будет отправлен.

Если при вводе 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 подходящие IPv4/IPv6-адреса отсутствуют, 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. Примените данную команду несколько раз, чтобы создать несколько адресов управления IPv4/IPv6.

Воспользуйтесь командой **no lldp management-address** без адреса управления, чтобы отключить адрес управления, анонсированный в LLDPDU. При отсутствии в списке действительного адреса управления, Management Address TLV отправлен не будет.

Пример

В данном примере показано, как настроить адрес управления IPv4 на интерфейсах Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/1-1/0/2
Switch(config-if-range)# lldp management-address 10.1.1.1
Switch(config-if-range)#
```

В примере ниже показано, как настроить адрес управления IPv6 на интерфейсах Ethernet 1/0/3 и Ethernet 1/0/4.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/3-1/0/4
Switch(config-if-range)# lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

В следующем примере показано, как удалить адрес управления 10.1.1.1 из интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2. Если 10.1.1.1 является последним адресом управления, Management Address TLV отправлен не будет.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/1-1/0/2
Switch(config-if-range)# no lldp management-address 10.1.1.1
Switch(config-if-range)#
```

В примере ниже показан процесс удаления адреса управления FE80::250:A2FF:FEBF:A056 из интерфейса Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# interface range ethernet 1/0/3-1/0/4
Switch(config-if-range)# no lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

В нижеприведенном примере показано, как удалить все адреса управления из интерфейса Ethernet 1/0/5. В этом случае на интерфейсе Ethernet 1/0/5 Management Address TLV отправлен не будет.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/5
Switch(config-if)# no lldp management-address
Switch(config-if)#
```

51.8 lldp med-tlv-select

Данная команда используется для указания дополнительного LLDP-MED TLV, который будет передан, инкапсулирован в LLDPDU и отправлен на соседние устройства. Чтобы отключить передачу TLV, воспользуйтесь формой **no** этой команды.

lldp med-tlv-select [capabilities | inventory-management | network-policy]
no lldp med-tlv-select [capabilities | inventory-management | network-policy]

Параметры

capabilities	(Опционально.) Укажите, чтобы передать LLDP-MED Capabilities TLV.
inventory-management	(Опционально.) Укажите, чтобы передать LLDP-MED

Inventory Management TLV.

network-policy	(Опционально.) Укажите, чтобы передать LLDP-MED Network Policy TLV.
-----------------------	---

По умолчанию

LLDP-MED TLV по умолчанию не выбран.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки физических портов. Используйте данную команду, чтобы включить/отключить передачу LLDP-MED TLV.

При отключении передачи Capabilities TLV будут также отключены LLDP-MED на физическом интерфейсе: LLDP-MED TLV не будут отправляться, даже если другие LLDP-MED TLV включены.

По умолчанию коммутатор отправляет LLDP-пакеты до тех пор, пока получает пакеты LLDP-MED от конечного устройства. Коммутатор отправляет пакеты LLDP-MED до тех пор, пока получает LLDP-пакеты.

Пример

В данном примере показано, как включить передачу LLDP-MED TLV и LLDP-MED Capabilities TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp med-tlv-select capabilities
Switch(config-if)#
```

51.9 lldp receive

Данная команда используется, чтобы включить на физическом интерфейсе получение LLDP-сообщений. Для отключения получения LLDP-сообщений воспользуйтесь формой **no** этой команды.

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

Данная команда применима исключительно для настройки физических портов. Используйте данную команду, чтобы включить на интерфейсе получение LLDP-сообщений. Если LLDP не включен, коммутатор не будет получать LLDP-сообщения.

Пример

В данном примере показано, как включить на физическом интерфейсе получение LLDP-сообщений.

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

51.10 lldp reinit

Данная команда используется для настройки минимального интервала перед повторной инициализацией на коммутаторе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

lldp reinit SECONDS
no lldp reinit

Параметры

SECONDS	Укажите время задержки инициализации LLDP на интерфейсе. Диапазон значений: от 1 до 10 секунд.
---------	--

По умолчанию

Значение по умолчанию – 2.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При перезапуске физического интерфейса LLDP будет выдержан заданный интервал времени между последней командой **disable** и повторной инициализацией.

Пример

В данном примере показано, как сконфигурировать интервал перед повторной инициализацией. Указанное значение – 5 секунд.

```
Switch# configure terminal
Switch(config)# lldp reinit 5
Switch(config)#
```

51.11 lldp run

Данная команда используется для глобального включения функции LLDP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

lldp run
no lldp run

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 глобально включить функцию LLDP и инициировать передачу, получение и обработку LLDP-пакетов на коммутаторе. Введите команду **lldp transmit** для контроля передачи LLDP-пакетов и команду **lldp receive** для контроля получения 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)#
```

51.12 lldp forward

Данная команда используется для включения состояния LLDP Forwarding. Чтобы вернуться 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)#
```

51.13 lldp tlv-select

Данная команда используется для указания TLV (type-length-value) в пределах 802.1AB Basic Management. TLV будет передан и инкапсулирован в LLDPDU, а также отправлен на соседние устройства. Чтобы вернуться 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

Данная команда применима исключительно для настройки физических портов. Используйте данную команду, чтобы указать дополнительные TLV, которые необходимо передать. Если выбрано анонсирование дополнительных TLV, они будут инкапсулированы в LLDPDU и отправлены на другие устройства.

Пример

В данном примере показано, как включить все поддерживаемые дополнительные 802.1AB Basic Management TLV.

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

В примере ниже показано, как включить анонсирование System Name TLV.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp tlv-select system-name
Switch(config-if)#
```

51.14 lldp transmit

Данная команда используется для включения анонсирования/передачи LLDP. Чтобы отключить передачу 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 физических портов. Используйте данную команду, чтобы включить передачу LLDP на физическом интерфейсе. Если LLDP не функционирует, коммутатор не будет передавать LLDP-сообщения.

Пример

В данном примере показано, как включить передачу LLDP.

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

51.15 lldp tx-delay

Данная команда используется для настройки таймера Transmission Delay, определяющего минимальный интервал между отправкой LLDP-сообщений на основе постоянно изменяющегося содержания MIB. Чтобы вернуться 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. 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)#
```

51.16 lldp tx-interval

Данная команда используется для настройки интервала LLDPDU Transmission. Чтобы вернуться 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. 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)#
```

51.17 snmp-server enable traps lldp

Данная команда используется для включения отправки LLDP trap и LLDP-MED trap. Чтобы отключить данную функцию, 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 **snmp-server enable traps lldp med**, чтобы включить отправку LLDP-MED-уведомлений.

Пример

В данном примере показано, как включить отправку LLDP-MED trap.

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

51.18 lldp notification enable

Данная команда используется для включения отправки уведомлений LLDP и LLDP-MED на интерфейсе. Чтобы отключить данную функцию, 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.

Введите команду **lldp med notification enable** для включения отправки уведомлений LLDP-MED.

Пример

В данном примере показано, как включить отправку уведомлений LLDP-MED для интерфейса Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp med notification enable
Switch(config-if)#
```

51.19 lldp subtype

Данная команда используется для настройки подтипа LLDP TLV.

lldp subtype port-id {mac-address | local}

Параметры

port-id	Укажите подтип Port ID TLV.
mac-address	Укажите, чтобы обозначить подтип Port ID TLV как «MAC Address (3)», а также чтобы закодировать MAC-адрес в поле «port ID».
local	Укажите, чтобы обозначить подтип Port ID TLV как «Locally assigned (7)», а также чтобы закодировать номер порта в поле «port ID».

По умолчанию

Подтип Port ID TLV по умолчанию – local (port number).

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы указать подтип LLDP TLV. Подтип Port ID указывает, как обозначен порт в поле port ID.

Пример

В данном примере показано, как сконфигурировать подтип Port ID TLV. Указанный подтип – mac-address.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp subtype port-id mac-address
Switch(config-if)#
```

51.20 show lldp

Данная команда используется для отображения общих настроек функции LLDP на коммутаторе.

show lldp

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить общие настройки функции LLDP на коммутаторе.

Пример

В данном примере показано, как отобразить общие настройки функции LLDP на коммутаторе.

```
Switch#show lldp
LLDP System Information
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00:11:22:33:44:55
  System Name             : Switch
  System Description      : D-Link DMS-3130-30PS System - 16*2.5GE PoE AT , 8*5GE PoE BT +
2*10GBASE-T + 4*25G SFP28
  System Capabilities Supported: Repeater, Bridge
  System Capabilities Enabled  : Repeater, Bridge

LLDP-MED System Information:
  Device Class            : Network Connectivity Device
  Hardware Revision       : A1
  Firmware Revision       : 1.00.003
  Software Revision       : 1.01.006
  Serial Number           :
  Manufacturer Name       : D-Link Corporation
  Model Name              : DMS-3130-30PS
  Asset ID                :
  PoE Device Type         : PSE Device
  PoE PSE Power Source    : Primary

LLDP Configurations
  LLDP State              : Disabled
  LLDP Forward State      : Disabled
  Message TX Interval     : 30
  Message TX Hold Multiplier: 4
  ReInit Delay            : 2
  TX Delay                 : 2

LLDP-MED Configuration:
  Fast Start Repeat Count : 4
Switch#
```

51.21 show lldp interface

Данная команда используется, чтобы отобразить настройки функции LLDP на физическом интерфейсе.

```
show lldp interface INTERFACE-ID [, | -]
```

Параметры

INTERFACE-ID	Укажите Interface ID для отображения. Доступны только физические интерфейсы.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.

-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
---	---

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о функции LLDP для каждого физического интерфейса.

Пример

В данном примере показано, как отобразить настройки функции LLDP для указанного физического интерфейса.

```
Switch#show lldp interface ethernet 1/0/5

Port ID: eth1/0/5
-----
Port ID                               :eth1/0/5
Admin Status                           :TX and RX
Notification                           :Disabled
Basic Management TLVs:
  Port Description                      :Enabled
  System Name                          :Enabled
  System Description                    :Enabled
  System Capabilities                  :Enabled
  Enabled Management Address:
    (None)
IEEE 802.1 Organizationally Specific TLVs:
  Port VLAN ID                         :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
  Link Aggregation                     :Disabled
  Maximum Frame Size                   :Disabled
  Power Via MDI                        :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)».

51.22 show lldp local interface

Данная команда используется для отображения информации о физическом интерфейсе, которая будет отправлена на соседние устройства в LLDP TLV.

show lldp local interface *INTERFACE-ID* [, | -] [**brief** | **detail**]

Параметры

<i>INTERFACE-ID</i>	Укажите Interface ID. Доступны только физические интерфейсы.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
brief	(Опционально.) Укажите, чтобы отобразить информацию в сокращенном формате.
detail	(Опционально.) Укажите, чтобы отобразить информацию в подробном формате. Если не указан ни параметр brief , ни параметр detail , информация будет отображена в стандартном формате.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить текущую анонсируемую локальную информацию в

исходящих LLDP-объявлениях для каждого физического интерфейса.

Пример

В данном примере показано, как отобразить локальную информацию для интерфейса Ethernet 1/0/5 в подробном формате.

```
Switch#show lldp local interface ethernet 1/0/5 detail
Port ID: eth1/0/5
-----
Port ID Subtype                : Local
Port ID                        : eth1/0/5
Port Description                : D-Link Corporation DMS-3130-30PS HW A1 firmware
1.01.006 Port 5 on Unit 1
Port PVID                      : 1
Management Address Count      : 1
    Address 1 : (default)
        Subtype                : IPv4
        Address                 : 10.90.90.90
        IF Type                 : IfIndex
        OID                     : 1.3.6.1.4.1.171.10.176.2.1
PPVID Entries Count           : 0
    (None)
VLAN Name Entries Count       : 0
Protocol Identity Entries Count : 2
    Entry 1 :
        Protocol Index          : 1
        Protocol ID             : 88 09 01
        Protocol Name           : LACP
--More-- or (q)uit (a)ll
```

В примере ниже показано, как отобразить локальную информацию для интерфейса Ethernet 1/0/5 в стандартном формате.

```
Switch#show lldp local interface ethernet 1/0/5

Port ID: eth1/0/5
-----
Port ID Subtype           : Local
Port ID                   : eth1/0/5
Port Description          : D-Link Corporation DMS-3130-30PS HW A1 firmware
1.01.006 Port 5 on Unit 1
Port PVID                  : 1
Management Address Count  : 1
PPVID Entries Count       : 0
VLAN Name Entries Count   : 0
Protocol Identity Entries Count : 2
MAC/PHY Configuration/Status : (See Detail)
Power Via MDI              : (See Detail)
Link Aggregation          : (See Detail)
Maximum Frame Size        : 1536
LLDP-MED capabilities     : (See Detail)
Network Policy            : (See Detail)

Switch#
```

В следующем примере показано, как отобразить локальную информацию для интерфейса Ethernet 1/0/5 в сокращенном формате.

```
Switch#show lldp local interface ethernet 1/0/5 brief

Port ID: eth1/0/5
-----
Port ID Subtype           : Local
Port ID                   : eth1/0/5
Port Description          : D-Link Corporation DMS-3130-30PS HW A1 firmware
1.01.006 Port 5 on Unit 1

Switch#
```

51.23 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.
Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об адресе управления.

Пример

В данном примере показано, как отобразить всю информацию об адресе управления.

```
Switch# show lldp management-address

Address 1 : (default)
-----
Subtype           : IPv4
Address           : 10.90.90.90
IF Type           : IfIndex
OID               : 1.3.6.1.4.1.171.10.118.2
Advertising Ports : -

Address 2 :
-----
Subtype           : IPv4
Address           : 10.90.90.90
IF Type           : IfIndex
OID               : 1.3.6.1.4.1.171.10.118.2
Advertising Ports : -

Total Entries : 2

Switch#
```

51.24 show lldp neighbor interface

Данная команда используется для отображения актуальной информации, полученной от соседнего устройства на указанном физическом интерфейсе.

show lldp neighbors interface *INTERFACE-ID* [, | -] [brief | detail]

Параметры

<i>INTERFACE-ID</i>	Укажите Interface ID. Доступны только физические интерфейсы.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов

от предыдущего. Пробелы до и после запятой недопустимы.

-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
brief	(Опционально.) Укажите, чтобы отобразить информацию в сокращенном формате.
detail	(Опционально.) Укажите, чтобы отобразить информацию в подробном формате. Если не указан ни параметр brief , ни параметр detail , информация будет отображена в стандартном формате.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию, полученную от соседних устройств.

Пример

В данном примере показано, как отобразить информацию о соседних устройствах, изученную LLDP на интерфейсе Ethernet 1/0/9, в подробном формате.

```
Switch# show lldp neighbor interface ethernet 1/0/9 detail

Port ID : eth1/0/9
-----
Remote Entities Count : 1
Entity 1
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-05
  Port ID Subtype        : Local
  Port ID                 : eth1/0/5
  Port Description        : RMON Port
  System Name             : Switch1
  System Description      : Stackable Ethernet Switch
  System Capabilities Supported : Repeater, Bridge
  System Capabilities Enabled   : Repeater, Bridge
  Management Address Count : 0
  (None)
  Port VLAN ID            : 0
  PPVID Entries Count     : 0
  (None)
  VLAN Name Entries Count : 0
  (None)
  Protocol ID Entries Count : 0
  (None)
  MAC/PHY Configuration/Status : (None)
  Power Via MDI            : (None)
```

```

Link Aggregation                : (None)
Maximum Frame Size              : 0
Unknown TLVs Count              : 0
(None)
LLDP-MED capabilities           :
LLDP-MED device class           : Endpoint device class III
  LLDP-MED capabilities support  :
    LLDP-MED capabilities        : Support
    Network Policy               : Support
    Location identification       : Not Support
    Extended power via MDI       : Support
    Inventory                     : Support
  LLDP-MED capabilities enabled  :
    LLDP-MED capabilities        : Enabled
    Network Policy               : Enabled
    Location identification       : Enabled
    Extended power via MDI       : Enabled
    Inventory                     : Enabled
  Extended power via MDI         :
    Power device type            : PD device
    Power Source                  : from PSE
    Power request                 : 8 watts
Network policy                   :
  Application type               : Voice
  VLAN ID                       : -
  Priority                       : -
  DSCP                           : -
  Unknown                        : True
  Tagged                         : -
  Inventory Management           :
  (None)

Switch#

```

В примере ниже показано, как отобразить информацию о Remote LLDP в стандартном формате.

```

Switch# show lldp neighbor interface ethernet 1/0/1

Port ID : 1
-----
Remote Entities Count : 2
Entity 1
  Chassis ID Subtype          : MAC Address
  Chassis ID                  : 00-01-02-03-04-01
  Port ID Subtype             : Local
  Port ID                     : eth1/0/1
  Port Description             : RMON Port 1 on Unit 1
  System Name                  : Switch1
  System Description           : Stackable Ethernet Switch
  System Capabilities Supported : Repeater, Bridge
  System Capabilities Enabled  : Repeater, Bridge
  Management Address Count     : 1

```

```

Port VLAN ID          : 1
PPVID Entries Count   : 5
VLAN Name Entries Count : 3
Protocol ID Entries Count : 2
MAC/PHY Configuration Status : (See Detail)
Power Via MDI         : (See Detail)
Link Aggregation      : (See Detail)
Maximum Frame Size    : 1536
LLDP-MED capabilities : (See Detail)
Network policy        : (See Detail)
Extended Power Via MDI : (See Detail)
Inventory Management  : (See Detail)
Unknown TLVs Count    : 2
Entity 2
Chassis ID Subtype    : MAC Address
Chassis ID            : 00-01-02-03-04-02
Port ID Subtype       : Local
Port ID               : eth1/0/1
Port Description      : RMON Port 1 on Unit 2
System Name           : Switch2
System Description    : Stackable Ethernet Switch
System Capabilities Supported : Repeater, Bridge
System Capabilities Enabled  : Repeater, Bridge
Management Address Count : 2
Port VLAN ID          : 1
PPVID Entries Count   : 5
VLAN Name Entries Count : 3
Protocol Id Entries Count : 2
MAC/PHY Configuration Status : (See Detail)
Power Via MDI         : (See Detail)
Link Aggregation      : (See Detail)
Maximum Frame Size    : 1536
LLDP-MED capabilities : (See Detail)
Extended power via MDI : (See Detail)
Network policy        : (See Detail)
Inventory Management  : (See Detail)
Unknown TLVs Count    : 2
Switch#

```

В следующем примере показано, как отобразить информацию о соседних устройствах на интерфейсах от Ethernet 1/0/1 до Ethernet 1/0/2 в кратком формате.

```

Switch# show lldp neighbor interface ethernet 1/0/1-1/0/2 brief

Port ID: eth1/0/1
-----
Remote Entities Count : 2
Entity 1
Chassis ID Subtype    : MAC Address
Chassis ID            : 00-01-02-03-04-01
Port ID Subtype       : Local
Port ID               : eth1/0/1

```

```
Port Description      : RMON Port 1 on Unit 3
Entity 2
Chassis ID Subtype   : MAC Address
Chassis ID           : 00-01-02-03-04-02
Port ID Subtype      : Local
Port ID              : eth1/0/2
Port Description     : RMON Port 1 on Unit 4
```

```
Port ID : eth1/0/2
```

```
-----
Remote Entities Count : 3
```

```
Entity 1
```

```
Chassis ID Subtype   : MAC Address
Chassis ID           : 00-01-02-03-04-03
Port ID Subtype      : Local
Port ID              : eth1/0/4
Port Description     : RMON Port 2 on Unit 1
```

```
Entity 2
```

```
Chassis ID Subtype   : MAC Address
Chassis ID           : 00-01-02-03-04-04
Port ID Subtype      : Local
Port ID              : eth1/0/5
Port Description     : RMON Port 2 on Unit 2
```

```
Entity 3
```

```
Chassis ID Subtype   : MAC Address
Chassis ID           : 00-01-02-03-04-05
Port ID Subtype      : Local
Port ID              : eth1/0/6
Port Description     : RMON Port 2 on Unit 3
```

```
Total Entries: 2
```

```
Switch#
```

51.25 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об обнаружении соседних устройств на коммутаторе.

Пример

В данном примере показано, как отобразить глобальную информацию о трафике LLDP.

```
Switch#show lldp traffic

Last Change Time      : 0 days 00:00:00
Total Inserts         : 0
Total Deletes         : 0
Total Drops           : 0
Total Ageouts         : 0

Switch#
```

Отображаемые параметры

Last Change Time	Время после последнего обновления до удаленной таблицы в днях, часах, минутах и секундах.
Total Inserts	Общее количество вставок в удаленную таблицу.
Total Deletes	Общее количество удалений из удаленной таблицы.
Total Drops	Общее количество случаев получения данных, которые не были добавлены в таблицу из-за непригодности.
Total Ageouts	Общее количество случаев удаления записей после истечения интервала Time to Live.

51.26 show lldp traffic interface

Данная команда используется для отображения информации о трафике LLDP на указанном физическом интерфейсе.

show lldp traffic interface *INTERFACE-ID* [, | -]

Параметры

<i>INTERFACE-ID</i>	Укажите Interface ID. Доступны только физические интерфейсы.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения одного диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.

- (Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.
Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить трафик LLDP на каждом физическом интерфейсе.

Пример

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

```
Switch#show lldp traffic interface ethernet 1/0/1

eth1/0/1
-----
Total Transmits      : 0
Total Discards       : 0
Total Errors         : 0
Total Receives       : 0
Total TLV Discards   : 0
Total TLV Unknowns   : 0
Total Ageouts        : 0

Switch#
```

Отображаемые параметры

Total Transmits	Общее количество LLDP-пакетов, переданных на порту.
Total Discards	Общее количество LLDP-кадров, отброшенных на порту.
Total Errors	Количество недействительных LLDP-кадров, полученных на порту.
Total Receives	Общее количество LLDP-пакетов, полученных на порту.
Total TLV Discards	Количество отброшенных TLV.
Total TLV Unknowns	Общее количество полученных на порту LLDP TLV, тип которых находится в зарезервированном диапазоне и не распознается.

Total Ageouts	Общее количество случаев удаления записей на порту после истечения интервала Time to Live.
----------------------	--

52. Команды Loopback Detection (LBD)

52.1 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	Укажите режим обнаружения петли port-based (на порту).
vlan-based	Укажите режим обнаружения петли VLAN-based (в VLAN).

По умолчанию

По умолчанию данная функция 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, воспользовавшись командой **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)#
```

52.2 loopback-detection (Interface)

Данная команда используется для включения функции LBD на интерфейсе. Для отключения функции на интерфейсе воспользуйтесь формой **no** этой команды.

loopback-detection
no loopback-detection

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 функцию LBD на интерфейсе. Команда применима исключительно для настройки интерфейсов физического порта и port-channel.

Пример

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

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

52.3 loopback-detection interval

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

loopback-detection interval SECONDS

no loopback-detection interval

Параметры

SECONDS	Укажите интервал передачи пакетов LBD. 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 настроить интервал передачи пакетов LBD, отправляемых для обнаружения петли.

Пример

В данном примере показано, как настроить временной интервал. Указанное значение – 20 секунд.

```
Switch# configure terminal
Switch(config)# loopback-detection interval 20
Switch(config)#
```

52.4 loopback-detection vlan

Данная команда используется для включения функции LBD на VLAN. Чтобы вернуться 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 (-a) / диапазон номеров VLAN. Диапазоны разделяются при помощи дефисов. Значения разделяются при помощи запятых.
-----------	--

По умолчанию

По умолчанию данная функция включена для всех VLAN.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команд

Используйте данную команду, чтобы настроить список VLAN, на которых включена функция LBD. Настройки команды будут применены, если на порту сконфигурирован режим обнаружения петли VLAN-based.

По умолчанию пакеты управления LBD отправляются на все VLAN, членом которых является данный порт. Пакеты управления LBD 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)#
```

52.5 show loopback-detection

Данная команда используется для отображения текущих настроек LBD.

show loopback-detection [interface INTERFACE-ID [, | -]]

Параметры

interface INTERFACE-ID	(Опционально.) Укажите интерфейс 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки и статус функции LBD.

Пример

В данном примере показано, как отобразить текущие настройки и статус функции LBD.

```
Switch#sh loopback-detection

Loop Detection      : Enabled
Detection Mode      : port-based
LBD enabled VLAN    : all VLANs
Interval           : 20 seconds
Action Mode         : Shutdown
Address Type        : Multicast
Function Version     : v4.07

Interface           State      Result      Time Left (sec)
-----
eth1/0/1            Enabled   Normal      -
eth1/0/2            Disabled Normal      -
eth1/0/3            Disabled Normal      -
eth1/0/4            Disabled Normal      -
eth1/0/5            Disabled Normal      -
eth1/0/6            Disabled Normal      -
eth1/0/7            Disabled Normal      -
eth1/0/8            Disabled Normal      -
eth1/0/9            Disabled Normal      -
eth1/0/10           Disabled Normal      -
eth1/0/11           Disabled Normal      -
eth1/0/12           Disabled Normal      -
eth1/0/13           Disabled Normal      -
--More-- or (q)uit (a)ll q
```

В примере ниже 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.

52.6 loopback-detection action

Данная команда используется для настройки режима LBD. Чтобы вернуться 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)#
```

52.7 snmp-server enable traps loopback-detection

Данная команда используется, чтобы включить отправку 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 отправку SNMP-уведомлений для LBD. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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)#
```

52.8 loopback-detection address-type

Данная команда используется, 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)#
```

53. Команды аутентификации MAC

53.1 mac-auth system-auth-control

Данная команда используется для глобального включения MAC-аутентификации. Чтобы отключить глобальную MAC-аутентификацию, 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. Сам коммутатор может выполнять аутентификацию на основе локальной базы данных или выполнять процесс аутентификации для клиентов на удаленном сервере с использованием протокола RADIUS.

Пример

В данном примере показано, как включить MAC-аутентификацию глобально.

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

53.2 mac-auth enable

Данная команда используется для включения MAC-аутентификации на указанном интерфейсе. Чтобы отключить MAC-аутентификацию, 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. Используйте команду, чтобы включить MAC-аутентификацию на указанном интерфейсе.

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 ethernet 1/0/1
Switch(config-if)# mac-auth enable
Switch(config-if)#
```

53.3 mac-auth password

Данная команда используется, чтобы настроить пароль аутентификации 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 MAC-аутентификации. Если указан пароль в обычном текстовом виде, длина строки не может превышать 16 символов.

По умолчанию

По умолчанию паролем является MAC-адрес клиента.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда позволяет настроить пароль, используемый 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 xxxxxxxx
Switch(config)#
```

53.4 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

<i>STRING</i>	Укажите, чтобы задать имя пользователя для MAC-аутентификации. Максимальное количество символов – 16.
---------------	--

По умолчанию

По умолчанию именем пользователя является MAC-адрес клиента.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить имя пользователя для аутентификации пользователей по MAC-адресу. Заданное имя пользователя применяется для аутентификации через локальную базу данных и удаленные серверы. Если команда не настроена, имя пользователя для аутентификации будет формироваться на основе MAC-адреса.

Пример

В данном примере показано, как настроить имя пользователя для MAC-аутентификации.

```
Switch# configure terminal
Switch(config)# mac-auth username user1
Switch(config)#
```

53.5 snmp-server enable traps mac-auth

Данная команда используется, чтобы 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 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 MAC-аутентификации.

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)#
```

54. Команды Mirror

54.1 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. Воспользуйтесь формой **no** этой команды, чтобы удалить интерфейс назначения сессии.

monitor session *SESSION-NUMBER* **destination interface** *INTERFACE-ID*
no monitor session *SESSION-NUMBER* **destination interface** *INTERFACE-ID*

Параметры

<i>SESSION-NUMBER</i>	Укажите номер сессии мониторинга. Диапазон значений: от 1 до 4.
<i>INTERFACE-ID</i>	Укажите интерфейс назначения для сессии мониторинга.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить интерфейс назначения для локальной сессии мониторинга или интерфейс назначения на коммутаторе назначения для сессии RSPAN.

В качестве интерфейсов назначения для сессий мониторинга можно использовать физические порты и port-channel. Для сессии мониторинга можно указать несколько интерфейсов источника, но только один интерфейс назначения. Интерфейс не может быть одновременно интерфейсом источника одной сессии и портом назначения другой сессии. Интерфейс можно сконфигурировать в качестве интерфейса назначения нескольких сессий, но в качестве интерфейса источника только одной сессии.

Введите команду **monitor session source remote vlan** на коммутаторе назначения сессии RSPAN для настройки VLAN, на которую туннелируются отслеживаемые пакеты источника с удаленного сайта.

Пример

В данном примере показано, как создать сессию мониторинга порта с номером 1, указав физический порт Ethernet 1/0/1 в качестве порта назначения, а три физических порта источника (от Ethernet 1/0/2 до Ethernet 1/0/4) в качестве портов источника.

```
Switch# configure terminal
Switch(config)# monitor session 1 destination interface ethernet 1/0/1
Switch(config)# monitor session 1 source interface ethernet 1/0/2-4
Switch(config)#
```


54.2 monitor session destination remote vlan

Данная команда используется, чтобы настроить RSPAN VLAN и порт 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. Диапазон значений: от 1 до 4.
VLAN-ID	Укажите RSPAN VLAN, используемую для туннелирования отслеживаемых пакетов на удаленный сайт. 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. 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.

Введите команду **monitor session destination remote vlan**, чтобы сконфигурировать порт назначения, используемый для передачи отслеживаемых пакетов, и RSPAN VLAN, применяемую 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 настроить несколько потоков замещения VLAN. RSPAN VLAN в удаленных сессиях применяется только для отслеживания трафика.

Используйте команду **monitor session source interface**, чтобы сконфигурировать порты источника, пакеты которых будут отслеживаться.

Введите команду **remote-span** в режиме VLAN Configuration Mode для указания VLAN в качестве RSPAN VLAN. Отслеживаемые пакеты будут туннелированы через trunk-порты-участники RSPAN VLAN следующих устройств.

Пример

В данном примере показано, как создать сессию RSPAN на коммутаторе источника. VLAN 100 указана в качестве RSPAN VLAN, порт назначения Ethernet 1/0/6 и три порта источника (Ethernet 1/0/2, Ethernet 1/0/3 и Ethernet 1/0/4) указаны в качестве отслеживаемых портов.

```
Switch# configure terminal
Switch(config)# monitor session 2 source interface ethernet 1/0/2-4
Switch(config)# monitor session 2 destination remote vlan 100 interface ethernet 1/0/6
Switch(config)#
```

54.3 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] [forwarding] | cpu rx}
no monitor session SESSION-NUMBER source interface {INTERFACE-ID [, | -] | cpu rx}

Параметры

SESSION-NUMBER	Укажите номер сессии мониторинга. 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.
Tx forwarding	Укажите для отслеживания пакетов, переданных портом, статус всех экземпляров STP-протокола которого – forwarding.
cpu rx	(Опционально.) Укажите, чтобы отслеживать пакеты, полученные центральным процессором.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

В качестве интерфейсов источника для сессий мониторинга можно использовать физические порты и port-channel.

Для сессии мониторинга можно указать несколько интерфейсов источника, но только один интерфейс назначения (destination). Интерфейс не может быть одновременно интерфейсом источника одной сессии и портом назначения другой сессии. Интерфейс можно сконфигурировать в качестве интерфейса назначения нескольких сессий, но в качестве интерфейса источника только одной сессии. Если направление не указано или указан параметр **both**, отслеживается как переданный, так и полученный трафик.

Пример

В данном примере показано, как создать сессию мониторинга порта с номером 1. Физический порт Ethernet 1/0/1 указан в качестве порта назначения, а три физических порта источника (от Ethernet 1/0/2 до Ethernet 1/0/4) указаны в качестве портов источника.

```
Switch# configure terminal
Switch(config)# monitor session 1 destination interface ethernet 1/0/1
Switch(config)# monitor session 1 source interface ethernet 1/0/2-4
Switch(config)#
```

54.4 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. 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 команд

Можно отследить только один список доступа за одну сессию (один список доступа может включать несколько потоков). Используйте команды **access-group** или **vlan map**, чтобы отследить пакет, отфильтрованный при помощи списка доступа, применяемого для аппаратного оборудования.

Пример

В данном примере показано, как создать сессию мониторинга с номером 2. Список доступа MAC «MAC-Monitored-flow» указан в качестве источника мониторинга.

```
Switch# configure terminal
Switch(config)# monitor session 2 destination interface ethernet 1/0/1
Switch(config)# monitor session 2 source acl MAC-Monitored-flow
Switch(config)#
```

54.5 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. Диапазон значений: от 1
----------------	---

до 4.

VLAN-ID	Укажите VLAN, через которую туннелируются отслеживаемые пакеты источника (source) с удаленного сайта. 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. Введите команду **monitor session destination interface**, чтобы настроить порт назначения, на который будут переданы отслеживаемые пакеты.

Каждую сессию необходимо сконфигурировать с уникальной RSPAN VLAN. Воспользуйтесь командой **remote-span** в режиме VLAN Configuration Mode, чтобы указать VLAN в качестве RSPAN VLAN.

Пример

В данном примере показано, как создать сессию RSPAN на коммутаторе назначения. VLAN 100 указана в качестве RSPAN VLAN, а порт Ethernet 1/0/4 указан в качестве порта назначения. Отслеживаемые пакеты прибывают на порт Ethernet 2/0/1 и будут переданы с порта Ethernet 1/0/4.

```
Switch# configure terminal
Switch(config)# vlan 100
Switch(config-vlan)# remote-span
Switch(config-vlan)# exit
Switch(config)# interface ethernet 2/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100
Switch(config-if)# exit
Switch(config)# interface ethernet 1/0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# exit
Switch(config)# monitor session 2 source remote vlan 100
Switch(config)# monitor session 2 destination interface ethernet 1/0/4
Switch(config)#
```

54.6 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. Диапазон значений: от 1 до 4.
VLAN-ID	Укажите, чтобы сконфигурировать VLAN ID для мониторинга на основе VLAN. Диапазон значений: от 1 до 4094.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона VLAN. Пробелы до и после дефиса недопустимы.
rx	Укажите, чтобы отслеживать пакеты, полученные на VLAN.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для одной сессии мониторинга можно указать несколько VLAN, однако одну VLAN нельзя сконфигурировать в качестве VLAN источника (source) нескольких сессий. При указании параметра **rx** будут зеркалироваться все входящие пакеты на указанном VLAN ID.

Пример

В данном примере показано, как создать сессию мониторинга с номером 2. В качестве VLAN источника мониторинга указаны три VLAN: VLAN 2, VLAN 3 и VLAN 4.

```
Switch# configure terminal
Switch(config)# monitor session 2 destination interface ethernet 1/0/1
Switch(config)# monitor session 2 source vlan 2-4 rx
Switch(config)#
```

54.7 remote-span

Данная команда используется для указания VLAN в качестве RSPAN VLAN. Чтобы вернуться 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 данную команду 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. Команда применяется 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 member-портов RSPAN VLAN.

Пример

В данном примере показано, как назначить VLAN 100 в качестве RSPAN VLAN на промежуточном коммутаторе в сессии RSPAN. Отслеживаемые пакеты прибывают на интерфейс Ethernet 1/0/1, а отправляются с интерфейса Ethernet 1/0/5.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100
Switch(config-if)# exit
Switch(config)# interface ethernet 1/0/5
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100
Switch(config-if)# exit
Switch(config)# vlan 100
Switch(config-vlan)# remote-span
Switch(config-vlan)#
```

54.8 no monitor session

Данная команда используется для удаления сессии мониторинга.

no monitor session *SESSION-NUMBER*

Параметры

<i>SESSION-NUMBER</i>	Укажите номер сессии мониторинга, которую необходимо удалить. 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)#
```

54.9 show monitor session

Данная команда используется для отображения указанной сессии / всех сессий мониторинга.

show monitor session [*SESSION-NUMBER* | **remote** | **local**]

Параметры

<i>SESSION-NUMBER</i>	(Опционально.) Укажите номер сессии для отображения.
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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду без указания номера сессии, чтобы отобразить все сессии мониторинга.

Пример

В данном примере показано, как отобразить сессию мониторинга порта с номером 1.

```
Switch#show monitor session 1

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#
```

55. Команды Multicast Listener Discovery (MLD) Snooping

55.1 clear ipv6 mld snooping statistics

Данная команда используется для сброса счетчиков статистики MLD Snooping на коммутаторе.

clear ipv6 mld snooping statistics {all | vlan VLAN-ID | interface INTERFACE-ID}

Параметры

all	Укажите, чтобы удалить статистику IPv6 MLD Snooping для всех VLAN и портов.
vlan VLAN-ID	Укажите VLAN. Если VLAN не указана, будет удалена статистика всех VLAN.
interface INTERFACE-ID	Укажите интерфейс, на котором необходимо удалить статистику.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы сбросить счетчики статистики MLD Snooping на коммутаторе.

Пример

В данном примере показано, как удалить всю статистику MLD Snooping.

```
Switch# clear ipv6 mld snooping statistics all
Switch#
```

55.2 ipv6 mld snooping

Данная команда используется для включения MLD Snooping. Чтобы отключить 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

Interface Configuration Mode.

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Чтобы применить MLD Snooping на VLAN, необходимо включить глобальное состояние MLD Snooping и MLD Snooping на интерфейсе. Настройки IGMP Snooping и MLD Snooping являются независимыми, поэтому их можно включать одновременно на одной и той же VLAN.

Пример

В данном примере показано, как отключить MLD Snooping на всех VLAN.

```
Switch# configure terminal
Switch(config)# no ipv6 mld snooping
Switch(config)#
```

В 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)#
```

55.3 ipv6 mld snooping fast-leave

Данная команда используется для включения функции MLD Snooping Fast Leave на интерфейсе. Чтобы отключить функцию MLD Snooping Fast Leave на интерфейсе, воспользуйтесь формой **no** этой команды.

ipv6 mld snooping fast-leave

no ipv6 mld snooping fast-leave

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 VLAN-интерфейсов. Используйте 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)#
```

55.4 ipv6 mld snooping last-listener-query-interval

Данная команда используется, 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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. 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)#
```

55.5 ipv6 mld snooping mrouter

Данная команда используется, чтобы настроить указанный интерфейс в качестве порта IPv6, подключенного к многоадресному маршрутизатору, или порта, которому запрещено подключаться к многоадресному маршрутизатору, на интерфейсе VLAN. Воспользуйтесь формой **no** этой команды, чтобы удалить интерфейс из списка multicast router-портов или портов, которым запрещено подключаться к многоадресному маршрутизатору.

ipv6 mld snooping mrouter {interface INTERFACE-ID [, | -] | forbidden interface INTERFACE-ID [, | -] | learn pimv6}

no ipv6 mld snooping mrouter {interface INTERFACE-ID [, | -] | forbidden interface INTERFACE-ID [, | -] | learn pimv6}

Параметры

interface	Укажите диапазон интерфейсов, подключенных к многоадресным маршрутизаторам.
forbidden interface	Укажите диапазон интерфейсов, не подключенных к многоадресным маршрутизаторам.
INTERFACE-ID	Укажите интерфейс или список интерфейсов. Пробелы до и после запятой недопустимы. Доступны физические интерфейсы или port-channel.
learn pimv6	Укажите, чтобы включить динамическое изучение на портах, подключенных к многоадресному маршрутизатору.

По умолчанию

Порт IPv6, подключенный к многоадресному маршрутизатору, не настроен.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. В качестве порта, подключенного к многоадресному маршрутизатору, можно использовать физический порт или port-channel. Указанный порт должен являться member-портом сконфигурированной VLAN. Нельзя указать member-порт port-channel.

Порт, подключенный к многоадресному маршрутизатору, может быть изучен динамически или сконфигурирован статически на устройстве MLD Snooping. При динамическом изучении устройство MLD Snooping будет анализировать пакеты MLD и PIMv6, чтобы выяснить, является ли связанное устройство маршрутизатором.

Пример

В данном примере показано, как сконфигурировать интерфейс Ethernet 1/0/1 в качестве порта, подключенного к многоадресному маршрутизатору MLD Snooping, а интерфейс Ethernet 1/0/2 в качестве порта, не подключенного к многоадресному маршрутизатору MLD Snooping, на VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping mrouter interface ethernet 1/0/1
Switch(config-vlan)# ipv6 mld snooping mrouter forbidden interface ethernet 1/0/2
Switch(config-vlan)#
```

В примере ниже 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)#
```

55.6 ipv6 mld snooping ignore-topology-change-notification

Данная команда используется, чтобы функция MLD Snooping игнорировала изменения STP и не отправляла запрос STP на интерфейс. 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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. 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 сходимости. 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)#
```

55.7 ipv6 mld snooping proxy-reporting

Данная команда используется для включения функции Proxy Reporting. Чтобы отключить данную функцию, 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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. 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)#
```

55.8 ipv6 mld snooping querier

Данная команда используется для включения MLD Snooping Querier на коммутаторе. Чтобы отключить 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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. Чтобы запустить MLD Snooping Querier, интерфейсу необходимо предварительно присвоить IPv6-адрес. При отсутствии у VLAN IPv6-адреса будет выслано сообщение warning. Если Querier включен, а IPv6-адрес удален, работа Querier будет приостановлена.

Если система может выполнить роль Querier, устройство будет анализировать пакеты MLD query, отправленные другими устройствами. При получении сообщения MLD query устройство с меньшим значением IPv6-адреса становится Querier. Если на интерфейсе также включен MLD-протокол, состояние MLD Snooping Querier будет отключено автоматически.

Пример

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


```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping querier
Switch(config-vlan)#
```

55.9 ipv6 mld snooping query-interval

Данная команда используется, 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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. Интервал MLD general query – это промежуток времени между запросами general query, отправляемыми Querier. Изменяя данный интервал, можно настроить количество сообщений MLD в сети. Чем больше значение интервала, тем реже будут отправляться сообщения MLD query.

Пример

В данном примере показано, как настроить интервал MLD snooping query на VLAN 1000. Указанное значение – 300 секунд.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping query-interval 300
Switch(config-vlan)#
```

55.10 ipv6 mld snooping query-max-response-time

Данная команда используется для настройки максимального времени ответа, анонсированного в запросах MLD snooping query. Чтобы вернуться 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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. Используйте данную команду, чтобы настроить период времени, в течение которого участник группы может ответить на сообщение MLD query. По истечении 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)#
```

55.11 ipv6 mld snooping query-version

Данная команда используется, чтобы настроить версию пакета general query, отправленного MLD Snooping Querier. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ipv6 mld snooping query-version {1 | 2}
no ipv6 mld snooping query-version

Параметры

1	Укажите версию пакета MLD general query, отправленного MLD Snooping Querier – 1.
2	Укажите версию пакета MLD general query, отправленного MLD Snooping Querier – 2.

По умолчанию

Версия по умолчанию – 2.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов.

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)#
```

55.12 ipv6 mld snooping rate-limit

Данная команда используется для настройки максимального количества входящих пакетов управления MLD в секунду. Чтобы отключить данное ограничение, воспользуйтесь формой **no** этой команды.

ipv6 mld snooping rate-limit *NUMBER*
no ipv6 mld snooping rate-limit

Параметры

<i>NUMBER</i>	Укажите максимальное количество пакетов управления MLD, обрабатываемых коммутатором на указанном интерфейсе в секунду.
---------------	--

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. Используйте данную

команду, чтобы указать максимальное количество пакетов управления MLD, обрабатываемых на интерфейсе в секунду.

Пример

В данном примере показано, как указать максимальное количество пакетов на интерфейсе VLAN 1000 в секунду. Заданное значение – 30 пакетов.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping rate-limit 30
Switch(config-vlan)#
```

55.13 ipv6 mld snooping report-suppression

Данная команда используется для включения функции MLD Report Suppression на VLAN. Чтобы отключить 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 опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. 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)#
```

55.14 ipv6 mld snooping robustness-variable

Данная команда используется, чтобы настроить значение 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

<i>VALUE</i>	Укажите значение robustness variable в диапазоне от 1 до 7.
--------------	---

По умолчанию

Значение по умолчанию – 2.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов.

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)#
```

55.15 ipv6 mld snooping static-group

Данная команда используется для настройки статической группы MLD Snooping. Чтобы удалить статическую группу, 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. Допустимые адреса имеют префикс ff00::/8.
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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. Используйте данную команду на интерфейсе VLAN, чтобы добавить статические записи о принадлежности к группе и/или записи источника (source).

Введите команду **ipv6 mld snooping static-group**, чтобы создать статическую группу MLD Snooping, если прикрепленный узел не поддерживает протокол MLD .

Пример

В данном примере показано, как добавить статическую группу и/или запись источника для MLD Snooping.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping static-group FF02::12:03 interface ethernet 1/0/5
Switch(config-vlan)#
```

55.16 ipv6 mld snooping suppression-time

Данная команда используется, чтобы настроить время 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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки и VLAN-интерфейсов. Функция Report Suppression будет блокировать дублированные пакеты MLD report или MLD leave, полученные в течение времени блокирования. Чем меньше время блокирования, тем чаще будут отправляться дублированные пакеты MLD.

Пример

В данном примере показано, как настроить время блокирования на VLAN 1000. Указанное значение – 125.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping suppression-time 125
Switch(config-vlan)#
```

55.17 ipv6 mld snooping minimum-version

Данная команда используется для настройки минимальной версии MLD, разрешенной на интерфейсе. Чтобы удалить заданное ограничение, 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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно для настройки VLAN-интерфейсов. Данные настройки используются только для фильтрации сообщений о принадлежности 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)#
```

55.18 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.
Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если не указаны дополнительные параметры, будет отображена информация об MLD Snooping для

всех VLAN, на которых включена данная функция.

Пример

В данном примере показано, как отобразить настройки MLD Snooping.

```
Switch# show ipv6 mld snooping

MLD snooping global state: Enabled

VLAN #1 configuration
  MLD snooping state           : Enabled
  Minimum version              : v1
  Fast leave                   : Enabled (host-based)
  Report suppression           : Disabled
  Suppression time             : 10 seconds
  Querier state                : Enabled (Non-active)
  Querier                     : -
  Query expiry time            : 0 seconds
  Query version                : v2
  Query interval               : 2000 seconds
  Max response time            : 10 seconds
  Robustness value             : 2
  Last member query interval   : 1 seconds
  Proxy reporting              : Enabled (Source ::)
  Rate limit                   : 30
  Ignore topology change       : Enabled  Ignore topology change : Disabled

Total Entries: 1

Switch#
```

55.19 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 IPv6-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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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

Пример

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

```
Switch# show ipv6 mld snooping groups

Total Group Entries : 1
Total Source Entries: 1

vlan 1, FF1E::1
Learned on port: 1/0/3

Switch#
```

55.20 show ipv6 mld snooping mrouter

Данная команда используется, чтобы отобразить информацию об автоматически изученном или настроенном вручную многоадресном маршрутизаторе MLD Snooping.

show ipv6 mld snooping mrouter [vlan VLAN-ID [, | -]]

Параметры

vlan VLAN-ID	(Опционально.) Укажите VLAN ID 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить интерфейсы динамически изученного или сконфигурированного вручную многоадресного маршрутизатора.

Пример

В данном примере показано, как отобразить информацию о многоадресном маршрутизаторе MLD Snooping.

```
Switch#show ipv6 mld snooping mrouter

VLAN    Ports
-----
1        1/0/3, 1/0/4  (static)
          1/0/6   (forbidden)
          1/0/7   (dynamic)

3        1/0/8   (static)
          1/0/9   (dynamic)

Total Entries: 2

Switch#
```

55.21 show ipv6 mld snooping static-group

Данная команда используется для отображения статически сконфигурированных групп MLD Snooping на коммутаторе.

show ipv6 mld snooping static-group [GROUP-ADDRESS | vlan VLAN-ID]

Параметры

<i>GROUP-ADDRESS</i>	(Опционально.) Укажите IPv6-адрес группы для отображения.
vlan <i>VLAN-ID</i>	(Опционально.) Укажите VLAN ID для отображения.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения статически сконфигурированных групп MLD Snooping на коммутаторе. Если 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#
```

55.22 show ipv6 mld snooping statistics

Данная команда используется для отображения статистики MLD Snooping на коммутаторе.

show ipv6 mld snooping statistics {interface [*INTERFACE-ID* [, | -]] | vlan [*VLAN-ID* [, | -]]}

Параметры

interface	Укажите, чтобы отобразить счетчики статистики для интерфейса.
<i>INTERFACE-ID</i>	(Опционально.) Укажите интерфейсы 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.
<i>VLAN-ID</i>	(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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статистику MLD Snooping.

Пример

В данном примере показано, как отобразить статистику MLD Snooping.

```
Switch#show ipv6 mld snooping statistics interface
```

```
Interface eth1/0/1 Statistics:
```

```
Rx: V1Report 0, v2Report 0, Query 0, v1Done 0
```

```
Tx: V1Report 0, v2Report 0, Query 0, v1Done 0
```

```
Interface eth1/0/2 Statistics:
```

```
Rx: V1Report 0, v2Report 0, Query 0, v1Done 0
```

```
Tx: V1Report 0, v2Report 0, Query 0, v1Done 0
```

```
Interface eth1/0/3 Statistics:
```

```
Rx: V1Report 0, v2Report 0, Query 0, v1Done 0
```

```
Tx: V1Report 0, v2Report 0, Query 0, v1Done 0
```

```
Total Entries: 3
```

```
Switch#show ipv6 mld snooping statistics vlan 1
```

```
VLAN 20 Statistics:
```

```
Rx: V1Report 0, v2Report 0, Query 0, v1Done 0
```

```
Tx: V1Report 0, v2Report 0, Query 0, v1Done 0
```

```
Total Entries: 1
```

```
Switch#
```

56. Команды Multicast VLAN

56.1 mvlan enable

Данная команда используется для включения функции Multicast VLAN и настройки некоторых ее параметров. Чтобы отключить данную функцию или вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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)#
```

56.2 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 или 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 данном примере показано, как включить параметр **forward-unmatched** и проигнорировать настройки VLAN.

```
Switch# configure terminal
Switch(config)# mvlan forward-unmatched
Switch(config)# mvlan ignore-vlan
Switch(config)#
```

56.3 mvlan vlan

Данная команда используется для создания Multicast VLAN. Чтобы удалить 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)#
```

56.4 member

Данная команда используется для настройки интерфейсов в качестве портов source (источник) или

receiver (получатель) для Multicast VLAN. Чтобы удалить порты 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.

У Multicast VLAN может быть 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 ethernet 1/0/1-4
Switch(config-mvlan)#
```

56.5 name

Данная команда используется для указания имени Multicast VLAN. Чтобы вернуться 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 используется 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)#
```

56.6 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 маршрутизатором uplink во время проверок IP Spoofing.

Чтобы изменить IP-адрес 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)#
```

56.7 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

<i>PROFILE-NAME</i>	Укажите имя профиля.
all	Укажите, чтобы удалить все профили Multicast VLAN.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Профиль 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)#
```

56.8 access-group

Данная команда используется для привязки профиля группы доступа к Multicast VLAN. Чтобы удалить привязку, 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)#
```

56.9 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

<i>IPV4-ADDRESS-START</i>	Укажите начальный многоадресный IPv4-адрес в диапазоне.
<i>IPV4-ADDRESS-END</i>	Укажите конечный многоадресный IPv4-адрес в диапазоне.
<i>IPV6-ADDRESS-START</i>	Укажите начальный многоадресный IPv6-адрес в диапазоне.
<i>IPV6-ADDRESS-END</i>	Укажите конечный многоадресный IPv6-адрес в диапазоне.

По умолчанию

Нет.

Режим ввода команды

Multicast VLAN Profile Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

В профиль Multicast VLAN могут быть добавлены несколько диапазонов. Диапазоны IP-адресов, указанные в одном профиле, должны быть в одном семействе адресов.

Пример

В данном примере показано, как добавить диапазон IPv4 в профиль под именем «profile mv_profile1».

```
Switch#configure terminal
Switch(config)#mvlan group-profile mv_profile1
Switch(config-mvlan-profile)#range 225.0.0.0 225.0.0.5
Switch(config-mvlan-profile)#
```

56.10 show mvlan group-profile

Данная команда используется для отображения настроек профиля группы многоадресной рассылки.

show mvlan group-profile [PROFILE-NAME]

Параметры

<i>PROFILE-NAME</i>	(Опционально.) Укажите имя профиля.
---------------------	-------------------------------------

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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#
```

56.11 show mvlan access-group

Данная команда используется для отображения привязок профилей группы многоадресной рассылки к Multicast VLAN.

show mvlan access-group [VLAN-ID]

Параметры

VLAN-ID	(Опционально.) Укажите VLAN ID.
---------	---------------------------------

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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#
```

56.12 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.

Любой режим конфигурирования.

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.

57. Команды Neighbor Discovery (ND) Inspection

57.1 ipv6 nd inspection policy

Данная команда используется для создания политики ND Inspection и входа в режим ND Inspection Policy Configuration Mode. Чтобы удалить политику ND Inspection, воспользуйтесь формой **no** этой команды.

```
ipv6 nd inspection policy POLICY-NAME  
no ipv6 nd inspection policy POLICY-NAME
```

Параметры

<i>POLICY-NAME</i>	Укажите имя политики ND Inspection.
--------------------	-------------------------------------

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 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)#
```

57.2 validate source-mac

Данная команда используется, чтобы проверить MAC-адрес на соответствие адресу Link Layer для ND-сообщений. Для отмены проверки 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)#
```

57.3 device-role

Данная команда используется для указания 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 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)#
```

57.4 mode

Данная команда используется для настройки режима ND Inspection. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

mode {precise | fuzzy}
no mode

Параметры

precise	Укажите, чтобы включить режим precise.
fuzzy	Укажите, чтобы включить 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 настроить режим ND Inspection. Когда включен режим **precise**, ND Inspection проверяет, совпадает ли адрес назначения с адресом источника в пакетах DANA/NA. В режиме **fuzzy** ND Inspection проверяет наличие адресов назначения и источника в таблице привязок.

Пример

В данном примере показано, как создать политику ND под именем «policy1» и настроить режим **fuzzy**.

```
Switch# configure terminal
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)# mode fuzzy
Switch(config-nd-inspection)#
```

57.5 ipv6 nd inspection attach-policy

Данная команда используется для применения политики ND Inspection на определенном интерфейсе. Чтобы удалить политику ND Inspection, воспользуйтесь формой **no** этой команды.

ipv6 nd inspection attach-policy [*POLICY-NAME*]
no ipv6 nd inspection attach-policy

Параметры

<i>POLICY-NAME</i>	(Опционально.) Укажите имя политики ND Inspection.
--------------------	--

По умолчанию

По умолчанию политика ND Inspection 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 под именем «policy1» на интерфейсе Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)# device-role host
Switch(config-nd-inspection)# validate source-mac
Switch(config-nd-inspection)# exit
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ipv6 nd inspection attach-policy policy1
Switch(config-if)#
```

57.6 show ipv6 nd inspection policy

Данная команда используется для отображения информации о политике ND Inspection.

show ipv6 nd inspection policy [*POLICY-NAME*]

Параметры

<i>POLICY-NAME</i>	(Опционально.) Укажите имя политики ND Inspection.
--------------------	--

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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#
```

58. Команды Network Access Authentication

58.1 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 может быть применена, только если указанная VLAN существует в качестве статической VLAN. Узел получает доступ к сети после успешного прохождения аутентификации. Если Guest VLAN настроена, узлу разрешается доступ только к Guest VLAN без прохождения аутентификации. Во время аутентификации пользователь, которому RADIUS-сервером была назначена VLAN, будет авторизован в назначенной VLAN. Невозможно назначить Guest VLAN и VLAN на порту trunk VLAN и порту tunnel VLAN.

Как правило, назначение Guest VLAN и VLAN действует для узлов, подключенных к нетегированным портам. Данный функционал не применим, если узлы обмениваются тегированным трафиком.

Если режим узла (Host Mode) аутентификации настроен как **multi-host**, порт будет добавлен как member-порт Guest VLAN, а PVID порта изменится 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 member-порт Guest VLAN, и PVID порта изменится на Guest VLAN. Узлам, которым разрешен доступ к Guest VLAN, предоставляется доступ к другим VLAN только после прохождения аутентификации. Когда один узел проходит аутентификацию, порт остается в Guest VLAN, а PVID порта не изменяется.

Если Guest VLAN отключена, порт выйдет из Guest VLAN и вернется к родной VLAN (Native). PVID изменится на PVID родной VLAN.

Пример

В данном примере показано, как указать VLAN 5 в качестве Guest VLAN.


```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication guest-vlan 5
Switch(config-if)#
```

58.2 authentication host-mode

Данная команда используется для указания режима аутентификации. Чтобы вернуться 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 узлы, 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 для аутентификации. Данный параметр используется, если различные VLAN на коммутаторе имеют различные требования к аутентификации. Если при использовании формы no не указаны конкретные VLAN, будут удалены все VLAN. То есть клиент будет аутентифицирован вне зависимости от того, к какой VLAN он принадлежит, если MAC-адрес клиента (независимо от VLAN) не аутентифицирован. После аутентификации клиенту не нужно будет проходить повторную аутентификацию из других VLAN. Это способствует управлению аутентификацией на 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 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 используется режим **multi-auth**.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если порт работает в режиме **multi-host** и аутентифицирован один из узлов, всем другим узлам будет разрешен доступ к порту. Согласно аутентификации 802.1X, если повторная аутентификация завершается неудачно или аутентифицированный пользователь выходит из учетной записи, порт будет заблокирован на период молчания (quiet period). Порт продолжит обрабатывать пакеты 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 на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication host-mode multi-host
Switch(config-if)#
```

58.3 authentication periodic

Данная команда используется для включения периодического повторения аутентификации для порта. Чтобы отключить периодическое повторение 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

Данная команда применяется для включения периодического повторения аутентификации для порта. Введите команду **authentication timer reauthentication**, чтобы настроить таймер 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 ethernet 1/0/1
Switch(config-if)# authentication periodic
Switch(config-if)#
```

58.4 authentication timer inactivity

Данная команда используется для настройки таймера бездействия (Inactivity Timer), по истечении которого неактивная сессия будет завершена. Чтобы отключить таймер бездействия, воспользуйтесь формой **no** этой команды.

authentication timer inactivity {SECONDS}
no authentication timer inactivity

Параметры

SECONDS	Укажите период времени в секундах, по истечении 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 (Inactivity Timer) настроен, сессия пользователя, которая не будет работать в течение настроенного периода времени, завершается. Значение таймера бездействия должно быть меньше, чем значение таймера, настроенного с помощью команды **authentication timer reauthentication**.

Пример

В данном примере показано, как настроить таймер бездействия для интерфейса Ethernet 1/0/1. Указанное значение – 240.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication timer inactivity 240
Switch(config-if)#
```

58.5 authentication timer reauthentication

Данная команда используется для настройки таймера, по истечении которого потребуется повторная аутентификация. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

authentication timer reauthentication {SECONDS}
no authentication timer reauthentication

Параметры

SECONDS	Укажите период времени, по истечении которого потребуется повторная аутентификация. Диапазон значений: от 1 до 86400.
----------------	---

По умолчанию

Значение по умолчанию – 3600 секунд.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для настройки таймера, по истечении которого потребуется повторная аутентификация. Введите команду **authentication periodic**, чтобы определить, будет ли производиться повторная аутентификация.

Пример

В данном примере показано, как настроить таймер повторной аутентификации для интерфейса Ethernet 1/0/1. Указанное значение – 200.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication timer reauthentication 200
Switch(config-if)#
```

58.6 authentication timer restart

Данная команда используется для настройки таймера, по истечении которого станет возможна повторная аутентификация после последней неудачной попытки. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

authentication timer restart SECONDS
no authentication timer restart

Параметры

SECONDS	Укажите период времени, 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 до истечения времени таймера.

Пример

В данном примере показано, как настроить таймер повторной аутентификации для интерфейса Ethernet 1/0/1. Указанное значение – 20.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# authentication timer restart 20
Switch(config-if)#
```

58.7 authentication username

Данная команда используется для создания пользователя в локальной базе данных аутентификации. Чтобы удалить пользователя из локальной базы 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 указаны ни 0, ни 7, по умолчанию используется обычный текст.
7	(Опционально.) Пароль в зашифрованном виде. Если не указаны ни 0, ни 7, по умолчанию используется обычный текст.
password PASSWORD	Укажите, чтобы задать пароль для MAC-аутентификации. Если указан пароль в обычном текстовом виде, строка не должна содержать более 32 символов.
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

Данная команда применяется для настройки локальной базы данных для аутентификации пользователей.

Пример

В данном примере показано, как создать локальную учетную запись с именем пользователя «user1» и паролем «pass1».

```
Switch# configure terminal
Switch(config)# authentication username user1 password pass1
Switch(config)#
```

58.8 clear authentication sessions

Данная команда используется для удаления сессий аутентификации.

clear authentication sessions {mac | wac | dot1x | all | interface *INTERFACE-ID* [mac | wac | dot1x] | mac-address *MAC-ADDRESS*}

Параметры

mac	Укажите для удаления всех MAC-сессий.
wac	Укажите для удаления всех WAC-сессий.
dot1x	Укажите для удаления всех сессий dot1x.
all	Укажите для удаления всех сессий.
interface <i>INTERFACE-ID</i>	Укажите для удаления сессий порта.
mac-address <i>MAC-ADDRESS</i>	Укажите для удаления всех сессий определенного пользователя.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для удаления сессий аутентификации.

Пример

В данном примере показано, как удалить сессии аутентификации на интерфейсе Ethernet 1/0/1.

```
Switch# clear authentication sessions interface ethernet 1/0/1
Switch#
```

58.9 authentication username mac-format

Данная команда используется для настройки формата MAC-адреса, который будет использоваться при аутентификации через RADIUS-сервер в качестве имени пользователя. Чтобы вернуться 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. Формат будет выглядеть следующим образом: AA-BB-CC-DD-EE-FF
colon	Укажите, чтобы использовать «:» в качестве разделителя. Формат будет выглядеть следующим образом: AA:BB:CC:DD:EE:FF
dot	Укажите, чтобы использовать «.» в качестве разделителя. Формат будет выглядеть следующим образом: AA.BB.CC.DD.EE.FF
none	Укажите, чтобы не использовать знак разделения. Формат будет выглядеть следующим образом: AABBCCDDEEFF
number	Укажите количество знаков разделения. Доступны следующие опции: 1: один разделитель; формат: AABBCD.DDEEFF 2: два разделителя; формат: AABB.CCDD.EEFF 5: пять разделителей; формат: AA.BB.CC.DD.EE.FF Если выбран параметр none , знаки разделения ограничителей не будут использоваться.

По умолчанию

По умолчанию для MAC-адреса аутентификации используются большие буквы.

По умолчанию знаком разделения MAC-адреса аутентификации является точка.

По умолчанию используется два знака разделения MAC-адреса аутентификации.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется 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)#
```

58.10 authentication compauth mode

Данная команда используется для указания режима Compound Authentication Mode. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

authentication compauth mode {any}

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 аутентификация 802.1X все равно будет необходима.
------------	--

По умолчанию

По умолчанию используется параметр **any**.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить/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 ethernet 1/0/1
Switch(config-if)#authentication compauth mode any
Switch(config-if)#
```

58.11 authentication max users

Данная команда используется, чтобы настроить максимальное количество аутентифицированных пользователей для всей системы или порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

authentication max users *NUMBER*

no authentication max users

Параметры

<i>NUMBER</i>	Укажите, чтобы задать максимальное количество аутентифицированных пользователей. Диапазон значений от 1 до 1000.
---------------	--

По умолчанию

Значение по умолчанию – 1000.

Режим ввода команды

Global Configuration Mode.

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда может применяться в режиме Global Configuration Mode и Interface Configuration Mode.

Если команда настроена в режиме Global Configuration Mode, задается ограничение максимального количества пользователей на всю систему.

В команде, настроенной 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.

Пример

В данном примере показано, как назначить максимальное количество аутентифицированных пользователей для системы.

```
Switch# configure terminal
Switch(config)# authentication max users 256
Switch(config)#
```

58.12 authentication mac-move deny

Данная команда используется для запрета MAC Move на коммутаторе. Чтобы вернуться 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 функция включена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы разрешить/запретить аутентифицированным узлам перемещаться по портам коммутатора. Команда позволяет настроить управление таким образом, чтобы только узлу, аутентифицированному на порту в режиме **multi-auth**, было разрешено перемещаться к другому порту.

Узел, которому разрешено перемещаться, может быть либо повторно аутентифицирован, либо напрямую перемещен на новый порт без повторной аутентификации на основе следующего правила. Если настройки аутентификации нового порта и оригинального (исходного) порта совпадают, повторная аутентификация не требуется. Для нового порта будут применены те же атрибуты авторизации. Аутентифицированный узел может перемещаться от порта 1 к порту 2 с теми же атрибутами авторизации без необходимости повторной аутентификации. Если настройки аутентификации у нового и оригинального порта различаются, 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.

Ситуация, в которой аутентифицированный узел перемещается на другой порт при отключенной функции MAC Move, 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)#
```

58.13 authorization disable

Данная команда используется, чтобы отключить принятие авторизованной конфигурации. Для включения принятия 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

Используйте данную команду, чтобы включить/отключить принятие авторизованной конфигурации. Если авторизация включена для аутентификации, авторизованные атрибуты, например, VLAN, приоритет 802.1p по умолчанию, полоса пропускания (bandwidth) и список управления доступом (ACL), назначенные RADIUS-сервером, будут приняты, если включено состояние авторизации. Полоса пропускания и 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)#
```

58.14 show authentication sessions

Данная команда используется для отображения информации об аутентификации.

show authentication sessions [mac | wac | dot1x | interface INTERFACE-ID [, | -] [mac | wac | dot1x] | mac-address MAC-ADDRESS]

Параметры

mac	(Опционально.) Укажите для отображения всех MAC-сессий.
wac	(Опционально.) Укажите для отображения всех WAC-сессий.
dot1x	(Опционально.) Укажите для отображения всех сессий dot1x.
interface <i>INTERFACE-ID</i>	(Опционально.) Укажите порт для отображения.
,	(Опционально.) 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 <i>MAC-ADDRESS</i>	(Опционально.) Укажите для отображения определенного пользователя.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду без параметров, чтобы отобразить сессии, ассоциированные со всеми портами.

Пример

В данном примере показано, как отобразить сессии на интерфейсе Ethernet 1/0/1.

```
Switch# show authentication sessions interface ethernet 1/0/1

Interface: eth1/0/1
MAC Address: 00-16-76-35-1A-38
Authentication VLAN: 1
Authentication State: Success
Accounting Session ID: 0000000000CB
Authentication Username: wac
Client IP Address: 10.90.90.9
Aging Time: 3590 sec
Method      State
  WEB-based Access Control: Success, Selected

Total Authenticating Hosts: 0
Total Authenticated Hosts: 1
Total Blocked Hosts: 0

Switch#
```

Отображаемые параметры

Interface	Принимающий интерфейс узла аутентификации.
MAC Address	MAC-адрес узла аутентификации.
Authentication VLAN	Исходная VLAN начала аутентификацию узла.
Authentication State	Состояние аутентификации узла. Start – принимается узел, но аутентификация не началась. 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 – система принимает и анализирует результат аутентификации данного метода для узла. Failure – узел не прошел аутентификацию с помощью данного метода. No Information – информация об аутентификации недоступна.
Aging Time/Block Time	Aging Time – период времени, в течение которого аутентифицированный узел будет находиться в аутентифицированном состоянии. По истечении данного времени узел будет возвращен в неаутентифицированное состояние. Blocked Time – если узел не смог пройти аутентификацию, следующая аутентификация не начнется в течение времени блокировки, если только пользователь не очистит состояние ввода entry state вручную.
Idle Time	Оставшееся время сессии аутентификации. Сессия, которая неактивна в течение указанного периода времени, будет завершена. Доступно только для сессий WEB.
802.1X Authenticator State	Состояние аутентификатора PAE 802.1X. Возможны следующие значения: INITIALIZE – аутентификатор находится в процессе инициализации и ожидает запросы на аутентификацию. DISCONNECTED – инициализация завершена, но ни одно запрашивающее устройство не подключено к порту. CONNECTING – коммутатор обнаружил, что запрашивающее устройство подключается к порту. PAE произведет попытку подключиться к запрашивающему устройству. AUTHENTICATING – запрашивающее устройство проходит аутентификацию. AUTHENTICATED – аутентификатор успешно аутентифицировал запрашивающее устройство. ABORTING – аутентификации преждевременно отменена из-за запроса на повторную авторизацию или запроса кадра EAPOL-Start, EAPOL-Logoff, тайм-аута аутентификации. HELD – коммутатор игнорирует или отбрасывает все EAPOL-пакеты для защиты от атак. В данное состояние можно перейти из состояния AUTHENTICATING после ошибки аутентификации.

FORCE_AUTH – запрашивающее устройство всегда авторизовано.

FORCE_UNAUTH – запрашивающее устройство всегда не авторизовано.

802.1X Backend State

Состояние Backend PAE 802.1X. Возможны следующие значения:

REQUEST – коммутатор получил пакет EAP-запроса от сервера аутентификации и отправил полученный пакет запрашивающему устройству в качестве EAPOL-инкапсулированного кадра.

RESPONSE – коммутатор получил EAPOL-инкапсулированный пакет EAP-ответа от запрашивающего устройства и отправил полученный 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 аутентификатор PAE и запрашивающее устройство.

TIMEOUT – на сервере аутентификации или запрашивающем устройстве настроен тайм-аут.

IDLE – коммутатор ожидает новую сессию аутентификации.

INITIALIZE – аутентификатор производит инициализацию.

59. Команды Network Protocol Port Protection

59.1 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)#
```

59.2 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

Данная 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#
```

60. Команды Open Shortest Path First Version 2 (OSPFv2)

60.1 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: 16-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)#
```

60.2 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

<i>AREA-ID</i>	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 суммарный 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)#
```

60.3 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 внутризональные 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)#
```

60.4 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

<i>AREA-ID</i>	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)#
```

60.5 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.
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.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 1 virtual-link 10.10.11.50 hello-interval 5
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)#
```

60.6 clear ip ospf

Данная команда используется для перезапуска процесса IPv4 OSPF.

clear ip ospf

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 очистить процесс OSPF.

```
Switch#clear ip ospf
Switch#
```

60.7 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] [metric-type TYPE-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 <i>METRIC-VALUE</i>	(Опционально.) Укажите стоимость, ассоциированную с генерированным маршрутом по умолчанию. Если параметр не указан, значение метрики по умолчанию равно 1. Диапазон значений: от 1 до 16777214.
metric-type <i>TYPE-VALUE</i>	(Опционально.) Укажите тип метрики для внешних (external) маршрутов, которые были перераспределены 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, 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

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)#
```

60.8 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 <i>METRIC-VALUE</i>	(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)#
```

60.9 distance ospf

Данная команда используется, чтобы настроить расстояние (distance) для определенных маршрутов OSPF. Для отмены назначения воспользуйтесь формой **no** этой команды.

distance ospf {intra-area | inter-area | external-1 | external-2} *DISTANCE*
no distance ospf

Параметры

intra-area	Укажите расстояние для внутризональных (intra-area) маршрутов OSPF.
inter-area	Укажите расстояние для межзональных (inter-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)#
```

60.10 graceful-restart helper

Данная команда используется, чтобы включить механизм плавного перезапуска OSPF (Graceful Restart) в режиме Helper Mode для локальной политики. Для отключения данной функции воспользуйтесь формой **no** этой команды.

graceful-restart helper [only-reload | max-grace-period SECONDS]

no graceful-restart helper [max-grace-period SECONDS]

Параметры

only-reload	(Опционально.) Укажите, чтобы механизм OSPF Graceful Restart и режим Helper Mode были включены только для перезагрузки.
max-grace-period <i>SECONDS</i>	(Опционально.) Укажите максимальный период плавного перезапуска (Graceful Restart). Диапазон значений: от 1 до 1800.

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 механизм плавного перезапуска OSPF (Graceful Restart) в режиме Helper Mode для локальной политики. При взаимодействии маршрутизаторов механизм Graceful Restart будет включен для всех устройств.

Пример

В данном примере показано, как включить механизм плавного перезапуска OSPF (Graceful Restart) в режиме Helper Mode для локальной политики только для перезагрузки. Настроенный максимальный период плавного перезапуска – 60.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#graceful-restart helper max-grace-period 60
Switch(config-router)#graceful-restart helper only-reload
Switch(config-router)#
```

60.11 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

<i>IP-ADDRESS</i>	Укажите IP-адрес узла.
<i>AREA-ID</i>	Укажите ID зоны, которая содержит запись тупикового (stub) узла.
cost <i>COST</i>	(Опционально.) Укажите стоимость записи тупикового (stub) узла.

Диапазон значений: от 1 до 16777215.

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)#
```

60.12 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 vlan 1
Switch(config-if)# ip ospf authentication message-digest
Switch(config-if)#
```

60.13 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

<i>PASSWORD</i>	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 vlan 1
Switch(config-if)# ip ospf authentication
Switch(config-if)# ip ospf authentication-key test
Switch(config-if)#
```

60.14 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

<i>COST</i>	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 vlan 1
Switch(config-if)# ip ospf cost 10
Switch(config-if)#
```

60.15 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

<i>SECONDS</i>	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.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip ospf dead-interval 10
Switch(config-if)#
```

60.16 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

<i>SECONDS</i>	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 vlan 1
Switch(config-if)# ip ospf hello-interval 3
Switch(config-if)#
```

60.17 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

<i>KEY-ID</i>	Укажите ID ключа. Диапазон значений: от 1 до 255.
<i>KEY</i>	Укажите ключ OSPF MD5 Message Digest. Строка ключа не должна содержать пробелов. 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.

В режиме MD5 Digest Mode при изменении ключа текущий обмен сообщениями не прерывается. Если при обмене OSPF-пакетами с соседним маршрутизатором используемый ключ был изменен на новый ключ, пакеты будут дублированы и отправлены и на старый, и на новый ключ. Пакеты будут дублироваться до тех пор, пока все маршрутизаторы в сети не изучат новый ключ. После отправки пакетов необходимо удалить старый ключ для прекращения взаимодействия с маршрутизатором, использующим старый ключ.

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 vlan 1
Switch(config-if)# ip ospf authentication message-digest
Switch(config-if)# ip ospf message-digest-key 10 md5 yourpass
Switch(config-if)#
```

60.18 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 vlan 1
Switch(config-if)# ip ospf network point-to-point
Switch(config-if)#
```

60.19 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

<i>PRIORITY</i>	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 vlan 1
Switch(config-if)# ip ospf priority 3
Switch(config-if)#
```

60.20 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 отработку syslog-сообщений при обнаружении/разрыве соединения с соседними устройствами OSPF.

Пример

В данном примере показано, как включить отработку 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)#
```

60.21 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)#
```

60.22 no area

Данная команда используется для удаления настроек, ассоциированных с зоной.

```
no area AREA-ID
```

Параметры

AREA-ID	Укажите ID зоны 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 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)#
```

60.23 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 vlan 1
Switch(config-router)#
```

60.24 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

<i>PROTOCOL</i>	Укажите исходный протокол, из которого необходимо перераспределить маршруты. Доступны следующие ключевые слова: connected , static , или rip .
metric <i>METRIC-VALUE</i>	(Опционально.) Укажите значение метрики для перераспределяемых маршрутов. Диапазон значений: от 1 до 16777214.
metric-type <i>TYPE-VALUE</i>	(Опционально.) Укажите тип метрики для внешних (external) маршрутов, которые были перераспределены в домен маршрутизации OSPF. Возможно одно из двух значений: 1: укажите, чтобы использовать внешнюю метрику типа 1. 2: укажите, чтобы использовать внешнюю метрику типа 2. Если тип метрики не указан, будет применена метрика типа 2.
route-map <i>MAP-NAME</i>	(Опционально.) Укажите карту маршрутов для фильтрации импортированных маршрутов из указанного исходного протокола маршрутизации.

По умолчанию

По умолчанию перераспределение маршрутов отключено.

По умолчанию для внешних (external) маршрутов используется метрика типа 2.

По умолчанию карта маршрутов настроена для перераспределения всех маршрутов.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12, 15.

Использование команды

Внешние (external) маршруты могут быть перераспределены в нормальные зоны (Normal Area) как внешние маршруты типа 5, а также могут быть перераспределены в зоны 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 BGP в домен OSPF.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# redistribute static metric 100
Switch(config-router)#
```

60.25 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)#
```

60.26 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

<i>ROUTER-ID</i>	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 должно 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)#
```


60.27 prefix-suppression

Данная команда используется для предотвращения анонсирования маршрутизаторами своих префиксов в качестве средства ускорения конвергенции OSPF. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

prefix-suppression
no prefix-suppression

Параметры

Нет.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы уменьшить количество анонсируемых LSA в зоне.

Пример

В примере ниже показано, как подключить данную опцию.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# prefix-suppression
```

60.28 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, а именно статистику всей системы и статистику по зонам. Ограничением для переполненной базы данных LSDB является максимальный размер таблицы LSA.

Пример

В данном примере показано, как отобразить общую информацию о протоколе OSPF.

```
Switch#show ip ospf

Operational Router ID 3.3.3.3
Conforms to RFC2328, and RFC1583 Compatibility flag is enabled
SPF schedule Hold time between two SPF's 10 secs
Number of external LSA 1. Checksum Sum 0x9886
Number of LSA originated 32
Number of LSA received 7
Number of current LSA 11
LSDB database overflow limit is No Limit
Number of areas attached to this router: 2
  Area 0.0.0.1
    Number of interface in this area is 1, active interface number is 1
    SPF algorithm executed 7 times
    Number of LSA 6
  Area 0.0.0.0 (BACKBONE)
    Number of interface in this area is 1, active interface number is 1
    SPF algorithm executed 7 times
    Number of LSA 4

Switch#
```

60.29 show ip ospf database

Данная команда используется для отображения суммарной 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 суммарную информацию базы данных OSPF.

Пример

В данном примере показано, как отобразить суммарную информацию базы данных OSPF.

```
Switch# show ip ospf database
```

```
Router Link States (Area 0.0.0.0)
Link Id      Adv Router   Age    Seq#    Chksm  Options  Rtr Opt
-----
1.1.1.1      1.1.1.1      45     80000005 aa09    -E-----
3.3.3.3      3.3.3.3      53     80000007 a75a    -E----- ---EB

Network Link States (Area 0.0.0.0)
Link Id      Adv Router   Age    Seq#    Chksm  Options  Rtr Opt
-----
20.1.2.1     3.3.3.3      53     80000001 8e97    -E-----

Network Summary States (Area 0.0.0.0)
Link Id      Adv Router   Age    Seq#    Chksm  Options  Rtr Opt
-----
192.168.10.0 3.3.3.3      322    80000001 fae1    -E-----

Router Link States (Area 0.0.0.1)
Link Id      Adv Router   Age    Seq#    Chksm  Options  Rtr Opt
-----
2.2.2.2      2.2.2.2      282    80000004 1145    ----- ---E-
3.3.3.3      3.3.3.3      281    80000005 b795    ----- ---EB
```

Network Link States (Area 0.0.0.1)						
Link Id	Adv Router	Age	Seq#	Chksm	Options	Rtr Opt
192.168.10.1	3.3.3.3	137	80000002	e3e2	-----	
Network Summary States (Area 0.0.0.1)						
Link Id	Adv Router	Age	Seq#	Chksm	Options	Rtr Opt
20.1.2.0	3.3.3.3	322	80000001	1229	-----	
NSSA LSA States (Area 0.0.0.1)						
Link Id	Adv Router	Age	Seq#	Chksm	Options	Rtr Opt
0.0.0.0	3.3.3.3	322	80000002	0f36	-----	
30.0.0.0	2.2.2.2	23	80000001	40da	--P---	
AS External States						
Link Id	Adv Router	Age	Seq#	Chksm	Options	Rtr Opt
30.0.0.0	3.3.3.3	22	80000001	9886		
Total Entries: 11						
Switch#						

60.30 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 ID маршрутизатора 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 1.1.1.1

Router Link States (Area 0.0.0.0)
Link Id      Adv Router   Age    Seq#       Chksm  Options  Rtr Opt
-----
1.1.1.1      1.1.1.1     143    80000005   aa09   -E-----
Total Entries: 1
Switch#
```

60.31 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

<i>LINK-STATE-ID</i>	(Опционально.) Укажите link state ID в виде IP-адреса.
<i>self-originate</i>	(Опционально.) Укажите self-originate link state.
<i>adv-router</i>	(Опционально.) Укажите, чтобы отобразить все summary LSA определенного маршрутизатора ASBR.
<i>IP-ADDRESS</i>	(Опционально.) Укажите IP-адрес анонсирующего маршрутизатора.

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

                Summary ASBR States (Area 0.0.0.0)
LS Age: 25
LS options: (E-Bit)
LS Type: ASBR Summary LSA
LS Id: 2.2.2.2 (address of ASBR)
Advertising Router: 3.3.3.3
LS Seq Number: 0x80000001
Checksum: 0xb096
Length: 28
  Network Mask: 0.0.0.0
  Metric: 1

Total Entries: 1

Switch#
```

60.32 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

<i>LINK-STATE-ID</i>	(Опционально.) Укажите link state ID в виде IP-адреса.
self-originate	(Опционально.) Укажите self-originate link state.
adv-router	(Опционально.) Укажите, чтобы отобразить все external LSA определенного маршрутизатора.
<i>IP-ADDRESS</i>	(Опционально.) Укажите IP-адрес анонсирующего маршрутизатора.

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

                AS External States
LS Age: 164
LS options: (E-Bit)
LS Type: AS External LSA
LS Id: 30.0.0.0 (network prefix)
Advertising Router: 3.3.3.3
LS Seq Number: 0x80000001
Checksum: 0x9886
Length: 36
Network Mask: 255.0.0.0
Options:(E-Bit)
Metric Type: 2
Metric:20
Forwarding Address:192.168.10.2
Tag:0

Total Entries: 1

Switch#
```

60.33 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

<i>LINK-STATE-ID</i>	(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.
<i>IP-ADDRESS</i>	(Опционально.) Укажите IP-адрес анонсирующего маршрутизатора.

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

                Network Link States (Area 0.0.0.0)

LS Age: 217
LS options: (E-Bit)
LS Type: Network LSA
LS Id: 20.1.2.1 (address of designated router)
Advertising Router: 3.3.3.3
LS Seq Number: 0x80000001
Checksum: 0x8e97
Length: 32
Network Mask: 255.255.255.0
  Attached Router: 3.3.3.3
  Attached Router: 1.1.1.1

                Network Link States (Area 0.0.0.1)

LS Age: 301
LS options: (None)
LS Type: Network LSA
LS Id: 192.168.10.1 (address of designated router)
Advertising Router: 3.3.3.3
LS Seq Number: 0x80000002
Checksum: 0xe3e2
Length: 32
Network Mask: 255.255.255.0
  Attached Router: 3.3.3.3
  Attached Router: 2.2.2.2

Total Entries: 2

Switch#
```

60.34 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

<i>LINK-STATE-ID</i>	(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.

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

                NSSA LSA States (Area 0.0.0.1)
LS Age: 509
LS options: (None)
LS Type: Type 7 LSA
LS Id: 0.0.0.0 ((null))
Advertising Router: 3.3.3.3
LS Seq Number: 0x80000002
Checksum: 0x0f36
Length: 36
Network Mask: 0.0.0.0
Options: (None)
Metric Type: 1
Metric:1
Forwarding Address:0.0.0.0
Tag:0
```

```
LS Age: 211
LS options: (N/P-Bit)
LS Type: Type 7 LSA
LS Id: 30.0.0.0 ((null))
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000001
Checksum: 0x40da
Length: 36
Network Mask: 255.0.0.0
Options: (E-Bit)
Metric Type: 2
Metric: 20
Forwarding Address: 192.168.10.2
Tag: 0

Total Entries: 2

Switch#
```

60.35 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
```

```

Router Link States (Area 0.0.0.0)
Link Id      Adv Router   Age    Seq#      Chksm  Options  Rtr Opt
-----
3.3.3.3      3.3.3.3      262    80000007  a75a   -E-----  ---EB

```

```

Network Link States (Area 0.0.0.0)
Link Id      Adv Router   Age    Seq#      Chksm  Options  Rtr Opt
-----
20.1.2.1     3.3.3.3      262    80000001  8e97   -E-----

```

```

Network Summary States (Area 0.0.0.0)
Link Id      Adv Router   Age    Seq#      Chksm  Options  Rtr Opt
-----
192.168.10.0 3.3.3.3      531    80000001  fae1   -E-----

```

```

Router Link States (Area 0.0.0.1)
Link Id      Adv Router   Age    Seq#      Chksm  Options  Rtr Opt
-----
3.3.3.3      3.3.3.3      491    80000005  b795   -E-----  ---EB

```

```

Network Link States (Area 0.0.0.1)
Link Id      Adv Router   Age    Seq#      Chksm  Options  Rtr Opt
-----
192.168.10.1 3.3.3.3      346    80000002  e3e2   -E-----

```

```

Network Summary States (Area 0.0.0.1)
Link Id      Adv Router   Age    Seq#      Chksm  Options  Rtr Opt
-----
20.1.2.0     3.3.3.3      531    80000001  1229   -E-----

```

```

NSSA LSA States (Area 0.0.0.1)
Link Id      Adv Router   Age    Seq#      Chksm  Options  Rtr Opt
-----
0.0.0.0      3.3.3.3      531    80000002  0f36   -E-----

```

```

AS External States
Link Id      Adv Router   Age    Seq#      Chksm  Options  Rtr Opt
-----
30.0.0.0     3.3.3.3      232    80000001  9886

```

```
Total Entries: 8
```

```
Switch#
```

60.36 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

<i>LINK-STATE-ID</i>	(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.
<i>IP-ADDRESS</i>	(Опционально.) Укажите IP-адрес анонсирующего маршрутизатора.

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

                Router Link States (Area 0.0.0.0)

LS Age: 279
LS options: (E-Bit)
LS Type: Router LSA
LS Id: 1.1.1.1 (address of router)
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000005
Checksum: 0xaa09
Length: 36
Number of Links: 1

    (Link ID) IP Address of Designated Router: 20.1.2.1
    (Link Data) Router IP Address: 20.1.2.100
    Link connected to: transit network
    Metric: 1

LS Age: 287
LS options: (E-Bit)
LS Type: Router LSA
```

```
LS Id: 3.3.3.3 (address of router)
Advertising Router: 3.3.3.3
LS Seq Number: 0x80000007
Checksum: 0xa75a
Length: 36
Number of Links: 1

(Link ID) IP Address of Designated Router: 20.1.2.1
(Link Data) Router IP Address: 20.1.2.1
Link connected to: transit network
Metric: 1

Router Link States (Area 0.0.0.1)

LS Age: 516
LS options: (None)
LS Type: Router LSA
LS Id: 2.2.2.2 (address of router)
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000004
Checksum: 0x1145
Length: 36
Number of Links: 1

(Link ID) IP Address of Designated Router: 192.168.10.1
(Link Data) Router IP Address: 192.168.10.2
Link connected to: transit network
Metric: 1

LS Age: 515
LS options: (None)
LS Type: Router LSA
LS Id: 3.3.3.3 (address of router)
Advertising Router: 3.3.3.3
LS Seq Number: 0x80000005
Checksum: 0xb795
Length: 36
Number of Links: 1

(Link ID) IP Address of Designated Router: 192.168.10.1
(Link Data) Router IP Address: 192.168.10.1
Link connected to: transit network
Metric: 1

Total Entries: 4

Switch#
```

60.37 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

<i>LINK-STATE-ID</i>	(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.
<i>IP-ADDRESS</i>	(Опционально.) Укажите IP-адрес анонсирующего маршрутизатора.

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

                Network Summary States (Area 0.0.0.0)
LS Age: 593
LS options: (E-Bit)
LS Type: Network Summary LSA
LS Id: 192.168.10.0 (network prefix)
Advertising Router: 3.3.3.3
LS Seq Number: 0x80000001
Checksum: 0xfae1
Length: 28
  Network Mask: 255.255.255.0
  Metric: 1

                Network Summary States (Area 0.0.0.1)
LS Age: 593
LS options: (None)
LS Type: Network Summary LSA
LS Id: 20.1.2.0 (network prefix)
Advertising Router: 3.3.3.3
LS Seq Number: 0x80000001
Checksum: 0x1229
Length: 28
  Network Mask: 255.255.255.0
  Metric: 1

Total Entries: 2

Switch#
```

60.38 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 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 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
vlan2 is up, line protocol is up
  Internet Address: 20.1.2.1/24, Area 0
  Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface Address 20.1.2.1
  Backup Designated Router (ID) 1.1.1.1, Interface Address 20.1.2.100
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Current Authentication Type: none

vlan10 is up, line protocol is up
  Internet Address: 192.168.10.1/24, Area 1
  Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface Address 192.168.10.1
  Backup Designated Router (ID) 2.2.2.2, Interface Address 192.168.10.2
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Current Authentication Type: none

Total Entries: 2
Switch#
```

60.39 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 для отображения.
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 о соседних устройствах OSPF. Если интерфейс не указан, будет отображена информация о соседних устройствах 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
2.2.2.2	1	Full/BACKUP	192.168.10.2	vlan 10
1.1.1.1	1	Full/BACKUP	20.1.2.100	vlan 2

```
Total Entries: 2  
Switch#
```

В примере ниже показано, как отобразить подробную информацию о соседних устройствах OSPF.

```
Switch# show ip ospf neighbor detail
```

```
Neighbor 2.2.2.2, interface address 192.168.10.2  
  In the area 0.0.0.1 via interface vlan 10  
  Neighbor priority is 1, State is Full, 5 state change  
  DR is 192.168.10.1, BDR is 192.168.10.2  
  Options: 0x0
```

```
Neighbor 1.1.1.1, interface address 20.1.2.100  
  In the area 0.0.0.0 via interface vlan 2  
  Neighbor priority is 1, State is Full, 4 state change  
  DR is 20.1.2.1, BDR is 20.1.2.100  
  Options: 0x42
```

```
Total Entries: 2  
Switch#
```

60.40 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 3.3.3.3 is up
  Transit area 0.0.0.1
  Local address 192.168.10.2
  Remote Address -
  Transmit Delay is 1 sec, State Point-To-Point
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Current Authentication Type: none

Total Entries: 1
Switch#
```

60.41 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#
```

60.42 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
OSPF log neighbor set.
Switch#

6609.225 (0,0,0,0): OSPF interface VLAN 10 moved from state IFO_DROTHER to state IFO_BACKUP,
on event IFO_NGB_CHANGE
6609.326 (0,0,0,0): OSPF neighbor 192.168.10.1 on VLAN 10 moved from state EX START to state
EXCHANGE, on event NegotiationDone
```

60.43 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
OSPF log interface set.
Switch#

6680.383 (0,0,0,0): OSPF Hello sent on interface VLAN 10.
6690.399 (0,0,0,0): OSPF Hello received on interface VLAN 10 from 3.3.3.3 at 192.168.10.1.
```

60.44 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
OSPF log tracing enabled
Switch#

[OSPF(1589)][6989865][ospfRedistCfgChangeHandle-1764]: Entry..
[OSPF(1589)][6989867][ospfReadFdsGet-1118]: rppiSockFd - 11, bestRtClientSockFd - 17,
syncDbSockFd - 7, rpcClientSockFd - 12, maxFds - 17.
```

60.45 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
OSPF log lsa-originating set.
Switch#

7130.555 (0,0,0,0): Originating area 0.0.0.1 interface All Router LSA 2.2.2.2. Reorig: FALSE.
Option: 0
```

60.46 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
OSPF log lsa-flooding set.
Switch#

7223.713 (0,0,0,0): Flooding OSPF Router LSA in area 0.0.0.1. LSID: 2.2.2.2, Adv Router:
2.2.2.2, Age: 0, SeqNo: 0x80000002
```

60.47 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
OSPF packet tracing enabled.
Switch#

6726.537 (0,0,0,0): OSPF DD received on interface VLAN 10 from router 3.3.3.3. MTU: 1500
Options: E  Flags: I/M/MS SeqNo: 1641 Length: 32
```

60.48 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
OSPF packet tracing enabled.
Switch#

6726.537 (0,0,0,0): OSPF DD sent on interface VLAN 10 to router 3.3.3.3. MTU: 1500 Options: E
Flags: SeqNo: 1641 Length: 52
```

60.49 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
OSPF log spf set.
Switch#

7650.745 (0,0,0,0): Recomputing all OSPF routes
7650.745 (0,0,0,0): Computing intra-area routes for area 0.0.0.1
```

60.50 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
OSPF log virtual-link set.
Switch#

7759.494 (0,0,0,0): Selected address 192.168.10.1 for virtual neighbor 3.3.3.3 in area 0.0.0.1
```

60.51 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
OSPF log route set.
Switch#

8034.948 (0,0,0,0): OSPFv2 adding network route to 192.168.10.0 255.255.255.0 in area 0.0.0.1.
Path type INTRA. Cost 1. Hops 1.
```

60.52 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
OSPF log redistribution set.
Switch#

118.501 (0,0,0,0): Redistributing 30.0.0.0/255.0.0.0 with type 2 metric 20 via next hop
192.168.20.3. Status: ROW_CREATE_AND_GO
```

60.53 debug ip ospf trace

Данная команда используется для включения функции отладки при установке флага трассировки пакетов OSPF. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды.

debug ip ospf trace

no debug ip ospf trace

Параметры

<i>Integer</i>	Укажите, чтобы задать значение типа данных Integer. Диапазон значений: от 0 до 2147483647.
----------------	--

По умолчанию

По умолчанию функция отладки при установке флага трассировки пакетов OSPF отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить функцию отладки при установке флага трассировки пакетов OSPF.

Пример

В данном примере показано, как включить функцию отладки при установке флага трассировки пакетов OSPF.

```
Switch# debug ip ospf trace 3
OSPF log trace set.
Switch#
```

61. Команды Open Shortest Path First Version 3 (OSPFv3)

61.1 area default-cost

Данная команда используется, чтобы установить стоимость по умолчанию (summary-default cost) тупиковой зоны (Stub Area). Чтобы отключить данную функцию, 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 IPv4-адреса.
COST	Укажите метрику или стоимость суммарного (summary) маршрута, которую OSPF будет использовать для вычисления кратчайшего пути к адресу назначения. Диапазон значений: от 1 до 16777215.

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 пограничном маршрутизаторе (ABR), который подключен 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
Switch(config-rtr)# area 1 stub
Switch(config-rtr)# area 1 default-cost 10
Switch(config-rtr)#
```

61.2 area range

Данная команда используется для объединения и суммирования маршрутов на границе зоны. Чтобы отключить данную функцию, 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 IPv4-адреса.
IPv6-PREFIX	Укажите IPv6-префикс.
PREFIX-LENGTH	Укажите длину IPv6-префикса.
advertise	(Опционально.) Укажите, чтобы анонсировать inter-area prefix LSA для заданного диапазона адресов.
no-summary	(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 IPv6-префикса 2001:0DB8:0:1::/64 и для Router ID 20.0.1.10.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf
Switch(config-rtr)# router-id 20.0.1.10
Switch(config-rtr)# area 1 range 2001:0DB8:0:1::/64
Switch(config-rtr)#
```

61.3 area stub

Данная команда используется для назначения зоны в качестве тупиковой зоны (Stub Area). Чтобы отключить данную функцию, 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 вводе 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 межзональных маршрутов (inter-area route), 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
Switch(config-rtr)# router-id 20.0.1.10
Switch(config-rtr)# area 1 stub
Switch(config-rtr)#
```

61.4 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

<i>AREA-ID</i>	Укажите ID зоны в виде IPv4-адреса.
<i>ROUTER-ID</i>	Укажите ID соседнего маршрутизатора канала. ID задается в виде IPv4-адреса.
hello-interval <i>SECONDS</i>	(Опционально.) Укажите интервал между пакетами hello, которые маршрутизатор отправляет на интерфейс. Диапазон значений: от 1 до 65535 секунд.
dead-interval <i>SECONDS</i>	(Опционально.) Укажите интервал, по истечении которого соседнее устройство считается недоступным, если не было получено ни одного пакета. Диапазон значений: от 1 до 65535 секунд.
transmit-delay <i>SECONDS</i>	(Опционально.) Укажите интервал, по истечении которого маршрутизатор будет отправлять пакет. Диапазон значений: от 0 до 3600 секунд.
retransmit-interval <i>SECONDS</i>	(Опционально.) Укажите интервал, по истечении которого маршрутизатор будет повторно отправлять пакет. Диапазон значений: от 0 до 3600 секунд.
instance <i>INSTANCE-ID</i>	(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).

В IPv6 OSPF все немагистральные зоны должны быть подключены к магистральной. При прерывании соединения с магистралью подключение будет восстановлено с помощью виртуального канала.

Возможна настройка виртуального канала между любыми двумя магистральными маршрутизаторами, у которых есть интерфейс в общей немагистральной зоне. Протокол считает, что эти два маршрутизатора объединены виртуальным каналом, как если бы между ними было установлено соединение типа «точка-точка». Для настройки сетевого подключения укажите ID транзитной зоны, а также ID соседнего маршрутизатора виртуального канала.

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 со значениями по умолчанию опциональных параметров.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf
Switch(config-rtr)# area 1 virtual-link 192.168.255.1
Switch(config-rtr)#
```

61.5 auto-cost reference-bandwidth

Данная команда применяется для указания референсного значения пропускной способности (reference-bandwidth), используемого IPv6 OSPF при вычислении метрики для интерфейсов. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

auto-cost reference-bandwidth *MBPS*
no auto-cost reference-bandwidth

Параметры

<i>MBPS</i>	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

Команда предназначена для указания референсного значения пропускной способности (reference-bandwidth), используемого IPv6 OSPF при вычислении метрики на интерфейсах.

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
Switch(config-rtr)# auto-cost reference-bandwidth 1000
Switch(config-rtr)#
```

61.6 clear ipv6 ospf

Данная команда используется для перезапуска OSPF на основе ID процесса маршрутизации OSPF.

clear ipv6 ospf

Параметры

Нет.

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 SPF. Если параметры не указаны, удаляются все процессы OSPF.

Пример

В данном примере показано, как удалить все процессы OSPF.

```
Switch# clear ipv6 ospf
Switch#
```

61.7 default-metric

Данная команда используется, 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

<i>METRIC-VALUE</i>	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**, чтобы настроить общее значение 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
Switch(config-rtr)# default-metric 10
Switch(config-rtr)# redistribute rip
Switch(config-rtr)#
```

61.8 distance ospf

Данная команда используется, чтобы настроить расстояние (distance) для определенных маршрутов OSPF. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

distance ospf {external-1 | external-2 | inter-area | intra-area} *DISTANCE*
no distance ospf {external-1 | external-2 | inter-area | intra-area}

Параметры

external-1	Укажите расстояние для внешних (external) маршрутов OSPF типа 1.
-------------------	--

external-2	Укажите расстояние для внешних (external) маршрутов OSPF типа 2.
inter-area	Укажите расстояние для межзоновых (inter-area) маршрутов OSPF.
intra-area	Укажите расстояние для внутризональных (intra-area) маршрутов OSPF.
DISTANCE	Укажите значение расстояния (distance) определенных маршрутов OSPF. Диапазон значений: от 1 до 255.

По умолчанию

Значение расстояния для всех маршрутов OSPF по умолчанию – 110.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить административное расстояние (administrative distance) для определенных маршрутов OSPF. Команда **distance ospf** действует как команда **distance**, которая определяет, какие маршруты будут установлены в таблице маршрутизации.

Административное расстояние представляет собой число от 1 до 255. Чем выше это значение, тем ниже рейтинг надежности 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
Switch(config-rtr)# distance ospf inter-area 50
Switch(config-rtr)#
```

61.9 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 area AREA-ID [instance INSTANCE-ID]
no ipv6 ospf area AREA-ID [instance]

Параметры

AREA-ID	Укажите ID зоны в виде IPv4-адреса.
---------	-------------------------------------

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 может быть изменен командой **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
Switch(config-if)# ipv6 ospf area 0 instance 2
Switch(config-if)#
```

61.10 ipv6 ospf cost

Данная команда используется для точного указания стоимости отправки пакета на интерфейсе. Чтобы вернуться 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 вводе 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 vlan 1
Switch(config-if)# ipv6 ospf cost 65
Switch(config-if)#
```

61.11 ipv6 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.

ipv6 ospf dead-interval SECONDS
no ipv6 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

Интервал 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 интервала должно быть одинаковым для всех маршрутизаторов в одной сети.

Пример

В данном примере показано, как установить интервал dead для IPv6 OSPF. Настроенное значение – 60 секунд.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 ospf dead-interval 60
Switch(config-if)#
```

61.12 ipv6 ospf hello-interval

Данная команда используется для указания интервала между пакетами hello, которые маршрутизатор отправляет на интерфейс. Чтобы вернуться 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

Значение, настроенное в данной команде, анонсируется в пакетах hello и должно быть одинаковым для всех маршрутизаторов и серверов доступа 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 интервал между пакетами hello. Установленное значение – 15 секунд.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 ospf hello-interval 15
Switch(config-if)#
```

61.13 ipv6 ospf priority

Данная команда используется для установки приоритета, по которому определяется назначенный маршрутизатор (Designated Router, DR) в сети. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

```
ipv6 ospf priority PRIORITY  
no ipv6 ospf priority
```

Параметры

<i>PRIORITY</i>	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 предназначена для установки приоритета, по которому определяется назначенный маршрутизатор (Designated Router, DR) OSPF в сети. Когда два маршрутизатора пытаются стать DR, в качестве DR будет назначен маршрутизатор с более высоким значением приоритета. Если приоритеты совпадают, выбирается маршрутизатор с более высоким значением Router ID.

Назначенными (designated) или резервными назначенными (backup designated) могут стать только маршрутизаторы с ненулевым значением приоритета. Приоритет настраивается только для сетей со множественным доступом (не «точка-точка»).

Пример

В данном примере показано, как установить приоритет маршрутизатора. Настроенное значение – 4.

```
Switch# configure terminal  
Switch(config)# interface vlan 1  
Switch(config-if)# ipv6 ospf priority 4  
Switch(config-if)#
```

61.14 ipv6 ospf retransmit-interval

Данная команда используется для установки времени повторной отправки LSA соседним устройствам на интерфейсе. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

```
ipv6 ospf retransmit-interval SECONDS  
no ipv6 ospf retransmit-interval
```


Параметры

<i>SECONDS</i>	Укажите время интервала, по истечении которого маршрутизатор будет повторно отправлять пакет. Диапазон значений: от 1 до 3600 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. Маршрутизатор, который не получает подтверждения в течение установленного времени (значение интервала retransmit), 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)#
```

61.15 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

<i>SECONDS</i>	Укажите интервал, по истечении которого маршрутизатор будет повторно отправлять пакет. Диапазон значений: от 1 до 3600 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)#
```

61.16 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
no ipv6 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 IPv6 OSPF.

Пример

В данном примере показано, как указать ID для процесса маршрутизации IPv6 OSPF и войти в режим Router Configuration Mode.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf
Switch(config-rtr)#
```

61.17 no area

Данная команда используется для удаления определенной созданной 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 настройки 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.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf
Switch(config-rtr)# no area 3
Switch(config-rtr)#
```

61.18 passive-interface

Данная команда используется для включения пассивного режима на указанном сетевом интерфейсе или 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 и активировать VLAN 1.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf
Switch(config-rtr)# passive-interface default
Switch(config-rtr)# no passive-interface vlan 1
Switch(config-rtr)#
```

61.19 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*] [**route-map** *MAP-NAME*]

no redistribute *PROTOCOL* [**metric**] [**metric-type**] [**route-map** *MAP-NAME*]

Параметры

PROTOCOL	Укажите исходный протокол, из которого необходимо перераспределить маршруты. Доступны следующие ключевые слова: connected , static , rip .
metric <i>METRIC-VALUE</i>	(Опционально.) Укажите значение метрики при перераспределении других процессов в IPv6 OSPF. Если значение метрики не указано, по умолчанию метрика равна 20.

metric-type <i>TYPE-VALUE</i>	(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.
route-map <i>MAP-NAME</i>	(Опционально.) Укажите карту маршрутов для фильтрации импортированных маршрутов из указанного исходного протокола маршрутизации. Если карта маршрутов не указана, будут перераспределены все маршруты.

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.

Когда 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
Switch(config-rtr)# redistribute rip
Switch(config-rtr)#
```

61.20 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

<i>ROUTER-ID</i>	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
Switch(config-rtr)# router-id 10.1.1.1
Switch(config-rtr)#
```

61.21 show ipv6 ospf

Данная команда используется для отображения общей информации о процессах маршрутизации OSPF.

show ipv6 ospf

Параметры

Нет.

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

Router ID 1.1.1.1
Conforms to RFC 2740
This router is an ABR; ABR Type is Standard (OSPFv3).
SPF schedule delay 2000 secs, Hold time between SPFs 5000 secs
Number of LSA originated 60
Number of LSA received 15
Number of areas in this router is 2
  Area 0.0.0.0 (BACKBONE) (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 10 times
    Number of LSA 7. Checksum Sum 0x39a23
    Number of Unknown LSA 0
    Area ranges are
  Area 0.0.0.1 (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
    It is a nssa area
    SPF algorithm executed 4 times
    Number of LSA 9. Checksum Sum 0x4cb64
    Number of Unknown LSA 0
    Area ranges are

Switch#
```

61.22 show ipv6 ospf border-routers

Данная команда используется, чтобы отобразить маршрутизаторы ABR и ASBR для экземпляра IPv6 OSPF.

show ipv6 ospf border-routers

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 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

Type          Router Id    Cost    Area ID      Next Hop      Next Hop
              Intf
-----
ABR, INTRA    30.1.1.2      10     0.0.0.0      fe80::200:78ff:fe77:6658  vlan2
Switch#
```

61.23 show ipv6 ospf database

Данная команда используется для отображения краткой информации базы данных процессов маршрутизации OSPF.

show ipv6 ospf database [external | inter-area prefix | inter-area router | link | network | prefix | router] [adv-router ROUTER-ID | self-originate] [area AREA-ID]

Параметры

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. Оба этих ключевых 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 краткую информацию базы данных процессов маршрутизации OSPF.

```
Switch# show ipv6 ospf database
```

Router Link States (Area 0.0.0.0)							
Adv Router	Link Id	Age	Sequence	Csum	Options	Rtr	Opt
1.1.1.1	0	690	80000008	519D	V6E--R-	---	EB
3.3.3.3	0	952	80000002	9B5D	V6E--R-	-----	
Network Link States (Area 0.0.0.0)							
Adv Router	Link Id	Age	Seq#	Csum	Options	Rtr	Count
3.3.3.3	2	953	80000001	5AB0	V6E--R-		2
Inter Area Prefix Link States (Area 0.0.0.0)							
Adv Router	Link Id	Age	Sequence	Csum	Prefix		
1.1.1.1	1	688	80000001	CDE7	2010:1:1::/64		
Inter Router States (Area 0.0.0.0)							
Adv Router	Link Id	Age	Sequence	Csum	Options	Rtr	Opt
1.1.1.1	33686018	221	80000002	54B5			
Link States (Area 0.0.0.0)							
Adv Router	Link Id	Age	Seq#	Csum	Options	Interface	
3.3.3.3	2	1020	80000002	FEB4	V6E--R-	vlan2	
1.1.1.1	521	521	80000002	30BE	V6E--R-	vlan2	
Intra Area Prefix Link States (Area 0.0.0.0)							
Adv Router	Link Id	Age	Seq#	Csum	Ref-lstype	Ref-LSID	Prefix
1.1.1.1	0	690	8000000A	5136	Router-LSA	0.0.0.0	2002:1:1::/64
3.3.3.3	2	951	80000001	DCA8	Network-LSA	0.0.0.2	2002:1:1::/64
Router Link States (Area 0.0.0.1)							
Adv Router	Link Id	Age	Sequence	Csum	Options	Rtr	Opt
1.1.1.1	0	638	80000007	A348	V6---R-	---	EB
2.2.2.2	0	647	80000005	7873	V6---R-	---	E-
Network Link States (Area 0.0.0.1)							
Adv Router	Link Id	Age	Seq#	Csum	Options	Rtr	Count
2.2.2.2	521	86	80000002	EB1F	V6---R-		2
Inter Area Prefix Link States (Area 0.0.0.1)							
Adv Router	Link Id	Age	Sequence	Csum	Prefix		
1.1.1.1	0	690	80000001	2F95	2002:1:1::/64		

```

NSSA LSA States (Area 0.0.0.1)
Adv Router      Link Id      Age      Sequence Csum Options Rtr Opt
-----
1.1.1.1         0           685      80000002 55DF
2.2.2.2         1           658      80000001 BD73

Link States (Area 0.0.0.1)
Adv Router      Link Id      Age      Seq#      Csum Options Interface
-----
2.2.2.2         521         681      80000003 9CD7 V6---R- vlan10
1.1.1.1         522         685      80000003 EFEF V6---R- vlan10

Intra Area Prefix Link States (Area 0.0.0.1)
Adv Router      Link Id      Age      Seq#      Csum Ref-lstype      Ref-LSID      Prefix
-----
1.1.1.1         0           638      80000009 6C0E Router-LSA        0.0.0.0      2010:1:1::/64
2.2.2.2         0           647      80000007 84EF Router-LSA        0.0.0.0      2010:1:1::/64
2.2.2.2         10521       648      80000001 8EA7 Network-LSA     0.0.2.9      2010:1:1::/64

AS External States
Adv Router      Link Id      Age      Sequence Csum Prefix
-----
1.1.1.1         0           640      80000001 DF40 2030:1:1::/64

Total Entries: 21

Switch#

```

В следующем примере показано, как отобразить информацию о router LSA.

```

Switch# show ipv6 ospf database router

Router Link States (Area 0.0.0.0)
LS Age: 770
LS Type: Router-LSA
LS Id: 0
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000008
Checksum: 0x519d
Length: 40
AS Boundary Router, Area Border Router
LS options: (R-Bit E-Bit V6-Bit)
Number of Links: 1

```

```
Link connected to: transit network (designated router)
Link Metric: 10
Local Interface ID: 521
Neighbor Interface ID: 2
Neighbor Router ID: 3.3.3.3
```

```
LS Age: 1032
LS Type: Router-LSA
LS Id: 0
Advertising Router: 3.3.3.3
LS Seq Number: 0x80000002
Checksum: 0x9b5d
Length: 40
LS options: (R-Bit E-Bit V6-Bit)
Number of Links: 1
```

```
Link connected to: transit network (designated router)
Link Metric: 10
Local Interface ID: 2
Neighbor Interface ID: 2
Neighbor Router ID: 3.3.3.3
```

Router Link States (Area 0.0.0.1)

```
LS Age: 717
LS Type: Router-LSA
LS Id: 0
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000007
Checksum: 0xa348
Length: 40
AS Boundary Router, Area Border Router
LS options: (R-Bit V6-Bit)
Number of Links: 1
```

```
Link connected to: transit network (designated router)
Link Metric: 10
Local Interface ID: 522
Neighbor Interface ID: 521
Neighbor Router ID: 2.2.2.2
```

```
LS Age: 727
LS Type: Router-LSA
LS Id: 0
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000005
Checksum: 0x7873
Length: 40
AS Boundary Router
LS options: (R-Bit V6-Bit)
Number of Links: 1

Link connected to: transit network (designated router)
Link Metric: 10
Local Interface ID: 521
Neighbor Interface ID: 521
Neighbor Router ID: 2.2.2.2

Switch#
```

В примере ниже показано, как отобразить информацию об LSA сети (network LSA).

```
Switch# show ipv6 ospf database network

Network Link States (Area 0.0.0.0)

LS Age: 1089
LS Type: Network-LSA
LS Id: 2
Advertising Router: 3.3.3.3
LS Seq Number: 0x80000001
Checksum: 0x5ab0
Length: 32
LS options: (R-Bit E-Bit V6-Bit)
Neighbor Router ID: 3.3.3.3
Neighbor Router ID: 1.1.1.1

Network Link States (Area 0.0.0.1)

LS Age: 222
LS Type: Network-LSA
LS Id: 521
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000002
Checksum: 0xeb1f
Length: 32
LS options: (R-Bit V6-Bit)
Neighbor Router ID: 2.2.2.2
Neighbor Router ID: 1.1.1.1

Switch#
```

В следующем примере показано, как отобразить информацию об inter-area prefix LSA.

```
Switch# show ipv6 ospf database inter-area prefix

                Inter Area Prefix Link States (Area 0.0.0.0)
LS Age: 891
LS Type: Inter-Area-Prefix-LSA
LS Id: 1
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000001
Checksum: 0xcde7
Length: 36
Metric: 10
IPv6 Prefix: 2010:1:1::/64 (None)

                Inter Area Prefix Link States (Area 0.0.0.1)
LS Age: 893
LS Type: Inter-Area-Prefix-LSA
LS Id: 0
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000001
Checksum: 0x2f95
Length: 36
Metric: 10
IPv6 Prefix: 2002:1:1::/64 (None)

Switch#
```

В нижеприведенном примере показано, как отобразить информацию об inter-area router LSA.

```
Switch# show ipv6 ospf database inter-area router

                Inter Router States (Area 0.0.0.0)
LS Age: 470
LS Type: Inter-Area-Router-LSA
LS Id: 33686018
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000002
Checksum: 0x54b5
Length: 32
LS options: (R-Bit V6-Bit)
Metric: 10
Destination Router ID: 2.2.2.2

Switch#
```

В нижеследующем примере показано, как отобразить информацию о внешних (external) LSA.

```
Switch# show ipv6 ospf database external
```

```
AS External States
LS Age: 927
LS Type: AS-External-LSA
LS Id: 0
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000001
Checksum: 0xdf40
Length: 52
Options: (E-Bit F-Bit)
Metric Type: 2
Metric: 20
IPv6 Prefix: 2030:1:1::/64 (None)
Forwarding Address: 2010:1:1::2

Total Entries: 1

Switch#
```

В примере ниже показано, как отобразить информацию об LSA канала (link LSA).

```
Switch# show ipv6 ospf database link
```

```
Link States (Area 0.0.0.0)
Interface: vlan2
LS Age: 1334
LS Type: Link-LSA
LS Id: 2
Advertising Router: 3.3.3.3
LS Seq Number: 0x80000002
Checksum: 0xfeb4
Length: 56
Router Priority: 1
LS options: (R-Bit E-Bit V6-Bit)
Link-Local Address: fe80::8226:89ff:fe8d:c201
Number of Prefixes: 1
IPv6 Prefix: 2002:1:1::/64 (None)

Interface: vlan2
LS Age: 835
LS Type: Link-LSA
LS Id: 521
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000002
Checksum: 0x30be
Length: 56
Router Priority: 1
LS options: (R-Bit E-Bit V6-Bit)
Link-Local Address: fe80::6263:4cff:fe51:6083
Number of Prefixes: 1
IPv6 Prefix: 2002:1:1::/64 (None)
```

```
Link States (Area 0.0.0.1)
Interface: vlan10
LS Age: 995
LS Type: Link-LSA
LS Id: 521
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000003
Checksum: 0x9cd7
Length: 56
Router Priority: 1
LS options: (R-Bit V6-Bit)
Link-Local Address: fe80::200:78ff:fe77:6658
Number of Prefixes: 1
IPv6 Prefix: 2010:1:1::/64 (None)

Interface: vlan10
LS Age: 999
LS Type: Link-LSA
LS Id: 522
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000003
Checksum: 0xefef
Length: 56
Router Priority: 1
LS options: (R-Bit V6-Bit)
Link-Local Address: fe80::6263:4cff:fe51:6084
Number of Prefixes: 1
IPv6 Prefix: 2010:1:1::/64 (None)

Switch#
```

В следующем примере показано, как отобразить информацию об intra-area-prefix LSA.


```
Switch# show ipv6 ospf database prefix

                Intra Area Prefix Link States (Area 0.0.0.0)
LS Age: 1051
LS Type: Intra-Area-Prefix-LSA
LS Id: 0
Advertising Router: 1.1.1.1
LS Seq Number: 0x8000000a
Checksum: 0x5136
Length: 44
Number of Prefixes: 1
Referenced LS Type: Router-LSA
Referenced LS Id: 0
Referenced Advertising Router: 1.1.1.1
IPv6 Prefix: 2002:1:1::/64 (None)
Metric: 10

LS Age: 1312
LS Type: Intra-Area-Prefix-LSA
LS Id: 2
Advertising Router: 3.3.3.3
LS Seq Number: 0x80000001
Checksum: 0xdca8
Length: 44
Number of Prefixes: 1
Referenced LS Type: Network-LSA
Referenced LS Id: 2
Referenced Advertising Router: 3.3.3.3
IPv6 Prefix: 2002:1:1::/64 (None)
Metric: 0

                Intra Area Prefix Link States (Area 0.0.0.1)
LS Age: 999
LS Type: Intra-Area-Prefix-LSA
LS Id: 0
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000009
Checksum: 0x6c0e
Length: 44
Number of Prefixes: 1
Referenced LS Type: Router-LSA
Referenced LS Id: 0
Referenced Advertising Router: 1.1.1.1
IPv6 Prefix: 2010:1:1::/64 (None)
Metric: 10

LS Age: 1008
LS Type: Intra-Area-Prefix-LSA
LS Id: 0
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000007
Checksum: 0x84ef
```

```
Length: 44
Number of Prefixes: 1
Referenced LS Type: Router-LSA
Referenced LS Id: 0
Referenced Advertising Router: 2.2.2.2
IPv6 Prefix: 2010:1:1::/64 (None)
Metric: 10

LS Age: 1009
LS Type: Intra-Area-Prefix-LSA
LS Id: 10521
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000001
Checksum: 0x8ea7
Length: 44
Number of Prefixes: 1
Referenced LS Type: Network-LSA
Referenced LS Id: 521
Referenced Advertising Router: 2.2.2.2
IPv6 Prefix: 2010:1:1::/64 (None)
Metric: 0

Total Entries: 5

Switch#
```

В данном примере показано, как отобразить все LSA анонсирующего маршрутизатора 3.3.3.3.

```
Switch# show ipv6 ospf database router adv-router 3.3.3.3

Router Link States (Area 0.0.0.0)

LS Age: 1423
LS Type: Router-LSA
LS Id: 0
Advertising Router: 3.3.3.3
LS Seq Number: 0x80000002
Checksum: 0x9b5d
Length: 40
LS options: (R-Bit E-Bit V6-Bit)
Number of Links: 1

Link connected to: transit network (designated router)
Link Metric: 10
Local Interface ID: 2
Neighbor Interface ID: 2
Neighbor Router ID: 3.3.3.3

Switch#
```

В нижеприведенном примере показано, как отобразить все self-originate LSA.

```
Switch# show ipv6 ospf database router self-originate

                Router Link States (Area 0.0.0.0)
LS Age: 89
LS Type: Router-LSA
LS Id: 0
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000009
Checksum: 0x4f9e
Length: 40
AS Boundary Router, Area Border Router
LS options: (R-Bit E-Bit V6-Bit)
Number of Links: 1

    Link connected to: transit network (designated router)
    Link Metric: 10
    Local Interface ID: 521
    Neighbor Interface ID: 2
    Neighbor Router ID: 3.3.3.3

                Router Link States (Area 0.0.0.1)
LS Age: 1166
LS Type: Router-LSA
LS Id: 0
Advertising Router: 1.1.1.1
LS Seq Number: 0x80000007
Checksum: 0xa348
Length: 40
AS Boundary Router, Area Border Router
LS options: (R-Bit V6-Bit)
Number of Links: 1

    Link connected to: transit network (designated router)
    Link Metric: 10
    Local Interface ID: 522
    Neighbor Interface ID: 521
    Neighbor Router ID: 2.2.2.2

Switch#
```

61.24 show ipv6 ospf interface

Данная команда используется для отображения информации об интерфейсе, связанном с OSPF.

show ipv6 ospf interface [INTERFACE-ID]

Параметры

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 интерфейсе, связанном с OSPF.

```
Switch#show ipv6 ospf interface

vlan2 is up, line protocol is up
  Link Local Address: fe80::6263:4cff:fe51:6083/64
  Interface ID: 521
  Area 0.0.0.0 (active), Instance ID 0, MTU 1500
  Router ID 1.1.1.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 3.3.3.3,
    Local Address fe80::8226:89ff:fe8d:c201
  Backup Designated Router (ID) 1.1.1.1,
    Local Address fe80::6263:4cff:fe51:6083
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Neighbor Count is 6   Hello received 142 sent 158, DD received 3 sent 6
  LS-Req received 1 sent 1, LS-Upd received 3 sent 18
  LS-Ack received 12 sent 2

vlan10 is up, line protocol is up
  Link Local Address: fe80::6263:4cff:fe51:6084/64
  Interface ID: 522
  Area 0.0.0.1 (active), Instance ID 0, MTU 1500
  Router ID 1.1.1.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 2.2.2.2,
    Local Address fe80::200:78ff:fe77:6658
```

```
Backup Designated Router (ID) 1.1.1.1,  
  Local Address fe80::6263:4cff:fe51:6084  
Timer intervals configured, Hello 10, Dead 40, Retransmit 5  
Neighbor Count is 7   Hello received 130 sent 127, DD received 2 sent 4  
LS-Req received 1 sent 1, LS-Upd received 8 sent 6  
LS-Ack received 4 sent 4  
  
Total Entries: 2  
  
Switch#
```

61.25 show ipv6 ospf neighbor

Данная команда используется для отображения информации о соседних устройствах OSPF по интерфейсам.

show ipv6 ospf neighbor [INTERFACE-ID] [NEIGHBOR-ID] [detail]

Параметры

<i>INTERFACE-ID</i>	(Опционально.) Укажите ID интерфейса для отображения информации о соседних устройствах.
<i>NEIGHBOR-ID</i>	(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 2.2.2.2, interface  address fe80::200:78ff:fe77:6658
  In the area 0.0.0.1 via interface vlan10
  Neighbor priority is 1, State is Full, 7 state change
  DR is 2.2.2.2, BDR is 1.1.1.1
  Options: 0x11

Neighbor 3.3.3.3, interface  address fe80::8226:89ff:fe8d:c201
  In the area 0.0.0.0 via interface vlan2
  Neighbor priority is 1, State is Full, 6 state change
  DR is 3.3.3.3, BDR is 1.1.1.1
  Options: 0x13

Total Entries: 2

Switch#
```

61.26 show ipv6 ospf virtual-links

Данная команда используется для отображения параметров и текущего состояния виртуальных каналов OSPF (virtual link).

show ipv6 ospf virtual-links

Параметры

Нет.

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 1.1.1.1 is up
  Transit area 0.0.0.1
  Local Peer Address 2010:1:1::2/128
  Remote Peer Address -
  Transmit Delay is 1 sec, State Point-To-Point
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Adjacency state -
Total Entries: 1

Switch#
```

61.27 debug ipv6 ospfv3 neighbor

Данная команда используется для включения функции отладки соседних устройств OSPF на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды. Команды **debug ipv6 ospfv3** только для IPv6 OSPFv3.

```
debug ipv6 ospfv3 neighbor
no debug ipv6 ospfv3 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 ipv6 ospfv3 neighbor
OSPF log neighbor set.
Switch#

6609.225 (0,0,0,0): OSPF interface VLAN 10 moved from state IFO DROTHER to state IFO BACKUP,
on event IFO_NGB_CHANGE
6609.326 (0,0,0,0): OSPF neighbor 192.168.10.1 on VLAN 10 moved from state EX START to state
EXCHANGE, on event NegotiationDone
```

61.28 debug ipv6 ospfv3 interface

Данная команда используется для включения функции отладки OSPF на интерфейсе коммутатора. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды. Команды **debug ipv6 ospfv3** только для IPv6 OSPFv3.

debug ipv6 ospfv3 interface
no debug ipv6 ospfv3 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 ipv6 ospfv3 interface
OSPF log interface set.
Switch#

6680.383 (0,0,0,0): OSPF Hello sent on interface VLAN 10.
6690.399 (0,0,0,0): OSPF Hello received on interface VLAN 10 from 3.3.3.3 at 192.168.10.1.
```

61.29 debug ipv6 ospfv3 log

Данная команда используется для включения отправки syslog-сообщений OSPF на маршрутизаторе.

Чтобы отключить отправку syslog-сообщений OSPF, воспользуйтесь формой **no** этой команды. Команды **debug ipv6 ospfv3** только для IPv6 OSPFv3.

debug ipv6 ospfv3 log
no debug ipv6 ospfv3 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 ipv6 ospfv3 log
OSPFv3 tracing enabled
Switch#

[OSPF(1589)][6989865][ospfRedistCfgChangeHandle-1764]: Entry..
[OSPF(1589)][6989867][ospfReadFdsGet-1118]: rppiSockFd - 11, bestRtClientSockFd - 17,
syncDbSockFd - 7, rpcClientSockFd - 12, maxFds - 17.
```

61.30 debug ip ospf lsa-originating/debug ipv6 ospfv3 lsa-originating

Данная команда используется для включения функции отладки OSPF при возникновении LSA на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды. Команды **debug ipv6 ospfv3** только для IPv6 OSPFv3.

debug ipv6 ospfv3 lsa-originating
no debug ipv6 ospfv3 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 ipv6 ospfv3 lsa-originating
OSPFv3 log lsa-originating set.
Switch#

7130.555 (0,0,0,0): Originating area 0.0.0.1 interface All Router LSA 2.2.2.2. Reorig: FALSE.
Option: 0
```

61.31 debug ip ospf lsa-flooding/debug ipv6 ospfv3 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. Команды **debug ipv6 ospfv3** только для IPv6 OSPFv3.

debug ipv6 ospfv3 lsa-flooding
no debug ipv6 ospfv3 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 ipv6 ospfv3 lsa-flooding
OSPFv3 log lsa-flooding set.
Switch#

7223.713 (0,0,0,0): Flooding OSPF Router LSA in area 0.0.0.1. LSID: 2.2.2.2, Adv Router:
2.2.2.2, Age: 0, SeqNo: 0x80000002
```

61.32 debug ipv6 ospfv3 packet

Данная команда используется для включения функции отладки и трассировки при получении пакетов OSPF на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды. Команды **debug ipv6 ospfv3** только для IPv6 OSPFv3.

debug ip ospf packet-receiving/debug ipv6 ospfv3 packet
no debug ip ospf packet-receiving/no debug ipv6 ospfv3 packet

Параметры

Нет.

По умолчанию

По умолчанию функция отладки 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 отслеживании пакетов OSPF на коммутаторе.

Пример

В данном примере показано, как включить функцию отладки при получении пакетов OSPF на коммутаторе.

```
Switch# debug ipv6 ospfv3 packet
OSPFv3 packet tracing enabled.
Switch#

6726.537 (0,0,0,0): OSPF DD received on interface VLAN 10 from router 3.3.3.3. MTU: 1500
Options: E  Flags: I/M/MS SeqNo: 1641 Length: 32
```

61.33 debug ipv6 ospfv3 spf

Данная команда используется для включения функции отладки OSPF при расчете SPF на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды. Команды **debug ipv6 ospfv3** только для IPv6 OSPFv3.

```
debug ipv6 ospfv3 spf
no debug ipv6 ospfv3 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 ipv6 ospfv3 spf
OSPFv3 log spf set.
Switch#
```

61.34 debug ipv6 ospfv3 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. Команды **debug ipv6 ospfv3** только для IPv6 OSPFv3.

```
debug ipv6 ospfv3 virtual-link
no debug ipv6 ospfv3 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 ipv6 ospfv3 virtual-link
OSPFv3 log virtual-link set.
Switch#

7759.494 (0,0,0,0): Selected address 192.168.10.1 for virtual neighbor 3.3.3.3 in area 0.0.0.1
```

61.35 debug ipv6 ospfv3 route

Данная команда используется для включения функции отладки маршрутов OSPF на коммутаторе. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды. Команды **debug ipv6 ospfv3** только для IPv6 OSPFv3.

```
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 ipv6 ospfv3 route
OSPFv3 log route set.
Switch#
```

61.36 debug ipv6 ospfv3 trace

Данная команда используется для включения функции отладки при установке флага трассировки пакетов OSPF. Чтобы отключить данную функцию, воспользуйтесь формой **no** этой команды. Команды **debug ipv6 ospfv3** только для IPv6 OSPFv3.

debug ipv6 ospfv3 trace
no debug ipv6 ospfv3 trace

Параметры

<i>Integer</i>	Укажите, чтобы задать значение типа данных Integer. Диапазон значений: от 0 до 2147483647.
----------------	--

По умолчанию

По умолчанию функция отладки при установке флага трассировки пакетов OSPF отключена.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы включить функцию отладки при установке флага трассировки пакетов OSPF.

Пример

В данном примере показано, как включить функцию отладки при установке флага трассировки пакетов OSPF.

```
Switch# debug ipv6 ospfv3 trace 3
OSPFv3 log trace set.
Switch#
```

62. Команды Power over Ethernet (PoE)



Примечание: команды PoE применимы только к модели DMS-3130-30PS.

62.1 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

<i>TEXT</i>	Укажите 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 интерфейсе Ethernet 3/0/1.

```
Switch(config)# interface ethernet 3/0/1
Switch(config-if)# poe pd description ForVOIPusage
```

62.2 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 интерфейсу Ethernet 3/0/1.

```
Switch(config)# interface ethernet 3/0/1
Switch(config-if)# poe pd legacy-support
```

62.3 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 назначен низкий приоритет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима для настройки физического порта.

Поскольку бюджет мощности ограничен, источника питания может быть недостаточно для подачи питания при добавлении к системе новых PD-устройств. В данном случае система PoE входит в критическую секцию. Подача питания новому добавленному PD-устройству будет зависеть от политики, настроенной в команде **poe policy preempt**.

Политика, для которой отключен режим Preempt Mode, обслуживается в первую очередь. Таким образом, новое PD-устройство не будет обеспечено питанием.

При включенном режиме Preempt Mode для политики PD-устройство с наименьшим приоритетом будет вытеснено новым подключенным PD-устройством с более высоким приоритетом.

Пример

В данном примере показано, как настроить наивысший приоритет на интерфейсе Ethernet 3/0/1.

```
Switch(config)# interface ethernet 3/0/1
Switch(config-if)# poe pd priority critical
Switch(config-if)# end
Switch(config)#
```

62.4 poe policy preempt

Данная команда позволяет при недостаточном бюджете мощности отключать питание PD-устройства с наименьшим приоритетом для освобождения мощности для нового подключенного PD-устройства с более высоким приоритетом. 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.
---------	--

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Поскольку бюджет мощности ограничен, источника питания может быть недостаточно для подачи питания при добавлении к системе новых PD-устройств. В данном случае система PoE входит в критическую секцию.

Подача питания новому добавленному PD-устройству будет зависеть от политики, настроенной в данной команде. Политика, для которой отключен режим Preempt Mode, обслуживается в первую очередь. Таким образом, новое PD-устройство не будет обеспечено питанием.

При включенном режиме Preempt Mode для политики PD-устройство с наименьшим приоритетом будет вытеснено новым подключенным PD-устройством с более высоким приоритетом.

Пример

В данном примере показано, как настроить режим Preempt Mode для политики обслуживания системной мощности PoE.

```
Switch(config)# poe unit 1 policy preempt
```

62.5 poe power-inline

Данная команда используется, чтобы настроить режим Power Management Mode (управление энергопотреблением) для портов PoE. Для удаления привязки профиля временного диапазона или возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.



Примечание: чтобы коммутатор продолжал обеспечивать бесперебойное электропитание во время перезагрузки системы, используйте приведенную ниже команду **Perpetual PoE**.

```
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 неограниченного значения.
time-range PROFILE-NAME	(Опционально.) Укажите имя профиля временного диапазона для настройки периода активации.
never	Укажите, чтобы отключить питание PD-устройства, подключенного к порту.

По умолчанию

По умолчанию используется параметр **auto**.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно на портах с поддержкой PoE.

При использовании параметра **auto** PD-устройство будет обнаружено автоматически для подачи питания. В команде возможно указание максимальной мощности для порта. Если не указано, максимальная мощность будет определена классом PD-устройства. PD-устройство не будет обеспечено питанием, если для его работы требуется мощность выше настроенной максимальной мощности.

Если к порту PoE привязан профиль временного диапазона, порт будет работать только в течение периода времени, указанного в профиле. Таким образом, PD-устройство будет обеспечено питанием только в указанный период времени.

Чтобы распределить бюджет мощности заранее, необходимо порт перевести в режим Static Mode. Бюджет мощности будет распределен на порт, даже если PD-устройство не подключено к порту. Если указана максимальная мощность, то указанное количество мощности выделяется заранее.

Настройка профиля временного диапазона является опциональной. Если профиль временного диапазона не указан, временной диапазон не назначается.

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

Пример

В данном примере показано, как настроить автоматическое обнаружение PD-устройства для подачи питания на интерфейсе Ethernet 3/0/1.

```
Switch(config)# interface range ethernet 3/0/1
Switch(config-if)# poe power-inline auto
```

В примере ниже показано, как настроить максимальную мощность на интерфейсе Ethernet 3/0/1. Настроенная максимальная мощность позволяет подключиться PD-устройству, для работы которого требуется не более 5000 мВт.

```
Switch(config)# interface ethernet 3/0/1
Switch(config-if)# poe power-inline auto max 5000
```

В следующем примере показано, как отключить обнаружение PD-устройства и прекратить подачу питания с интерфейса Ethernet 3/0/1.

```
Switch(config)# interface ethernet 3/0/1
Switch(config-if)# poe power-inline never
```

В примере ниже показан процесс привязки профиля временного диапазона «day_time» к интерфейсу Ethernet 3/0/1.

```
Switch(config)# interface ethernet 3/0/1
Switch(config-if)# poe power-inline auto time-range day_time
```

62.6 poe usage-threshold

Данная команда используется, чтобы настроить порог потребления для отправки уведомлений. 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

<i>PERCENTAGE</i>	Укажите порог потребления для отправки уведомлений. Диапазон значений: от 1 до 99. Единица измерения – проценты.
<i>UNIT-ID</i>	(Опционально.) Укажите Unit ID устройства для отображения.

По умолчанию

Значение по умолчанию – 99.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При превышении PD-устройством настроенного порога потребления будет выслано trap-сообщение «pethMainPowerUsageOnNotification». Trap-сообщение «pethMainPowerUsageOffNotification» свидетельствует о том, что процентное значение порога стало меньше указанного.

Пример

В данном примере показано, как настроить порог потребления для уведомлений до 50%.

```
Switch(config)# poe unit 1 usage-threshold 50
Switch(config)#
```

62.7 poe guard-band

Данная команда используется для настройки конфигурации защитной полосы (guard band). Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

poe unit *UNIT-ID* **guard-band** *MILLI-WATTAGE*
no poe unit *UNIT-ID* **guard-band**

Параметры

<i>UNIT-ID</i>	(Опционально.) Укажите Unit ID устройства для отображения.
guard-band <i>MILLI-WATTAGE</i>	Укажите количество мощности, которое необходимо сохранить для защитной полосы (guard band). Диапазон значений: от 0 до 15400 мВт.

По умолчанию

Значение по умолчанию – 15400 мВт.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Защитная полоса PoE обеспечивает защиту портов с поддержкой PoE от выключения и последующего включения при резком скачке потребляемой мощности PD. Указанное количество мощности в защитной полосе сохраняется для обеспечения регулирования при резком скачке потребляемой мощности PD.

Пример

В данном примере показано, как указать количество мощности для защитной полосы (guard band) на устройстве с Unit ID 1. Настроенное значение – 13 Вт.

```
Switch# configure terminal
Switch(config)# poe unit 1 guard-band 13000
Switch(config)#
```

62.8 poe perpetual

Данная команда используется для обеспечения непрерывного электропитания во время перезагрузки системы для устройств, подключенных к PoE. Чтобы отключить **poe perpetual**, воспользуйтесь формой **no** этой команды.

poe perpetual
no poe perpetual

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 обеспечить электропитание по Ethernet даже во время

перезагрузки системы.

Пример

В данном примере показано, как включить опцию Perpetual PoE.

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

62.9 snmp-server enable traps poe

Данная команда используется для включения отправки уведомлений о событиях PoE. Чтобы отключить отработку 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

<i>UNIT-ID</i>	(Опционально.) Укажите Unit ID устройства для отображения.
----------------	--

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить отработку trap-сообщений для PoE о превышении порога потребления.

Пример

В данном примере показано, как настроить отработку trap-сообщений о событиях PoE.

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

62.10 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 <i>INTERFACE-ID</i>	Укажите ID интерфейса. Допустимыми интерфейсами являются физические порты.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Privilege EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для отображения счетчиков записей статистики 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 интерфейсе Ethernet 3/0/1.

```
Switch# clear poe statistic interface ethernet 3/0/1
```

62.11 show poe power-inline

Данная команда используется для отображения статуса PoE для определенного порта PoE или всех портов PoE в системе коммутатора.

show poe power-inline [*INTERFACE-ID* [, | -]] {**status** | **configuration** | **statistics** | **measurement** | **lldp-classification** }

Параметры

<i>INTERFACE-ID</i>	Укажите ID интерфейса 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.
status	Укажите для отображения статуса PoE порта.
configuration	Укажите для отображения информации о настройках порта.
statistics	Укажите для отображения счетчиков ошибок.
measurement	Укажите для отображения напряжения, тока, потребляемой мощности и температуры.
lldp-classification	Укажите для отображения классификации data link layer, используя информацию о power via MDI TLV.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статус PoE порта, статус конфигурации power inline, счетчики статистики, результаты параметра **measurement** и классификацию data link layer. Если ID интерфейса не указан, будут отображены все интерфейсы PoE. Отображаются только интерфейсы с поддержкой PoE.

Пример

В данном примере показан вывод команды **show poe power-inline status**.


```
Switch> show poe power-inline status
Interface      State      Class    Max(W)  Used(W)  Description
-----
eth3/0/1       delivering class-1 4      3.4      IP-camera-1
eth3/0/2       delivering class-2 10     6.3      12345678901234567890123456789012
!--- Output suppressed...
eth4/0/1       delivering class-3 15.4    13.0eth4/0/2    delivering class-3 15.4    12.4
eth4/0/3       disabled   N/A      0        0
eth4/0/4       searching  N/A      11.0     0
!--- Output suppressed...
eth5/0/24      disabled   N/A      0        0
eth5/0/25      faulty[2]  N/A      0        0

Faulty code:
[1] MPS (Maintain Power Signature) Absent
[2] PD short
[3] Overload
[4] Power Denied
[5] Thermal Shutdown
[6] Startup Failure
[7] Classification Failure

Switch>
```

62.12 show poe power module

Данная команда используется для отображения настроек и фактических значений PD-устройств.

show poe power module [unit UNIT-ID] [detail]

Параметры

detail	(Опционально.) Укажите для отображения более подробной информации о питании и параметрах PD-устройств.
UNIT-ID	(Опционально.) Укажите Unit ID устройства для отображения.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.
Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить подробную информацию о питании и параметрах для PD-устройств.

Пример

В данном примере показано, как отобразить информацию о питании PoE системы.

```
Switch> show poe power module
```

Unit	Delivered(W)	Power Budget(W)	Usage-Threshold(%)	Guard Band(W)	Policy Preempt	Trap State
1	0.0	727.0	50	13.0	enabled	enabled

```
Switch>
```

63. Команды Policy-Based Routing (PBR)

63.1 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**

Команды, перечисленные выше, 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 данном случае политика не будет применена на интерфейсе.

Пример

В данном примере показано, как настроить политику маршрутизации для маршрутизации пакетов, соответствующих списку доступа IP «pbr-acl». Следующий узел (next hop) – 20.1.1.254.

```
Switch# configure terminal
Switch(config)# route-map pbr-map permit 1
Switch(config-route-map)# match ip address pbr-acl
Switch(config-route-map)# set ip next-hop 20.1.1.254
Switch(config-route-map)# exit
Switch(config)# interface vlan 100
Switch(config-if)# ip policy route-map pbr-map
Switch(config-if)#
```

63.2 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 ip precedence**
- **set ip next-hop**

- **set ip default next-hop**

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)#
```

63.3 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.

Любой режим конфигурирования.

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#
```

63.4 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#
```

64. Команды Port Security

64.1 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#
```

64.2 show port-security

Данная команда используется для просмотра текущих настроек Port Security.

show port-security *[[interface INTERFACE-ID [, | -]] [address] | vlan VLAN-ID [, | -]]*

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите ID интерфейса 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 <i>VLAN-ID</i>	(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.

Любой режим конфигурирования.

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 для диапазона интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/3.


```
Switch#show port-security interface ethernet 1/0/1-3
```

```

D:Delete-on-Timeout    P:Permanent
Interface      Max  Curr  Violation  Violation  Security  Admin  Current
No.            No.  No.    Act.       Count      Mode    State  State
-----
eth1/0/1       5    2     Restrict -          D      Enabled Forwarding
eth1/0/2       10   10    Shutdown -          D      Enabled Err-disabled
eth1/0/3       10    0    Shutdown -          P      Disabled -
Switch#
```

64.3 snmp-server enable traps port-security

Данная команда используется для включения отправки SNMP-уведомлений при обнаружении функционалом Port Security недопустимых адресов. 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)#
```

64.4 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 64.
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

Когда включена функция Port Security и для порта настроен режим **delete-on-timeout**, порт будет автоматически изучать безопасные записи и хранить их, пока не истечет их тайм-аут. Время хранения этих записей зависит от настроек, заданных командой **switchport port-security aging**. Если режим порта задан как постоянный (permanent), он будет автоматически изучать безопасные записи с неистекающим тайм-аутом. Автоматически изученные безопасные записи будут храниться в текущем файле конфигурации (running configuration).

При изменении состояния безопасности режима порта (port mode-security) счетчик нарушений будет сброшен, записи auto-permanent будут преобразованы в соответствующие динамические записи. При отключении режима порта port-security автоматически изученные безопасные записи будут удалены, включая динамические и постоянные (permanent), а также счетчик нарушений. При изменении настройки VLAN автоматически изученные динамические безопасные записи будут удалены.

Постоянные безопасные записи будут храниться в текущем файле конфигурации и могут быть сохранены в NVRAM при вводе команды **copy**. Настроенные пользователем безопасные MAC-адреса будут подсчитываться в максимальном количестве MAC-адресов на порт.

Так как постоянная (permanent) безопасная запись Port Security включена на порту, MAC-адрес нельзя перенести на другой порт.

При изменении настроек изученные адреса останутся неизменными, если максимальное число будет увеличено. Если максимальное число будет изменено на меньшее, чем существующее число изучаемых записей, команда будет отклонена.

У порта с поддержкой Port Security есть следующие ограничения:

- Функция Port Security не может функционировать одновременно с 802.1X, MAC-based Access Control (управление доступом на основе MAC), WAC и IMPB, которые предоставляют более широкие возможности управления безопасностью.
- Если порт указан в качестве порта назначения для функции зеркалирования, функция Port Security не может быть включена.
- Если порт указан в качестве порта агрегирования каналов, функция Port Security не может быть включена.

При превышении максимального количества безопасных пользователей, может быть предпринято одно из следующих действий:

- **Protect**— когда число безопасных MAC-адресов порта достигает максимального значения пользователей, разрешенного на порту, пакеты с неизвестным адресом источника будут отбрасываться до тех пор, пока какая-нибудь безопасная запись не будет удалена.
- **Restrict**— при нарушении безопасности происходит ограничение данных, а также возрастает счетчик нарушений безопасности.
- **Shutdown**— при нарушении безопасности интерфейс отключается на основе ошибок.

Пример

В данном примере показано, как настроить режим permanent для Port Security с 5 безопасными MAC-адресами, разрешенными на порту.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security mode permanent
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)#
```

В 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)#
```

64.5 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 1 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 FDB Table Aging.

Пример

В данном примере показано, как настроить время устаревания (Aging Time) динамически изученных безопасных MAC-адресов для интерфейса Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security aging time 1
Switch(config-if)#
```

В примере ниже показано, как настроить тип времени устаревания для интерфейса Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)#
```

64.6 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 64. 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 10
Switch(config)#
```

65. Команды энергосбережения

65.1 dim led

Данная команда используется для отключения индикаторов портов с целью энергосбережения. Чтобы не отключать индикаторы портов с целью энергосбережения, воспользуйтесь формой **no** этой команды.

dim led
no dim led

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для отключения индикаторов портов с целью энергосбережения. Используйте форму **no** этой команды, чтобы не отключать индикаторы портов с целью энергосбережения. Если данная функция включена, все индикаторы, отображающие статус порта, будут отключены с целью энергосбережения.

Пример

В данном примере показано, как отключить индикаторы портов с целью энергосбережения.

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

65.2 power-saving

Данная команда используется для включения отдельных функций энергосбережения. Чтобы отключить данные функции, воспользуйтесь формой **no** этой команды.

power-saving {link-detection | length-detection | port-shutdown | dim-led | hibernation}
no power-saving {link-detection | length-detection | port-shutdown | dim-led | hibernation}

Параметры

link-detection	Укажите, чтобы включать функцию энергосбережения в зависимости от статуса соединения.
-----------------------	---

length-detection	Укажите, чтобы включать функцию энергосбережения в зависимости от длины кабеля.
dim-led	Укажите, чтобы включать функцию энергосбережения по расписанию отключения индикаторов.
port-shutdown	Укажите, чтобы включать функцию энергосбережения по расписанию отключения порта.
hibernation	Укажите, чтобы включать функцию энергосбережения по расписанию режима сна системы. Данная функция не поддерживается коммутаторами, объединенными в физический стек.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте нижеперечисленные параметры в команде для включения/отключения отдельных функций энергосбережения:

- **link-detection** (обнаружение подключения). Энергосбережение устройства будет зависеть от неактивных портов.
- **length-detection** (обнаружение длины кабеля). Энергосбережение устройства будет зависеть от длины кабеля.
- **dim-led** (отключение индикаторов). Энергосбережение устройства будет зависеть от отключения всех индикаторов порта в указанный диапазон времени.
- **port-shutdown** (отключение порта). Энергосбережение устройства будет зависеть от отключения всех портов в указанный диапазон времени.
- **hibernation** (режим сна). Энергосбережение устройства будет зависеть от включения режима сна в указанный диапазон времени.

При включенной функции Energy-Efficient Ethernet (EEE) энергосбережение устройства будет обеспечено на портах с поддержкой EEE.

Пример

В данном примере показано, как отключить порты и перейти в режим сна для энергосбережения.

```
Switch# configure terminal
Switch(config)# power-saving port-shutdown
Switch(config)# power-saving hibernation
Switch(config)#
```


65.3 power-saving eee

Данная команда используется для включения функции Energy-Efficient Ethernet (EEE) на определенном порту/портах. 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 определенном порту/портах. В режиме Power-Saving EEE энергосбережение зависит от использования фактической пропускной способности и будет обеспечено при установленном соединении во время низкого использования трафика пакетов. Если передаваемые данные отсутствуют, на физическом интерфейсе будет включен режим Low Power Idle (LPI).



Примечание: данная команда применяется только на портах, подключенных на скорости 1 Гбит/с.

Пример

В данном примере показано, как включить функцию Power-Saving EEE.

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

65.4 power-saving dim-led time-range

Данная команда используется, чтобы настроить профиль временного диапазона для расписания отключения индикаторов (Dim LED). 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

<i>PROFILE-NAME</i>	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 (Dim LED). Если расписание настроено, все индикаторы порта будут отключены.

Пример

В данном примере показано, как добавить профиль временного диапазона для расписания отключения индикаторов.

```
Switch# configure terminal
Switch(config)# power-saving dim-led time-range off-duty
Switch(config)#
```

65.5 power-saving hibernation time-range

Данная команда используется для настройки профиля временного диапазона для расписания режима сна системы (Hibernation). Используйте форму **no**, чтобы удалить профиль указанного диапазона времени.



Примечание: данная функция не поддерживается коммутаторами, объединенными в физический стек.

power-saving hibernation time-range *PROFILE-NAME*
no power-saving hibernation time-range *PROFILE-NAME*

Параметры

<i>PROFILE-NAME</i>	Укажите имя профиля временного диапазона, который необходимо настроить. 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 не действуют сетевые функции. Будет работать только консольное соединение через порт RS232. Коммутатор, являющийся питающим устройством Power Sourcing Equipment (PSE), не будет обеспечивать порты электропитанием.

Пример

В данном примере показано, как добавить профиль временного диапазона для расписания режима сна системы.

```
Switch# configure terminal
Switch(config)# power-saving hibernation time-range off-duty
Switch(config)#
```

65.6 power-saving shutdown time-range

Данная команда используется, чтобы настроить профиль временного диапазона для расписания отключения порта (port shutdown). 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

<i>PROFILE-NAME</i>	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 (port shutdown). Если расписание настроено, указанный порт будет отключен.

Пример

В данном примере показано, как добавить профиль временного диапазона для расписания отключения порта.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# power-saving shutdown time-range off-duty
Switch(config-if)#
```

65.7 show power-saving

Данная команда используется для отображения информации о настройках энергосбережения.

show power-saving [link-detection] [length-detection] [dim-led] [port-shutdown] [hibernation] [eee]

Параметры

link-detection	(Опционально.) Укажите, чтобы отобразить настройки энергосбережения в зависимости от статуса соединения.
length-detection	(Опционально.) Укажите, чтобы отобразить настройки энергосбережения в зависимости от длины кабеля.
dim-led	(Опционально.) Укажите, чтобы отобразить настройки энергосбережения за счет отключения индикаторов.
port-shutdown	(Опционально.) Укажите, чтобы отобразить настройки энергосбережения за счет отключения порта.
hibernation	(Опционально.) Укажите, чтобы отобразить настройки энергосбережения для режима сна.
eee	(Опционально.) Укажите, чтобы отобразить настройки энергосбережения для функции EEE.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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

Function Version: 3.00

Link Detection Power Saving
  State: Disabled

Length Detection Power Saving
  State: Disabled

Scheduled Hibernation Power Saving
  State: Disabled

Administrative Dim-LED
  State: Enabled

Scheduled Dim-LED Power Saving
  State: Disabled

Scheduled Port-shutdown Power Saving
  State: Disabled

EEE_Enabled Ports

Switch#
```

66. Команды PPPoE Circuit-ID Tag Insertion

66.1 pppoe circuit-id-insert

Данная команда используется для включения PPPoE Circuit ID Insertion.

```
pppoe circuit-id-insert  
no pppoe circuit-id-insert
```

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для глобального включения PPPoE Circuit ID Insertion. Чтобы включить PPPoE Circuit Insertion на интерфейсе, используйте команду **pppoe circuit-id-insert** в режиме Interface Configuration Mode. PPPoE Circuit ID Insertion будет включена на интерфейсе, если функция настроена и глобально, и на интерфейсе.

Если PPPoE Circuit ID Insertion включена на интерфейсе, при получении PPPoE-пакетов PADI/PADR без поля Circuit ID коммутатор вставит поле Circuit ID и перенаправит пакеты. PPPoE-пакеты PADO/PADS с полем Circuit ID будут перенаправлены только после удаления поля.

Пример

В данном примере показано, как включить PPPoE Circuit ID Insertion глобально.

```
switch# configure terminal  
switch(config)# pppoe circuit-id-insert
```

В примере ниже показано, как отключить PPPoE Circuit ID Insertion глобально.

```
switch# configure terminal  
switch(config)# no pppoe circuit-id-insert
```

66.2 pppoe circuit-id-insert (interface)

Данная команда используется для включения PPPoE Circuit ID Insertion в режиме Interface Configuration Mode.

```
pppoe circuit-id-insert  
no pppoe circuit-id-insert
```

Параметры

Нет.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить PPPoE Circuit ID Insertion на интерфейсе физического порта. PPPoE Circuit ID Insertion будет включена на интерфейсе, если функция настроена и глобально, и на интерфейсе. Для глобального включения функции используйте команду **pppoe circuit-id-insert** в режиме Global Configuration Mode.

Если PPPoE Circuit ID Insertion включена на интерфейсе, при получении PPPoE-пакетов PADI/PADR без поля Circuit ID коммутатор вставит поле Circuit ID и перенаправит пакеты. PPPoE-пакеты PADO/PADS с полем Circuit ID будут перенаправлены только после удаления поля.

Пример

В данном примере показано, как включить PPPoE Circuit ID Insertion на интерфейсе Ethernet 1/0/1.

```
switch# configure terminal
switch(config)# interface ethernet 1/0/1
switch(config-if)# pppoe circuit-id-insert
```

В примере ниже показано, как отключить PPPoE Circuit ID Insertion на интерфейсе Ethernet 1/0/1.

```
switch# configure terminal
switch(config)# interface ethernet 1/0/1
switch(config-if)# no pppoe circuit-id-insert
```

66.3 pppoe circuit-id-insert format

Данная команда используется для настройки Circuit ID на определенном порту.

pppoe circuit-id-insert format { ip | mac | udf STRING }
no pppoe circuit-id-insert format

Параметры

ip	Укажите для использования IP-адреса в качестве содержимого опции Circuit ID.
mac	Укажите для использования MAC-адреса интерфейса VLAN 1 управления в качестве содержимого опции Circuit ID.

udf STRING Укажите для использования пользовательской строки в качестве содержимого опции Circuit ID. Максимальное количество символов – 32.

По умолчанию

По умолчанию настроен IP-адрес коммутатора, параметр **ip**.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда применяется для настройки интерфейса физического порта.

Пример

В данном примере показано, как настроить формат поля PPPoE Circuit ID на интерфейсе Ethernet 1/1. Настроенный формат – MAC-адрес устройства.

```
switch# configure terminal
switch(config)#interface ethernet 1/1
switch(config-if)# pppoe circuit-id-insert format mac
```

66.4 show pppoe circuit-id-insert

Данная команда используется для отображения настроек PPPoE Circuit ID Insertion.

show pppoe circuit-id-insert [interface INTERFACE-ID [, | -]]

Параметры

interface INTERFACE-ID	(Опционально.) Укажите интерфейс или диапазон интерфейсов, настройки PPPoE Circuit ID Insertion которых необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения настроек PPPoE Circuit ID Insertion. Если в качестве ключевых слов в команде указан ID интерфейса, будут отображены настройки указанного интерфейса/диапазона интерфейсов. Если интерфейсы не указаны, будут отображены глобальные настройки PPPoE Circuit ID Insertion.

Пример

В данном примере показано, как отобразить глобальные настройки PPPoE Circuit ID Insertion.

```
switch# show pppoe circuit-id-insert
Global PPPoE State : Enabled
```

В примере ниже показано, как отобразить глобальные настройки PPPoE Circuit ID Insertion на интерфейсах Ethernet 1/1 — Ethernet 1/4.

```
switch# show pppoe circuit-id-insert interface ethernet 1/0/1-4
Interface          State      Circuit ID Type  User Defined String
-----
eth1/1             Enabled   Switch  MAC
eth1/2             Enabled   Switch  IP
eth1/3             Enabled   udf      12345678901234567890123456789012
eth1/4             Disabled  Switch  IP
```

67. Команды Private VLAN

67.1 private-vlan

Данная команда 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 Isolated VLAN не могут обмениваться информацией друг с другом и с портами других Community VLAN на 2 уровне.
primary	Укажите для настройки VLAN в качестве Primary в домене Private VLAN.

По умолчанию

Нет.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Частный домен VLAN определяется одной основной (Primary) VLAN, одной изолированной (Isolated) VLAN и несколькими общедоступными (Community) VLAN. Используйте данную команду, чтобы указать роль Private VLAN перед дальнейшей настройкой Private VLAN с помощью других команд.

Пример

В данном примере показано, как настроить VLAN в качестве Private VLAN. VLAN 1000, VLAN 1001 и VLAN 1002 настроены в качестве Primary VLAN, Isolated VLAN и Community VLAN соответственно.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 1001
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 1002
Switch(config-vlan)# private-vlan community
Switch(config-vlan)#
```

67.2 private-vlan association

Данная команда 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 ID второстепенной VLAN: от 2 до 4094.
remove SECONDARY-VLAN-ID	Укажите, чтобы удалить связь указанной второстепенной сети VLAN с основной сетью VLAN.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона 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

Только одна Isolated VLAN может быть связана с основной сетью VLAN. Несколько общедоступных (Community) VLAN могут быть связаны с основной (Primary) VLAN. Второстепенная VLAN может быть связана только с одной основной (Primary) VLAN.

Пример

В данном примере показано, как связать второстепенную VLAN 1001 и второстепенную VLAN 1002 с основной VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# private-vlan association add 1001-1002
Switch(config-vlan)#
```

67.3 private-vlan synchronize

Данная команда используется для синхронизации второстепенных VLAN, чтобы 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)#
```

67.4 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.

switchport mode private-vlan {host | promiscuous}

Параметры

host	Укажите порт в качестве isolated port или community port.
promiscuous	Укажите порт в качестве promiscuous port.

По умолчанию

По умолчанию данная опция настроена в режиме Hybrid VLAN Mode.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для портов isolated или community используйте команду **switchport mode private-vlan host**, чтобы указать режим порта, и команду **switchport private-vlan host-association**, чтобы связать порт с второстепенной VLAN и основной VLAN.

Для порта promiscuous 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.

При смене режима интерфейса настройки, связанные с предыдущим режимом, будут утеряны.

Пример

В данном примере показано, как настроить физические порты в качестве портов Private VLAN. Здесь интерфейс Ethernet 1/0/1 указан как host port для Private VLAN, а интерфейс Ethernet 1/0/2 указан как promiscuous port для Private VLAN.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# exit
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)#
```

67.5 switchport private-vlan host-association

Данная команда используется для связи Private VLAN спортом 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 доступных ID: от 2 до 4094.
SECONDARY-VLAN-ID	Укажите ID второстепенной VLAN, которую необходимо ассоциировать. Диапазон доступных ID: от 2 до 4094.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Порт является isolated портом, если второстепенная VLAN, указанная в команде, будет являться Isolated VLAN. Порт является community портом, если второстепенная VLAN, указанная командой, является Community VLAN.

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)#
```

67.6 switchport private-vlan mapping

Данная команда используется для ассоциирования членства 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

add <i>SECONDARY-VLAN-ID</i>	Укажите, чтобы добавить членство в указанной второстепенной VLAN. Диапазон доступных ID Secondary VLAN: от 2 до 4094.
remove <i>SECONDARY-VLAN-ID</i>	Укажите, чтобы удалить членство в указанной второстепенной VLAN.
,	(Опционально.) Используется для перечисления нескольких VLAN или отделения одного диапазона номеров VLAN от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона номеров VLAN. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Команда настроит порт в качестве нетегированного члена указанной основной VLAN и маркировки 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)#
```

67.7 show vlan private-vlan

Данная команда используется для просмотра настроек Private VLAN.

show vlan private-vlan

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения списка Private VLAN, находящегося в домене VLAN, ассоциации второстепенного VLAN с основным VLAN и портов каждого Private VLAN.

Пример

В данном примере показано, как включить отображение настроек Private VLAN. В данном примере настроено 2 домена Private VLAN.

```
Switch#show vlan private-vlan
```

Primary VLAN	Secondary VLAN	Type	Interface
1000	1001	Isolated	eth1/0/1, eth1/0/16
	1002	Community	
	1003	Community	
2000	2001	Isolated	eth1/0/2, eth1/0/3
2000	2002	Community	eth1/0/2, eth1/0/3
2000	2003	Community	eth1/0/4, eth1/0/13, eth1/0/15

```
Total Entries: 6
```

```
Switch#
```


68. Команды Protocol Independent

68.1 distance

Данная команда используется, чтобы настроить административное расстояние (administrative distance) для протоколов маршрутизации, включая RIP and BGP. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

distance *DISTANCE*
no distance

Параметры

<i>DISTANCE</i>	Укажите административное расстояние. Диапазон значений: от 1 до 255.
-----------------	--

По умолчанию

Расстояние подключенного маршрута по умолчанию – 0.

Расстояние intra-area route протокола Open Shortest Path First (OSPF) по умолчанию – 80.

Расстояние inter-area route протокола OSPF по умолчанию – 90.

Расстояние type-1 AS external route протокола OSPF по умолчанию – 110.

Расстояние type-2 AS external route протокола OSPF по умолчанию – 115.

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. Маршрут, значение расстояния которого ниже, имеет более высокий приоритет, чем маршрут со значением выше. Маршруты, расстояние которых равно 255, не будут установлены для маршрутизации пакетов, поскольку в данном случае маршруты не являются доверенными. Если команда 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)#
```

68.2 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

<i>DISTANCE</i>	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 рейтинг надежности маршрута. В качестве расстояния может быть указано целое число от 1 до 255. Маршрут, значение расстояния которого ниже, имеет более высокий приоритет, чем маршрут со значением выше. Маршруты, расстояние которых равно 255, не будут установлены для маршрутизации пакетов, поскольку в данном случае маршруты не являются доверенными. Если команда применяется без параметров, указанным расстоянием будет значение маршрута по умолчанию настроенного протокола.

Пример

В данном примере показано, как настроить расстояние статического маршрута по умолчанию. Указанное расстояние – 150.

```
Switch#configure terminal
Switch(config)#distance default 150
Switch(config)#
```

68.3 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

<i>DISTANCE</i>	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 рейтинг надежности маршрута. В качестве расстояния может быть указано целое число от 1 до 255. Маршрут, значение расстояния которого ниже, имеет более высокий приоритет, чем маршрут со значением выше. Маршруты, расстояние которых равно 255, не будут установлены для маршрутизации пакетов, поскольку в данном случае маршруты не являются доверенными. Если команда применяется без параметров, указанным расстоянием будет значение маршрута по умолчанию настроенного протокола.

Пример

В данном примере показано, как настроить расстояние статического маршрута. Указанное расстояние – 100.

```
Switch# configure terminal
Switch(config)# distance static 100
Switch(config)#
```

68.4 distribute-list in

Данная команда используется, чтобы настроить список distribute list для фильтрации обновлений маршрута протокола 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

<i>ACCESS-LIST-NAME</i>	Укажите имя стандартного списка доступа IP, определяющего, какие полученные обновления маршрута должны быть приняты, а какие – анонсированы.
<i>INTERFACE-ID</i>	(Опционально.) Укажите интерфейс, к которому необходимо применить настроенный список distribute list.

По умолчанию

Нет.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если список доступа был применен к интерфейсу с использованием **distribute-list in** в команде, обновления маршрута, полученные указанным интерфейсом, фильтруются на основе списка доступа. Если ID интерфейса указан, список distribute list будет применен к указанному интерфейсу. Если ID интерфейса не указан, список distribute list будет применен ко всем интерфейсам.

Пример

В данном примере показано, как настроить список доступа для фильтрации обновлений маршрута протокола RIP. Заданный список доступа – East-ranch.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# distribute-list East-ranch in
Switch(config-router)#
```

68.5 ip route

Данная команда используется для создания записи статического маршрута. Чтобы удалить запись статического маршрута, воспользуйтесь формой **no** этой команды.

ip route NETWORK-PREFIX NETWORK-MASK {IP-ADDRESS [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 (next hop), который будет использоваться для достижения сети назначения.
null0	Укажите маршрут black hole route.
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 weight, то по умолчанию для пути в хэш-таблице используется одна копия.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте **0.0.0.0 0.0.0.0**, чтобы указать маршрут по умолчанию.

Доступны плавающие маршруты. Это означает, что можно создать два маршрута с одним адресом сети назначения, но с разными следующими узлами (next hop).

Пример

В данном примере показано, как добавить запись статического маршрута. Сетевой адрес – 20.0.0.0/8. Следующий узел – 10.1.1.254.

```
Switch# configure terminal
Switch(config)# ip route 20.0.0.0 255.0.0.0 10.1.1.254
Switch(config)#
```

68.6 ipv6 route

Данная команда используется для создания записи статического маршрута IPv6. Чтобы удалить запись статического маршрута IPv6, воспользуйтесь формой **no** этой команды.

ipv6 route {default | NETWORK-PREFIX/PREFIX-LENGTH} {[INTERFACE-ID] NEXT-HOP-ADDRESS [{ primary | backup | weight NUMBER}] [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.) Укажите маршрут как основной маршрут к назначению.

backup	(Опционально.) Укажите маршрут как резервный маршрут к назначению.
weight <i>NUMBER</i>	(Опционально.) Укажите, чтобы создать статический маршрут ECMP. Значение веса (weight) всегда должно быть равно 1.
DISTANCE	(Опционально.) Укажите административное расстояние статического маршрута. Диапазон значений: от 1 до 254. Чем ниже значение, тем выше приоритет маршрута. Если значение не указано, административный путь статического маршрута по умолчанию – 1.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Доступны плавающие маршруты. Это означает, что можно создать два маршрута с одним адресом сети назначения, но с разными следующими узлами (next hop). Если ни один из параметров (**primary** или **backup**) не указан, роль статического маршрута (основной/резервный) будет назначена автоматически. Основным маршрутом (primary) является самый приоритетный и всегда используется для продвижения, если находится в активном режиме. Если основной маршрут неактивен, используется резервный маршрут (backup). Если вес (weight) указан, статический маршрут будет маршрутом ECMP. Маршрут, настроенный как маршрут ECMP, не может быть указан в качестве основного или резервного, и наоборот.

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)#
```

68.7 ip route ecmp advance-control mode

Данная команда используется для увеличения или уменьшения значения ECMP (многопутевой маршрутизации). Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

```
ip route ecmp advance-control mode {VALUE1 | VALUE2 | VALUE3 | VALUE4}
no ip route ecmp advance-control mode
```

Параметры

VALUE1 ... VALUE4	Укажите значение ECMP (многопутевой маршрутизации) и количество следующих узлов (next hop) каждого ECMP, чтобы изменить их в соответствии с указанным значением. Доступные значения: 512, 256, 128 и 64.
-------------------	--

По умолчанию

Значение по умолчанию – 128.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы увеличить или уменьшить значение ECMP (многопутевой маршрутизации).

Команда применима как для IPv4 ECMP, так и для IPv6 ECMP.

Пример

В данном примере показано, как настроить значение ECMP (многопутевой маршрутизации). Указанное значение – 512.

```
Switch#configure terminal
Switch(config)#ip route ecmp advance-control mode 512

WARNING: The command does not take effect until after the next reboot.
Switch(config)#
```

68.8 ip route ecmp load-balance

Данная команда используется, чтобы настроить хэш-алгоритм балансировки нагрузки для определения записи следующего узла (next hop) из разных путей для достижения одного назначения. 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	Укажите алгоритм балансировки нагрузки, включающий младшие 5 бит IP-адреса источника. Данный параметр и crc32_lower/crc32_upper являются взаимоисключающими. При указании sip параметры crc32_lower и crc32_upper будут отменены.
-----	---

crc32_lower	Укажите алгоритм балансировки нагрузки, включающий младшие 5 бит CRC. Данный параметр и crc32_upper/sip являются взаимоисключающими. При указании crc32_lower параметры crc32_upper и sip будут отменены.
crc32_upper	Укажите алгоритм балансировки нагрузки, включающий старшие 5 бит CRC. Данный параметр и crc32_lower/sip являются взаимоисключающими. При указании crc32_upper параметры crc32_lower и sip будут отменены.
dip	Укажите алгоритм балансировки нагрузки, включающий IP-адрес назначения.
port	Укажите алгоритм балансировки нагрузки, включающий TCP-порт или UDP-порт.

По умолчанию

По умолчанию используется параметр **sip**.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить хэш-алгоритм балансировки нагрузки для определения записи следующего узла (next hop) из разных путей для достижения одного назначения.

Пример

В данном примере показано, как настроить алгоритм балансировки нагрузки. Указанный алгоритм – **dip**.

```
Switch#configure terminal
Switch(config)#ip route ecmp load-balance dip
Switch(config)#
```

68.9 show ip route

Данная команда используется для отображения записи в таблице маршрутизации.

show ip route [[IP-ADDRESS [MASK] | PROTOCOL]]

Параметры

IP-ADDRESS	(Опционально.) Укажите сетевой адрес, информацию о маршрутизации которого необходимо отобразить.
-------------------	--

<i>MASK</i>	(Опционально.) Укажите маску подсети для указанной сети.
<i>PROTOCOL</i>	(Опционально.) Укажите протокол маршрутизации или ключевые слова: static, connected.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

В таблицу маршрутизации занесены маршруты, информация о которых была получена из разных протоколов. При достижении одной сети несколькими маршрутами для маршрутизации пакетов будет назначен лучший маршрут, расстояние которого имеет более высокий приоритет, а следующий узел (next hop) доступен. Расстояние и следующий узел являются текущей записью маршрута. То есть, если следующий узел маршрута с самым приоритетным расстоянием недоступен, данный маршрут будет заменен другим маршрутом, расстояние которого будет следующим по значению приоритета.

Пример

В данном примере показано, как отобразить таблицу маршрутизации.

```
Switch#show ip route
Code: C - Connected, S - Static , R - RIP
      O - OSPF Derived, IA - OSPF Inter Area
      E1 - OSPF External Type 1, E2 - OSPF External Type 2
      N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
      * - candidate default, > - Selected route

Gateway of last resort is not set

S    170.10.0.0/16 [60/1] via 11.0.0.2, vlan 11
O    1.0.0.0/8 [80/2] via 11.0.0.1, vlan 11
O    2.0.0.0/8 [80/2] via 11.0.0.1, vlan 11
C    11.0.0.0/8 is directly connected, vlan 11
O    12.0.0.0/8 [80/3] via 11.0.0.1, vlan 11
O    13.0.0.0/8 [80/3] via 11.0.0.1, vlan 11
O    17.0.0.0/8 [80/3] via 11.0.0.1, vlan 11
O    18.0.0.0/8 [80/3] via 11.0.0.1, vlan 11
O    30.0.0.0/8 [80/2] via 11.0.0.1, vlan 11
O    40.0.0.0/8 [80/3] via 11.0.0.1, vlan 11
R    105.100.0.0/24 [100/2] via 11.0.0.5, vlan 11
C    107.100.0.0/16 is directly connected, vlan 1
C    172.18.64.0/21 is directly connected, mgmt_ipif
R    212.254.254.0/24 [100/2] via 11.0.0.254, vlan 11

Total Entries: 15

Switch#
```

68.10 show ip route summary

Данная команда используется для отображения краткой информации о текущих записях маршрутизации.

show ip route summary

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

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            1
Total          15
Multi-path      0

Switch#
```

68.11 show ipv6 route

Данная команда используется для отображения записи в таблице маршрутизации.

show ipv6 route **[[IPV6-ADDRESS | NETWORK-PREFIX]****IPPREFIX-LENGTH | INTERFACE-ID |**
PROTOCOL] [database]

Параметры

<i>IPV6-ADDRESS</i>	(Опционально.) Укажите IPv6-адрес, чтобы найти самый длинный префикс соответствующего IPv6-маршрута.
<i>NETWORK-PREFIX</i>	(Опционально.) Укажите сетевой адрес, информацию о маршрутизации которого необходимо отобразить.
<i>PREFIX-LENGTH</i>	(Опционально.) Укажите длину префикса для указанной сети.
<i>INTERFACE-ID</i>	(Опционально.) Укажите тип интерфейса.
<i>PROTOCOL</i>	(Опционально.) Укажите протокол маршрутизации.
database	(Опционально.) Укажите, чтобы отобразить все связанные записи в базе данных маршрутизации, а не только самый приоритетный маршрут.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

В таблицу маршрутизации занесены маршруты, информация о которых была получена из разных протоколов. При достижении одной сети несколькими маршрутами для маршрутизации пакетов будет назначен лучший маршрут, расстояние которого имеет более высокий приоритет, а следующий узел (next hop) доступен. Расстояние и следующий узел являются текущей записью маршрута. То есть, если следующий узел маршрута с самым приоритетным расстоянием недоступен, данный маршрут будет заменен другим маршрутом, расстояние которого будет следующим по значению приоритета.

Пример

В данном примере показано, как отобразить записи маршрутизации для IPv6.

```
Switch#show ipv6 route

IPv6 Routing Table
Code: C - connected, S - static, R - RIP
      SLAAC - Stateless address autoconfiguration

      O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
      ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2, K - kernel
      P - Net Prototype
S    1234::/64 [1/1] via FE80::206:28FF:FED8:FEAC, vlan 11
R    2000:17::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan 11
R    2000:18::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan 11
C    2001:DB8:0:5::/64 [0/1] is directly connected, vlan 11
O    2001:DB8:0:5::1/128 [110/10] via FE80::206:28FF:FED8:FE94, vlan 11
R    2001:DB8:0:3600::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan 11
R    2001:DB8:0:3620::/64 [71/2] via FE80::206:28FF:FED8:FE94, vlan 11
R    2016:3130::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan 11

Total Entries: 8 entries, 8 routes
Switch#
```

68.12 show ipv6 route summary

Данная команда используется для отображения текущего состояния таблицы маршрутизации IPv6.

show ipv6 route summary

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если система обслуживания обеспечивает продвижение IPv6-трафика, необходимо проверить таблицу переадресации/маршрутизации для выявления пути трафика, который будет применяться 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
SLAAC	0
OSPF	4
Total	16
Multi-path	0

```
Switch#
```

69. Команды Protocol Independent Multicast (PIM)

69.1 ip pim

Данная команда используется для включения PIM на интерфейсе для работы в разреженном (Sparse Mode, SM) режиме. Чтобы отключить данную функцию на интерфейсе, воспользуйтесь формой **no** этой команды.

```
ip pim {sparse-mode}
no ip pim
```

Параметры

sparse-mode	Укажите, чтобы включить режим SM.
--------------------	-----------------------------------

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 настроенным IP-адресом.

Разреженный режим (Sparse Mode). Когда многоадресный (multicast) трафик принимается на интерфейсе в режиме Sparse Mode, маршрутизатором первого перехода (First Hop Router) будет отправлено регистрационное (register) 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).

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)#
```

69.2 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(config)# interface vlan100
Switch(config-if)# ip pim bsr-border
```

Настройки можно проверить с помощью команды **show ip pim interface**.

69.3 ip pim bsr-candidate

Данная команда используется для назначения роли Candidate BSR маршрутизатору. Чтобы отменить назначение роли Candidate BSR маршрутизатору, воспользуйтесь формой **no** этой команды.

```
ip pim [vrf VRF-NAME] bsr-candidate INTERFACE-ID [HASH-MASK-LENGTH [PRIORITY] ]
[interval SECONDS]
no ip pim [vrf VRF-NAME] bsr-candidate
```

Параметры

vrf VRF-NAME	(Опционально.) Укажите экземпляр многоадресной VPN-маршрутизации и пересылки (VRF).
INTERFACE-ID	Укажите интерфейс, IP-адрес которого будет анонсирован как адрес BootStrap Router (BSR).
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 Candidate BSR. 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 Candidate BSR.

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 BSR.

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.



Примечание: команда доступна, только если указанный интерфейс существует.

Пример

В данном примере показано, как настроить IP-адрес маршрутизатора, которому назначена роль Candidate BSR, на интерфейсе VLAN 1 с длиной хэш-маски 20, приоритетом 192 и интервалом 120 секунд.

```
Switch(config)# ip pim bsr-candidate vlan1 20 192 interval 120
```

69.4 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

<i>PRIORITY</i>	Укажите значение приоритета DR в диапазоне от 0 до 2147483647. 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 качестве DR назначается маршрутизатор с наивысшим значением приоритета. Если несколько маршрутизаторов имеют наивысший приоритет, то DR становится маршрутизатор с наибольшим значением IP-адреса. Если существует маршрутизатор, у которого отсутствует значение приоритета в сообщениях hello, 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)#
```

69.5 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

<i>SECONDS</i>	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 во время подключения к сети или соединения. 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. Настроенное значение – 120 секунд.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip pim jp-timer 120
Switch(config-if)#
```

69.6 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, указанные для многоадресной рассылки IP, отправляют сообщения hello, чтобы обнаружить другие маршрутизаторы PIM. В режиме SM Mode сообщения hello также используются для определения назначенного маршрутизатора в каждом сегменте локальной сети. Заданный интервал запросов (Query Interval) 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 (Query Interval). Настроенное значение – 45 секунд.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip pim query-interval 45
Switch(config-if)#
```

69.7 ip pim rp-address

Данная команда используется, чтобы настроить статический адрес RP для многоадресных (multicast) групп. Для удаления адреса RP воспользуйтесь формой **no** этой команды.

ip pim rp-address *IP-ADDRESS* [*GROUP-ADDRESS GROUP-MASK* **[override]**]
no ip pim rp-address *IP-ADDRESS*

Параметры

<i>IP-ADDRESS</i>	Укажите IP-адрес RP.
<i>GROUP-ADDRESS</i> <i>GROUP-MASK</i>	(Опционально.) Укажите IP-адрес multicast-группы. Если адрес группы не указан, RP будет привязана ко всем multicast-группам.
override	(Опционально.) Укажите, чтобы отдать приоритет статическому RP и запретить использование динамических RP для заданной группы.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для статической привязки (mapping) 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.

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 pim rp-address 10.90.90.90 225.2.2.2 255.255.255.255
Switch(config)#
```

69.8 ip pim rp-candidate

Данная команда используется для назначения роли Candidate RP маршрутизатору. Чтобы отменить назначение, воспользуйтесь формой **no** этой команды.

ip pim rp-candidate {*INTERFACE-ID* [*GROUP-ADDRESS GROUP-MASK*] | *interval SECONDS* | *priority PRIORITY* | *wildcard-prefix-cnt* {0 | 1}}

no ip pim rp-candidate [*INTERFACE-ID*] [*GROUP-ADDRESS GROUP-MASK*] | *interval* | *priority* | *wildcard-prefix-cnt*}

Параметры

<i>INTERFACE-ID</i>	Укажите интерфейс, IP-адрес которого будет анонсирован как адрес Candidate RP (C-RP).
<i>GROUP-ADDRESS GROUP-MASK</i>	(Опционально.) Укажите IP-адрес multicast-группы. Если адрес группы не указан, коммутатор будет назначен Candidate RP для всех групп.
<i>interval SECONDS</i>	Укажите интервал между объявлениями Candidate RP. Диапазон значений: от 1 до 255 секунд. Если интервал не указан, значение по умолчанию – 60 секунд.
<i>priority PRIORITY</i>	Укажите значение приоритета RP. Диапазон значений: от 0 до 255. Если приоритет не указан, значение по умолчанию – 192.
<i>wildcard-prefix-cnt</i>	Укажите для установки в сообщении C-RP префикса произвольной

wildcard-группы (224.0.0.0/4). Доступны значения: 1 или 0. Значение по умолчанию – 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 применима исключительно на интерфейсе в режиме PIM-SM. 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. Префикс группы (239.0.0.0/8), ассоциирован с RP, имеющей адрес интерфейса VLAN 1.

```
Switch# configure terminal
Switch(config)# ip pim rp-candidate vlan1 239.0.0.1 255.255.255.0
Switch(config)#
```

69.9 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.

Любой режим конфигурирования.

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
Switch#show ip pim

PIM Information:

Register Probe Time: 10 seconds
Register Suppression Time: 60 seconds
Register Keepalive Time on RP: 190 seconds
SPT Threshold: 0

PIM Configurations:

RP Address (Not configured)

RP Candidate
priority: 192, interval: 60 seconds, wildcard-prefix-cnt: 0
(Not configured)
BSR Candidate
vlan1, hash-mask-length: 20, priority: 192, interval: 200 seconds
```

69.10 show ip pim bsr-router

Данная команда используется для отображения информации о BSR.

show ip pim bsr-router [candidate] elected]

Параметры

candidate	Укажите, чтобы отобразить информацию о таблице PIM BSR Candidate.
elected	Укажите, чтобы отобразить информацию о таблице PIM BSR Elected.

По умолчанию

Нет.

Режим ввода команды

EXEC Mode.
Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения информации о выбранном BSR и объявлениях (advertisement) 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 candidate
BSR Address..... 10.90.90.90
  BSR Priority..... 192
  BSR Hash Mask Length..... 20
  C-BSR Advertisement Interval (secs)..... 200
  Next Bootstrap message (hh:mm:ss)..... NA
Switch#
```

69.11 show ip pim interface

Данная команда используется для отображения информации об интерфейсе.

show ip pim interface [sparse-mode] [INTERFACE-ID] [detail]

Параметры

sparse-mode	(Опционально.) Укажите, чтобы отобразить информацию только для режима PIM Sparse Mode.
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.
Любой режим конфигурирования.

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

Nbr Cnt: Neighbor Count
Address      Interface    Mode    Nbr DR      DR      Generation
              Cnt Priority
-----
20.0.2.10    vlan1100    SM      0    1      20.0.2.10    1523416782

Total Entries: 1

Switch#
```

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

```
Switch#show ip pim interface detail

vlan1100
  Address      : 20.0.2.10
  PIM          : Enabled
  Mode         : Sparse
  Neighbor Count : 0
  DR           : 20.0.2.10
  DR Priority   : 1
  Generation ID : 1523416782
  Query Interval : 30 seconds
  Join Prune timer : 60 seconds
  BSR Domain Border : Disabled

Total Entries: 1

Switch#
```

69.12 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.

Любой режим конфигурирования.

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 - No DR Priority Present,
      G - Generation ID
Neighbor      Interface      Uptime/Expires      Ver DR Pri/Mode
-----
20.0.1.20     vlan1101      0DT00H01M45S/0DT00H01M29S v2  1 /DR,G

Total Entries: 1

Switch#
Switch#
```

69.13 show ip pim rp mapping

Данная команда используется для отображения точек встреч (Rendezvous Point, RP) и привязок (mapping) групп к RP.

show ip pim rp mapping

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить активные точки встречи (Rendezvous Point, RP), связанные с записями в таблице multicast-маршрутизации. Команда также применяется для отображения информации о привязках (mapping) RP, существующих на маршрутизаторе.

Пример

В данном примере показано, как отобразить точки встречи RP и привязки групп к RP.

```
Switch# show ip pim rp mapping

Group(s): 225.2.2.2/32
  RP: 10.90.90.90
  Info source: Static

Group(s): 239.0.0.1/32
  RP: 20.0.1.10
  Info source: 20.0.1.10, via bootstrap, priority 192
  Uptime: 00DT00H02M30S, expires: 00DT00H02M27S

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 о RP будет удалена. Если за это время маршрутизатором не получено сообщений об обновлении, информация о данной RP будет удалена.

69.14 show ip pim rp-hash

Данная команда используется для отображения RP, 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.

Любой режим конфигурирования.

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 239.0.0.1.

```
Switch# show ip pim rp-hash 239.0.0.1

Rp: 20.0.1.10
Info source: 20.0.1.10, via bootstrap
Uptime: 00DT00H00M00S, expires: 00DT00H00M00S

Switch#
```

В примере ниже показано, как отобразить RP с адресом группы 225.2.2.2.

```
Switch# show ip pim rp-hash 225.2.2.2

Rp: 10.90.90.90
Info source: Static

Switch#
```

70. Команды качества обслуживания (QOS)

70.1 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)#
```

70.2 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)#
```

70.3 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 <i>ACCESS-LIST-NAME</i>	name Укажите список доступа в качестве критерия соответствия. Трафик, разрешенный указанным списком доступа, будет классифицирован.
cos [inner] <i>COS-LIST</i>	Укажите значение (-я) определенного IEEE 802.1Q в качестве критерия соответствия. Диапазон значений: от 0 до 7. Для перечисления нескольких значений CoS используется запятая, а для обозначения диапазона значений – дефис. inner – (Опционально.) Укажите, чтобы сопоставить внутренний CoS пакетов QinQ с маркировкой 2 уровня класса обслуживания (Class of Service, CoS).
[ip] dscp <i>DSCP-LIST</i>	Укажите значения DSCP-метки в качестве критерия соответствия. 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 <i>PRECEDENCE-LIST</i>	<i>IP-</i> 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 <i>NAME</i>	<i>PROTOCOL-</i> 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.

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 использоваться 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 ethernet 1/0/1
Switch(config-if)# service-policy input cos-based-treatment
Switch(config-if)#
```

70.4 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

<i>NAME</i>	Укажите имя правила aggregate policing. Максимально допустимое количество символов – 32. Символы, используемые в данном параметре, чувствительны к регистру. Имена aggregate policer не должны совпадать и начинаться с цифры. Первым символом в имени обязательно должна быть буква.
<i>KBPS</i>	Укажите среднюю скорость в Кбит/с.
<i>BURST-NORMAL</i>	(Опционально.) Укажите нормальный размер всплеска (burst). Единица измерения – Кбайт.
<i>BURST-MAX</i>	(Опционально.) Укажите максимальный размер всплеска (burst). Единица измерения – Кбайт.
<i>CIR</i>	Укажите гарантированную полосу пропускания (committed information rate) в Кбит/с. Данный параметр является первым в алгоритме «корзина маркеров» (token bucket) для two-rate Metering.
<i>PIR</i>	Укажите пиковую скорость передачи (peak information rate) в Кбит/с. Данный параметр является вторым в алгоритме «корзина маркеров» (token bucket) для two-rate Metering.
<i>CONFORM-BURST</i>	(Опционально.) Укажите размер всплеска (burst) для первого параметра алгоритма «корзина маркеров» (token bucket). Единица измерения – Кбайт.
<i>PEAK-BURST</i>	(Опционально.) Укажите размер всплеска (burst) для второго параметра алгоритма «корзина маркеров» (token bucket). Единица измерения – Кбайт.
conform-action	(Опционально.) Укажите, чтобы действие было выполнено к green color packets (пакетам, «окрашенным» в зелёный цвет). Если не указано, будет применено действие по умолчанию transmit (передача пакетов).
exceed-action	Укажите, чтобы действие было выполнено к пакетам, превышающим разрешенную скорость. Если при использовании two rate policer данный параметр не указан, будет применено действие по умолчанию drop (отбрасывание).
violate-action	(Опционально.) Укажите, чтобы при использовании single rate policing действие было выполнено к пакетам, нормальный и максимальный размеры всплеска которых не соответствуют заданным параметрам. Укажите, чтобы действие было выполнено к пакетам, не соответствующим обоим параметрам CIR и PIR. Если при использовании single rate policer данный параметр не указан, будет создан single rate two color policer. Если при использовании two rate policer данный параметр не указан, будет применено действие по умолчанию drop (отбрасывание).

ACTION Укажите, чтобы действие было выполнено к пакетам. Ниже указаны ключевые слова:

drop – отбрасывание пакетов.

set-dscp-transmit *VALUE* – устанавливает значение IP DSCP и передает пакет с новым 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)#
```

70.5 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 ethernet 1/0/1
Switch(config-if)# mls qos cos 3
Switch(config-if)#
```

70.6 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 ethernet 1/0/1
Switch(config-if)# mls qos dscp-mutation mutemap1
Switch(config-if)#
```

70.7 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. Несколько значений CoS могут быть отделены запятой или списком диапазонов.
-----------------	--

green	Укажите для привязки к зеленому цвету.
yellow	Укажите для привязки к желтому цвету.
red	Укажите для привязки к красному цвету.

По умолчанию

По умолчанию все значения CoS привязаны к зеленому цвету.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Пакеты, поступающие на входной порт, могут быть «окрашены» на основе цветовой привязки DSCP (если порт является доверенным портом DSCP) или на основе цветовой привязки CoS (если порт является доверенным портом CoS).

Используйте данную команду в режиме Interface Configuration Mode, чтобы настроить цветовую привязку CoS. Если входной порт является доверенным портом CoS, полученный пакет будет инициализирован с цветом на основе настроенной привязки.

Пример

В данном примере показано, как настроить цветовую привязку CoS пакетов, поступающих на интерфейс Ethernet 1/0/1. Пакеты со значением CoS от 1 до 7 привязаны к красному цвету, а пакеты со значением 0 – к зеленому.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# mls qos map cos-color 1-7 to red
Switch(config-if)#
```

70.8 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 <i>DSCP-LIST</i>	Укажите список DSCP-меток для привязки к цвету. Диапазон значений: от 0 до 63. Несколько значений DSCP могут быть отделены запятой или списком диапазонов.
------------------------------	--

green	Укажите для привязки к зеленому цвету.
--------------	--

yellow	Укажите для привязки к желтому цвету.
---------------	---------------------------------------

red	Укажите для привязки к красному цвету.
------------	--

По умолчанию

По умолчанию привязка не настроена. Все значения DSCP привязаны к зеленому цвету.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда 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 ethernet 1/0/1
Switch(config-if)# mls qos map dscp-color 61-63 to yellow
Switch(config-if)#
```

70.9 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 <i>DSCP-LIST</i> to <i>COS-VALUE</i>	Укажите список DSCP-меток для привязки к значению CoS. Диапазон значений: от 0 до 63. Несколько DSCP могут быть отделены запятой (,) или дефисом (-). Пробелы до и после дефиса недопустимы.
---	--

<i>DSCP-LIST</i>	Укажите диапазон DSCP-меток.
------------------	------------------------------

По умолчанию

Значение CoS:	0	1	2	3	4	5	6	7
Значение DSCP:	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда позволяет привязать DSCP-метку доверенного порта DSCP к значению внутреннего CoS. Данное значение CoS будет привязано к очереди CoS на основе CoS в карте очереди, настроенной в команде **priority-queue cos-map**.

Пример

В данном примере показано, как привязать DSCP к CoS на интерфейсе Ethernet 1/0/6. DSCP-метки 12, 16 и 18 привязаны к CoS 1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/6
Switch(config-if)# mls qos map dscp-cos 12,16,18 to 1
Switch(config-if)#
```

70.10 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

<i>MAP-NAME</i>	Укажите имя карты DSCP Mutation без пробелов. Максимальное количество символов – 32.
<i>INPUT-DSCP-LIST</i>	Укажите список DSCP, значения которых необходимо «мутировать». Диапазон значений: от 0 до 63. Несколько DSCP могут быть отделены запятой (,) или дефисом (-). Пробелы до и после дефиса недопустимы.
<i>OUTPUT-DSCP</i>	Укажите значение DSCP, которое будет применено после «мутации» Mutation. Диапазон значений: от 0 до 63.

По умолчанию

По умолчанию параметры *OUTPUT-DSCP* и *INPUT-DSCP* равны.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Значение внутреннего DSCP пакета, полученного на интерфейсе, будет изменено на основе карты DSCP Mutation перед другими QoS-операциями. DSCP Mutation способствует объединению доменов с разными назначениями DSCP.

При настройке карты DSCP Mutation обратите внимание на то, что для каждого нового значения DSCP, которых нужно изменить, и для каждого нового значения, которые будут применены после «мутации» Mutation, необходимо использовать команду несколько раз.

Привязки DSCP-CoS и DSCP-color будут основываться на исходном DSCP пакета, а все последующие действия – на значении DSCP, которое будет применено после «мутации» Mutation.

Пример

В данном примере показано, как преобразовать DSCP 30 в DSCP 8 и DSCP 20 в DSCP 10. Имя карты Mutation – mutemap1.

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutemap1 30 to 8
Switch(config)# mls qos map dscp-mutation mutemap1 20 to 10
Switch(config)#
```

70.11 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 один раз.

Обслуживание всех пакетов прекращается, когда их счетчики достигают нуля или становятся меньше нуля, а также после полного осуществления передачи последнего пакета. При выполнении данного условия к каждому счетчику в очереди CoS будет добавлено значение quantum кредитов. Значение quantum для каждой очереди может отличаться в зависимости от пользовательских настроек.

Для включения режима Strict Priority для очереди CoS необходимо, чтобы для всех других очередей CoS с более высоким приоритетом также был установлен режим Strict Priority.

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 ethernet 1/0/1
Switch(config-if)# mls qos scheduler sp
Switch(config-if)#
```

70.12 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 ethernet 1/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)#
```

70.13 police

Данная команда используется для настройки Traffic Policing (ограничения трафика) с использованием single rate. Чтобы отменить 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

<i>KBPS</i>	Укажите среднюю скорость в Кбит/с.
<i>BURST-NORMAL</i>	(Опционально.) Укажите нормальный размер всплеска (burst). Единица измерения – Кбайт.
<i>BURST-MAX</i>	(Опционально.) Укажите максимальный размер всплеска (burst). Единица измерения – Кбайт.
conform-action	(Опционально.) Укажите, чтобы действие было выполнено к green color packets (пакетам «окрашенным» в зелёный цвет). Если не указано, будет выполнено действие по умолчанию transmit (передача пакетов).
exceed-action	Укажите, чтобы действие было выполнено к yellow color packets (пакетам, «окрашенным» в желтый цвет), превышающим разрешенную скорость.
violate-action	(Опционально.) Укажите, чтобы действие было выполнено к red color packets (пакетам, «окрашенным» в красный цвет). Если данный параметр не указан, используется single rate two color policer. Если данный параметр указан, используется single rate three color policer.
<i>ACTION</i>	Укажите, чтобы действие было выполнено к пакетам. Ниже указаны ключевые слова: drop – отбрасывание пакетов. set-dscp-transmit <i>VALUE</i> – устанавливает значение IP DSCP и передает пакет с новым 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. 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 пакетов 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 ethernet 1/0/1
Switch(config-if)# service-policy input police-setting
Switch(config-if)#
```

70.14 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

по 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)#
```

70.15 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

<i>CIR</i>	Укажите гарантированную полосу пропускания (committed information rate) в Кбит/с. Данный параметр является первым в алгоритме «корзина маркеров» (token bucket) для two-rate Metering.
<i>PIR</i>	Укажите пиковую скорость передачи (peak information rate) в Кбит/с. Данный параметр является вторым в алгоритме «корзина маркеров» (token bucket) для two-rate Metering.
<i>CONFORM-BURST</i>	(Опционально.) Укажите размер всплеска (burst) для первого параметра алгоритма «корзина маркеров» (token bucket). Единица измерения – Кбайт.
<i>PEAK-BURST</i>	(Опционально.) Укажите размер всплеска (burst) для второго параметра алгоритма «корзина маркеров» (token bucket). Единица измерения – Кбайт.
conform-action	(Опционально.) Укажите, чтобы действие было выполнено к green color packets (пакетам, «окрашенным» в зелёный цвет). Если не указано, будет выполнено действие по умолчанию transmit (передача пакетов).
exceed-action	(Опционально.) Укажите, чтобы действие было выполнено к yellow color packets (пакетам, «окрашенным» в желтый цвет), которые соответствуют PIR, но не соответствуют CIR. Если не указано, будет выполнено действие по умолчанию drop (отбрасывание).
violate-action	(Опционально.) Укажите, чтобы действие было выполнено к red color packets (пакетам, «окрашенным» в красный цвет), которые не соответствуют CIR и PIR. Если не указано, будет выполнено действие по умолчанию drop (отбрасывание).
<i>ACTION</i>	(Опционально.) Укажите, чтобы действие было выполнено к пакетам. Ниже указаны ключевые слова: drop – отбрасывание пакетов. set-dscp-transmit VALUE – устанавливает значение IP DSCP и передает пакет с новым 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 ethernet 1/0/3
Switch(config-if)# service-policy output policy1
Switch(config-if)#
```

70.16 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 данную команду, чтобы войти в режим Policy-map Configuration Mode и настроить/изменить политику для класса трафика. Одна карта политики может быть привязана к нескольким интерфейсам одновременно. Предыдущие привязки карты политики будут перезаписаны новыми.

Карты политики содержат классы трафика, которые включают в себя одну или более команд для соответствия пакетов и для организации пакетов в группы на основе типа протокола или приложения.

Пример

В данном примере показано, как создать карту политики под именем «policy» и настроить для нее две политики класса. Первый класс «class1» указывает политику для трафика, соответствующего списку управления доступом (ACL) «acl_rd». Второй класс является классом по умолчанию «class-default». В данный класс включены пакеты, которые не соответствуют настроенным классам.

```
Switch# configure terminal
Switch(config)# class-map class1
Switch(config-cmap)# match access-group name acl_rd
Switch(config-cmap)# exit
Switch(config)# policy-map policy
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 46
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 00
Switch(config-pmap-c)#
```

70.17 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)#
```

70.18 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.
<i>MIN-BANDWIDTH-KBPS</i>	Укажите минимальную разрешенную полосу пропускания в Кбит/с для указанной очереди.
<i>MAX-BANDWIDTH-KBPS</i>	Укажите максимальную полосу пропускания в Кбит/с для указанной очереди.
<i>MIN-PERCENTAGE</i>	Укажите минимальную полосу пропускания в процентах. Диапазон значений: от 1 до 100.
<i>MAX-PERCENTAGE</i>	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 ethernet 1/0/1
Switch(config-if)# queue 1 rate-limit 100 2000
Switch(config-if)# queue 2 rate-limit percent 10 percent 50
Switch(config-if)#
```

70.19 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.
<i>NUMBER-KBPS</i>	Укажите ограничение максимальной полосы пропускания в Кбит/с.
<i>PERCENTAGE</i>	Укажите для настройки ограничения в процентах. Диапазон значений: от 1 до 100.
<i>BURST-SIZE</i>	(Опционально.) Укажите ограничение для трафика всплеска (burst). Единица измерения – Кбайт.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Настроенное ограничение не должно превышать максимальную скорость на указанном интерфейсе. Если полученный трафик превышает 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 ethernet 1/0/5
Switch(config-if)# rate-limit input 2000 4096
Switch(config-if) #
```

70.20 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

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 ethernet 1/0/1
Switch(config-if)# service-policy input cust1-classes
Switch(config-if)# exit
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# service-policy input cust1-classes
Switch(config-if)#
```

Настроенная карта политики «cust2-classes» привязана к интерфейсу Ethernet 1/0/1 для входящего трафика.

```
Switch# configure terminal
Switch(config)# policy-map cust2-classes
Switch(config-pmap)# class gold
Switch(config-pmap-c)# police 1600 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# police 4000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze
Switch(config-pmap-c)# police 16000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# service-policy input cust2-classes
Switch(config-if)#
```

70.21 set

Данная команда используется для настройки полей нового приоритета (precedence), DSCP и CoS исходящего пакета. Также возможна настройка очереди CoS для пакета.

```
set {[ip] precedence PRECEDENCE | [ip] dscp DSCP | cos COS | cos-queue COS-QUEUE}  
no set {[ip] precedence PRECEDENCE | [ip] dscp DSCP | cos COS | cos-queue COS-QUEUE}
```

Параметры

precedence <i>PRECEDENCE</i>	Укажите новый приоритет пакета. Диапазон значений: от 0 до 7. Если указано ключевое слово ip , будет отмечен приоритет IPv4. Если не указано, будут отмечены приоритеты IPv4 и IPv6. Для пакетов IPv6 приоритетом являются три наиболее значимых бита класса трафика заголовка IPv6. Настройка приоритета не повлияет на выбор очереди CoS.
dscp <i>DSCP</i>	Укажите новый DSCP пакета. Диапазон значений: от 0 до 63. Если указано ключевое слово ip , будет отмечен IPv4 DSCP. Если не указано, будут отмечены IPv4 и IPv6 DSCP. Настройка DSCP не повлияет на выбор очереди CoS.
cos <i>COS</i>	Укажите новое значение CoS пакета. Диапазон значений: от 0 до 7. Настройка CoS не повлияет на выбор очереди CoS.
cos-queue <i>COS-QUEUE</i>	Укажите очередь CoS для пакетов. Новое значение очереди CoS заменит первоначальное. Очередь CoS не будет назначена, если карта политики привязана к исходящему потоку на интерфейсе.

По умолчанию

Нет.

Режим ввода команды

Policy-map Class Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду 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)# exit
Switch(config-pmap)#
```

70.22 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.

Любой режим конфигурирования.

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 «с3». IP-пакеты принадлежат настроенному классу «с2».


```
Switch# show class-map

Class Map match-any class-default
  Match any

Class Map match-all c2
  Match protocol ip

Class Map match-all c3
  Match access-group acl_home_user

Switch#
```

70.23 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.

Любой режим конфигурирования.

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#
```


70.24 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} | queue-statistics }

Параметры

interface <i>INTERFACE-ID</i>	Укажите интерфейсы, которые необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
cos	Укажите, чтобы отобразить CoS по умолчанию.
scheduler	Укажите, чтобы отобразить настройки механизма обслуживания очереди передачи.
trust	Укажите, чтобы отобразить статус trust порта.
rate-limit	Укажите, чтобы отобразить ограничение полосы пропускания, настроенной для порта.
queue-rate-limit	Укажите, чтобы отобразить ограничение полосы пропускания, настроенной для очереди.
dscp-mutation	Укажите, чтобы отобразить карту DSCP Mutation, привязанную к интерфейсу.
map dscp-color	Укажите, чтобы отобразить цветовую привязку DSCP.
map cos-color	Укажите, чтобы отобразить цветовую привязку CoS.
map dscp-cos	Укажите, чтобы отобразить привязку DSCP к CoS.
queue-statistics	Укажите, чтобы отобразить статистику по портам для каждой очереди.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения настроек уровня QoS на указанном интерфейсе.

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 ethernet 1/0/2-5 cos
```

Interface	CoS	Override
eth1/0/2	3	Yes
eth1/0/3	4	No
eth1/0/4	4	No
eth1/0/5	3	No

```
Switch#
```

В 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 ethernet 1/0/2-1/0/5 trust
```

Interface	Trust State
eth1/0/2	trust DSCP
eth1/0/3	trust CoS
eth1/0/4	trust DSCP
eth1/0/5	trust CoS

```
Switch#
```

В 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 ethernet 1/0/1-1/0/2 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 ethernet 1/0/1-2 dscp-mutation
```

Interface	DSCP Mutation Map
eth1/0/1	Mutate Map 1
eth1/0/2	Mutate Map 2

```
Switch#
```

В 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 ethernet 1/0/1-4 rate-limit
```

Interface	Rx Rate	Tx Rate	Rx Burst	Tx Burst
eth1/0/1	1000 kbps	No Limit	64 kbyte	No Limit
eth1/0/2	No Limit	2000 kbps	No Limit	2000 kbyte
eth1/0/3	10%(100000 kbps)	20%(200000 kbps)	64 kbyte	64 kbyte
eth1/0/4	2%	2000 kbps	64 kbyte	64 kbyte

```
Switch#
```

В 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 ethernet 1/0/1-2 queue-rate-limit
```

```
eth1/0/1
```

QID	Min Bandwidth	Max Bandwidth
0	-	-
1	16 kbps	10%(100000 kbps)
2	32 kbps	-
3	2%	50%
4	64 kbps	-
5	64 kbps	-
6	32 kbps	-
7	128 kbps	-

```
eth1/0/2
```

QID	Min Bandwidth	Max Bandwidth
0	-	-
1	16 kbps	-
2	32 kbps	-
3	32 kbps	-
4	64 kbps	-
5	64 kbps	-
6	32 kbps	-
7	128 kbps	-

```
Switch#
```

В следующем примере показано, как отобразить цветовую привязку DSCP для интерфейсов Ethernet 1/0/1 и Ethernet 1/0/2.

```
Switch# show mls qos interface ethernet 1/0/1-2 map dscp-color

eth1/0/1
  DSCP 0-7 are mapped to green
  DSCP 8-40 are mapped to red
  DSCP 41-43 are mapped to yellow
eth1/0/2
  DSCP 0 - 7 are mapped to green

Switch#
```

В нижеприведенном примере показано, как отобразить цветовую привязку CoS для интерфейсов Ethernet1/0/3 и Ethernet 1/0/4.

```
Switch# show mls qos interface ethernet 1/0/3-4 map cos-color

eth1/0/3
  CoS 0,1,2 are mapped to green
  CoS 3-4 are mapped to yellow
  CoS 6 are mapped to red
eth1/0/4
  CoS 0,1-6 are mapped to green

Switch#
```

В нижеследующем примере показано, как отобразить привязку DSCP к CoS для интерфейса Ethernet 1/0/1.

```
Switch# show mls qos interface ethernet 1/0/1 map dscp-cos

eth1/0/1
0  1  2  3  4  5  6  7  8  9
-----
00  00 00 00 00 00 00 00 00 01 01
10  01 01 01 01 01 01 01 02 02 02
20  02 02 02 02 03 03 03 03 03 01
30  03 03 04 04 04 04 04 04 04 04
40  05 05 05 05 05 05 05 05 06 06
50  06 06 06 06 06 06 07 07 07 07
60  07 07 07 07

Switch#
```

В примере ниже показано, как отобразить статистику очереди для интерфейса Ethernet 1/0/1.

```
Switch# show mls qos interface ethernet 1/0/1 queue-statistics

eth1/0/1
QID   Min Bandwidth   Packets/sec   Total packets   Drop packets
      Max Bandwidth Bytes/sec     Total Bytes     Drop Bytes
-----
0      0               0             0               0
      0               0             0               0
1      0               0             0               0
      0               0             0               0
2      0               0             0               0
      0               0             0               0
3      0               0             0               0
      0               0             0               0
4      0               0             0               0
      0               0             0               0
5      0               0             0               0
      0               0             0               0
6      0               0             0               0
      0               0             0               0
7      0               0             0               0
      0               0             0               0

Switch#
```

70.25 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.
Любой режим конфигурирования.

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  10 02 10 04 05 06 07 08 09
10  11 12 13 14 15 16 17 18 19
20  21 22 23 24 25 26 27 28 29
30  31 32 33 34 35 36 37 38 39
40  41 42 43 44 45 46 47 48 49
50  51 52 53 54 55 56 57 58 59
60  61 62 63

Switch#
```

70.26 show mls qos queueing

Данная команда используется, чтобы отобразить информацию об очередях QoS и настроек веса (weight) для разных алгоритмов обслуживания очередей на определенном интерфейсе или интерфейсах.

show mls qos queueing [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите ID интерфейса, для которого необходимо отобразить информацию о настройках веса (weight) разных алгоритмов обслуживания очередей.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

При указании ключевого слова **interface**, на определенном интерфейсе или интерфейсах будет отображен настроенный вес для разных алгоритмов обслуживания очередей (WRR или WDRR). Если **interface** не указан, отображается только системная карта привязки CoS к ID очереди.

Режим Scheduling, который настроен при помощи команды **mls qos scheduler**, определяет, какие настройки будут действовать для веса. Используйте команду **show mls qos interface scheduler**, чтобы отобразить настроенный алгоритм обслуживания очередей на интерфейсе.

Пример

В данном примере показано, как отобразить информацию об очередях QoS.

```
Switch#show mls qos 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
```

```
wdr bandwidth weights:
```

```
QID  Quantum
```

```
---  -
```

```
0      1
```

```
1      1
```

```
2      1
```

```
3      1
```

```
4      1
```

```
5      1
```

```
6      1
```

```
7      1
```

```
Switch#
```

70.27 show policy-map

Данная команда используется для отображения настроек карты политики.

show policy-map [*POLICY-NAME* | **interface** *INTERFACE-ID*]

Параметры

<i>POLICY-NAME</i>	(Опционально.) Укажите имя карты политики. Если не указано, будут отображены все карты политики.
--------------------	--

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите модуль и номер порта.
--------------------------------------	--

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1

Использование команды

Используйте данную команду, чтобы отобразить политики класса, настроенные для карты политики. Также команда применяется для отображения настроек политики класса определенных или всех существующих карт политики обслуживания.

Пример

В данном примере показано, как настроить two-rate Traffic Policing в карте политики под именем «policy1» для класса «police». Для ограничения трафика 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 ethernet 1/0/1
Router(config-if)# service-policy output policy1
Router(config-if)#
```

В примере ниже показано, как отобразить карту политики, настроенную в примере выше. Имя заданной карты политики – policy1.

```
Switch#show policy-map policy1

Policy Map policy1
Class Map police
police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-transmit 2
violate-action drop

Switch#
```

В следующем примере показано, как отобразить все карты политики на интерфейсе Ethernet 1/0/1.

```
Switch#show policy-map interface ethernet 1/0/1

Policy Map: policy1 : output
Class Map police
police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-transmit 2
violate-action drop

Switch#
```

70.28 wdr 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.

```
wdr queue bandwidth QUANTUM1...QUANTUM8
no wdr 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 wdr**.

Пример

В данном примере показано, как настроить значения quantum для очередей в режиме обслуживания очередей WDRR на интерфейсе Ethernet 1/0/1. Для очереди 0 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 ethernet 1/0/1
Switch(config-if)# mls qos scheduler wdr
Switch(config-if)# wdr queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

70.29 wrr queue bandwidth

Данная команда используется, чтобы настроить вес (weight) для очередей, обслуживаемых механизмом WRR. Для возврата к настройкам по умолчанию 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.

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 ethernet 1/0/1
Switch(config-if)# mls qos scheduler wrr
Switch(config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

70.30 hol-prevention

Данная команда используется, чтобы включить функцию HoL (Head-of-Line) Prevention на коммутаторе. Для отключения функции воспользуйтесь формой **no** этой команды.

hol-prevention

no hol-prevention

Параметры

Нет.

По умолчанию

Функция HoL Prevention по умолчанию включена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Head-of-line blocking (HOL blocking) – это событие, ограничивающее производительность, которое происходит, когда очередь пакетов приостанавливается из-за первого пакета.

Коммутаторы с буферизацией ввода могут подвергаться блокировке HOL, так как для перенаправления доступен только пакет, отправленный первым, (FIFO). Последующие пакеты не могут быть перенаправлены, если самый ранний пакет не будет перенаправлен из-за занятого выходного порта назначения (Congestion). Данное событие повлечет за собой снижение производительности системы.

При включении функции HoL Prevention пакеты потенциально могут быть переданы в обход застрявшего старого пакета к их соответствующим пунктам назначения.

Пример

В данном примере показано, как включить функцию HoL Prevention на коммутаторе.

```
Switch# configure terminal
Switch(config)# hol-prevention
```

71. Команды перезагрузки (Reboot)

71.1 reboot

Данная команда используется для перезагрузки коммутатора.

```
reboot [ <unit> | [force_agree] ]
```

Параметры

unit	(Опционально.) Укажите конфигурируемый модуль коммутатора.
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...
```

71.2 reboot schedule

Данная команда используется для настройки расписания перезагрузки. Чтобы отменить расписание перезагрузки, воспользуйтесь формой **no** этой команды.

```
reboot schedule {in MINUTES | at HH:MM [DDMTHYYYY]} [save_before_reboot]
no reboot schedule
```

Параметры

in MINUTES	Укажите период времени, по истечении которого будет выполнена перезагрузка коммутатора. Диапазон значений: от 1 до 43200 минут.
at	Укажите точную дату и время для перезагрузки коммутатора.

Запланированная перезагрузка должна быть выполнена в течение 30 дней.

HH:MM	Укажите время перезагрузки коммутатора.
DDMMTHYYYY	(Опционально.) Введите дату перезагрузки коммутатора. Если дата не указана, перезагрузка будет выполнена в указанное время текущего дня. Если указанное время прошло, перезагрузка выполняется на следующий день.
save_before_reboot	Укажите, чтобы сохранить все настройки перед перезагрузкой коммутатора.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить расписание перезагрузки. После перезагрузки коммутатора в журнале появится сообщение о том, что система была перезагружена при помощи команды **reboot schedule**.

Расписание перезагрузки не сохраняется в файле конфигурации и удаляется автоматически после перезагрузки или отключения коммутатора. Также указанное расписание перезагрузки отменяется, если коммутатор был отключен или перезагружен вручную перед применением данного расписания.

Пример

В данном примере показано, как сохранить настройки перед перезагрузкой коммутатора, которая будет выполнена через 10 минут.

```
Switch# reboot schedule in 10 save_before_reboot
Switch#
```

В данном примере показано, как настроить перезагрузку на 23:00, 27 апреля 2018 г.

```
Switch# reboot schedule at 23:00 27apr2018
Switch#
```

71.3 show reboot schedule

Данная команда используется для отображения настроек расписания перезагрузки.

show reboot schedule

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения настроек расписания перезагрузки.

Пример

В данном примере показано, как отобразить настройки расписания перезагрузки.

```
Switch#show reboot schedule

Reboot Schedule Settings
-----
Reboot scheduled at 27 Apr 2018 23:00:00 (in 35363 minutes)
Save before reboot: No

Switch#
```

72. Команды Remote Network MONitoring (RMON)

72-1 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

<i>INDEX</i>	Укажите индекс таблицы RMON. Диапазон значений: от 1 до 65535.
<i>owner NAME</i>	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

Номер записи группы статистики RMON является динамическим. Соответствующая запись в таблице будет доступна только на интерфейсе с включенной статистикой RMON.

Пример

В данном примере показано, как настроить запись статистики RMON на интерфейсе Ethernet 1/0/2. Индекс – 65. Имя владельца – guest.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# rmon collection stats 65 owner guest
Switch(config-if)#
```

72.2 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

<i>INDEX</i>	Укажите индекс таблицы RMON. Диапазон значений: от 1 до 65535.
<i>owner NAME</i>	Укажите имя владельца. Максимально допустимое количество символов в строке – 127.
<i>buckets NUM</i>	Укажите количество ячеек для сбора истории по группе статистики RMON. Диапазон значений: от 1 до 65535. Если не указано, используется значение по умолчанию – 50.
<i>interval SECONDS</i>	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

Номер записи группы статистики RMON является динамическим. Соответствующая запись в таблице будет доступна только на интерфейсе с включенной статистикой RMON. Настроенный интерфейс становится источником данных для созданной записи.

Пример

В данном примере показано, как включить сбор истории по группе статистики RMON MIB на интерфейсе Ethernet 1/0/8.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/8
Switch(config-if)# rmon collection history 101 owner it@domain.com interval 2000
Switch(config-if)#
```

72.3 rmon alarm

Данная команда используется, чтобы настроить запись уровня alarm (тревога) для мониторинга интерфейса. Для удаления записи 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

<i>INDEX</i>	Укажите индекс alarm. Диапазон значений: от 1 до 65535.
<i>VARIABLE</i>	Укажите идентификатор объекта переменной для выборки.
<i>INTERVAL</i>	Укажите интервал в секундах для выборки переменной и проверки соответствия пороговых значений. 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 <i>VALUE</i>	Укажите верхнее пороговое значение. Диапазон значений: от 0 до 2147483647.
<i>RISING-EVENT-NUMBER</i>	(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 <i>VALUE</i>	Укажите нижнее пороговое значение. Диапазон значений: от 0 до 2147483647.
<i>FALLING-EVENT-NUMBER</i>	(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 <i>STRING</i>	(Опционально.) Укажите строку владельца. Максимальное 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)#
```

72.4 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

<i>INDEX</i>	Укажите индекс записи события. Диапазон значений: от 1 до 65535.
log	(Опционально.) Укажите, чтобы генерировать сообщения в системном журнале для уведомлений.
trap <i>COMMUNITY</i>	(Опционально.) Укажите, чтобы генерировать сообщения SNMP trap для уведомлений. Максимальное количество символов – 127.
owner <i>NAME</i>	Укажите имя владельца. Максимальное количество символов – 127.
description <i>TEXT</i>	(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
Switch(config)#
```

72.5 show rmon alarm

Данная команда используется для отображения конфигурации alarm.

show rmon alarm

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить таблицу RMON alarm.

Пример

В данном примере показано, как отобразить таблицу RMON alarm.

```
Switch# show rmon alarm

Alarm index 23, owned by IT
  Monitors OID: 1.3.6.1.2.1.2.2.1.10.1
  every 120 second(s)
  Taking delta samples, last value was 2500
  Rising threshold is 2000, assigned to event 12
  Falling threshold is 1100, assigned to event 12
  On startup enable rising or falling alarm

Switch#
```

72.6 show rmon events

Данная команда используется для отображения таблицы событий RMON.

show rmon events

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить таблицу событий RMON.

Пример

В данном примере показано, как отобразить таблицу событий RMON.

```
Switch# show rmon events

Event 1, owned by manager1
  Description is Errors
  Event trigger action: log & trap sent to community manager
  Last triggered time: 13:12:15, 2013-03-02

Event 2, owned by manager2
  Description is Errors
  Event trigger action: log & trap
  Last triggered time:

Switch#
```

72.7 show rmon history

Данная команда используется для отображения информации об истории статистики RMON.

show rmon history

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить историю статистики для всех настроенных записей.

Пример

В данном примере показано, как отобразить историю статистики RMON Ethernet.

```
Switch# show rmon history

Index 23, owned by Manager, Data source is eth4/0/2
Interval: 30 seconds
Requested buckets: 50, Granted buckets: 50
Sample #1
  Received octets: 303595962, Received packets: 357568
  Broadcast packets: 3289, Multicast packets: 7287
  Estimated utilization: 19
  Undersized packets: 213, Oversized packets: 24
  Fragments: 2, Jabbers: 1
  CRC alignment errors: 0, Collisions: 0
Drop events : 0
Sample #2
  Received octets: 303596354, Received packets: 357898
  Broadcast packets: 3329, Multicast packets: 7337
  Estimated utilization: 19
  Undersized packets: 213, Oversized packets: 24
  Fragments: 2, Jabbers: 1
  CRC alignment errors: 0, Collisions: 0
Drop events : 0

Switch#
```

72.8 show rmon statistics

Данная команда используется для отображения статистики RMON Ethernet.

show rmon statistics

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статистику для всех настроенных записей.

Пример

В данном примере показано, как отобразить статистику RMON.

```
Switch# show rmon statistics

Index 32, owned by it@domain.com, Data Source is eth4/0/3
Received Octets : 234000, Received packets : 9706
Broadcast packets: 2266, Multicast packets: 192
Undersized packets: 213, Oversized packets: 24
Fragments: 2, Jabbers: 1
CRC alignment errors: 0, Collisions: 0
Drop events : 0
Packets in 64 octets: 256, Packets in 65-127 octets : 236
Packets in 128-255 octets : 129, Packets in 256-511 octets : 10
Packets in 512-1023 octets : 38, Packets in 1024-1518 octets : 2200

Switch#
```

72.9 snmp-server enable traps rmon

Данная команда используется для включения отправки RMON trap. Чтобы отключить отправки 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 отправки trap, уведомляющих о поднятии тревоги.
falling-alarm	(Опционально.) Укажите, чтобы настроить отправки trap, уведомляющих об отмене тревоги.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить/отключить отправку RMON trap.

Пример

В данном показано, как включить отправку RMON trap, уведомляющих о поднятии и об отмене тревоги.

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


73. Команды Route Map

73.1 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)#
```

73.2 match ip address

Данная команда используется для настройки правила соответствия маршрута на основе стандартного списка доступа IP. 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)#
```

73.3 match ip next-hop

Данная команда используется для настройки правила соответствия маршрутов следующему узлу (next hop) на основе стандартного списка доступа IP. Чтобы отменить правило, воспользуйтесь формой **no** этой команды.

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 в режиме Route-map Configuration Mode, чтобы настроить правило соответствия маршрутов следующему узлу, IP-адрес которого будет проверен в соответствии со стандартным списком доступа IP.

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)#
```

73.4 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)#
```

73.5 match ipv6 address

Данная команда используется для настройки правила соответствия маршрутов на основе стандартного списка доступа IPv6. Чтобы удалить 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 в режиме Route-map Configure Mode, чтобы настроить правило соответствия маршрутов списку доступа IPv6.

Пример

В данном примере показано, как создать список доступа IPv6 «myacl» и запись карты маршрутов с соответствием списку доступа IPv6.

```
Switch# configure terminal
Switch(config)# ipv6 access-list myacl
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 myacl
Switch(config-route-map)#
```

73.6 match ipv6 next-hop

Данная команда используется для настройки правила соответствия маршрутов следующему узлу (next hop) на основе стандартного списка доступа IPv6. Чтобы удалить 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 в режиме Route-map Configuration Mode, 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 «myacl» и запись карты маршрутов с соответствием следующему узлу (next hop) на основе списка доступа IPv6.

```
Switch# configure terminal
Switch(config)# ipv6 access-list myacl
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 next-hop myacl
Switch(config-route-map)#
```

73.7 match route-type

Данная команда используется для настройки правила соответствия типа маршрутов OSPF. Чтобы удалить правило, воспользуйтесь формой **no** этой команды.

```
match route-type {internal | external [type-1 | type-2] | nssa-external}
no match route-type
```

Параметры

internal	Укажите внутризонавые (intra-area) и межзонавые (inter-area) маршруты OSPF.
external	Укажите внешний маршрут автономной системы OSPF. 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.
nssa-external	Укажите маршрут nssa-external type-1 и type-2 OSPF.

По умолчанию

Нет.

Режим ввода команды

Route-map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте 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)#
```

73.8 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. Для удаления определенных следующих узлов по умолчанию воспользуйтесь формой **no** этой команды.

```
set ipv6 default next-hop IPV6-ADDRESS
no set ipv6 default next-hop
```

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. Команда доступна, только если политика маршрутизации включает в себя IPv6-пакеты.

Пример

В данном примере показано, как настроить следующий узел по умолчанию (default next hop) с соответствием списку доступа IPv6 «myacl».

```
Switch# configure terminal
Switch(config)# ipv6 access-list myacl
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 myacl
Switch(config-route-map)# set ipv6 default next-hop 2000::1
Switch(config-route-map)#
```

73.9 set ipv6 next-hop

Данная команда используется, чтобы настроить следующий узел (next hop) для маршрутизации пакетов, которые соответствуют настроенным правилам последовательностей карты маршрутов. Для удаления определенных следующих узлов воспользуйтесь формой **no** этой команды.

set ipv6 next-hop {IPv6-ADDRESS | recursive IPv6-ADDRESS}
no set ipv6 next-hop [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

Данная команда применяется для маршрутов на основе политики IPv6. Команда доступна, только если политика маршрутизации включает в себя пакеты IPv6.

Пример

В данном примере показано, как настроить следующий узел (next hop) с соответствием списку доступа IPv6 «myacl».

```
Switch# configure terminal
Switch(config)# ipv6 access-list myacl
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 myacl
Switch(config-route-map)# set ipv6 next-hop 2000::1
Switch(config-route-map)# exit
```

73.10 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*

no set ipv6 precedence

Параметры

NUMBER

Укажите одно из нижеперечисленных значений для заголовка IPv6:

- 0 – Routine
- 1 – Priority.
- 2 – Immediate.
- 3 – Flash.
- 4 – Flash-override.
- 5 – Critical.
- 6 – Internet.
- 7 – Network.

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.

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 ipv6 address myacl
Switch(config-route-map)# set ipv6 precedence 5
Switch(config-route-map)#
```

73.11 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

<i>VALUE</i>	Укажите метрику маршрута в диапазоне от 0 до 4294967294.
--------------	--

По умолчанию

Нет.

Режим ввода команды

Route-map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду в режиме Route-map Configuration Mode, чтобы настроить правило соответствия метрики маршрутов.

Пример

В данном примере показано, как создать запись карты маршрутов с соответствием метрике маршрутов.

```
Switch# configure terminal
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match metric 10
Switch(config-route-map)#
```

73.12 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)#
```

73.13 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.

Любой режим конфигурирования.

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#
```

73.14 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. Созданный список – Strict-Control. Затем создается карта маршрутов, соответствующая IP-адресу из списка доступа 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 vlan 100
Switch(config-if)# ip policy route-map myPolicy
Switch(config-if)#
```

73.15 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 следующих узлов 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

На маршрутизаторе возможна настройка нескольких next hop. Если next hop уже были настроены, новые настроенные next hop будут добавлены в список ранее настроенных узлов. Если первый указанный next hop на маршрутизаторе отключен, для маршрутизации пакетов будет выбран второй указанный next hop.

Пример

В данном примере показан процесс настройки политики PBR, с помощью которой пакеты будут отправлены на следующий узел (next hop) 120.1.2.2. IP-адрес источника – 10.1.1.0/24. Принимающий интерфейс – VLAN 100. Сначала создается основной список доступа IP, разрешающий префикс 10.1.1.0/24. Созданный список – Strict-Control. Затем создается карта маршрутов, соответствующая IP-

адресу из списка префиксов созданного списка «Strict-Control». 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 vlan 100
Switch(config-if)# ip policy route-map myPolicy
Switch(config-if)#
```

73.16 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)#
```

73.17 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. Для удаления определенных следующих узлов 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 узлов default next hop. Если узлы default next hop уже были настроены, новые настроенные узлы default next hop будут добавлены в список ранее настроенных узлов. Если первый указанный узел default next hop на маршрутизаторе отключен, для маршрутизации пакетов будет выбран второй указанный узел default next hop.

Пример

В данном примере показано, как настроить маршрут на основе политики IPv6.

```
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)#
```

73.18 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

<i>VALUE</i>	Укажите метрику маршрута в диапазоне от 0 до 4294967294.
--------------	--

По умолчанию

Нет.

Режим ввода команды

Route-map Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы изменить метрику маршрутов.

Пример

В данном примере показано, как настроить метрику маршрутов, которые соответствуют карте маршрутов. Настроенная метрика – 100.

```
Switch# configure terminal
Switch(config)# route-map example permit 10
Switch(config-route-map)# match ip address IPACL_01
Switch(config-route-map)# set metric 100
Switch(config-route-map)#
```


73.19 set metric-type

Данная команда используется для указания типа внешнего (external) маршрута автономной системы OSPF.

```
set metric-type {type-1 | type-2}
no set metric-type
```

Параметры

type-1	Укажите, чтобы использовать внешний маршрут OSPF с метрикой type-1.
type-2	Укажите, чтобы использовать внешний 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 автономной системы OSPF.

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)#
```

74. Команды Router Advertisement (RA) Guard

74.1 ipv6 nd raguard policy

Данная команда используется для создания политики Router Advertisement (RA) Guard Policy и 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)#
```

74.2 device-role

Данная команда используется для указания 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)#
```

74.3 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)#
```

74.4 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

<i>POLICY-NAME</i>	(Опционально.) Укажите имя политики RA Guard Policy.
--------------------	--

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Может быть применена только одна политика RA Policy. Если имя политики не указано, политика по умолчанию настроит устройство в качестве узла.

Пример

В данном примере показано, как применить политику RA Guard Policy на интерфейсе Ethernet 1/0/3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# ipv6 nd raguard attach-policy raguard1
Switch(config-if)#
```

74.5 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

<i>POLICY-NAME</i>	(Опционально.) Укажите имя политики Ipv6 RA Guard Policy.
--------------------	---

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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 «raguard1» на всех интерфейсах, на которых применена данная политика.

```
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)#
```

75. Команды Routing Information Protocol (RIP)

75.1 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

<i>METRIC-VALUE</i>	Укажите значение метрики по умолчанию в диапазоне от 0 до 16.
---------------------	---

По умолчанию

Значение по умолчанию – 0.

Режим ввода команды

Router Configuration Mode.

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)#
```

75.2 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

<i>DISTANCE</i>	Укажите административное расстояние в диапазоне от 1 до 255. Чем ниже значение, тем выше приоритет маршрута.
-----------------	--

По умолчанию

Расстояние RIP по умолчанию – 100.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить расстояние, которое представляет рейтинг надежности маршрута. В качестве расстояния может быть указано целое число от 1 до 255. Маршрут, значение расстояния которого ниже, имеет более высокий приоритет, чем маршрут со значением выше. Маршруты, расстояние которых равно 255, не будут установлены для маршрутизации пакетов, поскольку в данном случае маршруты не являются доверенными.

Пример

В данном примере показано, как настроить расстояние маршрутов RIP. Заданное значение – 100.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# distance 100
Switch(config-router)#
```

75.3 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 исключительно для RIP version 2. RIP version 1 не поддерживает аутентификацию.

Пример

В данном примере показано, как включить аутентификацию на интерфейсе VLAN 2.

```
Switch# configure terminal
Switch(config)# interface vlan 2
Switch(config-if)# ip rip authentication mode text
Switch(config-if)#
```

75.4 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

<i>PASSWORD</i>	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 vlan 3
Switch(config-if)# ip rip authentication mode text
Switch(config-if)# ip rip authentication text-password test1
Switch(config-if)#
```

75.5 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 vlan 1
Switch(config-if)# ip rip receive version 1 2
Switch(config-if)#
```

75.6 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 vlan 100
Switch(config-if)# ip rip send version 1
Switch(config-if)#
```

75.7 ip rip v2-broadcast

Данная команда используется для включения отправки пакетов обновлений RIP version 2 в качестве широковещательных пакетов, а не многоадресных 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 широковещательные пакеты вместо многоадресных пакетов в целях снижения нагрузки на ненужных узлах в локальной сети для обработки широковещательного пакета.

Используйте данную команду, чтобы настроить широковещательную рассылку обновлений RIP version 2 на 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 vlan 100
Switch(config-if)# ip rip send version 2
Switch(config-if)# ip rip v2-broadcast
Switch(config-if)#
```

75.8 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.

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)#
```

75.9 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. 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.

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 vlan 1
Switch(config-router)#
```

75.10 distribute-list (RIP)

Данная команда используется для фильтрации сетей в обновлениях маршрутизации. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

distribute-list *ACCESS-LIST-NAME* **in** *INTERFACE-NAME*
no redistribute-list *ACCESS-LIST-NAME* **in** *INTERFACE-NAME*

Параметры

<i>ACCESS-LIST-NAME</i>	Укажите имя списка доступа ACL.
in	Укажите для фильтрации входящих обновлений маршрутизации.
Interface name	Укажите имя интерфейса, на который приходит обновление.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду **distribute-list** для фильтрации анонсированных и обработанных маршрутов в обновлениях маршрутизации.

Пример

В данном примере показано, как использовать стандартный список доступа IP для фильтрации входящих обновлений маршрутизации.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# distribute-list Access01?
Switch(config-router)#
```

75.11 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

<i>PROTOCOL</i>	Укажите протокол, маршруты которого необходимо перераспределить. Доступны следующие ключевые слова: connected , ospf , static . Укажите static для перераспределения статических IP-маршрутов. Укажите connected для перераспределения маршрутов, установленных автоматически на основе настроек IP-адреса на интерфейсе.
metric <i>METRIC-VALUE</i>	(Опционально.) Укажите значение метрики для перераспределяемых маршрутов. Диапазон значений: от 0 до 16.
route-map <i>MAP-NAME</i>	(Опционально.) Укажите карту маршрута (route map) для фильтрации маршрутов, перераспределяемых в текущий протокол маршрутизации. Если не указано, будут перераспределены все маршруты.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Router Configuration Mode.

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)#
```

75.12 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 настроек 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)#
```

75.13 show ip rip database

Данная команда используется для отображения базы данных маршрутизации Routing Information Protocol (RIP).

show ip rip database [IP-ADDRESS MASK | NETWORK-PREFIX/PREFIX-LENGTH]

Параметры

<i>IP-ADDRESS MASK</i>	(Опционально.) Укажите адрес, информацию о маршрутизации которого необходимо отобразить.
<i>NETWORK-PREFIX/PREFIX-LENGTH</i>	(Опционально.) Укажите префикс подсети и длину префикса сети, которую необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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

   Network            Next Hop        Metric  From           If           Time
Rc  11.0.0.0/8
R   105.100.0.0/24     11.0.0.5          2       11.0.0.5       vlan11      0DT0H0M2S
Rc  107.100.0.0/16
R   212.254.254.0/24  11.0.0.254        2       11.0.0.254     vlan11      0DT0H0M10S

Total Entries: 4 entries, 4 routes

Switch#
```

75.14 show ip rip interface

Данная команда используется для отображения определенной информации о RIP на интерфейсе.

show ip rip interface

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется 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: Disable
    Authentication Mode: None
    Passive Interface: Disable
    IP Interface Address:
      11.0.0.3/255.0.0.0:

vlan1 is up, line protocol is up:
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Send v2-broadcast: Disable
    Authentication Mode: None
    Passive Interface: Disable
    IP Interface Address:
      107.100.0.1/255.255.0.0:

Total Entries : 2

Switch#
```

75.15 timers basic

Данная команда используется для настройки таймеров сетевого протокола RIP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

timers basic *UPDATE INVALID FLUSH*
no timers

Параметры

<i>UPDATE</i>	Укажите интервал update, по истечении которого будет отправлено сообщение с обновлениями. Диапазон значений: от 1 до 65535 секунд.
<i>INVALID</i>	Укажите таймер invalidate. Диапазон значений: от 1 до 65535 секунд.
<i>FLUSH</i>	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.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы изменить таймеры протокола RIP.

Пример

В данном примере показано, как настроить таймеры RIP. 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)#
```

75.16 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.

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)#
```

76. Команды Routing Information Protocol Next Generation (RIPng)

76.1 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#
```

76.2 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

<i>METRIC-VALUE</i>	Укажите значение метрики по умолчанию в диапазоне от 0 до 16.
---------------------	---

По умолчанию

Значение по умолчанию – 0.

Режим ввода команды

Router Configuration Mode.

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)#
```

76.3 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

<i>DISTANCE</i>	Укажите административное расстояние в диапазоне от 1 до 254. Чем ниже значение, тем выше приоритет маршрута.
-----------------	--

По умолчанию

Расстояние RIPng по умолчанию – 120.

Режим ввода команды

Router Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить расстояние, которое представляет рейтинг надежности маршрута. В качестве расстояния может быть указано целое число от 1 до 254. Маршрут, значение расстояния которого ниже, имеет более высокий приоритет, чем маршрут со значением выше.

Пример

В данном примере показано, как настроить расстояние маршрутов RIPv6. Настроенное значение – 100.

```
Switch# configure terminal
Switch(config)# ipv6 router rip
Switch(config-rtr)# distance 100
Switch(config-rtr)#
```

76.4 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 vlan 1
Switch(config-if)# ipv6 rip enable
Switch(config-if)#
```

76.5 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

<i>METRIC-VALUE</i>	Укажите значение, которое необходимо добавить к метрике маршрута IPv6 RIP, полученного на настраиваемом интерфейсе. Диапазон значений: от 0 до 16.
---------------------	--

По умолчанию

Значение по умолчанию – 1.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Метрика относится к счетчику промежуточных узлов. Перед вставкой полученного маршрута IPv6 RIP в таблицу маршрутизации, к метрике данного маршрута будет добавлено значение по умолчанию – 1. Используйте данную команду, чтобы настроить метрику маршрутов, полученных на разных интерфейсах. Данная настройка влияет на приоритет маршрута.

Пример

В данном примере показано, как настроить метрику с шагом 3 для маршрутов, полученных на VLAN 1.

```
Switch# configure terminal  
Switch(config)# interface vlan 1  
Switch(config-if)# ipv6 rip metric-offset 3  
Switch(config-if)#
```

76.6 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. Для отключения маршрутизации 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)#
```

76.7 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)#
```

76.8 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

<i>PROTOCOL</i>	Укажите протокол, маршруты которого необходимо перераспределить. Доступны следующие ключевые слова: connected , ospf , static . Укажите static для перераспределения статических IP-маршрутов. Укажите connected для перераспределения маршрутов, установленных автоматически на основе настроек IP-адреса на интерфейсе.
metric <i>METRIC-VALUE</i>	(Опционально) Укажите метрику для перераспределяемых маршрутов. 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)#
```

76.9 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 RIPv6 через интерфейс. Однако обработка пакетов RIPv6, полученных на данном интерфейсе от других маршрутизаторов, не будет приостановлена.

Пример

В данном примере показано, как отключить отставку обновлений маршрутизации на интерфейсе.

```
Switch#configure terminal
Switch(config)#ipv6 router rip
Switch(config-rtr)#passive-interface vlan 1
Switch(config-rtr)#
```

76.10 show ipv6 rip

Данная команда используется для отображения информации о RIPv6 на интерфейсе.

show ipv6 rip [database]

Параметры

database	(Опционально.) Укажите для отображения записи базы данных маршрутизации RIPv6.
-----------------	--

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию о настройках протокола RIPv6.

Для отображения записи базы данных маршрутизации RIPv6 примените команду **show ipv6 rip database**.

Пример

В данном примере показано, как отобразить информацию о настройках RIPv6.

```
Switch#show ipv6 rip

IPv6 RIP process, port 521, multicast-group FF02::9
  Administrative distance is 71
  Maximum paths is 16
  Updates every 30 seconds, expire after 180 seconds
  Garbage collect after 120 seconds
  Split horizon is on; poison reverse is on
  Periodic updates 6, trigger updates 1

Interfaces:
  vlan1
  vlan11      (passive)
Redistribution:
  Redistributing static with metric 10

Switch#
```

76.11 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)#
```

76.12 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 таймеры 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)#
```

76.13 debug ipv6 rip

Данная команда используется для включения функции отладки IPv6 RIP. Чтобы отключить функцию, 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#
```

76.14 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 vlan 1 has changed the link state to UP
```

76.15 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 FE80::1 , Index 1
```

76.16 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
```

76.17 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 об отладке.

Пример

В данном примере показано, как включить отладку маршрута IPv6 RIP на коммутаторе.


```
Switch#debug ipv6 rip route
Switch#
Switch#
  Add a RIPng route to V6 route table dst= 2016:3130:: nexthop= FE80::206:28FF:FED8:FEAC
Switch#
Switch#
```

77. Команды Safeguard Engine

77.1 clear cpu-protect counters

Данная команда используется для сброса счетчиков защиты ЦПУ.

```
clear cpu-protect counters {all | sub-interface [manage | protocol | route] | type [PROTOCOL-NAME]}
```

Параметры

all	Укажите для сброса всех счетчиков защиты ЦПУ.
sub-interface [manage protocol route]	Укажите для сброса счетчиков защиты ЦПУ под-интерфейсов. Если под-интерфейс не указан, будут сброшены счетчики защиты ЦПУ всех под-интерфейсов.
type [PROTOCOL-NAME]	Укажите для сброса счетчиков защиты ЦПУ определенного протокола. Если имя протокола не указано, будут сброшены 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#
```

77.2 cpu-protect safeguard

Данная команда используется для включения или настройки функции Safeguard Engine. Чтобы отключить функцию, 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.
<i>RISING-THRESHOLD</i>	(Опционально.) Укажите, чтобы установить значение в процентах верхнего порога загрузки ЦПУ, при котором включается функция Safeguard Engine. Если загрузка ЦПУ превысит указанное значение, механизм Safeguard Engine начнет функционировать. Диапазон значений: от 20 до 100.
<i>FALLING-THRESHOLD</i>	(Опционально.) Укажите, чтобы установить значение в процентах нижнего порога загрузки ЦПУ, при котором выключается функция Safeguard Engine. Если загрузка ЦПУ снизится до указанного значения, механизм Safeguard Engine перестанет функционировать. 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)#
```

77.3 cpu-protect sub-interface

Данная команда используется, чтобы настроить пропускную способность (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 пакетов для под-интерфейса управления (management). Указанное пороговое значение – 1000 пакетов в секунду.

```
Switch# configure terminal  
Switch(config)# cpu-protect sub-interface manage pps 1000  
Switch(config)#
```

77.4 cpu-protect type

Данная команда используется, чтобы настроить пропускную способность (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

<i>PROTOCOL-NAME</i>	Укажите имя протокола, который необходимо настроить.
<i>pps RATE</i>	Укажите пороговое значение. Единица измерения – пакеты в секунду. Если установлено значение 0, будут отброшены все пакеты указанного протокола.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

ЦПУ должно обрабатывать следующие пакеты: протоколы маршрутизации, протоколы 2 уровня и пакеты для управления. ЦПУ, перегруженное предназначенным для него трафиком, будет тратить много времени на обработку ненужного трафика, что повлияет на процессы маршрутизации. Чтобы уменьшить нагрузку на ЦПУ, используйте данную команду для настройки порогового значения пакетов указанного протокола.

В соответствии с назначением пакетов, предназначенных для ЦПУ, маршрутизатор создает три виртуальных под-интерфейса для обработки пакетов:

- **manage** – пакеты предназначены для любого интерфейса маршрутизатора или интерфейса системы управления сетью через протокол интерактивного доступа, такого как Telnet или SSH;
- **protocol** – 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.

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
gvrp	GARP VLAN Registration Protocol	Protocol
icmpv4	IPv4 Internet Control Message 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
pppoe	Point-to-Point Protocol over Ethernet	Protocol
rip	Routing Information Protocol	Protocol
snmp	Simple Network Management Protocol	Manage
ssh	Secured shell	Manage
stp	Spanning Tree Protocol (802.1D)	Protocol
telnet	Telnet	Manage
tftp	Trivial File Transfer Protocol	Manage
vrrp	Virtual Router Redundancy Protocol	Protocol
web	HTTP and HTTPS	Manage

Пример

В данном примере показано, как настроить пороговое значение пакетов протокола OSPF. Указанное пороговое значение – 100 пакетов в секунду.

```
Switch# configure terminal
Switch(config)# cpu-protect type ospf pps 100
Switch(config)#
```

77.5 show cpu-protect safeguard

Данная команда используется для отображения настроек и статуса функции Safeguard Engine.

show cpu-protect safeguard

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки и статус функции Safeguard Engine.

Пример

В данном примере показано, как отобразить настройки и текущий статус Safeguard Engine.

```
Switch#show cpu-protect safeguard

Safeguard Engine State: Disabled
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.
--------------------------------	---

77.6 show cpu-protect sub-interface

Данная команда используется для отображения пропускной способности (rate limit) и статистики под-интерфейса.

```
show cpu-protect sub-interface {manage | protocol | route}
```

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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

Total                               Drop
-----
103                                12

Switch#
```

77.7 show cpu-protect type

Данная команда используется для отображения пропускной способности (rate limit) и статистики защиты ЦПУ.

show cpu-protect type {*PROTOCOL-NAME*}

Параметры

PROTOCOL-NAME [UNIT- Укажите для отображения настроенного значения rate limit и статистики ID] указанного протокола СМ-карты и всех существующих IO-карт.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить 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
```

```
Total
```

```
Drop
```

```
0
```

```
0
```

```
Switch#
```

77.8 snmp-server enable traps safeguard-engine

Данная команда используется, чтобы включить отправку 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)#
```

78. Команды управления картой Secure Digital (SD)

В данной главе представлена конфигурация, связанная со съемными устройствами, включая USB-накопители для хранения данных.

78.1 sdcard-mgmt backup

Данная команда используется, чтобы войти в режим SD Card Management Backup Configuration Mode и создать/изменить запись резервного копирования по расписанию для управления SD-картой. Для удаления записи резервного копирования воспользуйтесь формой **no** этой команды.

sdcard-mgmt backup *ENTRY-NAME*
no sdcard-mgmt backup *ENTRY-NAME*

Параметры

<i>ENTRY-NAME</i>	Укажите имя записи резервного копирования по расписанию для управления SD-картой. 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 SD Card Management Backup Configuration Mode и создать/изменить запись резервного копирования по расписанию для управления SD-картой. Максимальное количество настраиваемых записей – 15.

Пример

В данном примере показано, как войти в режим SD Card Management Backup Configuration Mode и создать запись резервного копирования по расписанию для управления SD-картой.

```
Switch#configure terminal
Switch(config)#sdcard-mgmt backup entry1
Switch(config-sdcard-mgmt-backup)#
```

78.2 type

Данная команда используется для указания типа записи резервного копирования по расписанию.

type {configuration | log}

Параметры

configuration	Укажите, чтобы настроить запись резервного копирования для конфигурации.
log	Укажите, чтобы настроить запись резервного копирования для журнала.

По умолчанию

Нет.

Режим ввода команды

SD Card Management Backup Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы указать тип записи резервного копирования по расписанию.

Пример

В данном примере показано, как настроить запись резервного копирования для конфигурации.

```
Switch#configure terminal
Switch(config)#sdcard-mgmt backup entry1
Switch(config-sdcard-mgmt-backup)#type configuration
Switch(config-sdcard-mgmt-backup)#
```

78.3 sdcard-mgmt execute-config

Данная команда используется, чтобы войти в режим SD Card Management Execute Configuration Mode и создать/изменить запись принудительного применения конфигурации по расписанию для управления SD-картой. Для удаления записи воспользуйтесь формой **no** этой команды.

sdcard-mgmt execute-config *ENTRY-NAME*
no sdcard-mgmt execute-config *ENTRY-NAME*

Параметры

<i>ENTRY-NAME</i>	Укажите имя записи принудительного применения конфигурации по расписанию для управления SD-картой. 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 SD Card Management Execute Configuration Mode и создать/изменить запись принудительного применения конфигурации по расписанию для управления SD-картой. Максимальное количество настраиваемых записей – 15.

Пример

В данном примере показано, как войти в режим SD Card Management Execute Configuration Mode и создать запись принудительного применения конфигурации по расписанию для управления SD-картой.

```
Switch#configure terminal
Switch(config)#sdcard-mgmt execute-config execute_entry
Switch(config-sdcard-mgmt-execute)#
```

78.4 mode

Данная команда используется для настройки режима записи принудительного применения конфигурации по расписанию.

mode {increase | reset}

Параметры

increase	Укажите, чтобы текущая конфигурация не была сброшена перед принудительным применением конфигурации.
reset	Укажите, чтобы текущая конфигурация была сброшена перед принудительным применением конфигурации.

По умолчанию

Режим по умолчанию – **reset**.

Режим ввода команды

SD Card Management Execute Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить режим записи принудительного применения

конфигурации по расписанию.

Пример

В данном примере показано, как включить режим **increase** для записи принудительного применения конфигурации по расписанию.

```
Switch#configure terminal
Switch(config)#sdcard-mgmt execute-config execute_entry
Switch(config-sdcard-mgmt-execute)#mode increase
Switch(config-sdcard-mgmt-execute)#
```

78.5 time-range

Данная команда используется для указания временного диапазона расписания резервного копирования в режиме SD Card Management Backup Configuration Mode или расписания принудительного применения конфигурации в режиме SD Card Management Execute Configuration Mode.

time-range NAME

Параметры

NAME	Укажите имя временного диапазона.
------	-----------------------------------

По умолчанию

Нет.

Режим ввода команды

SD Card Management Backup Configuration Mode.

SD Card Management Execute Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если указанный временной интервал отсутствует, расписание будет создано без предупреждения, но оно не станет активным до момента создания соответствующего временного диапазона.

Пример

В данном примере показано, как указать временной диапазон расписания для резервного копирования конфигурации.

```
Switch#configure terminal
Switch(config)#sdcard-mgmt backup backentry
Switch(config-sdcard-mgmt-backup)#type configuration
Switch(config-sdcard-mgmt-backup)#time-range time1
Switch(config-sdcard-mgmt-backup)#
```

78.6 filename

Данная команда используется, чтобы указать имя файла назначения для резервного копирования конфигурации/журнала по расписанию в режиме SD Card Management Backup Configuration Mode или имя файла источника для принудительного применения конфигурации по расписанию в режиме SD Card Management Execute Configuration Mode.

filename *FILE-URL*

Параметры

<i>FILE-URL</i>	Укажите URL файла. Если текущее местоположение напрямую не относится к файловой системе SD-карты, необходимо указать полный каталог.
-----------------	--

По умолчанию

Нет.

Режим ввода команды

SD Card Management Backup Configuration Mode.

SD Card Management Execute Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если файл назначения для резервного копирования уже существует, то он будет перезаписан в соответствии с расписанием.

Пример

В данном примере показано, как указать имя файла для резервного копирования журнала по расписанию.

```
Switch#configure terminal
Switch(config)#sdcard-mgmt backup backup_log
Switch(config-sdcard-mgmt-backup)#time-range timel
Switch(config-sdcard-mgmt-backup)#type log
Switch(config-sdcard-mgmt-backup)#filename d:/backup_log
Switch(config-sdcard-mgmt-backup)#
```

78.7 activate

Данная команда используется для активации записи резервного копирования по расписанию или принудительного применения конфигурации по расписанию. Чтобы деактивировать запись, воспользуйтесь формой **no** этой команды.

activate

no activate

Параметры

Нет.

По умолчанию

По умолчанию запись деактивирована.

Режим ввода команды

SD Card Management Backup Configuration Mode.

SD Card Management Execute Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команды **type**, **filename** и **time-range** должны быть настроены до того, как запись резервного копирования по расписанию будет активирована. Если указанный временной интервал отсутствует, расписание будет создано без предупреждения, но оно не станет активным до момента создания соответствующего временного диапазона.

Команды **filename** и **time-range** должны быть настроены до того, как запись принудительного применения конфигурации по расписанию будет активирована. Если указанный временной интервал отсутствует, расписание будет создано без предупреждения, но оно не станет активным до момента создания соответствующего временного диапазона.

Пример

В данном примере показано, как активировать запись резервного копирования журнала по расписанию.

```
Switch#configure terminal
Switch(config)#sdcard-mgmt backup backup_log
Switch(config-sdcard-mgmt-backup)#activate
Switch(config-sdcard-mgmt-backup)#
```

78.8 show sdcard-mgmt

Данная команда используется для отображения настроек записей резервного копирования и принудительного применения конфигурации по расписанию.

show sdcard-mgmt [backup [configuration | log] | execute-config]

Параметры

backup	(Опционально.) Укажите, чтобы отобразить записи резервного копирования по расписанию.
configuration	(Опционально.) Укажите, чтобы отобразить записи резервного копирования конфигурации по расписанию.
log	(Опционально.) Укажите, чтобы отобразить записи резервного

копирования журнала по расписанию.

execute-config	(Опционально.) Укажите, чтобы отобразить записи принудительного применения конфигурации по расписанию.
-----------------------	--

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда применяется для отображения настроек записей резервного копирования и принудительного применения конфигурации по расписанию.

Пример

В данном примере показано, как отобразить настройки записей резервного копирования и принудительного применения конфигурации по расписанию.

```
Switch#show sdcard-mgmt

Backup entry name : entry1
Time Range       :
Type             : configuration
Filename         :
State            : Disabled

Backup entry name : backup_log
Time Range       : time01
Type             : log
Filename         : /d:/backup_log
State            : Enabled

Backup entry name : tt
Time Range       :
Type             :
Filename         :
State            : Disabled
-----

Execute entry name : tt
Time Range       :
Mode             : increase
Filename         :
State            : Disabled Total Entries: 3

Total Entries
```

78.9 execute config

Данная команда используется для настройки принудительного применения конфигурации из файловой системы SD-карты вручную.

execute config *FILE-URL* [**increase**]

Параметры

<i>FILE-URL</i>	Укажите URL файла. Если текущее местоположение напрямую не относится к файловой системе SD-карты, необходимо указать полный каталог.
increase	(Опционально.) Укажите, чтобы текущая конфигурация не была сброшена перед принудительным применением конфигурации. Если данный параметр не указан, текущая конфигурация будет сброшена перед принудительным применением конфигурации.
reset	Укажите, чтобы текущая конфигурация была сброшена перед принудительным применением конфигурации.

По умолчанию

По умолчанию текущая конфигурация будет сброшена перед принудительным применением конфигурации.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для настройки принудительного применения конфигурации из файловой системы SD-карты вручную.

Пример

В данном примере показано, как загрузить и принудительно применить конфигурацию.

```
Switch# configure terminal
Switch(config)# execute config d:/config-vlan-1 increase
Load configuration ----- Done
Executing script file d:/config-vlan-1 .....
Executing done

Switch(config)#
```

79. Команды сервера Secure File Transfer Protocol (SFTP)

79.1 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)#
```

79.2 ip sftp timeout

Данная команда используется, чтобы настроить таймер простоя (Idle Timer) для SFTP-сервера на коммутаторе. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

ip sftp timeout SECONDS
no ip sftp timeout

Параметры

SECONDS	Укажите значение таймера простоя (Idle Timer) для SFTP-сервера. Диапазон значений: от 30 до 600 секунд. Сессия SFTP завершается, если по истечении времени таймера простоя, установленного для указанной сессии, SFTP-сервер не обнаруживает никаких действий.
---------	--

По умолчанию

Таймер простоя (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 простоя (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 простоя 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 простоя (Idle Timer) для SFTP-сервера на 600 секунд.

```
Switch# configure terminal
Switch(config)# ip sftp timeout 600
Switch(config)#
```

79.3 show ip sftp

Данная команда используется для отображения настроек SFTP-сервера.

show ip sftp

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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#
```

80. Команды Secure Shell (SSH)

80.1 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#
```

80.2 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#
```

80.3 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 SSH на 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)#
```

80.4 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 SSH-сервер.

Пример

В данном примере показано, как включить SSH-сервер.

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

80.5 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

<i>TCP-PORT</i>	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)#
```

80.6 show crypto key mypubkey

Данная команда используется для отображения пар открытых ключей RSA или DSA.

show crypto key mypubkey {rsa | dsa}

Параметры

rsa	Укажите, чтобы отобразить информацию об открытом ключе RSA.
dsa	Укажите, чтобы отобразить информацию об открытом ключе DSA.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы отобразить пары открытых ключей RSA или DSA.

Пример

В данном примере показано, как отобразить информацию об открытом ключе RSA.

```
Switch# show crypto key mypubkey rsa

% Key pair was generated at: 09:48:40, 2013-11-29
Key Size: 768 bits
Key Data:
AAAAB3Nz aCl yc2EA AAADAQAB AAAAQwCN 6IRFHCBf jsHvYjQG iCL0p2kz 2v38ULC8
kAKra/Ze mG7IW3eC 8STcrkr5 s7l9H/bh jG/oqkwj S1UJSGqR e/sj6Ws=

Switch#
```

80.7 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.

Любой режим конфигурирования.

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#
```

80.8 show ssh

Данная команда используется для отображения статуса подключений SSH-сервера.

show ssh

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить статус подключений SSH на коммутаторе.

Пример

В данном примере показано, как отобразить информацию о подключениях SSH.

```
Switch# show ssh
```

```
SID Ver. Cipher                      Userid                      Client IP Address
--- -- -
0   V2  3des-cbc/sha1-96             zhang3                      192.168.0.100
1   V2  3des-cbc/hmac-sha1          lee4567890123456          2000::243

Total Entries: 2

Switch#
```

Отображаемые параметры

SID	Уникальный номер, идентифицирующий сессию SSH.
Ver	Версия SSH указанной сессии.
Cipher	Криптографический/Hashed Message Authentication Code (HMAC) алгоритм, используемый SSH-клиентом.
Userid	Имя пользователя сессии.
Client IP Address	IP-адрес клиента для установленной сессии SSH.

80.9 ssh user authentication-method

Данная команда используется, чтобы настроить метод аутентификации SSH для учетной записи пользователя. Для возврата 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 не указано, будет проверено только имя узла.
IPV6-ADDRESS	(Опционально.) Укажите необходима ли дополнительная проверка IPv6-адреса клиента для аутентификации на основе узла. Если не указано, будет проверено только имя узла.

По умолчанию

По умолчанию используется метод аутентификации по паролю.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы настроить метод аутентификации для пользователя. Имя пользователя должно быть пользователем, созданным при помощи команды **username**. По умолчанию применяется метод аутентификации по паролю. Системой будет предложено ввести пароль.

Для аутентификации пользователя при помощи открытого ключа SSH скопируйте файл открытого ключа пользователя в файловую систему. Когда пользователь пытается войти в учетную запись на коммутаторе через SSH-клиента (используя метод открытого ключа SSH), SSH-клиент автоматически передаст коммутатору открытый ключ и подпись с закрытым ключом. Если и открытый ключ, и подпись верны, пользователь будет аутентифицирован, и вход в учетную запись коммутатора будет разрешен.

- Для аутентификации пользователя при помощи открытого ключа SSH или метода на основе узла необходимо указать файл открытого ключа пользователя или файл ключа узла клиента в одном и том же формате. Файл ключа может содержать несколько ключей. Каждый ключ должен быть определен одной строкой. Максимально допустимая длина строки составляет 8 Kb.
- Каждый ключ состоит из следующих разделенных пробелами полей: *keytype*, *base64-encoded key*, *comment*. Ввод полей *keytype* и *base64-encoded key* обязателен, ввод поля *comment* – необязателен. Поле *keytype* может являться *ssh-dss* или *ssh-rsa*.

Пример

В данном примере показано, как настроить метод аутентификации с открытым ключом для пользователя «user1».

```
Switch# configure terminal
Switch(config)# ssh user user1 authentication-method publickey c:/user1.pub
Switch(config)#
```

81. Команды Secure Sockets Layer (SSL)

81.1 no certificate

Данная команда используется для удаления импортированного сертификата.

no certificate *NAME*

Параметры

<i>NAME</i>	Укажите имя сертификата, который необходимо удалить.
-------------	--

По умолчанию

Нет.

Режим ввода команды

Certificate Chain Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте команду **show crypto pki trustpoints**, чтобы отобразить список имен импортированных сертификатов. Затем в команде **no certificate** укажите импортированные сертификаты доверенной точки (trust point), которые необходимо удалить. Если указанный сертификат является локальным, соответствующий закрытый ключ также будет удален.

Пример

В данном примере показано, как удалить импортированный сертификат. Имя сертификата – tongken.ca. 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)#
```

81.2 crypto pki import

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

<i>TRUSTPOINT</i>	Укажите имя trust point, которое ассоциировано с импортированными сертификатами и парами ключей.
<i>FILE-SYSTEM</i>	Укажите файловую систему для сертификатов и пар ключей. После указанной файловой системы необходимо использовать двоеточие «:». Чтобы указать каталог системной flash-памяти, введите flash: c:/directory/filename . Чтобы указать каталог USB, введите flash: d:/directory/filename .
<i>DIRECTORY</i>	(Опционально.) Укажите имя каталога для импорта сертификатов и пар ключей. Возможен импорт в локальную память или на TFTP-сервер.
<i>FILE-NAME</i>	Укажите имя сертификатов и пар ключей, которые необходимо импортировать. По умолчанию к имени сертификата ЦС добавляется .ca, к закрытому ключу – .prv и к сертификату – .crt.
password <i>PASSWORD-PHRASE</i>	(Опционально.) Настройка пароля SSL crypto trust point.
tftp	Укажите URL источника для сетевого TFTP-сервера.
<i>IP-ADDRESS</i>	Укажите IP-адрес TFTP-сервера.
ca	Укажите, чтобы импортировать только сертификат ЦС.
local	Укажите, чтобы импортировать локальный сертификат и пары ключей.
both	Укажите, чтобы импортировать сертификат ЦС, локальный сертификат и пары ключей.

По умолчанию

Нет.

Режим ввода команды

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)#
```

81.3 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 вводе 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)#
```

81.4 crypto pki certificate chain

Данная команда используется для входа в режим конфигурации 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 конфигурации 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 конфигурации Certificate Chain Configuration Mode.

```
Switch# configure terminal
Switch(config)# crypto pki certificate chain TP1
Switch(config-cert-chain)#
```

81.5 primary

Данная команда используется для назначения указанной доверенной точки (trust point) в качестве основной trust point коммутатора. Чтобы отменить назначение, 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

Данная команда предназначена для указания доверенной точки (trust point) в качестве основной. Заданная trust point будет применяться по умолчанию, если система не может определить, какую trust point центра сертификации необходимо использовать. В качестве основной может быть настроена только одна trust point. После назначения 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)#
```

81.6 show crypto pki trustpoints

Данная команда используется для отображения trust point, настроенных на коммутаторе.

show crypto pki trustpoints [*TRUSTPOINT*]

Параметры

<i>TRUSTPOINT</i>	(Опционально.) Укажите имя trust point для отображения.
-------------------	---

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Любой режим конфигурирования.

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#
```

81.7 show ssl-service-policy

Данная команда используется для отображения политики SSL service policy.

show ssl-service-policy [*POLICY-NAME*]

Параметры

<i>POLICY-NAME</i>	(Опционально.) Укажите имя политики SSL service policy.
--------------------	---

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode

Любой режим конфигурирования.

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      : policy1
  Enabled CipherSuites :
    DHE_DSS_WITH_3DES_EDE_CBC_SHA,
    RSA_WITH_3DES_EDE_CBC_SHA,
    RSA_WITH_RC4_128_SHA,
    RSA_WITH_RC4_128_MD5,
    RSA_EXPORT_WITH_RC4_40_MD5
  Session Cache Timeout: 600
  Secure Trustpoint    : TP1

SSL Policy Name      : policy2
  Enabled CipherSuites :
    RSA_WITH_3DES_EDE_CBC_SHA,
    RSA_WITH_RC4_128_MD5,
    RSA_EXPORT_WITH_RC4_40_MD5
  Session Cache Timeout: 1200
  Secure Trustpoint    : TP2

Switch#
```

81.8 ssl-service-policy

Данная команда используется для настройки политики SSL service policy. Чтобы удалить политику SSL service policy, воспользуйтесь формой **no** этой команды.

ssl-service-policy *POLICY-NAME* [*ciphersuite* [*rsa-aes-128-gcm-sha256*] [*rsa-aes-256-gcm-sha384*] [*dhe-dss-3des-edc-cbc-sha*] [*rsa-3des-edc-cbc-sha*] [*rsa-rc4-128-sha*] [*rsa-rc4-128-md5*] [*rsa-*

```
export-rc4-40-md5] [ecdhe-rsa-aes-128-gcm-sha256] [ecdhe-rsa-aes-256-gcm-sha384] | secure-  
trustpoint TRUSTPOINT | session-cache-timeout TIME-OUT | version [ssl3.0] [tls1.0] [tls1.1] [tls1.2]]  
no ssl-service-policy POLICY-NAME [ciphersuite [rsa-aes-128-gcm-sha256] [rsa-aes-256-gcm-  
sha384] [dhe-dss-3des-ede-cbc-sha] [rsa-3des-ede-cbc-sha] [rsa-rc4-128-sha] [rsa-rc4-128-md5] [rsa-  
export-rc4-40-md5] [ecdhe-rsa-aes-128-gcm-sha256] [ecdhe-rsa-aes-256-gcm-sha384] | secure-  
trustpoint TRUSTPOINT | session-cache-timeout TIME-OUT | version [ssl3.0] [tls1.0] [tls1.1] [tls1.2]]
```

Параметры

<i>POLICY-NAME</i>	Укажите имя политики SSL service policy.
version	(Опционально.) Укажите версию TLS. ssl3.0 – укажите, чтобы устройство поддерживало SSL версии 3.0. 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. С помощью данного параметра можно указать несколько версий по порядку.
ciphersuite	(Опционально.) Укажите шифрование cipher suite, которое будет использовать служба безопасности при установлении соединения с удаленным узлом. Чтобы использовать обмен ключами RSA с 128-битным шифрованием AES и 256-битным SHA для дайджеста сообщений, укажите rsa-aes-128-gcm-sha256. Чтобы использовать обмен ключами RSA с 256-битным шифрованием AES и 384-битным SHA для дайджеста сообщений, укажите rsa-aes-256-gcm-sha384. 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 ECDHE RSA с 128-битным шифрованием AES и 256-битным SHA для дайджеста сообщений, укажите ecdhe-rsa-aes-128-gcm-sha256. Чтобы использовать обмен ключами ECDHE RSA с 256-битным шифрованием AES и 384-битным SHA для дайджеста сообщений, укажите ecdhe-rsa-aes-256-gcm-sha384.

Если шифрование cipher suite не настроено, клиент и сервер SSL согласовывают наиболее подходящее шифрование из списка доступных cipher suite. Будет выбрано шифрование, которое поддерживается и SSL-клиентом, и SSL-сервером. Возможно использование нескольких cipher suite. Используйте форму **no**, чтобы отключить выбранные cipher suite.

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. Воспользуйтесь формой **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. Если данный параметр не указан, тайм-аут кэша сессий по умолчанию составляет 600 секунд. Воспользуйтесь формой **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.

Пример

В данном примере показано, как настроить политику SSL service policy, которая ассоциирована с trust point «TP1». Указанная политика SSL service policy – «ssl-server».

```
Switch# configure terminal
Switch(config)# ssl-service-policy ssl-server secure-trustpoint TP1
Switch(config)#
```


82. Команды sFlow

82.1 sflow receiver

Данная команда используется, чтобы настроить получателя для агента sFlow. Получатели не могут быть добавлены или удалены из агента sFlow. Для возврата к настройкам по умолчанию 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 срока 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 срока 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)#
```

82.2 sflow sampler

Данная команда используется, чтобы создать или настроить выборку для агента sFlow. Для удаления одной выборки воспользуйтесь формой **no** этой команды.

sflow sampler *INSTANCE* [**receiver** *RECEIVER*] [**inbound** | **outbound**] [**sampling-rate** *RATE*]
[**max-header-size** *SIZE*]
no sflow sampler *INSTANCE*

Параметры

<i>INSTANCE</i>	Укажите индекс экземпляра, если с одним интерфейсом ассоциировано несколько выборок. Диапазон значений: от 1 до 65535.
receiver <i>RECEIVER</i>	(Опционально.) Укажите индекс получателя указанной выборки. Если параметр не указан, значение равно нулю. Пользователь не может указать «0» в качестве данного значения.
inbound	(Опционально.) Укажите для выборки входящих пакетов. По умолчанию используется данное направление выборки.
outbound	(Опционально.) Укажите для выборки исходящих пакетов.
sampling-rate <i>RATE</i>	(Опционально.) Укажите частоту выборки пакетов. Диапазон значений: от 0 до 65536. Если параметр не указан или указан «0», выборка будет отключена.
max-header-size <i>SIZE</i>	(Опционально.) Укажите максимальное количество байтов, которое необходимо скопировать из пакетов выборки. 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 вводе 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)# sflow receiver 1 owner owner-name
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# sflow sampler 1 receiver 1 inbound sampling-rate 1024 max-header-size 128
Switch(config-if)#
```

82.3 sflow poller

Данная команда используется, чтобы создать или настроить опрос для агента sFlow. Для удаления опроса воспользуйтесь формой **no** этой команды.

sflow poller *INSTANCE* [**receiver** *RECEIVER*] [**interval** *SECONDS*]
no sflow poller *INSTANCE*

Параметры

<i>INSTANCE</i>	Укажите индекс экземпляра, если с одним интерфейсом ассоциировано несколько опросов. Диапазон значений: от 1 до 65535.
receiver <i>RECEIVER</i>	(Опционально.) Укажите индекс получателя указанного опроса. Если параметр не указан, значение равно нулю. Пользователь не может указать «0» в качестве данного значения.
interval <i>SECONDS</i>	(Опционально.) Укажите максимальное количество секунд между последовательными выборками опроса. 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 вводе 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 ethernet 1/0/1
Switch(config-if)# sflow poller 1 receiver 1 interval 20
Switch(config-if)#
```

82.4 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.

Любой режим конфигурирования.

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.;1.02
sFlow Agent Address      : 10.90.90.90
sFlow Agent IPv6 Address :
Receivers Information
Index                    : 1
Owner                    : collector1
Expire Time              : 86400
Current Countdown Time   : 86384
Max Datagram Size        : 1400
Address                  : 10.1.1.2
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.

83. Команды Simple Mail Transfer Protocol (SMTP)

83.1 smtp server

Данная команда используется для настройки SMTP-сервера и порта. Чтобы вернуть порт к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

```
smtp server {IP-ADDRESS | IPV6-ADDRESS} [port PORT]
no smtp server [port]
```

Параметры

<i>IP-ADDRESS</i>	Укажите IPv4-адрес SMTP-сервера.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес SMTP-сервера.
<i>PORT</i>	Укажите номер TCP-порта для подключения к SMTP-серверу. 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)#
```

83.2 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)#
```

83.3 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 отставку syslog-сообщений получателям по электронной почте и настроить критерии фильтрации, используйте команду **logging smtp**.

Пример

В данном примере показано, как добавить адрес электронной почты получателя. Добавленный адрес – receiver@domain.com.

```
Switch# configure terminal
Switch(config)# smtp recipient receiver@domain.com
Switch(config)#
```

83.4 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)#
```

83.5 show smtp

Данная команда используется для отображения информации об SMTP.

show smtp

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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#
```

83.6 smtp send-testmsg

Данная команда используется для проверки доступности SMTP-сервера.

smtp send-testmsg

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы проверить доступность SMTP-сервера. Электронные письма отправляются всем настроенным получателям.

Пример

В данном примере показано, как отправить тестовое письмо всем пользователям, которые находятся в текущем настроенном списке получателей.

```
Switch# smtp send-testmsg  
  
Subject: This is the test message subject!  
Content: This is the test message content!  
  
Sending mail, please wait!  
  
Switch#
```

84. Команды Simple Network Management Protocol (SNMP)

84.1 show snmp

Данная команда используется для отображения настроек SNMP.

show snmp {community | host | view | group | engineID}

Параметры

community	Укажите, чтобы отобразить информацию об SNMP-сообществе.
host	Укажите, чтобы отобразить информацию о получателе SNMP trap.
view	Укажите, чтобы отобразить информацию об SNMP view.
group	Укажите, чтобы отобразить информацию об SNMP-группе.
engineID	Укажите, чтобы отобразить информацию о SNMP local engine ID.

По умолчанию

Нет.

Режим ввода команды

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

GroupName: public                      SecurityModel: v2c
  ReadView      : CommunityView        WriteView      :
  NotifyView    : CommunityView

GroupName: initial                    SecurityModel: v3/noauth
  ReadView      : restricted            WriteView      :
  NotifyView    : restricted

GroupName: private                    SecurityModel: v1
  ReadView      : CommunityView        WriteView      : CommunityView
  NotifyView    : CommunityView

GroupName: private                    SecurityModel: v2c
  ReadView      : CommunityView        WriteView      : CommunityView
  NotifyView    : CommunityView

Total Entries: 5
```

В нижеследующем примере показано, как отобразить SNMP engine ID.

```
Switch#show snmp engineID

Local SNMP engineID: 800000ab03f07d6834001000

Switch#
```

84.2 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

Total Entries: 1

Switch#
```


84.3 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*]

no snmp-server community [0 | 7] *COMMUNITY-STRING*

Параметры

0 <i>COMMUNITY-STRING</i>	(Опционально.) Укажите строку community string в форме обычного текста. Максимальное количество символов в строке – 32. Данное значение используется по умолчанию.
7 <i>COMMUNITY-STRING</i>	(Опционально.) Укажите строку community string в зашифрованном виде.
view <i>VIEW-NAME</i>	(Опционально.) Укажите имя ранее настроенного view, которое доступно указанному SNMP-сообществу.
ro	(Опционально.) Укажите право «только чтение».
rw	(Опционально.) Укажите право «чтение/запись».
access <i>IP-ACL-NAME</i>	(Опционально.) Укажите имя стандартного списка доступа, дающего возможность пользователю использовать указанную строку community string при доступе к агенту SNMP. Укажите доступного пользователя в поле адреса источника записи списка доступа.

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 SNMPv2с. При настройке сообщества с помощью команды **snmp-server community** будут созданы две записи SNMP-группы: одна для SNMPv1 и другая для SNMPv2с, у которых имя сообщества совпадает 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)#
```

84.4 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 33220000000000000000000000000000.

```
Switch# configure terminal
Switch(config)# snmp-server engineID local 3322
Switch(config)#
```

84.5 snmp-server group

Данная команда предназначена 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]
no snmp-server group GROUP-NAME {v1 | v2c | v3 {auth | noauth | priv}}
```

Параметры

GROUP-NAME	Укажите имя группы. Максимально допустимое количество символов в строке – 32. Пробелы в строке недопустимы.
v1	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv1.
v2c	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv2c.
v3	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv3.
auth	Укажите для аутентификации пакетов. Данный параметр не используется для шифрования пакетов.
noauth	Укажите для отмены аутентификации и шифрования пакетов.
priv	Укажите для аутентификации и шифрования пакетов.
read READ-VIEW	(Опционально.) Укажите, чтобы обеспечить доступ на чтение пользователю данной группы.
write WRITE-VIEW	(Опционально.) Укажите, чтобы обеспечить доступ на запись пользователю данной группы.
notify NOTIFY-VIEW	(Опционально.) Укажите, чтобы обеспечить доступ для уведомлений пользователю данной группы. В данном уведомлении описывается объект, о состоянии которого пользователь данной группы узнает с помощью SNMP trap.
access IP-ACL-NAME	(Опционально.) Укажите стандартный IP-адрес списка управления доступом (ACL) для ассоциирования с группой.

По умолчанию

Group Name	Version	Security Level	Read Name	View Write Name	View Notify View
Initial	SNMPv3	noauth	Restricted	None	Restricted

ReadGroup	SNMPv1	noauth	CommunityView	None	CommunityView
ReadGroup	SNMPv2c	noauth	CommunityView	None	CommunityView
WriteGroup	SNMPv1	noauth	CommunityView	CommunityView	CommunityView
WriteGroup	SNMPv2c	noauth	CommunityView	CommunityView	CommunityView

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Для определения пользователя SNMP-группы необходимо указать разрешенную модель безопасности и право с помощью параметров *READ-VIEW*, *WRITE-VIEW* и *NOTIFY-VIEW*. Модель безопасности позволяет пользователю применить 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 выборе 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)#
```

84.6 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}
```

Параметры

<i>IP-ADDRESS</i>	Укажите IPv4-адрес узла-получателя сервера для SNMP-уведомлений.
<i>IPV6-ADDRESS</i>	Укажите IPv6-адрес узла-получателя сервера для SNMP-уведомлений.
version	(Опционально.) Укажите версию SNMP, которую необходимо использовать для отправки SNMP trap. Если версия не указана, по умолчанию используется SNMPv1. 1 – SNMPv1. 2c – SNMPv2c. 3 – SNMPv3.
auth	(Опционально.) Укажите для аутентификации пакетов. Данный параметр не используется для шифрования пакетов.
noauth	Укажите для отмены аутентификации и шифрования пакетов.
priv	Укажите для аутентификации и шифрования пакетов.
<i>COMMUNITY-STRING</i>	Введите строку community string, которую необходимо отправить с notify-пакетами уведомлений. При указании версии 3 строка community string используется в качестве имени пользователя, как показано в примере команды snmp-sever user .
port <i>PORT-NUMBER</i>	(Опционально.) Укажите номер UDP-порта. Номер UDP-порта trap по умолчанию – 162. Диапазон номеров UDP-порта: от 1 до 65535. Некоторые номера портов могут конфликтовать с другими протоколами.

По умолчанию

По умолчанию используется версия 1.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

SNMP-уведомления отправляются в виде SNMP trap. Для отправки SNMP-уведомлений необходимо создать по крайней мере одного получателя при помощи команды **snmp-server host**. Для созданного пользователя укажите версию SNMP trap-пакетов. При указании SNMPv1 и SNMPv2c уведомления SNMP trap будут отправлены в PDU (Trap Protocol Data Unit). При указании SNMPv3 уведомления SNMP trap будут отправлены в SNMPv2-TRAP-PDU с заголовком SNMPv3.

При указании SNMPv1 или SNMPv2c для отправки SNMP trap на определенный узел указанная строка community string выступает в качестве строки SNMP trap.

При указании SNMPv3 для отправки SNMP trap на определенный узел укажите, необходима ли аутентификация и шифрование отправленных пакетов. Указанная строка community string выступает в качестве имени пользователя в пакетах SNMPv3. При использовании команд **snmp-server user** или **snmp-server user v3** сначала необходимо создать пользователя.

При отправке SNMP trap система проверит уведомления view, ассоциированные с указанным пользователем или именем сообщества. Если переменные привязки (binding variables), которые должны быть отправлены с SNMP trap, отсутствуют в уведомлениях view, уведомления не будут отправлены на данный сервер.

Пример

В данном примере показано, как настроить SNMP trap-получателя с указанием версии 1 и со строкой community string «comaccess». SNMP trap-получатель – 163.10.50.126.

```
Switch# configure terminal
Switch(config)# snmp-server community comaccess rw
Switch(config)# snmp-server host 163.10.50.126 version 1 comaccess
Switch(config)#
```

В 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 данном примере показано, как настроить SNMP trap-получателя с указанием версии 1 и со строкой community string «comaccess». SNMP trap-получатель – 163.10.50.126. Номер UDP-порта – 50001.

```
Switch# configure terminal
Switch(config)# snmp-server community comaccess rw
Switch(config)# snmp-server host 163.10.50.126 version 1 comaccess port 50001
Switch(config)#
```

84.7 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

<i>INTERFACE-ID</i>	Укажите интерфейс, IP-адрес которого будет использован в качестве адреса источника для отправки пакетов SNMP trap.
---------------------	--

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

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 vlan 100
Switch(config)#
```

84.8 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* {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *AUTH-PASSWORD* [**priv** {**des** *PRIV-PASSWORD* | **aes** *PRIV-PASSWORD*}]}} [**access** *IP-ACL-NAME*]
no snmp-server user *USER-NAME* *GROUP-NAME* {**v1** | **v2c** | **v3**}

Параметры

<i>USER-NAME</i>	Укажите имя пользователя. Максимальное количество символов в строке – 32. Пробелы в строке недопустимы.
<i>GROUP-NAME</i>	Укажите имя группы, к которой принадлежит данный пользователь. Пробелы в строке недопустимы.
v1	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv1.
v2c	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv2c.
v3	Укажите, чтобы пользователь данной группы использовал модель безопасности SNMPv3.
encrypted	(Опционально.) Укажите для шифрования пароля.

auth	(Опционально.) Укажите тип аутентификации.
md5	(Опционально.) Укажите использование аутентификации HMAC-MD5.
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. Пароль может содержать от 8 до 16 символов. При указании параметра encrypted фиксированная длина пароля – 32 символа.
access IP-ACL-NAME	(Опционально.) Укажите стандартный IP-адрес ACL для ассоциирования с пользователем.

По умолчанию

По умолчанию настроен один пользователь.

Имя пользователя – initial.

Имя группы – initial.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Для создания SNMP-пользователя укажите модель безопасности, которая будет использована данным пользователем, и группу, для которой создан данный пользователь. Для создания SNMPv3-пользователя необходимо указать пароль для аутентификации и шифрования.

Невозможно удалить SNMP-пользователя, который был ассоциирован с SNMP-сервером.

Пример

В данном примере показано, как настроить пароль в форме обычного текста для пользователя «user1» в группе «public» в версии SNMPv3.


```
Switch# configure terminal
Switch(config)# snmp-server user user1 public v3 auth md5 authpassword priv des privpassword
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 v3 encrypted auth md5
00112233445566778899AABBCCDDEEFF
Switch(config)#
```

84.9 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. При указании семейства под-деревьев используйте подстановочный знак (*) перед каждым идентификатором под-дерева.
included	Укажите под-дерево, которое необходимо включить в SNMP view.
excluded	Укажите под-дерево SNMPv1, которое необходимо исключить из SNMP view.

По умолчанию

VIEW-NAME	OID-TREE	View Type
Restricted	1.3.6.1.2.1.1	Included
Restricted	1.3.6.1.2.1.11	Included
Restricted	1.3.6.1.6.3.10.2.1	Included
Restricted	1.3.6.1.6.3.11.2.1	Included
Restricted	1.3.6.1.6.3.15.1.1	Included

CommunityView	1	Included
CommunityView	1.3.6.1.6.3	Excluded
CommunityView	1.3.6.1.6.3.1	Included

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы создать view MIB-объектов.

Пример

В данном примере показано, как создать MIB view и предоставить доступ для чтения SNMP-группе, ассоциированной с данным MIB view. Настроенный MIB view – interfacesMibView. SNMP-группа – guestgroup.

```
Switch# configure terminal
Switch(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)# snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)#
```

84.10 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 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 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 ethernet 1/0/1-9

Interface          Trap state
-----
eth1/0/1           Enabled
eth1/0/2           Enabled
eth1/0/3           Enabled
eth1/0/4           Enabled
eth1/0/5           Enabled
eth1/0/6           Enabled
eth1/0/7           Enabled
eth1/0/8           Enabled
eth1/0/9           Enabled

Switch#
```

84.11 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#
```

84.12 show snmp-server trap-sending

Данная команда используется для отображения состояния отправки SNMP trap на порту.

show snmp-server trap-sending [interface *INTERFACE-ID* [, | -]]

Параметры

<i>INTERFACE-ID</i>	(Опционально.) Укажите интерфейсы 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 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 ethernet 1/0/1-9
```

Port	Trap Sending
-----	-----
eth1/0/1	Enabled
eth1/0/2	Enabled
eth1/0/3	Enabled
eth1/0/4	Enabled
eth1/0/5	Enabled
eth1/0/6	Enabled
eth1/0/7	Enabled
eth1/0/8	Enabled
eth1/0/9	Enabled
Switch#	

84.13 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-сервер.

Пример

В данном примере показано, как включить SNMP-сервер.

```
Switch# configure terminal
Switch(config)# snmp-server
Switch(config)#
```

84.14 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)#
```

84.15 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 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)#
```

84.16 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)#
```

84.17 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

<i>TEXT</i>	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. Настроенная строка – HQ 15F.

```
Switch# configure terminal
Switch(config)# snmp-server location HQ 15F
Switch(config)#
```

84.18 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.
------	---

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
Switch(config)#
```

84.19 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 отключить 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 с интерфейса Ethernet 1/0/8.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/8
Switch(config-if)# snmp-server trap-sending disable
Switch(config-if)#
```

84.20 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

<i>PORT-NUMBER</i>	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)#
```

84.21 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)#
```

84.22 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 отставку SNMP trap об обнаружении/разрыве соединения (link-up / link-down) на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# no snmp trap link-status
Switch(config-if)#
```

85. Команды Single IP Management (SIM)

85.1 sim

Данная команда используется для включения функции Single IP Management. Чтобы отключить функцию Single IP Management, 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)#
```

85.2 sim role

Данная команда используется для смены роли Candidate Switch на Commander Switch или Commander Switch на Candidate Switch.

sim role {commander [GROUP-NAME] | candidate}

Параметры

commander	Укажите для передачи роли Commander Switch устройству.
<i>GROUP-NAME</i>	(Опционально.) Укажите имя группы, назначая устройству роль Commander Switch.
candidate	Укажите для передачи роли Candidate Switch устройству.

По умолчанию

Имя группы Single IP Management по умолчанию – default.
Роль устройства по умолчанию – Candidate Switch.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12

Использование команды

Технология Single IP Management предусматривает три роли: Candidate Switch и Commander Switch (назначаются пользователем), а также Member Switch (назначается при помощи команды **sim group-member** на Commander Switch).

В SIM-группу входит Commander Switch и множество Member Switch. При смене роли устройства, например, с Commander Switch на Candidate Switch все роли участников SIM-группы будут изменены на Candidate Switch.

Пример

В данном примере показано, как создать SIM-группу.

```
Switch# configure terminal
Switch(config)# sim role commander my-group
Switch(config)#
```

85.3 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-уровневого пароля, Commander Switch позволит данному Candidate Switch присоединиться к SIM-группе в качестве Member Switch.

Пример

В данном примере показано, как добавить один Candidate Switch к SIM-группе.

```
Switch# configure terminal
Switch(config)# sim group-member 1 secret
Switch(config)#
```

85.4 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

<i>SECONDS</i>	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)#
```

85.5 sim interval

Данная команда используется, чтобы настроить SIM-интервал в секундах для отправки сообщений протокола Single IP Management. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

sim interval *SECONDS*
no sim interval

Параметры

<i>SECONDS</i>	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)#
```

85.6 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)#
```

85.7 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#
```

85.8 copy sim

Данная команда используется для копирования файлов участникам SIM-группы.

copy sim *SOURCE-URL DESTINATION-URL* [**member** *MEMBER-LIST*]

Параметры

<i>SOURCE-URL</i>	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.
<i>DESTINATION-URL</i>	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 <i>MEMBER-LIST</i>	(Опционально.) Укажите Member Switch, чтобы загрузить файл. Может быть указано несколько Member Switch одновременно. Для отделения нескольких ID используйте «,»; для отделения диапазона Interface ID используйте «-».

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда может использоваться на Commander Switch для выгрузки файлов с Member Switch

на сервер. Для различия Member Switch ID каждому Member Switch ID будет добавлено имя файла.

Пример

В данном примере показано, как загрузить программное обеспечение (firmware) на Member Switch 1.

```
Switch# copy sim tftp: //10.10.10.58/switch.had firmware member 1

Download firmware 10.10.10.58/ switch.had to member 1 ?(y/n) [n] y

ID   MAC Address      Status
-----
1    00-02-01-03-01-03 SUCCESS

Switch#
```

В 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#
```

85.9 snmp-server enable traps sim

Данная команда используется, чтобы включить отправку trap-сообщений для SIM. Для отключения отправки 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)#
```

85.10 show sim

Данная команда используется для отображения информации о Single IP Management.

show sim [{candidates [CANDIDATE-ID] | members [MEMBER-ID] | group [COMMANDER-MAC]
[neighbor]}

Параметры

candidates	(Опционально.) Укажите, чтобы отобразить информацию обо всех Candidate Switch.
<i>CANDIDATE-ID</i>	(Опционально.) Укажите, чтобы отобразить подробную информацию об одном определенном Candidate Switch.
members	(Опционально.) Укажите, чтобы отобразить информацию обо всех Member Switch.
<i>MEMBER-ID</i>	(Опционально.) Укажите, чтобы отобразить подробную информацию об одном определенном Member Switch.
group	(Опционально.) Укажите, чтобы отобразить информацию о других SIM-группах.
<i>COMMANDER-MAC</i>	(Опционально.) Укажите, чтобы отобразить подробную информацию об одной определенной группе.
neighbor	(Опционально.) Укажите, чтобы отобразить информацию о соседних устройствах.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения информации о Single IP Management.

Пример

В данном примере показано, как отобразить подробную информацию о локальной SIM на Commander Switch.

```
Switch#show sim

Group Name       : my-group
SIM Version      : VER-2.01
Firmware Version : 1.01.006
Management VLAN  : 100
Device Name      : Switch
MAC Address      : F0-7D-68-36-30-B0
Platform        : DMS-3130-30TS
SIM State        : Enabled
Role State       : Commander
Discovery Interval : 60 sec
Hold Time        : 120 sec
Trap             : Enabled

Switch#
```

В примере ниже показано, как отобразить подробную информацию о локальной SIM на Member Switch.

```
Switch# show sim

SIM Version      : VER-2.01
Firmware Version : 1.01.006
Device Name      :
MAC Address      : F0-7D-00-36-30-B0
Platform        : DMS-3130-30TS
SIM State        : Enabled
Role State       : Member
Discovery Interval : 30 sec
Hold Time        : 100 sec

-----CS Info-----
CS Group Name    : my-group
CS MAC Address   : F0-7D-68-36-30-B0
CS Hold Time     : 90 s

Switch#
```

В следующем примере показано, как отобразить список участников SIM-группы.

```
Switch#show sim members
```

Member			Hold Firmware		
ID	MAC Address	Platform	Time	Version	Device Name
1	F0-7D-00-36-30-B0	DMS-3130-30TS	100	1.01.006	
2	F0-7D-01-36-30-B0	DMS-3130-30TS	80	1.01.006	

Total Entries : 2

```
Switch#
```

В нижеприведенном примере показано, как отобразить подробную информацию об участнике SIM-группы.

```
Switch# show sim members 1
```

```
Sim Member Information :
Member ID       : 1
Firmware Version : 1.01.006
Device Name     :
MAC Address     : F0-7D-00-36-30-B0
Platform        : DMS-3130-30TS
Hold Time       : 100 sec

Switch#
```

В нижеследующем 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	DMS-3130-30TS	90	1.01.006	

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   : 1.01.006
Device Name       :
MAC Address       : EE-FF-00-00-12-12
Platform          : DMS-3130-30TS
Hold Time         : 100 sec

Switch#
```

В следующем примере показано, как отобразить краткую информацию о группе.


```
Switch# show sim group
* -means Commander switch.

SIM Group Name : default

  ID  MAC Address      Platform      Hold   Firmware
  Time Version         Device Name
-----
*1   00-02-00-00-08-12  DMS-3130-30TS  40    1.01.006
  2   00-07-15-34-00-50
  3   00-01-02-03-00-10

SIM Group Name : SIM2

  ID  MAC Address      Platform      Hold   Firmware
  Time Version         Device Name
-----
*1   00-01-02-03-04-11  DMS-3130-30TS  40    1.01.006
  2   00-55-55-00-55-11

Total Entries : 2

Switch#
```

В нижеприведенном примере показано, как отобразить подробную информацию о группе.

```
Switch# show sim group 00-02-00-00-08-12

Sim Group Information :

[*** Commander Info ***]

MAC Address : 00-02-00-00-08-12
Group Name  : default
Device Name :
Firmware Version : 1.01.006
Platform    : DMS-3130-30TS
Number of Members : 2
Hold Time   : 100 sec

[*** Member Info (1/2)***]
MAC Address : 00-07-15-34-00-50

[*** Member Info (2/2)***]
MAC Address : 00-01-02-03-00-10

Switch#
```

В нижеследующем 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#
```

86. Команды Spanning Tree Protocol (STP)

86.1 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 <i>INTERFACE-ID</i>	Укажите интерфейс порта, на котором необходимо запустить действие обнаружения.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

С помощью данной команды во время миграции протокола порт будет переведен в состояние *SEND_RSTP*. Данное действие можно использовать, чтобы проверить, все ли устаревшие мосты на LAN были удалены. При отсутствии моста STP на данной LAN порт будет работать в выбранном режиме RSTP или MSTP. В противном случае порт будет работать в режиме STP.

Пример

В данном примере показано, как запустить процесс миграции протокола для всех портов.

```
Switch# clear spanning-tree detected-protocols all

Clear spanning-tree detected-protocols? (y/n) [n] y

Switch#
```

86.2 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* [, | -]] | mpt *INSTANCE-ID*]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите ID интерфейса, который необходимо отобразить.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.
mpt <i>INSTANCE-ID</i>	Укажите ID экземпляра MPT, который необходимо отобразить.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду 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: 00-AD-24-A2-D6-01
    Hello Time: 2s Max Age: 20s Forward Delay: 15s
Bridge ID Priority: 32768 (priority 32768 sys-id-ext 0)
    Address: 00-AD-24-A2-D6-01
    Hello Time: 2s Max Age: 20s Forward Delay: 15s
Topology Changes Count: 0

Interface      Role      State      Cost      Priority Link
-----      ----      -
eth2/0/1      designated forwarding 20000      128.31    p2p      edge

Switch#show spanning-tree mpt 3

MPT Instance ID: 3
Root ID Priority: 32768
    Address: 00-AD-24-A2-D6-01
    Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
Bridge ID Priority: 32768 (priority 32768 sys-id-ext 0)
    Address: 00-AD-24-A2-D6-01
    Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
Topology Changes Count: 0

Interface      Role      State      Cost      Priority Link
-----      ----      -
Switch#
```

86.3 show spanning-tree mpt configuration

Данная команда используется для отображения конфигурации, касающейся MPT (Multiple Process Tree).

show spanning-tree mpt configuration

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения настроек, касающихся MPT, а именно: созданные деревья MPT и их темебер-порты. Дерево MPT с ID экземпляром 0 относится к дереву RSTP по умолчанию.

Пример

В данном примере показано, как отобразить информацию о конфигурации MPT.

```
Switch#  
  
Switch# show spanning-tree mpt configuration  
There are totally 2 MPT tree instances.  
  
MPT Instance ID 1:  
Name                : MPT-Instance1  
Bridge priority      : 4096  
Hello time           : 2 seconds  
Max Age              : 20 seconds  
Forward Delay time   : 15 seconds  
  
Member ports         : eth1/0/9, eth1/0/10, eth1/0/11, eth1/0/12,  
                      eth1/0/13, eth1/0/14, eth1/0/15, eth1/0/16  
  
MPT Instance ID 2:  
Name                : Campus-East  
Bridge priority      : 4096  
Hello time           : 2 seconds  
Max Age              : 20 seconds  
Forward Delay time   : 15 seconds  
Member ports         : eth1/0/1, eth1/0/2, eth1/0/3, eth1/0/4,  
                      eth1/0/5, eth1/0/6, eth1/0/7, eth1/0/8  
  
Switch#
```

86.4 show spanning-tree mst

Данная команда используется для отображения информации о Multiple Spanning Tree (MST) и экземплярах (instance).

show spanning-tree mst {configuration | instance *INTANCE-ID* [interface *INTERFACE-ID*]}

Параметры

configuration	Укажите настройки MST оборудования.
----------------------	-------------------------------------

instance <i>INSTANCE-ID</i>	Укажите номер экземпляра.
interface <i>INTERFACE-ID</i>	Укажите ID интерфейса для отображения.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить информацию об 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#
```

86.5 show spanning-tree configuration interface

Данная команда используется для отображения информации о настройках интерфейса STP.

show spanning-tree configuration interface [*INTERFACE-ID* [, | -]]

Параметры

<i>INTERFACE-ID</i>	(Опционально.) Укажите ID интерфейса 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.

Любой режим конфигурирования.

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 ethernet 1/0/1

eth1/0/1
MPT Instance ID: 2
Spanning tree state : Enabled
Port path cost: 0
Port priority: 128
Port Identifier: 128.1
Link type: auto
Port fast: edge
Guard root: Disabled
Loop guard: Disabled
TCN filter : Disabled
Bpdu forward: Disabled

Switch#
```

86.6 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 параметры в форме **no** данной команды не указаны, 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)#
```

86.7 spanning-tree mpt

Данная команда используется для назначения member-порта экземпляру дерева MPT. Чтобы снова назначить порт в качестве дерева RSTP по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree mpt *INSTANCE-ID*

no spanning-tree mpt [*INSTANCE-ID*]

Параметры

<i>INSTANCE-ID</i>	Укажите ID экземпляра в диапазоне от 1 до 32.
--------------------	---

По умолчанию

Порты устройства относятся к дереву RSTP по умолчанию.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы назначить member-порт экземпляру дерева MPT. Экземпляр MPT

необходимо создать перед привязкой порта.

Пример

В данном примере показано, как создать экземпляр 1 дерева MPT с дальнейшим назначением порта 3 в качестве member-порта.

```
Switch(config)# spanning-tree mpt instance 1
Switch(config-mpt)#exit
Switch(config)# interface ethernet 1/0/3
Switch(config-if)# spanning-tree mpt 1
Switch(config-if)#
```

Для проверки настроек введите команду **show spanning-tree mpt**.

86.8 spanning-tree mpt instance

Данная команда используется для создания экземпляра дерева MPT и входа в режим MPT Configuration Mode. Чтобы удалить экземпляр дерева MPT, воспользуйтесь формой **no** этой команды.

spanning-tree mpt instance *INSTANCE-ID*
no spanning-tree mpt instance [*INSTANCE-ID*]

Параметры

<i>INSTANCE-ID</i>	Укажите ID экземпляра в диапазоне от 1 до 32. «0» представляет дерево RSTP по умолчанию.
--------------------	--

По умолчанию

По умолчанию экземпляры MPT не созданы.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Дерево MSTP предоставляет множество процессов RSTP, каждый из которых относится к одному дереву RSTP. Изначально функция RSTP представляет только одно дерево RSTP. Все порты устройства принадлежат к одному дереву RSTP. При наличии нескольких процессов RSTP порты устройства могут быть назначены разным деревьям RSTP.

Команды, относящиеся к MPT, действуют, только когда режим Spanning Tree настроен как STP или RSTP.

По умолчанию все порты устройства относятся к дереву RSTP по умолчанию.

Используйте команду **spanning-tree mpt instance** в режиме Global Configuration Mode, чтобы создать дерево MPT и войти в режим MPT Configuration Mode. Если экземпляр уже создан, команда сразу же войдет в режим MPT Configuration Mode.

Для удаления дерева MPT введите команду **no spanning-tree mpt instance** в режиме Global

Configuration Mode. Порты, принадлежащие удаленному экземпляру MPT, вернутся к дереву RSTP по умолчанию. Если ID экземпляра не указан, все экземпляры MPT будут удалены.

Примените команду **spanning-tree mpt** в режиме Interface Configuration Mode, чтобы настроить member-порты для дерева MPT.

Пример

В данном примере показано, как создать экземпляр 1 дерева MPT.

```
Switch(config)# spanning-tree mpt instance 1
Switch(config-mpt)#
```

Для проверки настроек введите команду **show spanning-tree mpt**.

86.9 name (STP MPT Configuration)

Данная команда используется, чтобы настроить имя для экземпляра дерева MPT. Для отмены настройки имени воспользуйтесь формой **no** этой команды.

name *INSTANCE-NAME*
no name

Параметры

<i>INSTANCE-NAME</i>	Укажите имя экземпляра. Максимальное количество символов – 32.
----------------------	--

По умолчанию

Имя экземпляра дерева MPT по умолчанию – MTP-InstanceX, где X – это ID экземпляра.

Режим ввода команды

MPT Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить имя для экземпляра дерева MPT.

Пример

В данном примере показано, как создать экземпляр дерева MPT 1 и настроить его имя.

```
Switch(config)# spanning-tree mpt instance 1
Switch(config-mpt)#name CAMPUS-EAST
Switch(config-mpt)#
```

86.10 spanning-tree mst configuration

Данная команда используется для входа в режим MST Configuration и настройки MSTP-региона. Чтобы вернуться 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

Используйте данную команду, чтобы войти в режим MST Configuration.

Пример

В данном примере показано, как войти в режим MST Configuration.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#
```

86.11 instance

Данная команда используется для привязки VLAN к экземпляру MST. Чтобы удалить указанный экземпляр MST, воспользуйтесь командой **no instance INSTANCE-ID**. Для возврата привязки VLAN к экземпляру по умолчанию (CIST) введите команду **no instance INSTANCE-ID vlans VLAN-ID [, | -]**.

instance INSTANCE-ID vlans VLAN-ID [, | -]
no instance INSTANCE-ID [vlans VLAN-ID [, | -]]

Параметры

INSTANCE-ID	Укажите ID экземпляра MSTP, к которому необходимо привязать указанные 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 привязаны к CIST, значение экземпляра которого 0.

Режим ввода команды

MST Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы привязать VLAN к экземпляру MST. Во время привязки VLAN к несуществующему экземпляру MST, экземпляр MST будет создан автоматически.

Пример

В данном примере показано, как привязать несколько VLAN к экземпляру MST.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance 2 vlans 1-100
Switch(config-mst)#
```

86.12 name (STP MST Configuration)

Данная команда используется для настройки имени MST-региона. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

name NAME

no name

Параметры

NAME	Укажите имя MST-региона. 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

Используйте данную команду, чтобы настроить имя MST-региона. Если у коммутаторов совпадают VLAN Mapping и номер версии конфигурации, но различаются имена регионов, они принадлежат к разным MST-регионам.

Пример

В данном примере показано, как настроить имя MST-региона. Указанное имя – MSTP.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#name MSTP
Switch(config-mst)#
```

86.13 revision

Данная команда используется, чтобы настроить номер ревизии для MST. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

revision *REVISION*
no revision

Параметры

<i>REVISION</i>	При совпадении имен укажите другой уровень ревизии. Диапазон значений: от 0 до 65535.
-----------------	---

По умолчанию

Значение по умолчанию – 0.

Режим ввода команды

MST Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить номер ревизии для MST. Коммутаторы с идентичной конфигурацией принадлежат к разным MST-регионам, если их номера ревизии не совпадают.

Пример

В данном примере показано, как настроить номер ревизии MST. Указанное значение – 2.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#revision 2
Switch(config-mst)#
```

86.14 spanning-tree mst

Данная команда используется, чтобы 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

<i>INSTANCE-ID</i>	Укажите ID экземпляра MSTP. Диапазон значений: от 0 до 64. Значение экземпляра по умолчанию, CIST – 0.
cost <i>COST</i>	Укажите стоимость пути экземпляра. Диапазон значений: от 0 до 200000000.
port-priority <i>PRIORITY</i>	Укажите приоритет порта экземпляра. Диапазон значений: от 0 до 240 с шагом 16.

По умолчанию

Стоимость определяется на основе скорости порта. Чем выше скорость, тем меньше стоимость. MST всегда использует стоимость «длинного» пути (long path cost).

Приоритет порта по умолчанию – 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 ethernet 1/0/3
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 ethernet 1/0/3
Switch(config-if)#spanning-tree mst 0 port-priority 64
Switch(config-if)#
```

86.15 spanning-tree mst max-hops

Данная команда используется для настройки максимального числа переходов MSTP. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

spanning-tree mst max-hops *HOP-COUNT*
no spanning-tree mst max-hops

Параметры

<i>HOP-COUNT</i>	Укажите максимальное число переходов MSTP. Диапазон значений: от 1 до 40.
------------------	---

По умолчанию

Максимальное число переходов MSTP по умолчанию – 20.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить максимальное число переходов MSTP.

Пример

В данном примере показано, как настроить максимальное число переходов MSTP.

```
Switch#configure terminal
Switch(config)#spanning-tree mst max-hops 19
Switch(config)#
```

86.16 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 в режиме Global Configuration Mode, чтобы включить функцию Spanning Tree глобально.

Пример

В данном примере показано, как включить функцию Spanning Tree.

```
Switch# configure terminal
Switch(config)# spanning-tree global state enable
Switch(config)#
```

86.17 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)#
```

86.18 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 функция включена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если Spanning Tree включено, BPDU, полученный портом, будет либо отправлен, либо обработан. Используя данную команду, не допускайте появления петель. Данная команда не будет применена, если функция L2PT включена для STP.

Пример

В данном примере показано, как включить Spanning Tree на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# spanning-tree state enable
Switch(config-if)#
```

86.19 spanning-tree cost

Данная команда используется для настройки значения стоимости пути на указанном порту. Чтобы стоимость пути определялась автоматически, воспользуйтесь формой **no** этой команды.

spanning-tree cost COST

no spanning-tree cost

Параметры

<i>COST</i>	Укажите стоимость пути для порта. Диапазон значений: от 1 до 2000000000.
-------------	--

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 ethernet 1/0/7
Switch(config-if)# spanning-tree cost 20000
Switch(config-if)#
```

86.20 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

<i>SECONDS</i>	Укажите интервал между отправкой одного BPDU-сообщения для назначенного порта (designated port). Диапазон значений: от 1 до 2 секунд.
----------------	---

По умолчанию

Интервал отправки hello-сообщений по умолчанию – 2 секунды.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется, чтобы указать интервал отправки hello-сообщений, используемых в версии MSTP для определенного порта. Команда применима 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 ethernet 1/0/1
Switch(config-if)#spanning-tree mst hello-time 1
Switch(config-if)#
```

86.21 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 физического порта и port-channel.

Функция STP Loop Guard обеспечивает дополнительную защиту от петель в L2 домене (петель STP). Петля STP образуется, когда заблокированный порт в резервной топологии ошибочно переходит в состояние forwarding, по причине того, что один из портов (не обязательно заблокированный порт) перестает получать пакеты BPDU протокола STP, работа которого зависит от непрерывного получения

и передачи BPDU на основе роли порта. Назначенный порт (designated port) передает BPDU, а не назначенный порт (non-designated port) получает BPDU.

Когда один из портов в физически резервной топологии перестает получать BPDU, протокол STP определяет, что в данной топологии отсутствуют петли. В итоге роль заблокированного порта изменяется с альтернативного/резервного порта (alternate/backup port) на назначенный (designated) порт, который переходит в состояние forwarding. В данной ситуации образуется петля.

Пример

В данном примере показано, как включить функцию Loop Guard на интерфейсе Ethernet 1/0/3.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/3
Switch(config-if)#spanning-tree loop-guard
Switch(config-if)#
```

86.22 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 данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

BPDU Guard предотвращает превращение порта в корневой порт и ограничивает доступ внешним мостам, находящимся не под полным контролем администратора, к основному региону сети активной топологии связующего дерева.

Порт, которому было отказано в присвоении роли корневого порта (root port), сможет работать только в качестве назначенного порта (designated port). При получении конфигурационного BPDU с более высоким приоритетом порт начнет работать в качестве альтернативного порта (alternate port) в состоянии blocking. Получение BPDU с более высоким приоритетом не повлияет на построение STP. Порт будет прослушивать сообщения BPDU. Если время ожидания получения BPDU с наибольшим приоритетом истечет, порт начнет работать в качестве назначенного порта.

Когда функция Guard Root сработает и порт начнет работать в качестве альтернативного порта, будет сгенерировано системное сообщение. Данные настройки действительны для всех версий Spanning

Tree.

Пример

В данном примере показано, как предотвратить смену роли порта на роль корневого порта (root port) для интерфейса Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# spanning-tree guard root
Switch(config-if)#
```

86.23 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 ethernet 1/0/7
Switch(config-if)# spanning-tree link-type point-to-point
Switch(config-if)#
```

86.24 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 экземпляры MSTP 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)#
```

86.25 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

Режим по умолчанию – Fast Edge Mode.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

На порту может быть установлен один из трех режимов Port Fast 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 ethernet 1/0/7
Switch(config-if)# spanning-tree portfast edge
Switch(config-if)#
```

86.26 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

<i>PRIORITY</i>	Укажите приоритет порта в диапазоне от 0 до 240.
-----------------	--

По умолчанию

Значение по умолчанию – 128.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При присвоении роли порту используется его идентификатор, который состоит из приоритета и номера порта. Чем ниже число, тем выше приоритет. Данный параметр применим только в режимах RSTP или STP.

Пример

В данном примере показано, как настроить приоритет для интерфейса Ethernet 1/0/7 со значением 0.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/7
Switch(config-if)# spanning-tree port-priority 0
Switch(config-if)#
```

86.27 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

<i>PRIORITY</i>	Укажите Bridge-ID Spanning Tree, который состоит из приоритета и MAC-адреса моста. Bridge-ID является важным фактором в топологии Spanning Tree. Диапазон значений: от 0 до 61440.
-----------------	--

По умолчанию

Значение по умолчанию – 32768.

Режим ввода команды

Global Configuration Mode.

MPT Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Выбор корневого моста зависит от значения приоритета моста и системного MAC-адреса. Значение приоритета моста должно делиться на 4096. Чем меньше число, тем выше приоритет.

Данные настройки применимы для версий STP и RSTP протокола Spanning Tree. В режиме MSTP используйте команду **spanning-tree mst priority**, чтобы настроить приоритет для MSTP-экземпляра.

Пример

В данном примере показано, как настроить приоритет моста STP со значением 4096.

```
Switch# configure terminal
Switch(config)# spanning-tree priority 4096
Switch(config)#
```

86.28 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 ethernet 1/0/7
Switch(config-if)# spanning-tree tcnfilter
Switch(config-if)#
```

86.29 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

<i>VALUE</i>	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)#
```

86.30 spanning-tree forward-bpdu

Данная команда используется для включения BPDU Forwarding в Spanning Tree. Чтобы отключить BPDU 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 BPDU Forwarding в Spanning Tree.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# spanning-tree forward-bpdu
Switch(config-if)#
```

86.31 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)#
```

87. Команды стекирования

87.1 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 4 порта SFP28 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#
```

87.2 stack bandwidth

Данная команда используется для изменения пропускной способности порта стекирования. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

stack bandwidth {4-port-SFP28}
no stack bandwidth

Параметры

4-port-SFP28	Укажите, чтобы использовать для стекирования 4 порта SFP28.
---------------------	---

По умолчанию

По умолчанию используются и доступны для настройки только 4 порта SFP28.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для изменения пропускной способности порта стекирования. Пропускную способность необходимо настроить перед стекированием коммутаторов.

Необходимо включить физическое стекирование и при необходимости указать в настройках количество портов (4), которые будут использованы для стекирования.

Если для стекирования используется четыре порта SFP28, между двумя коммутаторами будет установлено соединение на скорости до 200 Гбит/с в режиме полного дуплекса.

- Коммутаторы DMS-3130-30TS/30PS: физические порты 27, 28, 29 и 30.

Пример

В данном примере показано, как изменить пропускную способность и использовать для стекирования 4 порта.

```
Switch#stack bandwidth 4-port-SFP28

WARNING: The command does not take effect until the next reboot.
Switch#
```

87.3 stack renumber

Данная команда используется для назначения Unit ID коммутатору вручную.

switch oldunit renumber newunit

Параметры

oldunit	Укажите текущий Unit ID коммутатора, который необходимо изменить.
NEW-UNIT-ID	Укажите новый Unit ID, который необходимо назначить коммутатору.

По умолчанию

По умолчанию Unit ID назначается автоматически.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

После выполнения данной команды коммутатор будет настроен при помощи информации о конфигурации нового коммутатора, если информация есть. Информация о конфигурации прежнего коммутатора сохранится, однако сам коммутатор будет отключен от сети. Команда используется на основном устройстве (Primary Master Box).



Примечание: если Unit ID основного устройства (Primary Master Box) был изменен, текущая конфигурация больше не применяется (т. е. устройства в стеке действуют так, как если бы конфигурация была удалена).

Пример

В данном примере показано, как изменить Unit ID основного коммутатора (Primary Master Box).
Прежний ID – 1. Новый ID – 3.

```
Switch(config)#switch 1 renumber 3
All the switches in the stack will be reset to perform Manager unit renumbering and the
configuration data for the old unit number will remain in the configuration file.
Are you sure you want to renumber? (y/n) y
Rebooting system!
```

В данном примере показано, как изменить Unit ID дополнительного коммутатора (Slave). Прежний ID – 7. Новый ID – 5.

```
Switch(config)#switch 7 renumber 5
System will reset the specified switch unit to perform unit renumbering and the configuration
data for the old unit number will remain in the configuration file.
Are you sure you want to renumber? (y/n) y

Switch(config)#
```

87.4 switch priority

Данная команда используется для настройки приоритета коммутатора в стеке. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

switch unit priority value

no switch unit priority

Параметры

<i>unit</i>	Укажите ID коммутатора.
<i>value</i>	Укажите приоритет, который необходимо назначить unit коммутатора в стеке. Диапазон значений: от 0 до 15. Чем выше номер, тем выше

приоритет. 0 означает, что приоритет не будет назначен.

По умолчанию

По умолчанию приоритет не назначен.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12

Использование команды

Используйте данную команду для назначения коммутатора основным устройством (Primary Master Box). Основным устройством становится коммутатор с наивысшим приоритетом. Следующие по приоритету коммутаторы будут выбраны в качестве резервных устройств (Backup). Если текущее основное устройство недоступно, в качестве основного устройства будет назначен коммутатор следующий по приоритету.

Пример

В данном примере показано, как настроить приоритет unit 2 коммутатора со значением 10.

```
Switch(config)# switch 2 priority 10
Switch#
```

87.5 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 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, 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)#
```

87.6 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 technology is Stacking Lite Ver 0.1
The number of box can be stacked is restricted by max box count and max stack cost.
Stacking Mode       : Enabled
Trap State          : Enabled
Max Stack Cost      : 12
Max Box Count       : 9
Current Stack Cost   : 1
Current Box Count    : 1
My Box ID           : 2
Master Box ID        : 2
BK Master Box ID     : -
Topology            : Duplex_Chain
```

Box ID	Module Name	Priority	MAC	PROM/Runtime Version	H/W Ver.	Switch Status	Stack Cost
1	--	-	--	--	-	Not Present	-
2	DMS-3130-30PS	10	00:AD:24:A2:D6:00	1.00.003/1.01.006	A1	OK	1
3	--	-	--	--	-	Not Present	-
4	--	-	--	--	-	Not Present	-
5	--	-	--	--	-	Not Present	-
6	--	-	--	--	-	Not Present	-
7	--	-	--	--	-	Not Present	-
8	--	-	--	--	-	Not Present	-
9	--	-	--	--	-	Not Present	-

```
Stack Bandwidth:
```

Box ID	Interface	Link Status	Link Speed (Gb/s)	Link Partner Box ID
2	0/27	Link Down	25	-
2	0/28	Link Down	25	-
2	0/29	Link Down	25	-
2	0/30	Link Down	25	-

```
Running-Config Synchronization to BK Master:
Status           : -
Switch#
```

88. Команды Storm Control

88.1 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 и настройки отправки SNMP-уведомлений для Storm Control.



Примечание: для одноадресного трафика (включая неизвестный и известный одноадресный трафик) только действие отключение (shutdown) будет запускать журналы и генерировать trap-сообщения (действие указано как отключение порта из-за ошибки во время шторма). Обратитесь к команде **storm-control** ниже.

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)#
```

88.2 storm-control

Данная команда используется для защиты устройства от штормовых атак широковещательных и

многоадресных пакетов или пакетов с неизвестным адресом назначения. Чтобы вернуться 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 ограничения 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 level) PPS.
level kbps KBPS-RISE [KBPS-LOW]	Укажите пороговое значение скорости передачи трафика, полученного на порту, в битах в секунду. Доступный диапазон значений: от 1 до 2147483647. Если минимальный уровень (low level) KBPS не указан, значение по умолчанию составляет 80% от указанного максимального (rise level) 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 и многоадресных пакетов или пакетов с неизвестным адресом назначения отключена.

При возникновении шторма по умолчанию storm-пакеты будут отброшены.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Функция Storm Control используется для защиты сети от штормовых атак широковещательных и многоадресных пакетов или пакетов с неизвестным адресом назначения лавинной рассылки. Используйте команду **storm-control**, чтобы включить Storm Control для определенного типа трафика на интерфейсе.



Примечание: trap-сообщения могут срабатывать при возникновении и/или предотвращении штормов. Обратитесь к приведенной выше команде **snmp-server enable traps storm-control**. Однако для одноадресных пакетов только действие отключение (shutdown) будет запускать журналы и журналы событий.

Пример

В данном примере показано, как включить Storm Control для управления широковещательным штормом на интерфейсах Ethernet 1/0/1 и Ethernet 1/0/2. На Ethernet 1/0/1 установлен порог до 500 пакетов в секунду с действием отключения (shutdown). На интерфейсе порта 3,2 установлен порог до 70% с действием отбрасывания (drop).

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# storm-control broadcast level pps 500
Switch(config-if)# storm-control action shutdown
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# storm-control broadcast level 70 60
Switch(config-if)# storm-control action drop
Switch(config-if)#
```

88.3 storm-control polling

Данная команда используется, чтобы настроить интервал 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. Доступный 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. Доступный диапазон значений: от 0 до 360. 0 означает, что при обнаружении шторма порт в режиме shutdown сразу же будет отключен из-за ошибки.

Infinite означает, что порт в режиме **shutdown** не будет отключен из-за ошибки даже при обнаружении шторма.

По умолчанию

Интервал опроса по умолчанию – 5 секунд.
Количество попыток по умолчанию – 3.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы указать интервал выборки для подсчета количества полученных пакетов.

Пример

В данном примере показано, как указать интервал опроса со значением 15 секунд.

```
Switch# configure terminal
Switch(config)# storm-control polling interval 15
Switch(config)#
```

88.4 show storm-control

Данная команда используется для отображения текущих настроек функции Storm Control.

show storm-control interface *INTERFACE-ID* [, | -] [broadcast | multicast | unicast]

Параметры

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

Любой режим конфигурации.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если ID интерфейса не указан, будут отображены настройки всех интерфейсов.

Если тип пакета не указан, будут отображены настройки всех типов Storm Control.

Пример

В данном примере показано, как отобразить текущие настройки Storm Control для широковещательных пакетов.

```
Switch# show storm-control interface ethernet 1/0/1-1/0/6 broadcast
```

Interface	Action	Threshold	Current	State
eth1/0/1	Drop	500/300 pps	200 pps	Forwarding
eth1/0/2	Drop	80/64 %	20 %	Forwarding
eth1/0/3	Drop	80/64 %	70 %	Forwarding
eth1/0/4	Shutdown	500/300 pps	100 pps	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 для диапазона интерфейсов от Ethernet 1/0/1 до Ethernet 1/0/2.

```
Switch# show storm-control interface ethernet 1/0/1-2
```

```

Polling Interval      : 15 sec          Shutdown Retries      : Infinite
Trap                  : Disabled
Interface    Storm    Action    Threshold    Current    State
-----
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.

89. Команды Super VLAN

89.1 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 используется для указания VLAN в качестве Super VLAN. Super VLAN применяется 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 and Proxy ND will be enabled automatically on this super VLAN.
Switch(config-vlan)#
```

89.2 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

<i>VLAN-ID</i>	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 применяется 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 and Proxy ND will be enabled automatically on this super VLAN.

Switch(config-vlan)#subvlan 5-7
Switch(config-vlan)#
```

89.3 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

<i>START-IP-ADDRESS</i>	Укажите начальный IP-адрес необходимой Sub-VLAN.
<i>END-IP-ADDRESS</i>	Укажите конечный IP-адрес необходимой Sub-VLAN.

По умолчанию

Нет.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима только на Sub-VLAN и используется для настройки ее диапазона/диапазонов IP-адресов, что может сократить издержки, если на коммутаторе подключена опция Proxy ARP между Sub-VLAN. Некорректная настройка диапазонов IP-адресов может привести к ошибкам маршрутизации IP-трафика. У Sub-VLAN может быть один или более диапазонов IP-адресов. Настраиваемый диапазон IP-адресов не должен совпадать с существующими диапазонами адресов других Sub-VLAN и должен принадлежать подсети интерфейса Super VLAN. В пределах Sub-VLAN настраиваемый диапазон IP-адресов будет объединен с другим диапазоном/диапазонами при необходимости.

Пример

В данном примере показано, как настроить диапазон IP-адресов Sub-VLAN 5.

```
Switch# configure terminal
Switch(config)# vlan 5
Switch(config-vlan)# subvlan-address-range 192.168.10.1 192.168.10.50
Switch(config-vlan)#
```

89.4 show supervlan

Данная команда используется для отображения настроек Super VLAN и ее Sub-VLAN.

show supervlan [*VLAN-ID* [, | -]]

Параметры

<i>VLAN-ID</i>	(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.

Любой режим конфигурации.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения настроек Super VLAN и ее Sub-VLAN.

Пример

В данном примере показано, как отобразить настройки всех Super VLAN.

```
Switch#show supervlan

SuperVLAN ID  SubVLAN ID  SubVLAN Status  SubVLAN IP Address Range
-----
10            5            Active          192.168.10.1 - 192.168.10.50
              6            Inactive        192.168.10.51 - 192.168.10.60
              7            Inactive        192.168.10.61 - 192.168.10.70

Switch#
```

90. Команды Surveillance VLAN

90.1 surveillance vlan

Данная команда используется для глобального включения функции Surveillance VLAN и ее настройки. Чтобы отключить функцию Surveillance VLAN, воспользуйтесь формой **no** этой команды.

surveillance vlan *VLAN-ID*
no surveillance vlan

Параметры

<i>VLAN-ID</i>	Укажите VLAN ID Surveillance VLAN в диапазоне от 2 до 4094.
----------------	---

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте 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)#
```

90.2 surveillance vlan aging

Данная команда используется, чтобы настроить время устаревания (Aging Time) для устаревших динамических member-портов Surveillance VLAN. Для возврата 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, чтобы настроить время 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 на 30 минут.

```
Switch# configure terminal
Switch(config)#surveillance vlan aging 30
Switch(config)#
```

90.3 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 используется на портах доступа и гибридных портах.

Чтобы включить функцию Surveillance VLAN, необходимо ввести 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 ethernet 1/0/1
Switch(config-if)#surveillance vlan enable
Switch(config-if)#
```

90.4 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

Данная команда применяется, чтобы добавить один или несколько OUI Surveillance VLAN. OUI используется для идентификации трафика видеонаблюдения с помощью функции Surveillance VLAN.

Если MAC-адреса источника полученных пакетов соответствуют любому из шаблонов OUI, полученный пакет распознается как surveillance.

OUI, полученный с устройства видеонаблюдения в Surveillance VLAN, не может совпадать с OUI по умолчанию.

OUI по умолчанию не может быть удален.

Пример

В данном примере показано, как добавить OUI для устройств Surveillance.


```
Switch# configure terminal
Switch(config)# surveillance vlan mac-address 00-01-02-03-00-00 ff-ff-ff-ff-00-00 component-
type vms description user1
Switch(config)#
```

90.5 surveillance vlan qos

Данная команда используется, чтобы настроить приоритет CoS для входящего трафика Surveillance VLAN. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

surveillance vlan qos *COS-VALUE*
no surveillance vlan qos

Параметры

<i>COS-VALUE</i>	Укажите приоритет Surveillance VLAN в диапазоне от 0 до 7.
------------------	--

По умолчанию

Значение по умолчанию – 5.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда 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. Настроенное значение – 7.

```
Switch# configure terminal
Switch(config)# surveillance vlan qos 7
Switch(config)#
```

90.6 show surveillance vlan

Данная команда используется для отображения настроек Surveillance VLAN.

show surveillance vlan [**interface** [*INTERFACE-ID* [, | -]]]
show surveillance vlan device [**interface** [*INTERFACE-ID* [, | -]]]

Параметры

device	Укажите, чтобы отобразить информацию об изученных устройствах Surveillance.
interface	(Опционально.) Укажите, чтобы отобразить информацию о Surveillance VLAN на портах.
INTERFACE-ID	(Опционально.) Укажите порт, о котором необходимо отобразить информацию.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
–	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду для отображения настроек Surveillance VLAN.

Чтобы отобразить глобальные настройки Surveillance VLAN, введите команду **show surveillance vlan**. Для отображения настроек Surveillance VLAN на интерфейсах примените команду **show surveillance vlan interface**. Чтобы отобразить устройства Surveillance, информация о котором была получена через OUI, воспользуйтесь командой **show surveillance vlan device**.

Пример

В данном примере показано, как отобразить глобальные настройки Surveillance VLAN.

```
Switch#show surveillance vlan

Surveillance VLAN ID   : Unassigned
Surveillance VLAN CoS  : 5
Aging Time             : 720 minutes

Surveillance VLAN OUI  :

OUI Address           Mask                Component Type           Description
-----
--
28:10:7B:00:00:00     FF:FF:FF:E0:00:00     D-Link Device           IP Surveillance Device
28:10:7B:20:00:00     FF:FF:FF:F0:00:00     D-Link Device           IP Surveillance Device
B0:C5:54:00:00:00     FF:FF:FF:80:00:00     D-Link Device           IP Surveillance Device
F0:7D:68:00:00:00     FF:FF:FF:F0:00:00     D-Link Device           IP Surveillance Device

Total OUI : 4
Switch#
```

91. Команды портов коммутатора

91.1 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-TX и 1000Base-T, 2.5GBase-T, 5GBase-T и 10GBase-T параметр по умолчанию – **auto**.

Параметр для всех оптоволоконных портов в режиме дуплекса – **full**.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Пожалуйста, обратитесь к руководству по установке серии DMS-3130, чтобы получить информацию о возможностях портов коммутатора.

Чтобы включить функцию автосогласования, необходимо указать параметр **auto** или для скорости, или для режима дуплекса. При фиксированном значении режима дуплекса и указании параметра **auto** для скорости будет согласована только скорость. При фиксированном значении скорости и указании параметра **auto** для режима дуплекса будет согласован только режим дуплекса.

Функция автосогласования не будет поддерживаться на оптоволоконных портах.

Пример

В данном примере показано, как установить фиксированную скорость 100 Мбит/с и настроить режим дуплекса, определенный автосогласованием, на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# speed 100
Switch(config-if)# duplex auto
Switch(config-if)#
```

91.2 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. Фактическое действие, выполняемое средствами аппаратного обеспечения, может отличаться от заданного, так как возможность управления потоком настраивается как на текущем, так и на удаленном порту/устройстве.

При установлении фиксированной скорости заданная настройка управления потоком будет окончательной. При установлении скорости, определенной автосогласованием, окончательная примененная настройка управления потоком будет основана на согласовании настроек локального устройства и коммутатора. В данном случае настройка управления потоком осуществляется с помощью локального устройства.

Данная команда не поддерживается коммутаторами, объединенными в физический стек.

Пример

В данном примере показано, как включить управление потоком на интерфейсе Ethernet 1/0/1.

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

91.3 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

Режим по умолчанию – Auto-MDIX Mode.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда неприменима на порту, к которому подключен оптоволоконный кабель.

Пример

В данном примере показано, как настроить режим Auto-MDIX Mode на интерфейсе Ethernet 1/0/1.

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

91.4 speed

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



Примечание: пожалуйста, обратитесь к руководству по установке серии DMS-3130, чтобы получить информацию о поддерживаемой скорости на каждом порту.

speed { 100 | 1000 | 2500 | 5giga | 10giga | 25giga [master | slave] | auto [SPEED-LIST]}
no speed

Параметры

100	Укажите, чтобы установить скорость 100 Мбит/с.
1000	Укажите, чтобы установить скорость 1000 Мбит/с на медных портах.
10giga	Укажите, чтобы установить скорость 10 Гбит/с.
2500	Укажите, чтобы установить скорость 2500 Мбит/с.
5giga	Укажите, чтобы установить скорость 5 Гбит/с.
25giga	Укажите, чтобы установить скорость 25 Гбит/с.
master slave	Укажите статус порта: Master (основное устройство) или Slave (дополнительное устройство). Данный параметр не применим к устройствам, подключенным к оптоволоконным портам со скоростью 100 Мбит/с или 10/25 Гбит/с.
auto	Укажите, чтобы включить на медных портах функцию автосогласования, с помощью которой скорость и управление потоком будут согласованы с оборудованием на противоположной стороне. Функция автосогласования не поддерживается на оптоволоконных портах.
auto-downgrade	Укажите, чтобы включить автоматическое понижение анонсированной скорости. Автоматическое понижение анонсированной скорости не поддерживается на оптоволоконных портах.
SPEED-LIST	(Опционально.) Укажите список скоростей, применяемых для автосогласования. Если используются несколько скоростей, необходимо отделить их запятой (,). Если список скоростей не указан, будут анонсированы все варианты скорости.

По умолчанию

Для интерфейсов 100Base-TX, 1000Base-T, 2.5GBase-T, 5GBase-T и 10GBase-T по умолчанию скорость определяется автоматически.

По умолчанию на оптоволоконных портах будет установлена скорость 25 Гбит/с.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если указанная скорость не поддерживается аппаратно, будет отображено сообщение об ошибке.

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.

Для оптоволоконных портов функция автосогласования включена не будет.

Пример

В данном примере показано, как на интерфейсе Ethernet 1/0/1 включить автосогласование, при котором будут использоваться только скорости 100 Мбит/с или 1000 Мбит/с.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# speed auto 100,1000
Switch(config-if)#
```

91.5 speed auto-downgrade

Данная команда используется для включения автоматического понижения анонсированной скорости, в случае если соединение на доступной скорости невозможно. Чтобы отключить данную опцию, воспользуйтесь формой **no** этой команды.

speed auto-downgrade
no speed auto-downgrade

Параметры

Нет.

По умолчанию

По умолчанию данная опция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для включения автоматического понижения анонсированной скорости, в случае если соединение на доступной скорости невозможно.

Данная команда неприменима к оптоволоконным портам.

Пример

В данном примере показано, как включить автоматическое понижения анонсированной скорости.


```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#speed auto-downgrade
Switch(config-if)#
```

92. Команды управления системными файлами

92.1 boot config

Данная команда используется для указания конфигурационного файла, который будет применен при следующем запуске устройства.

boot config *URL*

Параметры

<i>URL</i>	Укажите URL конфигурационного файла, который будет применен 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

Данная команда предназначена для указания конфигурационного файла, который будет применен 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)#
```

92.2 boot image

Данная команда используется для указания файла образа, который будет применен при следующем запуске устройства.

boot image [*check*] *URL*

Параметры

check	(Опционально.) Укажите данный параметр для отображения информации о программном обеспечении для указанного файла (номер версии и описание модели).
--------------	--

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

Данная команда предназначена для указания файла образа, который будет применен 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» в качестве файла образа для загрузки.

```
Switch# configure terminal
Switch(config)# boot image c:/switch-image1
Switch(config)#
```

В примере ниже показано, как проверить указанный файл образа под именем «c:/runtime». Информация о файле будет отображена после подтверждения его контрольной суммы.

```
Switch#configure terminal
Switch(config)#boot image check c:/image1

-----
Image information
-----
Version: 1.00.009
Switch(config)#
```

В следующем примере показано, как проверить указанный файл образа под 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)#
```

92.3 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 применением 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#
```

92.4 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 применением 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...
```

92.5 configure replace

Данная команда используется для замены текущей конфигурации указанным конфигурационным файлом.

configure replace **{tftp: //location/filename | flash: FILENAME}** **[force]**

Параметры

tftp:	Укажите конфигурационный файл с TFTP-сервера.
<i>//location/filename</i>	Укажите URL конфигурационного файла на TFTP-сервере.
flash:	Укажите, что конфигурационный файл из NVRAM.
<i>FILENAME</i>	Укажите имя конфигурационного файла, хранящегося в NVRAM.
force	(Опционально.) Укажите, чтобы принудительно применить команду без дополнительного подтверждения.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду, чтобы заменить текущую конфигурацию указанным конфигурационным файлом. Текущая конфигурация будет удалена перед применением указанной конфигурации.



Примечание: при выполнении данной команды текущая конфигурация полностью меняется на конфигурацию указанного файла. В указанном конфигурационном файле должна быть представлена полная конфигурация, а не частичная.

Перед применением данной команды сохраните резервную копию конфигурации с помощью команды **сору** или выгрузите профиль конфигурации на TFTP-сервер.

Пример

В данном примере показано, как заменить текущую конфигурацию файлом «config.cfg», загруженным с TFTP-сервера.

```
Switch# configure replace tftp: //10.0.0.66/config.cfg
```

```
This will apply all necessary additions and deletions  
to replace the current running configuration with the  
contents of the specified configuration file, which is  
assumed to be a complete configuration, not a partial  
configuration. [y/n]: y
```

```
Accessing tftp://10.0.0.66/config.cfg...  
Transmission start...  
Transmission finished, file length 45422 bytes.  
Executing script file config.cfg .....  
Executing done
```

```
Switch#
```

В 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#
```

92.6 copy

Данная команда используется для копирования файлов.

copy *SOURCE-URL* *DESTINATION-URL*

copy *SOURCE-URL* {**tftp**: [*//LOCATION*]} *DESTINATION-URL*}

copy {**tftp**: [*//LOCATION*]} *SOURCE-URL*} *DESTINATION-URL*

Параметры

<i>SOURCE-URL</i>	Укажите URL источника исходного файла, который необходимо скопировать. Особые формы URL представлены следующими ключевыми словами: Укажите 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.
<i>DESTINATION-URL</i>	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 об unit в абсолютном пути будет назначен основное устройство (Master).

LOCATION	Укажите IPv4-адрес TFTP/FTP/RCP-сервера или IPv6-адрес TFTP/FTP-сервера.
----------	--

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Используйте данную команду для копирования файлов в файловую систему, загрузки/выгрузки конфигурационного файла или файла образа, загрузки системного журнала на TFTP-сервер. Чтобы выгрузить текущую конфигурацию или сохранить ее в качестве загрузочной конфигурации, укажите **running-config** в качестве URL источника. Чтобы сохранить текущую конфигурацию в качестве загрузочной конфигурации, укажите **startup-config** в качестве URL назначения.

Если в качестве назначения указана загрузочная конфигурация, файл источника будет скопирован в файл, указанный в команде **boot config**. Исходный файл загрузочной конфигурации будет перезаписан.

Чтобы применить необходимый конфигурационный файл к текущей конфигурации, при использовании команды **copy** укажите **running-config** в качестве URL назначения. Данный конфигурационный файл будет сразу же применен, используя метод **increment**. Указанная конфигурация будет объединена с текущей конфигурацией. Текущая конфигурация будет удалена только после применения указанной конфигурации.

Если в качестве источника указан системный журнал, а в качестве назначения указан URL, текущий системный журнал будет скопирован на указанный URL.

Чтобы отобразить файл на удаленном TFTP-сервере, необходимо использовать URL с префиксом «tftp: //».

Чтобы загрузить образ программного обеспечения, примените команду **copy tftp: //** для загрузки файла с TFTP-сервера в файловую систему. Чтобы указать данный файл в качестве файла образа для загрузки, введите 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#
```

В данном примере показан процесс 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 8315060 bytes.
Transmission to slave start..... Done.
Transmission to slave finished, file length 8315060 bytes.
Please wait, programming flash..... Done.
Wait slave programming flash complete...
Done.

Switch#
```

```
Switch# copy tftp: //10.1.1.254/image flash: image

Address of remote host [10.1.1.254]?
Source filename [image.had]?
Destination filename [image.had]?
Accessing tftp://10.1.1.254/image.had...
Transmission start...
Transmission finished, file length 8315060 bytes.
Transmission to slave start..... Done.
Transmission to slave finished, file length 8315060 bytes.
Please wait, programming flash..... Done.
Wait slave programming flash complete...
Done.

Switch#
```

92.7 ip tftp source-interface

Данная команда используется для указания интерфейса, IP-адрес которого будет применяться 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

<i>INTERFACE-ID</i>	Укажите интерфейс, IP-адрес которого 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 применен в качестве адреса источника для инициирования TFTP-пакетов. Чтобы загрузить программное обеспечение через порт управления Out-Of-Band Management Port, укажите ID интерфейса данного порта.

Данная команда поддерживает только интерфейсы Loopback, MGMT и VLAN.

Пример

В данном примере показано, как загрузить программное обеспечение через порт управления Out-Of-Band.

```
Switch# configure terminal
Switch(config)# ip tftp source-interface mgmt 0
Switch(config)#
```

92.8 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда используется для отображения настроек конфигурационного файла и загрузочного образа.

Пример

В данном примере показано, как отобразить информацию о загрузке системы.

```
Switch# show boot

Unit 2
  Boot image: /c:/image1
  Boot config: /c:/config.cfg

Switch#
```

92.9 show running-config

Данная команда используется для отображения команд текущего конфигурационного файла.

show running-config

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда используется для отображения текущей конфигурации.

Пример

В данном примере показано, как отобразить содержимое текущего конфигурационного файла.

```
Switch#show running-config

!Current Configuration:
!
!System Description "DMS-3130-30PS"
!System Software Version "1.01.006"
!System Up Time          "0 days 5 hrs 7 mins 1 secs"
!Current SNTP Synchronized Time: SNTP Client Mode Is Disabled
!
stack
member 3 2

configure terminal
time-range TIME01
periodic weekly Sunday 02:00 to Sunday 04:00
exit
ip http timeout-policy idle 1800
username test privilege 15 password 0 test
ssh user test authentication-method password
power-saving length-detection
power-saving dim-led time-range Screening-profile
line console
exit

line telnet
password 0 test
session-timeout 10
login local
exit

line ssh
exit

interface mgmt 0
ip address 192.168.0.1 255.255.255.0
exit
interface vlan 1
ip address 10.90.90.90 255.0.0.0
exit

interface null 0
exit
monitor session 1 destination remote vlan access-list ACL01 replace vlan 5
monitor session 2 destination remote vlan access-list test-ACL replace vlan 7
interface L2vlan 1
counting any rx
counting any tx
exit
exit

Switch#
```

92.10 show startup-config

Данная команда используется для отображения содержимого конфигурационного загрузочного файла.

show startup-config

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Команда 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
!Current Configuration:
!
!System Description "DMS-3130-30PS"
!System Software Version "1.01.006"
!System Up Time          "0 days 4 hrs 50 mins 21 secs"
!Current SNTP Synchronized Time: SNTP Client Mode Is Disabled
!
stack
member 3 2
configure terminal
time-range TIME01
periodic weekly Sunday 02:00 to Sunday 04:00
exit
ip http timeout-policy idle 1800
username test privilege 15 password 0 test
ssh user test authentication-method password
power-saving length-detection
power-saving dim-led time-range Screening-profile
line console
exit
line telnet
password 0 test
session-timeout 10
login local
exit
line ssh
exit
interface mgmt 0
ip address 192.168.0.1 255.255.255.0
exit
interface vlan 1
ip address 10.90.90.90 255.0.0.0
exit
interface null 0
exit
monitor session 1 destination remote vlan access-list ACL01 replace vlan 5
monitor session 2 destination remote vlan access-list test-ACL replace vlan 7
interface L2vlan 1
counting any rx
counting any tx
exit
exit
Switch#
```

93. Команды System Log

93.1 clear logging

Данная команда используется для удаления сообщений логирования из буфера системного логирования.

clear logging

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Команда позволяет удалить все сообщения логирования из буфера системного логирования.

Пример

В данном примере показано, как удалить все сообщения логирования из буфера системного логирования.

```
Switch# clear logging

Clear logging? (y/n) [n] y

Switch#
```

93.2 logging on

Данная команда используется для включения логирования системных сообщений. Чтобы отключить логирование системных сообщений, воспользуйтесь формой **no** этой команды.

logging on

no logging on

Параметры

Нет.

По умолчанию

По умолчанию опция включена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Для включения логирования системных сообщений используйте команду **logging on** в режиме Global Configuration Mode. Данная команда отправляет сообщения об отладке (debug) или ошибке (error) в процессе логирования, при котором сохраняются сообщения асинхронно с процессом, генерирующим данные сообщения. Чтобы отключить логирование системных сообщений, воспользуйтесь формой **no** этой команды.

Процесс логирования управляет распределением сообщений логирования на различные точки назначения, например, буфер логирования, сессии терминала, сервер syslog. Сообщения системного логирования также известны как сообщения системных ошибок. Логирование можно включить и отключить для каждой из точек назначения индивидуально, применив команды **logging buffered**, **logging server** и **logging global configuration**. Однако если отключена команда **logging on**, сообщения на данные точки назначения отправляться не будут. Если команда **logging on** включена, одновременно будет включен **logging buffered**.

Пример

В данном примере показано, как включить логирование системных сообщений.

```
Switch# configure terminal
Switch(config)# logging on
WARNING: The command takes effect and the logging buffered is enabled at the same time.
Switch(config)#
```

93.3 logging buffered

Данная команда используется для включения логирования системных сообщений в локальный буфер сообщений. Чтобы отключить логирование системных сообщений в локальный буфер сообщений, воспользуйтесь формой **no** этой команды. Примените команду **default logging buffered** для возврата 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 на этом уровне важности или более серьезном уровне будут логироваться в буфер сообщений. Доступны значения: от 0 до 7, где 0 – наиболее важный уровень. Коды уровней важности: emergencies (чрезвычайные) – система не работоспособна (0), alerts (предупреждения) – система требует немедленного вмешательства (1),
----------------	---

	critical – состояние системы критическое (2), errors – сообщения об ошибках (3), warnings – предупреждения о возможных проблемах (4), notifications – уведомления о нормальных, но важных событиях (5), informational – информационные сообщения (6), debugging – отладочные сообщения (7). Если значение не указано, значение уровня по умолчанию – warnings (4).
SEVERITY-NAME	(Опционально.) Укажите название уровня важности системных сообщений. Имена уровней важности: emergencies (0), alerts (1), critical (2), errors (3), warnings (4), notifications (5), informational (6), debugging (7).
discriminator	(Опционально.) Укажите discriminator для фильтрации сообщений, отправляемых в локальный буфер.
write-delay SECONDS	(Опционально.) Укажите задержку периодической записи буфера логирования во flash-память на указанное количество секунд.

По умолчанию

По умолчанию используется уровень важности warning (4).

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Системные сообщения можно логировать в локальный буфер сообщений, локальную консоль или в другие места. Сообщения должны быть введены в локальный буфер сообщений перед отправкой в другие точки назначения.

Команда не будет применена, если указанный discriminator не существует. В таком случае будут применяться настройки по умолчанию.

Укажите уровень важности сообщений для ограничения системных сообщений, логируемых в буфер (это позволит уменьшить число логированных сообщений). Сообщения указанного уровня или выше будут логироваться в буфер. Если буфер будет заполнен, старые записи будут удалены, чтобы освободить место, необходимое для новых сообщений.

Содержимое буфера сообщений периодически будет сохраняться во flash-память, чтобы сообщения можно было восстановить при перезагрузке. Интервал сохранения записей из буфера во flash-память можно указать. Содержимое сообщений логирования во flash будет перезагружено в буфер логирования при перезагрузке.

Пример

В данном примере показано, как включить логирование сообщений в буфер логирования и ограничить логирование сообщений с уровнем важности errors или выше.

```
Switch# configure terminal
Switch(config)# logging buffered severity errors
Switch(config)#
```

93.4 logging console

Данная команда используется для включения логирования системных сообщений в локальной консоли. Чтобы отключить логирование сообщений в локальной консоли и вернуть настройки по умолчанию, воспользуйтесь формой **no** этой команды.

logging console [severity {SEVERITY-LEVEL | SEVERITY-NAME}] [discriminator NAME]
no logging console

Параметры

SEVERITY-LEVEL	(Опционально.) Укажите уровень важности системных сообщений. Сообщения на этом уровне важности или более серьезном уровне будут логироваться в буфер сообщений. Значение может быть от 0 до 7, где 0 – наиболее важный уровень. Коды уровней важности: emergencies (чрезвычайные) – система не работоспособна (0), alerts (предупреждения) – система требует немедленного вмешательства (1), critical – состояние системы критическое (2), errors – сообщения об ошибках (3), warnings – предупреждения о возможных проблемах (4), notifications – сообщения о нормальных, но важных событиях (5), informational – информационные сообщения (6), debugging – отладочные сообщения (7). Если значение не указано, значение уровня по умолчанию – warnings (4).
SEVERITY-NAME	(Опционально.) Укажите название уровня важности системных сообщений. Имена уровней важности: emergencies (0), alerts (1), critical (2), errors (3), warnings (4), notifications (5), informational (6), debugging (7).
discriminator	(Опционально.) Укажите discriminator для фильтрации сообщений, отправляемых в локальный буфер.

По умолчанию

По умолчанию опция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Системные сообщения можно логировать в локальный буфер сообщений, локальную консоль или другие точки назначения. Сообщения должны быть введены в локальный буфер сообщений перед

отправкой в консоль.

Команда не будет применена, если указанный discriminator не существует. В таком случае будут применяться настройки по умолчанию.

Укажите уровень важности сообщений для ограничения системных сообщений, логируемых в консоли. Сообщения указанного уровня или выше будут логироваться в локальную консоль.

Пример

В данном примере показано, как включить логирование сообщений в локальную консоль и ограничить логирование сообщений с уровнем важности errors или выше.

```
Switch# configure terminal
Switch(config)# logging console severity errors
Switch(config)#
```

93.5 logging discriminator

Данная команда используется при создании discriminator для дальнейшей фильтрации syslog-сообщений, отправляемых в различные точки назначения. Чтобы удалить discriminator, воспользуйтесь формой **no** этой команды.

logging discriminator *NAME* [**facility** {**drops** *STRING* | **includes** *STRING*}] [**severity** {**drops** *SEVERITY-LIST* | **includes** *SEVERITY-LIST*}]
no discriminator *NAME*

Параметры

<i>NAME</i>	Укажите имя discriminator.
facility	(Опционально.) Укажите подфильтр согласно настройке facility.
<i>STRING</i>	Укажите одно или более имен facility. Если используется несколько имен, они должны быть разделены запятой, без пробелов до и после запятой.
includes	Укажите для включения совпадающих сообщений. Несовпадающие сообщения будут фильтроваться.
drops	Укажите для фильтрации совпадающих сообщений.
severity	(Опционально.) Укажите подфильтр на основе совпадений с уровнем важности.
<i>SEVERITY-LIST</i>	Укажите список уровней важности для фильтрации или включения.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Настройка существующего параметра discriminator. При вводе команды прежние настройки будут заменены новыми. Ассоциируйте discriminator с командами **logging buffered** и **logging server**.

Пример

В данном примере показано, как создать discriminator под именем «buffer-filter», указывающим два подфилтра, один на основе уровня важности, а другой на основе facility.

```
Switch# configure terminal
Switch(config)# logging discriminator buffer-filter facility includes STP severity includes 1-4,6
Switch(config)#
```

93.6 logging server

Данная команда используется для создания серверного узла syslog, чтобы логировать системные сообщения, или вывода при отладке. Чтобы удалить серверный узел syslog, воспользуйтесь формой **no** этой команды.

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 серверного узла syslog.
IPV6-ADDRESS	Укажите IPv6-адрес серверного узла логирования.
SEVERITY-LEVEL	(Опционально.) Укажите код уровня важности системных сообщений. Сообщения на этом уровне важности или более серьезном будут логироваться в буфер сообщений. Значение может быть от 0 до 7, где 0 – наиболее важный уровень. Коды уровней важности: emergencies – система не работоспособна (0), alerts – система требует немедленного вмешательства (1), critical – состояние системы критическое (2), errors – сообщения об ошибках (3), warnings – предупреждения о возможных проблемах (4), notifications – сообщения о нормальных, но важных событиях (5), informational – информационные сообщения (6), debugging – отладочные сообщения (7). Если значение не указано, значение уровня по умолчанию – 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).

<i>FACILITY-NUM</i>	(Опционально.) Укажите десятичное значение от 0 до 23 для facility. Если значение не указано, по умолчанию будет использоваться local7 (23). Для более подробной информации обратитесь к параграфу Использование команды .
<i>FACILITY-NAME</i>	(Опционально.) Укажите имя для facility. Если значение не указано, по умолчанию будет использоваться local7 (23). Для более подробной информации обратитесь к параграфу Использование команды .
discriminator NAME	(Опционально.) Укажите для фильтрации сообщений на сервер логирования согласно настройке discriminator.
port UDP-PORT	(Опционально.) Укажите номер порта UDP, который будет использоваться сервером syslog. Диапазон значений от 1024 до 65535, а также 514 (распространенный порт IANA). Если значение не указано, номер UDP-порта по умолчанию – 514.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Системные сообщения можно логировать в локальный буфер сообщений, локальную консоль или на удаленные узлы. Перед отправкой на сервер логирования сообщения должны быть введены в локальный буфер сообщений.

Ниже представлена таблица значений Facility.

Номер Facility	Имя Facility	Описание
0	kern	Сообщения ядра
1	user	Сообщения уровня пользователя
2	mail	Система почты
3	daemon	Системные daemon
4	auth1	Сообщения системы безопасности/авторизации
5	syslog	Сообщения, генерируемые syslog
6	lpr	Подсистема Line Printer
7	news	Подсистема сетевых новостей

8	uucp	Подсистема UUCP
9	clock1	Clock daemon
10	auth2	Сообщения системы безопасности/авторизации
11	ftp	FTP daemon
12	ntp	Подсистема NTP
13	logaudit	Аудит логирования
14	logalert	Предупреждение логирования
15	clock2	Clock daemon (note 2)
16	local0	Локальное использование 0 (local0)
17	local1	Локальное использование 1 (local1)
18	local2	Локальное использование 2 (local2)
19	local3	Локальное использование 3 (local3)
20	local4	Локальное использование 4 (local4)
21	local5	Локальное использование 5 (local5)
22	local6	Локальное использование 6 (local6)
23	local7	Локальное использование 7 (local7)

Пример

В данном примере показано, как включить логирование системных сообщений с уровнем важности выше warnings на удаленном узле 20.3.3.3.

```
Switch# configure terminal
Switch(config)# logging server 20.3.3.3 severity warnings
Switch(config)#
```

93.7 logging smtp

Данная команда позволяет настроить отправку системных сообщений на электронную почту. Чтобы отключить отправку системных сообщений на электронную почту и вернуть настройки по умолчанию, воспользуйтесь формой **no** этой команды.

logging smtp [severity {SEVERITY-LEVEL | SEVERITY-NAME}] [discriminator NAME]
no logging smtp

Параметры

<i>SEVERITY-LEVEL</i>	(Опционально.) Укажите код уровня важности системных сообщений. Сообщения на этом уровне важности или более серьезным уровнем будут логироваться в буфер сообщений. Значение может быть от 0 до 7, где 0 – наиболее важный уровень. Коды уровней важности: emergencies – система не работоспособна (0), alerts – система требует немедленного вмешательства (1), critical – состояние системы критическое (2), errors – сообщения об ошибках (3), warnings – предупреждения о возможных проблемах (4), notifications – сообщения о нормальных, но важных событиях (5), informational – информационные сообщения (6), debugging – отладочные сообщения (7). Если значение не указано, значение уровня по умолчанию – warnings (4).
<i>SEVERITY-NAME</i>	(Опционально.) Укажите название уровня важности системных сообщений. Имена уровней важности: emergencies (0), alerts (1), critical (2), errors (3), warnings (4), notifications (5), informational (6), debugging (7).
<i>discriminator NAME</i>	(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. Перед отправкой на электронную почту сообщения необходимо логировать в локальный буфер.

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)#
```


93.8 logging source-interface

Данная команда используется, чтобы указать IP-адрес интерфейса, который будет применяться в качестве адреса источника для отправки syslog-пакетов. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

logging source-interface *INTERFACE-ID*
no logging source-interface

Параметры

<i>INTERFACE-ID</i>	Укажите IP-адрес интерфейса, который будет использоваться в качестве адреса источника для отправки syslog-пакетов.
---------------------	--

По умолчанию

По умолчанию используется IP-адрес ближайшего интерфейса.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы задать IP-адрес интерфейса, который будет применяться в качестве адреса источника для отправки syslog-пакетов.

Для команды поддерживаются только интерфейсы Loopback, MGMT и VLAN.

Пример

В данном примере показано, как настроить VLAN 100 в качестве интерфейса источника для syslog-пакетов.

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

93.9 show logging

Данная команда используется для просмотра системных сообщений, хранящихся в локальном буфере.

show logging [**all** | [*REF-SEQ*] [**+** *NN* | **-** *NN*]]

Параметры

all	(Опционально.) Укажите для отображения всех записей журнала, начиная с последних.
------------	---

REF-SEQ	(Опционально.) Укажите для отображения с номера, следующего за указанным.
+ NN	(Опционально.) Укажите количество сообщений, появившихся после указанного номера, следующим за указанным. Если значение не указано, отображение начинается от самых давних сообщений в буфере.
- NN	(Опционально.) Укажите количество сообщений, появившихся до указанного номера, следующим за указанным. Если значение не указано, отображение начинается от самых последних сообщений в буфере.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Команда применяется для просмотра системных сообщений, хранящихся в локальном 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 параметры не указаны, будет отображено 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: 55
```

```
#55    2022-08-25 11:53:18 CRIT(2) System cold start
```

```
#54    2022-08-25 11:52:31 CRIT(2) Stacking topology is Chain. Master (Unit 2, MAC: 00-AD-24-A2-D6-00) .
```

```
#53    2022-08-24 17:48:26 CRIT(2) System warm start
```

93.10 show attack-logging

Данная команда используется для просмотра зарегистрированных сообщений об атаках.

show attack-logging unit *UNIT-ID* [index *INDEX*]

Параметры

<i>UNIT-ID</i>	Укажите модуль (unit), для которого необходимо отобразить зарегистрированные сообщения об атаке.
index <i>INDEX</i>	Укажите список порядковых номеров записей для отображения. Если значение не указано, отображаться будут все данные из журнала атак.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для просмотра зарегистрированных сообщений журнала об атаках. 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 unit 1 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#
```

93.11 clear attack-logging

Данная команда используется для удаления сообщений об атаках.

clear attack-logging {unit *UNIT-ID* | all}

Параметры

unit <i>UNIT-ID</i>	Укажите модуль (unit), для которого необходимо удалить логированные сообщения об атаке.
all	Укажите для удаления всех записей.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для удаления сообщений об атаках.

Пример

В данном примере показано, как удалить все зарегистрированные сообщения об атаках.

```
Switch# clear attack-logging all
Clear attack log? (y/n) [n] y

Switch#
```

94. Команды времени и SNTP

94.1 clock set

Данная команда используется для установки системного времени вручную.

clock set *HH:MM:SS DAY MONTH YEAR*

Параметры

<i>HH:MM:SS</i>	Укажите текущее время: часы (24-часовой формат), минуты и секунды.
<i>DAY</i>	Укажите текущий день месяца.
<i>MONTH</i>	Укажите текущий месяц (January, Jan, February, Feb и т. д.).
<i>YEAR</i>	Укажите текущий год без сокращений.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если система синхронизируется с помощью любого действующего внешнего механизма синхронизации, такого как SNTP, необходимо установить системное время. Используйте данную команду, если другие источники времени недоступны. Время, указанное в данной команде, принадлежит к часовому поясу, заданному конфигурацией команды **clock timezone**. Если устройство поддерживает функцию RTC (часы реального времени), время синхронизируется с RTC. Настроенные часы не будут сохранены в файле конфигурации.

Сервер SNTP является основным источником времени: даже если системное время было настроено вручную, при подключении к серверу SNTP время будет синхронизировано с его показателями.

Пример

В данном примере показано, как вручную установить системное время на 18:00, 4 июля 2013 г.

```
Switch# clock set 18:00:00 4 Jul 2013
Switch#
```

94.2 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.
<i>WEEK</i>	Укажите номер недели месяца (от 1 до 4) или слово «last», с помощью которого будет указана последняя неделя месяца.
<i>DAY</i>	Укажите день недели (sun, mon и т. д.).
<i>DATE</i>	Укажите день месяца (от 1 до 31).
<i>MONTH</i>	Укажите порядковый номер месяца в диапазоне от 1 до 12, где 1 – это январь, 2 – февраль и т. д.
<i>YEAR</i>	Укажите года, чтобы задать необходимый интервал для применения перехода на летнее время.
<i>HH:MM</i>	Укажите время (24-часовой формат) в часах и минутах.
<i>OFFSET</i>	(Опционально.) Укажите количество минут, которое нужно добавить при переходе на летнее время. Значение по умолчанию – 60. 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 применяется 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)#
```

94.3 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, которых необходимо прибавить к UTC.
-	Укажите количество часов, которых необходимо вычесть из UTC.
HOURS-OFFSET	Укажите разницу во времени с UTC в часах.
MINUTES-OFFSET	(Опционально.) Укажите разницу во времени с UTC в минутах.

По умолчанию

Часовой пояс по умолчанию – UTC.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Время, полученное с сервера SNTP, синхронизируется с форматом UTC. При 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)#
```

94.4 show clock

Данная команда используется для отображения информации о времени и дате.

show clock

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Также данная команда 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         : 18:09:39, 2022-08-25
Time Zone            : UTC +00:00
Daylight Saving Time : Disabled

Switch#
```

94.5 show sntp

Данная команда используется для отображения информации о сервере SNTP.

show sntp

Параметры

Нет.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения информации о сервере SNTP.

Пример

В данном примере показано, как отобразить информацию об SNTP.

```
Switch#show sntp

SNTP Status           : Enabled
SNTP Poll Interval    : 720 sec

SNTP Server Status:

SNTP Server           Version Last Receive
-----
10.0.0.11             4      00:02:02
10::2
FE80::1111vlan 1
-----

Total Entries:3

Switch#
```

94.6 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 отличие от NTP, не предоставляет сложные механизмы фильтрации и статистической обработки. Кроме того, SNTP не проверяет подлинность трафика, хотя с помощью настройки расширенного списка доступа можно обеспечить определённую степень защиты.

Введите данную команду один раз для каждого сервера NTP. Настроить систему и включить SNTP можно также с помощью команды **sntp broadcast client global configuration**. Чтобы создать несколько серверов SNTP, введите данную команду несколько раз, используя разные IP-адреса серверов SNTP.

Воспользуйтесь формой **no** этой команды, 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)#
```

94.7 sntp enable

Данная команда используется для включения функции SNTP. Чтобы отключить 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 используется для включения/отключения функции SNTP.

Пример

В данном примере показано, как включить функцию SNTP.

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

94.8 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. Указанное значение – 100 секунд.

```
Switch# configure terminal
Switch(config)# sntp interval 100
Switch(config)#
```

95. Команды временного диапазона

95.1 periodic

Данная команда используется в режиме Time-Range Configuration Mode 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 rdtme
Switch(config-time-range)# periodic daily 9:00 to 12:00
Switch(config-time-range)# periodic weekly saturday 00:00 to monday 00:00
Switch(config-time-range)# no periodic daily 9:00 to 12:00
Switch(config-time-range)#
```

95.2 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если параметр не указан, будут отображены все настроенные профили диапазона времени.

Пример

В данном примере показано, как отобразить все настроенные профили.

```
Switch#show time-range

Time Range Profile: lunchtime
Daily 12:00 to 13:00

Time Range Profile: rdttime
Weekly Saturday 00:00 to Monday 00:00
Daily 09:00 to 12:00

Total Entries :2

Switch#
```

95.3 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**, применяемой 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 под именем «rdtime».

```
Switch# configure terminal
Switch(config)# time-range rdtime
Switch(config-time-range)#
```

96. Команды Traffic Segmentation

96.1 show traffic-segmentation forward

Данная команда используется для отображения конфигурации Traffic Segmentation на указанных или всех портах.

show traffic-segmentation forward [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите интерфейсы для отображения. Допустимый интерфейс: физический порт или port-channel.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Если параметр не указан, будет отображена конфигурация Traffic Segmentation для всех портов.

Пример

В данном примере показано, как отобразить конфигурацию Traffic Segmentation для интерфейса Ethernet 1/0/1.

```
Switch#show traffic-segmentation forward interface ethernet 1/0/1

Interface      Forwarding Domain
-----
eth1/0/1       eth1/0/3-1/0/6

Total Entries: 1

Switch#
```

96.2 traffic-segmentation forward

Данная команда используется для ограничения продвижения пакетов в L2 домене, приходящих на настроенный порт. Чтобы удалить ограничения продвижения пакетов в L2 домене, воспользуйтесь формой **no** этой команды.

traffic-segmentation forward interface *INTERFACE-ID* [, | -]
no traffic-segmentation forward interface *INTERFACE-ID* [, | -]

Параметры

<i>INTERFACE-ID</i>	Укажите разрешенные интерфейсы необходимых физических портов.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Если домен продвижения пакетов задан Traffic Segmentation, то пакеты, получаемые на порту, будут ограничены пакетами, отправленными интерфейсами внутри заданного L2 домена. Если ограничение продвижения пакетов в домене L2 не указано, то получение на порту пакетов не ограничено.

Команду **traffic-segmentation forward** можно применять несколько раз. Все последующие интерфейсы будут добавлены в список участников домена. Воспользуйтесь формой **no** этой команды, 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 ethernet 1/0/1
Switch(config-if)#traffic-segmentation forward interface ethernet 1/0/3-6
Switch(config-if)#
```

97. Команды Virtual LAN (VLAN)

97.1 acceptable-frame

Данная команда используется для настройки допустимых типов кадров на порту. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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 параметром по умолчанию является **untagged-only**.

Для режима Other VLAN Mode параметром по умолчанию является **admit-all**.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда используется для настройки допустимых типов кадров на порту.

Пример

В данном примере показано, как настроить допустимый тип кадров **tagged-only** для интерфейса Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# acceptable-frame tagged-only
Switch(config-if)#
```

97.2 ingress-checking

Данная команда используется для включения проверки входящих кадров, получаемых на порту. Чтобы отключить проверку, воспользуйтесь формой **no** этой команды.

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 на интерфейсе. При включенной проверке пакет будет отброшен в том случае, если принимающий порт не является member-портом 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 ethernet 1/0/1
Switch(config-if)# ingress-checking
Switch(config-if)#
```

97.3 mac-vlan

Данная команда используется для создания привязки VLAN на основе MAC-адреса. Чтобы удалить привязку VLAN на основе MAC-адреса, воспользуйтесь формой **no** этой команды.

mac-vlan *MAC-ADDRESS* **vlan** *VLAN-ID* [**priority** *COS-VALUE*]

no mac-vlan *MAC-ADDRESS*

Параметры

<i>MAC-ADDRESS</i>	MAC-адрес для привязки.
vlan <i>VLAN-ID</i>	VLAN ID для привязки VLAN на основе MAC-адреса.
priority <i>COS-VALUE</i>	(Опционально.) Значение приоритета CoS. Если параметр не указан, то значением CoS по умолчанию является 0.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для создания привязки VLAN на основе MAC-адреса. Классификация привязки будет применена к пакетам, получаемым коммутатором. По умолчанию приоритет для классификации VLAN для нетегированного пакета является MAC-based > Subnet-based > Protocol VLAN.

Пример

В данном примере показано, как создать привязку VLAN ID на основе MAC-адреса для MAC-адреса 00-80-cc-00-00-11.

```
Switch# configure terminal
Switch(config)# mac-vlan 00-80-cc-00-00-11 vlan 101 priority 4
Switch(config)#
```

97.4 protocol-vlan profile

Данная команда используется для создания группы протоколов. Чтобы удалить определенную группу протоколов, воспользуйтесь формой **no** этой команды.

protocol-vlan profile *PROFILE-ID* **frame-type** {ethernet2 | snap | llc} **ether-type** *TYPE-VALUE*
no protocol-vlan profile *PROFILE-ID*

Параметры

<i>PROFILE-ID</i>	Группа протоколов, которую следует 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 <i>TYPE-VALUE</i>	Указывает тип. Данное значение должно быть 2-байтным в шестнадцатеричной форме.

По умолчанию

Нет.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду **protocol-vlan profile** в режиме Global Configuration Mode для создания группы протоколов. Затем используйте команду **protocol-vlan profile** в режиме Interface Configuration Mode для настройки классификации VLAN для группы протоколов, получаемых на порту.

Пример

В данном примере показано, как создать VLAN-группу протоколов с идентификатором группы 10, указав, что будет использоваться протокол IPv6 (тип кадров – Ethernet2, значение – 0x86dd).

```
Switch# configure terminal
Switch(config)# protocol-vlan profile 10 frame-type ethernet2 ether-type 0x86dd
Switch(config)#
```

97.5 protocol-vlan profile (Interface)

Данная команда используется, чтобы настроить привязку VLAN для группы протоколов на порту. Для удаления привязки VLAN на порту воспользуйтесь формой **no** этой команды.

protocol-vlan profile *PROFILE-ID* **vlan** *VLAN-ID* [**priority** *COS-VALUE*]
no protocol-vlan profile *PROFILE-ID*

Параметры

<i>PROFILE-ID</i>	Идентификатор группы протоколов, который должен классифицироваться.
vlan <i>VLAN-ID</i>	VLAN ID для protocol VLAN. Для каждой группы привязки может быть указан только один VLAN ID.
priority <i>COS-VALUE</i>	(Опционально.) Значение приоритета CoS. Если параметр не указан, то значением CoS по умолчанию является 0.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы указать VLAN для группы протоколов на порту. В результате, пакет, полученный на порту, который соответствует указанной группе протоколов, будет определен в указанную VLAN. VLAN не должна обязательно существовать для настройки команды. Приоритет

классификации VLAN для нетегированного пакета является MAC-based > Subnet-based > Protocol VLAN.

Пример

В данном примере показано, как создать привязку VLAN на интерфейсе Ethernet 1/0/1 для классификации пакетов в группе протоколов 10 в VLAN 3000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# protocol-vlan profile 10 vlan 3000
Switch(config-if)#
```

97.6 show protocol-vlan profile

Данная команда используется для отображения параметров настройки, касающихся protocol VLAN.

show protocol-vlan {profile [PROFILE-ID [, | -]] | interface [INTERFACE-ID [, | -]]}

Параметры

profile	Группа протоколов.
<i>PROFILE-ID</i>	(Опционально.) Группа протоколов 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 интерфейсов. Пробелы до и после дефиса недопустимы.
interface	Укажите интерфейсы для отображения.
<i>INTERFACE-ID</i>	(Опционально.) 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.

Любой режим конфигурирования.

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 с интерфейса Ethernet 1/0/1 по интерфейс Ethernet 1/0/3.

```
Switch# show protocol-vlan interface ethernet 1/0/1-3
```

Interface	Protocol Group ID	VLAN	Priority
eth1/0/1	1	1	5
eth1/0/2	10	3	0
	11	2001	4
	12	3002	1
eth1/0/3	2	100	6

```
Switch#
```

В примере ниже показано, как отобразить настройки профиля группы протоколов.

```
Switch#show protocol-vlan profile
```

Profile ID	Frame-type	Ether-type
1	Ethernet2	0x86DD (IPv6)
2	Ethernet2	0x0800 (IP)
3	Ethernet2	0x0806 (ARP)

```
Total Entries: 3
```

```
Switch#
```

97.7 show vlan

Данная команда используется, чтобы отобразить параметры для всех настроенных VLAN или одной VLAN на коммутаторе.

show vlan [VLAN-ID [, | -] | interface [INTERFACE-ID [, | -]] | mac-vlan]

Параметры

VLAN-ID	(Опционально.) Укажите список VLAN для отображения информации о member-портах. Если VLAN не указана, то отображаются все VLAN. 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.
interface <i>INTERFACE-ID</i>	(Опционально.) Укажите порт для отображения настроек, касающихся 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.) Указывается для отображения информации о VLAN на основе MAC-адресов.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить параметры для всех настроенных VLAN или одной VLAN на коммутаторе.

Пример

В данном примере показано, как отобразить все текущие записи VLAN.

```
Switch# show vlan

VLAN 1
  Name : default
  Tagged Member Ports  :
  Untagged Member Ports : 1/0/1-1/0/8

Total Entries : 1

Switch#
```

В примере ниже 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 ethernet 2/0/1-2/0/4

eth2/0/1
  VLAN mode           : Hybrid
  Native VLAN         : 1
  Hybrid untagged VLAN : 1
  Hybrid tagged VLAN   :
  Ingress checking     : Enable
  Acceptable frame type : Admit-All
  Dynamic tagged VLAN  :
  VLAN Precedence     : MAC-VLAN

eth2/0/2
  VLAN mode           : Hybrid
  Native VLAN         : 1
  Hybrid untagged VLAN : 1
  Hybrid tagged VLAN   :
  Ingress checking     : Enable
  Acceptable frame type : Admit-All
  Dynamic tagged VLAN  :
  VLAN Precedence     : MAC-VLAN

eth2/0/3
  VLAN mode           : Hybrid
  Native VLAN         : 1
  Hybrid untagged VLAN : 1
  Hybrid tagged VLAN   :
  Ingress checking     : Enable
  Acceptable frame type : Admit-All
  Dynamic tagged VLAN  :
  VLAN Precedence     : MAC-VLAN

eth2/0/4
  VLAN mode           : Hybrid
  Native VLAN         : 1
  Hybrid untagged VLAN : 1
  Hybrid tagged VLAN   :
  Ingress checking     : Enable
  Acceptable frame type : Admit-All
  Dynamic tagged VLAN  :
  VLAN Precedence     : MAC-VLAN

Switch#
```

В следующем 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#
```

97.8 switchport access vlan

Данная команда используется, чтобы указать access VLAN для интерфейса. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

switchport access vlan *VLAN-ID*
no switchport access vlan

Параметры

<i>VLAN-ID</i>	Укажите access VLAN интерфейса.
----------------	---------------------------------

По умолчанию

По умолчанию access VLAN является VLAN 1.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда вступает в силу, когда интерфейс настроен в режиме доступа (Access Mode) или режиме Dot1q-tunnel Mode. VLAN, указанная в качестве access VLAN, не должна обязательно существовать для настройки команды.

Может быть указана только одна access VLAN. Следующая команда перезаписывает предыдущую.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в режиме доступа (Access Mode) с access VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1000
Switch(config-if)#
```

97.9 switchport hybrid allowed vlan

Данная команда используется, чтобы указать тегированные или нетегированные VLAN для гибридного порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

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	Указывает порт в качестве тегированного для указанной (-ых) VLAN.
untagged	Указывает порт в качестве нетегированного для указанной (-ых) VLAN.
remove	Укажите порт, который необходимо удалить из указанной (-ых) VLAN.
VLAN-ID	Укажите список разрешенных VLAN или список VLAN, который необходимо добавить или удалить из списка разрешенных VLAN. Если параметр не задан, указанный список VLAN перезапишет список разрешенных 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 гибридный порт является нетегированным member-портом 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 member-портом нескольких VLAN.

Когда разрешенная VLAN указана только как VLAN ID, следующая команда перезапишет предыдущую команду. Если новый нетегированный разрешенный список VLAN перекрывается с текущим списком тегированных разрешенных VLAN, то перекрывающаяся часть будет изменена на нетегированную разрешенную VLAN. С другой стороны, если новый список тегированных разрешенных VLAN перекрывается с текущим списком нетегированных разрешенных VLAN, то перекрывающаяся часть

будет изменена на тегированную разрешенную VLAN. Последняя команда вступит в силу. 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 ethernet 1/0/1
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid allowed vlan add tagged 1000
Switch(config-if)# switchport hybrid allowed vlan add untagged 2000,3000
Switch(config-if)#
```

97.10 switchport hybrid native vlan

Данная команда используется для указания native VLAN ID гибридного порта. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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 – VLAN 1.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При настройке привязки гибридного порта к его native VLAN используйте команду **switchport hybrid allowed vlan**, чтобы добавить native VLAN в ее разрешенную VLAN. Указанная VLAN не должна обязательно существовать для применения этой команды. Команда вступает в силу, когда интерфейс настроен в гибридном режиме.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве гибридного интерфейса и задать PVID со значением 20.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid allowed vlan add untagged 1000,20
Switch(config-if)# switchport hybrid native vlan 20
Switch(config-if)#
```

97.11 switchport mode

Данная команда используется, чтобы указать режим VLAN для порта. Для возврата к настройкам по умолчанию воспользуйтесь формой **no** этой команды.

switchport mode {access | hybrid | trunk | dot1q-tunnel}
no switchport mode

Параметры

access	Укажите для работы порта в качестве порта доступа.
hybrid	Укажите для работы порта в качестве гибридного порта.
trunk	Укажите для работы порта в качестве trunk-порта.
dot1q-tunnel	Укажите для работы порта в качестве порта dot1q-tunnel.

По умолчанию

Параметр по умолчанию – **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-tunnel mode** порт действует как порт UNI в service VLAN.

При изменении режима switch-port mode настройки, связанные с VLAN и ассоциированные с предыдущим режимом, будут утеряны.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве trunk-порта.

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

97.12 switchport trunk allowed vlan

Данная команда используется для настройки VLAN, которым разрешено получать и отправлять трафик на указанный интерфейс в тегированном формате. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

switchport trunk allowed vlan {all | [add | remove | except] VLAN-ID [, | -]}
no switchport trunk allowed vlan

Параметры

all	Укажите для разрешения всех VLAN на интерфейсе.
add	Укажите для добавления указанного списка VLAN в список разрешенных VLAN.
remove	Укажите для удаления указанного списка VLAN из списка разрешенных VLAN.
except	Укажите для разрешения всех 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 диапазона VLAN. Использование пробела до и после дефиса недопустимо. 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 членом VLAN. Когда для разрешенной VLAN

установлен параметр **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 member-порта VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 1000
Switch(config-if)#
```

97.13 switchport trunk native vlan

Данная команда используется для указания native VLAN ID интерфейса в режиме trunk. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

switchport trunk native vlan {VLAN-ID | tag}
no switchport trunk native vlan [tag]

Параметры

VLAN-ID	Укажите native VLAN для trunk-порта.
tag	Укажите, чтобы включить режим тегирования 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 trunk-порт настроен в тегированном режиме (Tagged Mode) для native VLAN, допустимый тип кадров порта должен быть настроен как «tagged-only», чтобы принимать только тегированные кадры. Когда trunk-порт работает в нетегированном режиме (Untagged Mode) для native VLAN, передавая нетегированный пакет для native VLAN и тегированные пакеты для всех остальных VLAN, допустимые типы кадров порта должны быть настроены как «admit-all» для корректной работы.

Указанная VLAN не должна обязательно существовать для настройки команды.

Пример

В данном примере показано, как настроить интерфейс Ethernet 1/0/1 в качестве интерфейса trunk и native VLAN 20.


```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 20
Switch(config-if)#
```

97.14 vlan

Данная команда используется для добавления VLAN и входа в режим VLAN Configuration Mode. Чтобы удалить VLAN, воспользуйтесь формой **no** этой команды.

vlan *VLAN-ID* [, | -]
no vlan *VLAN-ID* [, | -]

Параметры

<i>VLAN-ID</i>	Укажите идентификатор VLAN, которая должны быть добавлена, удалена или настроена. Диапазон значений VLAN ID: от 1 до 4094. VLAN ID 1 не может быть удален.
,	(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

VLAN ID 1 существует в системе в качестве VLAN по умолчанию.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду **vlan** в режиме Global Configuration Mode для создания VLAN. Ввод команды **vlan** с VLAN ID обеспечивает вход в режим настройки VLAN (VLAN Configuration Mode). Ввод VLAN ID существующей VLAN не создает новую VLAN, но разрешает пользователю изменить параметры VLAN для указанной VLAN. Когда пользователь вводит ID новой VLAN, VLAN будет создана автоматически. Используйте команду **no vlan** для удаления VLAN. VLAN по умолчанию не может быть удален. Если удаленная VLAN является access VLAN порта, то access VLAN порта будет сброшена в VLAN 1.

Пример

В данном примере показано, как добавить новые VLAN, назначив новые VLAN с VLAN ID от 1000 до 1005.


```
Switch# configure terminal
Switch(config)# vlan 1000-1005
Switch(config-vlan)#
```

97.15 name

Данная команда используется для указания имени VLAN. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

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 (включая начальные нули), которые равны VLAN ID.

Режим ввода команды

VLAN Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для указания имени VLAN. Имя VLAN должно быть уникальным в административном домене.

Пример

В данном примере показано, как настроить имя VLAN «admin-vlan» для VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# name admin-vlan
Switch(config-vlan)#
```

98. Команды Virtual LAN (VLAN) Tunnel

98.1 switchport mode dot1q-tunnel

Данная команда используется для указания внутреннего идентификатора протокола тега (TPID, Tag Protocol Identifier) системы. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

switchport mode dot1q-tunnel

Параметры

Нет.

По умолчанию

По умолчанию порт коммутатора функционирует как гибридный порт.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

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

Порт 802.1Q tunnel выступает в роли UNI-порта сервисной VLAN. Trunk-порт, тегированный как member-порт сервисной VLAN, выступает в роли NNI-порта сервисной VLAN.

802.1Q tunnel может работать на основе порта (port-based tunnel), на основе VLAN (VLAN-based tunnel) или на основе потока (flow-based tunnel). В туннеле на основе порта все принятые пакеты отправляются через общую сервисную VLAN. В туннеле на основе VLAN пакеты могут отправляться через разные сервисные VLAN, при этом сервисная VLAN определяется на основе таблицы соответствия VLAN. В туннеле, основанном на потоке, пакеты отправляются через разные сервисные VLAN. Сервисная VLAN определяется согласно правилу соответствия VLAN на основе потока. Ниже указан приоритет (precedence) для классификации входящих пакетов:

flow-based VLAN tunnel > VLAN-based tunnel > port-based tunnel.

Для туннеля на основе портов сервисная VLAN задаётся командой **switchport access vlan**, то есть порт будет настроен как нетегированный member-порт сервисной VLAN.

Для туннеля на основе VLAN или туннеля на основе потока порт следует настроить как нетегированный member-порт всех сервисных VLAN, заданных в таблице или профиле соответствия. Нетегированное членство в сервисной VLAN задаётся командой **switchport hybrid allowed vlan**.

Пример

В данном примере показано, как перевести порт в режим Dot1q-tunnel Mode.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config)# switchport mode dot1q-tunnel
Switch(config)#
```

98.2 dot1q inner ethertype

Данная команда используется для указания внутреннего TPID системы. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

dot1q inner ethertype *VALUE*
no dot1q inner ethertype

Параметры

<i>VALUE</i>	Укажите внутренний TPID системы в шестнадцатеричном виде. 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. Указанное значение – 0x9100.

```
Switch# configure terminal
Switch(config)# dot1q inner ethertype 0x9100
Switch(config)#
```

98.3 dot1q tunneling ethertype

Данная команда используется для указания внешнего TPID сервисной VLAN. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

dot1q tunneling ethertype *VALUE*
no dot1q tunneling ethertype

Параметры

<i>VALUE</i>	Укажите внешний TPID сервисной VLAN в шестнадцатеричном виде. 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 member-порт 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, чтобы идентифицировать тег 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. Указанное значение – 0x88a8.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1q tunneling ethertype 0x88a8
Switch(config-if)#
```

98.4 switchport vlan mapping

Данная команда используется для указания записи VLAN Translation на trunk-порту или записи привязки сервисной VLAN на порту dot1q tunnel. Чтобы удалить запись VLAN Translation или запись 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

<i>ORIGINAL-VLAN</i>	Укажите исходный VLAN ID, соответствующий входящим пакетам, в диапазоне от 1 до 4094.
<i>ORIGINAL-INNER-VLAN</i>	(Опционально.) Укажите, чтобы сопоставить исходную внутреннюю VLAN с внутренним VID для входящих пакетов на порту в режиме trunk. Диапазон значений: от 1 до 4094.

<i>RESULTANT-VLAN</i>	Укажите translated ID сервисной VLAN в диапазоне от 1 до 4094, чтобы заменить исходную VLAN для соответствующих пакетов.
<i>RESULTANT-INNER-VLAN</i>	(Опционально.) Укажите новую внутреннюю (inner) VLAN, чтобы заменить исходную внутреннюю VLAN на порту в режиме Trunk Mode.
<i>DOT1Q-TUNNEL-VLAN</i>	Укажите, чтобы добавить ID сервисной VLAN для соответствующих пакетов на порту в режиме Dot1q-tunnel Mode.
<i>COS-VALUE</i>	(Опционально.) Укажите приоритет правила. Если приоритет тега сервисной VLAN не задан, будет использовано значение по умолчанию – 0.
,	(Опционально.) Используется для перечисления нескольких VLAN или 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

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применима исключительно 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.

В таблице ниже показаны действия пакетов при VLAN Mapping.

Конфигурация VLAN Mapping	Режим порта	Входящие пакеты	Действие с тегом	Исходящие пакеты
mapping original-vlan <i>ORIGINAL-VLAN resultant-vlan</i>	dot1q tunnel (UNI)	C-TAG	Замена C-TAG	Один S-TAG
vlan RESULTANT-VLAN	Trunk (NNI)	S-TAG	Замена S-TAG	Новый S-TAG
mapping original-vlan <i>ORIGINAL-VLAN dot1q-tunnel DOT1Q-TUNNEL-VLAN</i>	dot1q tunnel (UNI)	C-TAG	Добавление S-TAG	Двойной тег
mapping original-vlan <i>ORIGINAL-VLAN resultant-vlan</i> vlan RESULTANT-VLAN <i>RESULTANT-INNER-VLAN</i>	dot1q tunnel (UNI)	C-TAG	Добавление S-TAG Замена C-TAG	Двойной тег
mapping original-vlan <i>ORIGINAL-VLAN ORIGINAL-INNER-VLAN resultant-vlan</i> <i>RESULTANT-VLAN</i>	Trunk (NNI)	Двойной тег	Замена S-TAG	Новый S-TAG
mapping original-vlan <i>ORIGINAL-VLAN ORIGINAL-INNER-VLAN resultant-vlan</i> <i>RESULTANT-VLAN</i> <i>RESULTANT-INNER-VLAN</i>	Trunk (NNI)	Двойной тег	Замена S-TAG и C-TAG	Новый S-TAG и C-TAG

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 ethernet 1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport vlan mapping original-vlan 100 resultant-vlan 1100
Switch(config-if)# switchport vlan mapping original-vlan 200 resultant-vlan 1200
Switch(config-if)#
```

В примере ниже показано, как настроить записи VLAN Mapping на порту 802.1Q tunnel.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/2
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# switchport vlan mapping original-vlan 600 resultant-vlan 1600
Switch(config-if)# switchport vlan mapping original-vlan 700 dot1q-tunnel 1700
Switch(config-if)# switchport access vlan 1600
Switch(config-if)# switchport hybrid allowed vlan add untagged 1700
Switch(config-if)#
```

98.5 dot1q-tunnel insert dot1q-tag

Данная команда используется для вставки тега dot1q VLAN. Чтобы удалить вставку 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 ethernet 1/0/1
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# dot1q-tunnel insert dot1q-tag 10
Switch(config-if)#
```

98.6 vlan mapping miss drop

Данная команда используется, чтобы включить функцию VLAN Mapping Missdrop для отбрасывания несоответствующих пакетов. Для отключения функции 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 используется для интерфейсов физического порта и port-channel, на которых включен режим 802.1Q Tunnel Mode. При включенной функции VLAN Mapping Missdrop пакеты, исходная VLAN которых не соответствует записям и правилам VLAN Mapping, будут отброшены.

Пример

В данном примере показано, как включить функцию VLAN Mapping Missdrop для интерфейса порта 1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# vlan mapping miss drop
Switch(config-if)#
```

98.7 dot1q-tunnel trust inner-priority

Данная команда используется для установки доверенного приоритета dot1q. Чтобы удалить настройку, 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 ethernet 1/0/1
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# dot1q-tunnel trust inner-priority
Switch(config-if)#
```

98.8 vlan mapping profile

Данная команда используется для создания профиля VLAN Mapping или входа в режим конфигурации профиля VLAN Mapping. Чтобы удалить профиль VLAN Mapping, воспользуйтесь формой **no** этой команды.

vlan mapping profile ID [type [ethernet] [ip] [ipv6]]
no vlan mapping profile ID

Параметры

<i>ID</i>	Укажите ID профиля VLAN Mapping. ID с более низким значением имеет более высокий приоритет. 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 применяться 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)#
```

98.9 vlan mapping rule

Данная команда используется для настройки правил профиля VLAN Mapping. Чтобы удалить ранее настроенные правила, 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. 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 <i>VALUE</i>	(Опционально.) Укажите тип Ethernet.
src-ip <i>NETWORK-PREFIX</i>	(Опционально.) Укажите IPv4-адрес источника.
dst-ip <i>NETWORK-PREFIX</i>	(Опционально.) Укажите IPv4-адрес назначения.
src-ipv6 <i>IPV6-NETWORK-PREFIX</i> <i>PREFIX</i> <i>PREFIX-LENGTH</i>	(Опционально.) Укажите IPv6-адрес источника.
dst-ipv6 <i>IPV6-NETWORK-PREFIX</i> <i>PREFIX</i> <i>PREFIX-LENGTH</i>	(Опционально.) Укажите IPv6-адрес назначения.
dscp <i>VALUE</i>	(Опционально.) Укажите значение DSCP.
src-port <i>VALUE</i>	(Опционально.) Укажите номер TCP-порта/UDP-порта источника.
dst-port <i>VALUE</i>	(Опционально.) Укажите номер TCP-порта/UDP-порта назначения.
ip-protocol <i>VALUE</i>	(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 <i>VLAN-ID</i>	Укажите новый внешний (outer) VLAN ID.
priority <i>COS-VALUE</i>	(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 <i>VLAN-ID</i>	Укажите новый внутренний (inner) VLAN ID.

По умолчанию

Нет.

Режим ввода команды

VLAN Mapping Profile Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду для настройки правил профиля VLAN Mapping. Если профиль применен на интерфейсе, коммутатор сопоставит входящие пакеты в соответствии с правилами профиля. При соответствии пакетов правилу внешний (outer) VID будет добавлен или заменен. (Опционально.) Укажите приоритет нового внешнего тега или укажите новый внутренний (inner) VID пакетов.

Порядок соответствия зависит от порядкового номера правила профиля и прекращается при первом

совпадении. Если порядковый номер не указан, значение будет назначено автоматически. Порядковый номер начинается с 10 с шагом 10. На одном интерфейсе можно настроить несколько различных типов профилей.

Пример

В данном примере показано, как настроить правила для профиля 1 VLAN Mapping.

```
Switch# configure terminal
Switch(config)# vlan mapping profile 1 type ip
Switch(config-vlan-map)# rule 10 match src-ip 100.1.1.0/24 dot1q-tunnel outer-vid 100
Switch(config-vlan-map)# rule 20 match dst-ip 200.1.1.0/24 dot1q-tunnel outer-vid 200
Switch(config-vlan-map)#
```

98.10 switchport vlan mapping profile

Данная команда используется для применения правил профиля VLAN Mapping к указанному интерфейсу. Чтобы удалить привязку, воспользуйтесь формой **no** этой команды.

switchport vlan mapping profile *PROFILE-ID*
no switchport vlan mapping profile *PROFILE-ID*

Параметры

<i>PROFILE-ID</i>	(Опционально.) Укажите ID профиля VLAN Mapping.
-------------------	---

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы применить профиль VLAN Mapping к указанному физическому порту или port-channel в режиме Dot1q-tunnel Mode.

Если профиль применен к интерфейсу, коммутатор проверит входящие пакеты в соответствии с правилами профиля. Если пакеты соответствуют правилу, то к ним будет применено действие правила.

Если настроить порт не в соответствии с правилами режима Dot1q-tunnel Mode, конфигурация профиля VLAN Mapping будет удалена.

Пример

В данном примере показано, как настроить профиль VLAN Mapping и применить его для порта 1 802.1Q tunnel. Пакеты клиентов, поступающие из 100.1.1.0/24, будут добавлены в S-VLAN 100, а пакеты, поступающие на 200.1.1.0/24, будут добавлены в S-VLAN 200.

```
Switch# configure terminal
Switch(config)# vlan mapping profile 1 type ip
Switch(config-vlan-map)# rule 10 match src-ip 100.1.1.0/24 dot1q-tunnel outer-vid 100
Switch(config-vlan-map)# rule 20 match dst-ip 200.1.1.0/24 dot1q-tunnel outer-vid 200
Switch(config-vlan-map)# exit
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# switchport vlan mapping profile 1
Switch(config-if)#
```

98.11 show dot1q ethertype

Данная команда используется для отображения настроек TPID.

show dot1q ethertype [*INTERFACE-ID* [- | ,]]

Параметры

<i>INTERFACE-ID</i>	(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.

Любой режим конфигурирования.

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#
```

98.12 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 для отображения. Если интерфейсы не указаны, будут отображены все порты 802.1Q tunnel.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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#
```

98.13 show vlan mapping

Данная команда используется для отображения настроек VLAN Mapping.

show vlan mapping [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите интерфейсы для отображения. Если интерфейсы не указаны, будут отображены все VLAN Mapping.
,	(Опционально.) Используется для перечисления нескольких интерфейсов или отделения диапазона интерфейсов от предыдущего. Пробелы до и после запятой недопустимы.
-	(Опционально.) Используется для обозначения диапазона интерфейсов. Пробелы до и после дефиса недопустимы.

По умолчанию

Нет.

Режим ввода команды

User/Privileged EXEC Mode.

Любой режим конфигурирования.

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#
```

98.14 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.

Любой режим конфигурирования.

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#
```

99. Команды Virtual Router Redundancy Protocol (VRRP)

99.1 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 [new-master] [auth-fail]
no snmp-server enable traps vrrp [new-master] [auth-fail]

Параметры

new-master	(Опционально.) Укажите, чтобы настроить отправку trap для нового основного устройства (new master). Если отправка trap включена, при переходе устройства в режим Master будет выслано trap-сообщение.
auth-fail	(Опционально.) Укажите, чтобы настроить отправку trap ошибки аутентификации. Если отправка trap включена и маршрутизатором был получен пакет, ключ аутентификации или тип аутентификации которого конфликтует с ключом аутентификации или типом аутентификации этого маршрутизатора, будет выслано trap-сообщение.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы включить отправку VRRP trap. Если 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)#
```

99.2 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

<i>STRING</i>	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. У устройств в одной VRRP-группе должен быть 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)#
```

99.3 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

<i>VRID</i>	Укажите идентификатор виртуального маршрутизатора, чтобы распознавать группу VRRP. Диапазон значений: от 1 до 255.
<i>IP-ADDRESS</i>	Укажите IP-адрес для созданной группы виртуального маршрутизатора.

По умолчанию

Нет.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы создать виртуальный маршрутизатор и задать для него IP-адрес. Маршрутизаторы одной VRRP-группы должны быть настроены с помощью одного и того же ID и IP-адреса.

Группа виртуальных маршрутизаторов представлена одним идентификатором (Router 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.

VRID должен быть уникальным при включении VRRPv2 и VRRPv3 на одном и том же IP-интерфейсе.

Пример

В данном примере показано, как создать VRRP-группу на интерфейсе VLAN 1. Идентификатор виртуального маршрутизатора – 7. IP-адрес виртуального маршрутизатора – 10.1.1.1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp 7 ip 10.1.1.1
Switch(config-if)#
```

99.4 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)#
```

99.5 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)#
```

99.6 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 недоступным. Виртуальные маршрутизаторы одной VRRP-группы должны использовать одинаковые значения таймера.

Пример

В данном примере показано, как указать интервал между VRRP advertisement для VRRP 7 на интерфейсе VLAN 1. Настроенный интервал – 10 секунд.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp 7 timers advertise 10
Switch(config-if)#
```

99.7 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 vlan 1
Switch(config-if)# vrrp 7 preempt
Switch(config-if)#
```

99.8 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)#
```

99.9 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)#
```

99.10 show vrrp

Данная команда используется для отображения настроек VRRP.

show vrrp [interface *INTERFACE-ID* [*VRID*]]

Параметры

<i>INTERFACE-ID</i>	(Опционально.) Укажите ID интерфейса.
<i>VRID</i>	(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 2 - Version2
  State is Master
  Virtual IP Address is 192.168.0.3
  Virtual MAC Address 00-00-5E-00-01-02
  Advertisement interval is 1 seconds
  Preemption is enabled
  Priority is 100
  No critical IP address
  Master Router is 10.90.90.90
Total Entries: 1

Switch#
```

99.11 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      2    2  NA  100      Y  Master 192.168.0.3
Total Entries: 1

Switch#
```

100. Команды Virtual Router Redundancy Protocol Version 3 (VRRPv3)

100.1 vrrp address-family

Данная команда используется для создания виртуального VRRP-маршрутизатора и входа в режим Address Family Configuration Mode с использованием IPv4 или IPv6. Чтобы удалить группу, 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. 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 vlan 3
Switch(config-if)#vrrp 1 address-family ipv4
Switch(config-af-vrrp)#
```

100.2 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. Чтобы отключить ответ 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 vlan 3
Switch(config-if)#vrrp 1 address-family ipv4
Switch(config-af-vrrp)#non-owner-ping
Switch(config-af-vrrp)#
```

100.3 address

Данная команда используется, чтобы настроить виртуальный адрес 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

<i>IP-ADDRESS</i>	Укажите виртуальный IPv4-адрес виртуального маршрутизатора.
<i>IPV6 -ADDRESS</i>	Укажите виртуальный IPv6-адрес виртуального маршрутизатора.

По умолчанию

Нет.

Режим ввода команды

VRRP Address Family Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить виртуальный адрес IPv4 или IPv6 для одного виртуального маршрутизатора. Маршрутизаторы одной VRRP-группы должны быть настроены с помощью одного и того же ID и адреса. IP-адрес может быть как действительным адресом, настроенным на маршрутизаторах, так и неиспользуемым адресом. Если виртуальный адрес совпадает с действительным адресом интерфейса, данный виртуальный маршрутизатор является владельцем IP-адреса.

Пример

В данном примере показано, как настроить виртуальный адрес IPv4 для VRRP-группы.

```
Switch#configure terminal
Switch(config)#interface vlan 3
Switch(config-if)#vrrp 1 address-family ipv4
Switch(config-af-vrrp)#address 10.1.1.1
Switch(config-af-vrrp)#
```

100.4 priority

Данная команда используется для настройки приоритета виртуального маршрутизатора. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

priority *PRIORITY*
no priority

Параметры

<i>PRIORITY</i>	Укажите приоритет виртуального маршрутизатора в диапазоне от 1 до 254.
-----------------	--

По умолчанию

Приоритет по умолчанию – 100.

Режим ввода команды

VRRP Address Family Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Основное устройство (Master) VRRP-группы определяется исходя из приоритета. Виртуальный

маршрутизатор с наивысшим приоритетом становится основным устройством (Master), а другие маршрутизаторы с более низким приоритетом становятся резервными устройствами (Backup) для VRRP-группы. Если значения приоритетов маршрутизаторов равны, сравниваются их IP-адреса – маршрутизатору с наибольшим IP-адресом будет присвоен статус основного устройства (Master).

Маршрутизатор, владеющий IP-адресом VRRP-группы, всегда выступает в роли основного устройства (Master) и имеет самый высокий приоритет – 255.

Пример

В данном примере показано, как настроить приоритет. Указанное значение – 200.

```
Switch#configure terminal
Switch(config)#interface vlan 3
Switch(config-if)#vrrp 1 address-family ipv4
Switch(config-af-vrrp)#priority 200
Switch(config-af-vrrp)#
```

100.5 timers advertise

Данная команда используется для настройки интервала между последовательными VRRP advertisement. Чтобы вернуться к настройкам по умолчанию, воспользуйтесь формой **no** этой команды.

timers advertise *INTERVAL*
no timers advertise

Параметры

<i>INTERVAL</i>	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

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 – 1000 сантисекунд.

```
Switch#configure terminal
Switch(config)#interface vlan 3
Switch(config-if)#vrrp 1 address-family ipv4
Switch(config-af-vrrp)#timers advertise 1000
Switch(config-af-vrrp)#
```

100.6 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.

preempt

no preempt

Параметры

Нет.

По умолчанию

По умолчанию используется режим Preempt Mode.

Режим ввода команды

VRRP Address Family Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте команду **no preempt**, чтобы отключить функцию Preempt для сохранения статуса участников VRRP-группы.

Пример

В данном примере показано, как отключить функцию Preempt.

```
Switch#configure terminal
Switch(config)#interface vlan 3
Switch(config-if)#vrrp 1 address-family ipv4
Switch(config-af-vrrp)#no preempt
Switch(config-af-vrrp)#
```

100.7 shutdown

Данная команда используется для отключения виртуального маршрутизатора. Чтобы вернуться 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 vlan 3
Switch(config-if)#vrrp 1 address-family ipv4
Switch(config-af-vrrp)#shutdown
Switch(config-af-vrrp)#
```

100.8 track critical-ip

Данная команда используется для настройки критического IP-адреса виртуального маршрутизатора. Чтобы удалить критический IP-адрес, воспользуйтесь формой **no** этой команды.

track critical-ip {IP-ADDRESS | [INTERFACE-ID] IPV6-ADDRESS}
no track critical-ip

Параметры

<i>IP-ADDRESS</i>	Укажите критический IP-адрес.
<i>INTERFACE-ID</i>	(Опционально.) Укажите интерфейс критического IP-адреса, который необходимо использовать.
<i>IPV6-ADDRESS</i>	Укажите 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)#
```

100.9 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. 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

vlan2 - Group 1 - Version3 - Address-Family IPv6
  State is Master
  Virtual IP Address is fe80::1
  Virtual MAC Address 00-00-5E-00-02-01
  Advertisement interval is 100 centi-seconds
  Preemption is enabled
  Priority is 100
  No critical IP address
  Disable non owner ping
  Master Router is fe80::6263:4cff:fe51:6083
Total Entries: 1

Switch#
```

101. Команды Voice VLAN

101.1 voice vlan

Данная команда используется для глобального включения функции Voice VLAN и её настройки. Чтобы отключить функцию, воспользуйтесь формой **no** этой команды.

```
voice vlan VLAN-ID  
no voice vlan
```

Параметры

VLAN-ID	Укажите VLAN 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. Заданную 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)#
```

101.2 voice vlan aging

Данная команда используется, чтобы настроить время устаревания (Aging Time) для устаревших динамических member-портов Voice VLAN. Для возврата 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, чтобы настроить время 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 на 30 минут.

```
Switch# configure terminal
Switch(config)# voice vlan aging 30
Switch(config)#
```

101.3 voice vlan enable

Данная команда используется для включения функции Voice VLAN на портах. Чтобы отключить функцию, 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 ethernet 1/0/1
Switch(config-if)# voice vlan enable
Switch(config-if)#
```

101.4 voice vlan mac-address

Данная команда используется для добавления уникального идентификатора организации (OUI), определяемого с устройства системы IP-телефонии. Чтобы удалить OUI устройства системы IP-телефонии, воспользуйтесь формой **no** этой команды.

voice vlan mac-address *MAC-ADDRESS MASK* [*description TEXT*]
no voice vlan mac-address *MAC-ADDRESS MASK*

Параметры

<i>MAC-ADDRES</i>	Укажите MAC-адрес OUI.
<i>MASK</i>	Укажите соответствующую битовую маску MAC-адреса OUI.
description <i>TEXT</i>	(Опционально.) Укажите описание 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, чтобы добавить уникальный идентификатор организации (OUI), определяемого с устройства системы IP-телефонии. OUI применяется для идентификации VoIP-трафика с помощью функции Voice VLAN. Если MAC-адреса источника полученных пакетов соответствуют любому из шаблонов OUI, полученные пакеты распознаются как VoIP-пакеты.

OUI, определяемый с устройства системы IP-телефонии, не может совпадать с OUI по умолчанию. OUI по умолчанию не может быть удален.

Пример

В данном примере показано, как добавить OUI для устройства системы IP-телефонии.

```
Switch# configure terminal
Switch(config)# voice vlan mac-address 00-02-03-00-00-00 FF-FF-FF-00-00-00 description User1
Switch(config)#
```

101.5 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 членство Voice VLAN автоматически.
tag	Укажите, чтобы изучить тегированных member-портов Voice VLAN.

untag Укажите, чтобы изучить нетегированных member-портов 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 Tagged Mode**) и фиксирует VoIP-устройство через OUI, он автоматически присоединится к Voice VLAN как тегированный порт. Если VoIP-устройство отправляет тегированные пакеты, коммутатор изменит их приоритет. Нетегированные пакеты отправляются в PVID VLAN порта.

Когда порт работает в авнетегированном режиме (**Auto Untagged Mode**) и получает информацию о VoIP-устройстве через OUI, он автоматически присоединится к Voice VLAN как нетегированный порт. Если VoIP-устройство отправляет тегированные пакеты, коммутатор изменит их приоритет. Нетегированные пакеты отправляются в Voice VLAN.

Когда коммутатор принимает пакеты LLDP-MED, он проверяет VLAN ID, флаги тега и приоритета, настройкам которых он должен следовать.

Если автоматическое изучение отключено, используйте команду **switchport hybrid vlan** для настройки порта в качестве тегированного или нетегированного member-порта Voice VLAN.

Пример

В данном примере показано, как настроить автотегированный режим (**Auto Tagged Mode**) на интерфейсе Ethernet 1/0/1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# voice vlan mode auto tag
Switch(config-if)#
```

101.6 voice vlan qos

Данная команда используется для настройки приоритета CoS для входящего трафика Voice VLAN. Используйте форму **no**, чтобы вернуться к настройкам по умолчанию.

voice vlan qos COS-VALUE
no voice vlan qos

Параметры

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 применяется 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 со значением 7.

```
Switch# configure terminal
Switch(config)# voice vlan qos 7
Switch(config)#
```

101.7 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.
Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Данная команда используется для отображения настроек Voice VLAN.

Пример

В данном примере показано, как отобразить глобальные настройки Voice VLAN.

```
Switch#show voice vlan

Voice VLAN ID      : 3
Voice VLAN CoS     : 5
Aging Time         : 720 minutes
Member Ports       : eth1/0/1-1/0/5
Dynamic Member Ports : eth1/0/1-1/0/3

Voice VLAN 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 ethernet 1/0/6-10
```

Interface	State	Mode
-----	-----	-----
eth1/0/6	Enabled	Manual
eth1/0/7	Enabled	Manual
eth1/0/8	Enabled	Manual
eth1/0/9	Enabled	Manual
eth1/0/10	Disabled	Auto/Untag

```
Switch#
```

В следующем примере показано, как отобразить распознанные VoIP-устройства на интерфейсах Ethernet 1/0/1-1/0/2.

```
Switch#show voice vlan device interface ethernet 1/0/1-2
```

Interface	Device Address	Start Time	Status
-----	-----	-----	-----
eth1/0/1	00-03-6B-00-00-01	2012-03-19 09:00	Active
eth1/0/1	00-03-6B-00-00-02	2012-03-20 10:09	Aging
eth1/0/1	00-03-6B-00-00-05	2012-03-20 12:04	Active
eth1/0/2	00-03-6B-00-00-0a	2012-03-19 08:11	Aging
eth1/0/2	33-00-61-10-00-11	2012-03-20 06:45	Aging

```
Total Entries: 5
```

```
Switch#
```

В нижеприведенном примере показано, как отобразить VoIP-устройства, обнаруженные через LLDP-MED, на интерфейсах Ethernet1/0/1-1/0/2.

```
Switch# show voice vlan lldp-med device interface eth1/0/1-2
```

```
Index           : 1  
Interface       : eth1/0/1  
Chassis ID Subtype : MAC Address  
Chassis ID      : 00-E0-BB-00-00-11  
Port ID Subtype  : Network Address  
Port ID         : 172.18.1.1  
Create Time     : 2012-03-19 10:00  
Remain Time     : 108 Seconds
```

```
Index           : 2  
Interface       : eth1/0/2  
Chassis ID Subtype : MAC Address  
Chassis ID      : 00-E0-BB-00-00-12  
Port ID Subtype  : Network Address  
Port ID         : 172.18.1.2  
Create Time     : 2012-03-20 11:00  
Remain Time     : 105 Seconds
```

```
Total Entries: 2
```

```
Switch#
```

102. Команды Web-аутентификации

102.1 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 аутентификации узлов, подключенных к порту, через Web-браузер.

Пример

В данном примере показано, как включить функцию Web-аутентификации на интерфейсе Ethernet 1/0/1.

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

102.2 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 <i>STRING</i>	Укажите заголовок страницы Web-аутентификации. Максимальное количество символов – 128.
login-window-title <i>STRING</i>	Укажите заголовок окна для ввода логина/пароля страницы Web-аутентификации. Максимальное количество символов – 64.
username-title <i>STRING</i>	Укажите название поля для ввода имени пользователя на странице Web-аутентификации. Максимальное количество символов – 32.
password-title <i>STRING</i>	Укажите название поля для ввода пароля на странице Web-аутентификации. Максимальное количество символов – 32.
logout-window-title <i>STRING</i>	Укажите заголовок окна выхода из системы (logout) на странице Web-аутентификации. Максимальное количество символов – 64.
copyright-line <i>LINE-</i> NUMBER title <i>STRING</i>	Укажите информацию об авторских правах построчно на страницах Web-аутентификации. Максимальное количество строк – 5. Максимальное количество символов для каждой строки – 128.

По умолчанию

Заголовок страницы по умолчанию не установлен.

Заголовок окна для ввода логина/пароля по умолчанию – «Authentication Login».

Название поля для ввода имени пользователя по умолчанию – «User Name».

Название поля для ввода пароля по умолчанию – «Password».

Заголовок окна выхода из системы (logout) по умолчанию – «Logout From The Network».

Информация об авторских правах по умолчанию не указана.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Элементы страницы Web-аутентификации могут быть настроены от имени администратора. Существуют две страницы Web-аутентификации: (1) страница входа и (2) страница выхода.

Введите имя пользователя и пароль на странице входа. Используйте кнопку **Logout**, чтобы выйти из сети.

Пример

В данном примере показано, как изменить информацию об авторских правах в двух строках нижней части страницы аутентификации:

Строка 1: Copyright @ 2018 All Rights Reserved

Строка 2: Site: http://support.website.com

```
Switch# configure terminal
Switch(config)# web-auth page-element copyright-line 1 title Copyright @ 2018 All Rights Reserved
Switch(config)# web-auth page-element copyright-line 2 title Site: http://support.website.com
Switch(config)#
```

102.3 web-auth success redirect-path

Данная команда используется для настройки URL, на который клиент будет по умолчанию 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

<i>STRING</i>	Укажите URL, на который клиент будет по умолчанию переадресован после успешной аутентификации. Если URL не указан, будет отображена страница выхода Web-аутентификации. Максимальное количество символов переадресации – 128.
---------------	---

По умолчанию

По умолчанию отображается страница выхода Web-аутентификации.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Данная команда применяется для указания Web-страницы, которую необходимо отобразить узлам, прошедшим Web-аутентификацию.

Пример

В данном примере показано, как настроить путь переадресации, который будет использован по умолчанию после прохождения Web-аутентификации. Указанный путь – http://www.website.com.

```
Switch# configure terminal
Switch(config)# web-auth success redirect-path http://www.website.com
Switch(config)#
```

102.4 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

Включите функцию Web-аутентификации, чтобы получить доступ к сети Интернет через коммутатор. Коммутатор может выступать как в роли сервера аутентификации, выполняя аутентификацию на основе локальной базы данных, так и в роли клиента RADIUS, выполняя процесс аутентификации по протоколу RADIUS с помощью удаленного сервера RADIUS. В процессе аутентификации используется протокол HTTP или HTTPS.

Пример

В данном примере показано, как включить функцию Web-аутентификации на коммутаторе глобально.

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

102.5 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.

Все процессы Web-аутентификации взаимодействуют с данным IP-адресом. Однако из-за того, что виртуальный IP-адрес не отвечает ни на один пакет ICMP или запрос ARP, настройка виртуального IP-адреса в той же подсети, что и IP-адреса интерфейса коммутатора или подсети узла недопустима. В противном случае, функция Web-аутентификация будет работать некорректно.

Перед использованием указанного URL необходимо настроить виртуальный IP-адрес. Чтобы получить виртуальный IP-адрес, используйте FQDN URL, который хранится на DNS-сервере. Полученный IP-адрес должен соответствовать виртуальному IP-адресу, настроенному с помощью команды. Если IPv4 или IPv6-адрес не настроен, Web-аутентификация невозможна.

Пример

В данном примере показано, как настроить виртуальный IPv4 и FQDN URL для Web-аутентификации. 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)#
```

102.6 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)#
```

103. Команды Weighted Random Early Detection (WRED)

103.1 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

<i>COS-VALUE</i>	Укажите очереди CoS, для которых необходимо включить функцию WRED. Диапазон значений: от 0 до 7.
<i>profile ID</i>	(Опционально.) Укажите профиль WRED, который необходимо применить. Если профиль не указан, будет использовано пороговое значение по умолчанию.

По умолчанию

По умолчанию данная функция отключена.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

При получении пакета текущий средний размер очереди рассчитывается аппаратно.

$$avg_Qsize = current_Qsize + \frac{old_avg_Qsize - current_Qsize}{2^{weight}}$$

Если текущий средний размер очереди меньше минимального порогового значения, поступающий пакет помещается в очередь. Если текущая длина очереди находится между минимальным и максимальным пороговыми значениями очереди, пакет будет либо отброшен, либо будет помещен в очередь в зависимости от вероятности отбрасывания пакета, которая рассчитывается по следующей формуле:

$$Drop\ Probability = \frac{avg_Qsize - MinThreshold}{MaxThreshold - MinThreshold} * MaxDropRate$$

Если средний размер очереди превышает максимальное пороговое значение, будут отброшены все пакеты. Если указанный профиль не существует, будет использовано пороговое значение по умолчанию.

Пример

В данном примере показано, как включить функцию WRED для очереди 5 на интерфейсе Ethernet 1/0/1 и применить профиль 10 WRED.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# random-detect 5 profile 10
Switch(config-if)#
```

103.2 random-detect exponential-weight

Данная команда используется, чтобы настроить exponential weight factor WRED для расчета среднего размера очереди. Для возврата 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

<i>COS-VALUE</i>	Укажите очереди CoS, на которых необходимо установить экспоненту. Диапазон значений: от 0 до 7.
exponent <i>VALUE</i>	Укажите значение экспоненты в диапазоне от 0 до 15.

По умолчанию

Exponential weight factor по умолчанию – 9.

Режим ввода команды

Interface Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Используйте данную команду, чтобы настроить exponential weight factor WRED для расчета среднего размера очереди.

Пример

В данном примере показано, как настроить значение экспоненты для очереди 5 на интерфейсе Ethernet 1/0/1. 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)#
```

103.3 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* [**green** | **yellow** | **red**] **min-threshold** *VALUE* **max-threshold** *VALUE*

max-drop-rate *VALUE*
no random-detect profile *ID*

Параметры

<i>ID</i>	Укажите ID профиля WRED, который необходимо установить.
green	(Опционально.) Укажите параметры отбрасывания WRED, которые необходимо установить для зеленых пакетов.
yellow	(Опционально.) Укажите параметры отбрасывания WRED, которые необходимо установить для желтых пакетов.
red	(Опционально.) Укажите параметры отбрасывания WRED, которые необходимо установить для красных пакетов.
min-threshold <i>VALUE</i>	Укажите минимальное количество ячеек в очереди, после достижения которого пакеты будут отброшены при помощи WRED.
max-threshold <i>VALUE</i>	Укажите максимальное количество ячеек в очереди, после достижения которого все пакеты, предназначенные для данной очереди, будут отброшены при помощи WRED.
max-drop-rate <i>VALUE</i>	Укажите вероятность сброса, в случае если средний размер очереди достигнет максимального порога. Если значение равно нулю, пакет не будет отброшен или отмечен для ECN.

По умолчанию

Значение параметра **min-threshold** по умолчанию – 20.

Значение параметра **max-threshold** по умолчанию – 80.

Значение параметра **max-drop-rate** по умолчанию – 0.

Режим ввода команды

Global Configuration Mode.

Уровень команды по умолчанию

Уровень 12.

Использование команды

Различные типы пакетов могут быть поставлены в очередь в разных bucket lists, для которых могут быть заданы различные пороговые значения.

Пример

В данном примере показано, как настроить параметры отбрасывания WRED для пакетов всех типов и цветов в профиле 10.

```
Switch# configure terminal
Switch(config)# random-detect profile 10 min-threshold 30 max-threshold 50 max-drop-rate 10
Switch(config)#
```

103.4 show queueing random-detect

Данная команда используется для отображения настроек WRED на указанном интерфейсе.

show queueing random-detect [interface *INTERFACE-ID* [, | -]]

Параметры

interface <i>INTERFACE-ID</i>	(Опционально.) Укажите ID интерфейса 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.

Любой режим конфигурирования.

Уровень команды по умолчанию

Уровень 1.

Использование команды

Используйте данную команду, чтобы отобразить настройки WRED. Если ID интерфейса не указан, будут отображены настройки WRED для всех портов системы.

Пример

В данном примере показано, как отобразить настройки WRED и состояние очереди CoS на интерфейсе Ethernet 1/0/1.

```
Switch#show queueing random-detect interface ethernet 1/0/1

Current WRED configuration:

eth1/0/1
CoS  WRED State  Exp-weight-constant  Profile
---  -
0    Disabled    9                    1
1    Disabled    9                    1
2    Enabled     9                    1
3    Disabled    9                    1
4    Disabled    9                    1
5    Disabled    9                    1
6    Disabled    9                    1
7    Disabled    9                    1

Switch#
```

103.5 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.

Любой режим конфигурирования.

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
GREEN	20	80	10
YELLOW	20	80	10
RED	20	80	8

```
Switch#
```

104. Команды CPU Port Statistics

104.1 debug show cpu port

Данная команда используется для отображения статистики по пакетам Layer 2 или Layer 3, полученным ЦПУ.

debug show cpu port [I2 | I3 [unicast | multicast] | protocol NAME]

Параметры

I2	(Опционально.) Укажите, чтобы отобразить счетчики статистики по пакетам Layer 2.
I3	(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.

По умолчанию

Нет.

Режим ввода команды

Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 15.

Использование команды

Данная команда используется 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
-----	-----	-----	-----
UNKNOWN	0	0	0
DOT1X	0	0	0
ARP	0	6	0
BGP	0	0	0
CFM	0	0	0
CISCO_MAC1	0	0	0
CISCO_MAC2	0	0	0
CTP	0	0	0
DHCP	0	24	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
IP	0	0	0
IPv6	0	15	0
LACP	0	0	0
--More-- or (q)uit (a)ll			

104.2 debug clear cpu port

Данная команда используется для сброса всех счетчиков по пакетам Layer 2 и 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

Используйте данную команду, чтобы сбросить все счетчики по пакетам Layer 2 и Layer 3, полученным ЦПУ.

Пример

В данном примере показано, как сбросить все счетчики статистики.

```
Switch#debug clear cpu port
```

```
Switch#
```

105. Команды Virtual LAN (VLAN) Counter

105.1 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 interfaces ethernet 1/0/1 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 ethernet 1/0/2
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 ethernet 1/0/10 multicast tx
Switch(config-if)#
```

105.2 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 <i>INTERFACE-ID</i>	(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

User/Privileged EXEC Mode.

Уровень команды по умолчанию

Уровень 1.

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
10	RX Unicast	1/0/1
20	RX Any	
30	RX Any	1/0/5-1/0/6,1/0/10
20	TX Any	
30	TX Any	1/0/5-1/0/6,1/0/10

```
Total Entries: 5
```

```
Switch#
```

Приложение А. Восстановление пароля (Password Recovery)

В данной главе представлен процесс сброса паролей на коммутаторах D-Link серии DMS-3130.

Необходимо аутентифицировать любого пользователя, который пытается получить доступ к сети. Основным методом аутентификации пользователей с соответствующими правами является локальная авторизация с помощью имени пользователя (Username) и пароля (Password). В случаях, когда пароли забыты или утеряны, администратору сети необходимо сбросить эти пароли. В данной главе приведена подробная информация о том, как выполнить сброс с помощью функции восстановления пароля.

Ниже представлена информация об использовании функции Password Recovery на коммутаторе для восстановления паролей.

Для сброса пароля выполните следующее:

- В целях безопасности для функции восстановления пароля требуется физический доступ пользователя к устройству. Поэтому данная функция применима только при наличии прямого подключения к консольному порту устройства. Пользователю необходимо подключиться с помощью программы-эмулятора терминала на ПК к консольному порту коммутатора.
- Включите питание коммутатора. После 100% загрузки **UART init** пользователю в течение 2 секунд необходимо нажать горячую клавишу **[^] (Shift+6)** для того, чтобы войти в режим восстановления пароля (Password Recovery Mode). При входе в данный режим все порты будут отключены.

```
Boot Procedure                                     V1.00.003
-----
Power On Self Test ..... 100 %

MAC Address   : F0-7D-68-34-00-10
H/W Version   : A1

Please Wait, Loading 1.01.006 Runtime Image ..... 100 %
UART init     ..... 100 %

Password Recovery Mode

Switch(reset-config)#
```

В режиме восстановления пароля могут быть использованы следующие команды:

no enable password	Данная команда используется для удаления всех паролей любого уровня учетных записей.
no login password	Данная команда используется для удаления методов локальной авторизации.
no username	Данная команда используется для удаления всех локальных пользовательских учетных записей.
password-recovery	Данная команда используется для инициирования процесса по восстановлению пароля.

reload	Данная команда используется для сохранения и перезагрузки коммутатора.
reload clear running-config	Данная команда используется для сброса текущей конфигурации и восстановления настроек по умолчанию с дальнейшей перезагрузкой коммутатора.
show running-config	Данная команда используется для отображения текущей конфигурации.
show username	Данная команда используется для отображения информации о локальных пользовательских учетных записей.

Приложение Б. Записи системного журнала

В таблице ниже перечислены все записи и их соответствующие значения, появляющиеся в системном журнале коммутатора.

802.1X

Описание записей журнала	Уровень
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. username: пользователь, проходящий аутентификацию. interface-id: имя интерфейса. macaddr: 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. macaddr: 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.	Предупреждение
---------------------------------	----------------

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.

Описание события: ошибка входа из-за тайм-аута или неверной конфигурации AAA-сервера.	Предупреждение
---	----------------

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.

Описание события: успешное включение привилегий.	Информационный
--	----------------

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.

Описание события: ошибка включения привилегий.	Предупреждение
--	----------------

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.

Описание события: Удаленный сервер не отвечает на запрос аутентификации с Предупреждение 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.

Описание события: RADIUS назначил атрибуты допустимого VLAN ID. Информационный

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.

Описание события: RADIUS назначил атрибуты допустимой полосы пропускания. Информационный

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.

Описание события: RADIUS назначил атрибуты допустимого приоритета. Информационный

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.

Описание события: RADIUS назначил ACL Script, который не может быть Предупреждение 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.

ARP

Описание записей журнала	Уровень
--------------------------	---------

Описание события: добровольный ARP-запрос (Gratuitous ARP) обнаружил, что Предупреждение 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: ID модуля в стеке. Значение должно быть целым числом.

portNum: номер логического порта устройства. Значение должно быть целым числом.

ipif_name: имя интерфейса коммутатора, из-за IP-адреса которого возник конфликт.

Auto-save

Описание записей журнала	Уровень
--------------------------	---------

Описание события: информация о настройках DDP сохраняется автоматически. Информационный

Сообщение в журнале: [Unit <unitID>,]Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>)

Описание параметров:

Unit: Unit ID.

username: имя текущего пользователя.

ipaddr: IP-адрес клиента.

BPDU Protection

Описание записей журнала	Уровень
--------------------------	---------

Описание события: атака BPDU. Информационный

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).

Описание события: атака BPDU устранена.

Информационный

Сообщение в журнале: <interface-id> recover from BPDU under protection state.

Описание параметров:

interface-id: интерфейс, на котором обнаружена атака STP BPDU.

CFM

Описание записей журнала	Уровень
Описание события: обнаружен кросс-коннект. Сообщение в журнале: CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Interface:<interface-id>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) Описание параметров: vlanid: идентификатор VLAN MEP. mdlevel: уровень MD MEP. interface-id: номер интерфейса MEP. mepdirection: возможные параметры направления MEP: inward или outward. mepid: MEPID, значение которого равно нулю, неизвестен. macaddr: MAC-адрес MEP, значение которого состоит из всех нулей, неизвестен. Note: в режиме CFM hardware информация об удаленных MEP (mepid и macaddr) неизвестна.	Критический
Описание события: обнаружена ошибка CFM CCM. Сообщение в журнале: CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) Описание параметров: vlanid: идентификатор VLAN MEP. mdlevel: уровень MD MEP. interface-id: номер интерфейса MEP. mepdirection: возможные параметры направления MEP: inward или outward. mepid: MEPID, значение которого равно нулю, неизвестен. macaddr: MAC-адрес MEP, значение которого состоит из всех нулей, неизвестен. Note: в режиме CFM hardware информация об удаленных MEP (mepid и macaddr) неизвестна.	Предупреждение
Описание события: не удастся получить пакет CCM удаленной MEP. Сообщение в журнале: CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>) Описание параметров: vlanid: идентификатор VLAN MEP.	Предупреждение

mdlevel: уровень MD MEP.

interface-id: номер интерфейса MEP.

mepdirection: возможные параметры направления MEP: inward или outward.

mepid: значение MEP ID.

macaddr: MAC-адрес MEP.

Описание события: сообщение об ошибке MAC удаленной MEP.

Предупреждение

Сообщение в журнале: CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>)

Описание параметров:

vlanid: идентификатор VLAN MEP.

mdlevel: уровень MD MEP.

interface-id: номер интерфейса MEP.

mepdirection: возможные параметры направления MEP: inward или outward.

mepid: значение MEP ID.

macaddr: MAC-адрес MEP.

Описание события: удаленная MEP обнаружила дефекты CFM.

Информационный

Сообщение в журнале: CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>)

Описание параметров:

vlanid: идентификатор VLAN MEP.

mdlevel: уровень MD MEP.

interface-id: номер интерфейса MEP.

mepdirection: возможные параметры направления MEP: inward или outward.

mepid: значение MEP ID.

macaddr: MAC-адрес MEP.

Расширение CFM

Описание записей журнала	Уровень
--------------------------	---------

Описание события: обнаружено состояние AIS.

Уведомление

Сообщение в журнале: AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>)

Описание параметров:

vlanid: идентификатор VLAN MEP.

mdlevel: уровень MD MEP.

interface-id: номер интерфейса MEP.

mepdirection: направление MEP: inward или outward.

mepid: значение MEPID.

Описание события: состояние AIS устранено.

Уведомление

Сообщение в журнале: AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>)

Описание параметров:

vlanid: идентификатор VLAN MEP.

mdlevel: уровень MD MEP.

interface-id: номер интерфейса MEP.

mepdirection: направление MEP: inward или outward.

mepid: значение MEPID.

Описание события: обнаружено состояние LCK.

Уведомление

Сообщение в журнале: LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>)

Описание параметров:

vlanid: идентификатор VLAN MEP.

mdlevel: уровень MD MEP.

interface-id: номер интерфейса MEP.

mepdirection: направление MEP: inward или outward.

mepid: значение MEPID.

Описание события: состояние LCK устранено.

Уведомление

Сообщение в журнале: LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>)

Описание параметров:

vlanid: идентификатор VLAN MEP.

mdlevel: уровень MD MEP.

interface-id: номер интерфейса MEP.

mepdirection: направление MEP: inward или outward.

mepid: значение MEPID.

Конфигурация/ПО

Описание записей журнала	Уровень
--------------------------	---------

Описание события: ПО обновлено успешно.	Информационный
---	----------------

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.

Описание события: не удалось обновить ПО. Предупреждение

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.

Описание события: ПО успешно выгружено.

Информационный

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.

Описание события: не удалось выгрузить ПО.

Предупреждение

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.

Описание события: конфигурация успешно загружена.

Информационный

Сообщение в журнале: [Unit <unitID>,]Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)

Описание параметров:

unitID: Unit ID.

session: сессия пользователя.
username: имя текущего пользователя.
ipaddr: IP-адрес клиента.
macaddr: MAC-адрес клиента.
serverIP: IP-адрес сервера.
pathFile: путь и имя файла на сервере.

Описание события: не удалось загрузить конфигурацию. Предупреждение

Сообщение в журнале: [Unit <unitID>,]Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)

Описание параметров:

unitID: Unit ID.
session: сессия пользователя.
username: имя текущего пользователя.
ipaddr: IP-адрес клиента.
macaddr: MAC-адрес клиента.
serverIP: IP-адрес сервера.
pathFile: путь и имя файла на сервере.

Описание события: конфигурация успешно выгружена. Информационный

Сообщение в журнале: [Unit <unitID>] Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)

Описание параметров:

unitID: Unit ID.
session: сессия пользователя.
username: имя текущего пользователя.
ipaddr: IP-адрес клиента.
macaddr: MAC-адрес клиента.
serverIP: IP-адрес сервера.
pathFile: путь и имя файла на сервере.

Описание события: не удалось выгрузить конфигурацию. Предупреждение

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.

Описание события: не удалось загрузить файлы неизвестного типа.	Предупреждение
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.	

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).	Предупреждение
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.	
Описание события: Событие о дублированном адресе во время процесса DAD будет добавлено в журнал, после того как DUT получит сообщение Neighbor Advertisement (NA).	Предупреждение
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.	

DDM

Описание записей журнала	Уровень
Описание события: какой-либо из параметров SFP превысил порог warning (предупреждение).	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.

Описание события: какой-либо из параметров SFP превысил порог alarm Критический (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.

Описание события: какой-либо из параметров SFP вернулся к нормальному Предупреждение 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).

DHCPv6 Client

Описание записей журнала

Уровень

Описание события: состояние DHCPv6-клиента на указанном интерфейсе Информационный изменено администратором.

Сообщение в журнале: DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled].

Описание параметров:

<ipif-name>: имя интерфейса DHCPv6-клиента.

Описание события: DHCPv6-клиент получил IPv6-адрес от сервера DHCPv6.

Информационный

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.

Описание события: IPv6-адрес, полученный от сервера DHCPv6, обновляется.

Информационный

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.

Описание события: IPv6-адрес, полученный от сервера DHCPv6, успешно Информационный 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.

Описание события: выполняется повторная привязка IPv6-адреса, полученного от Информационный 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.

Описание события: повторная привязка IPv6-адреса, полученного от сервера Информационный 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.

Описание события: IPv6-адрес, полученный от сервера DHCPv6, удален. Информационный

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.

Описание события: состояние DHCPv6-клиента PD на указанном интерфейсе Информационный 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.

Описание события: DHCPv6-клиент PD получил IPv6-префикс от делегирующего Информационный 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.

ipif-name: имя интерфейса DHCPv6-клиента PD.

Описание события: IPv6-префикс, полученный от делегирующего Информационный маршрутизатора, обновляется.

Сообщение в журнале: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> starts renewing.

Описание параметров:

ipv6networkaddr: IPv6-префикс, полученный от делегирующего маршрутизатора.

ipif-name: имя интерфейса DHCPv6-клиента PD.

Описание события: IPv6-префикс, полученный от делегирующего Информационный маршрутизатора, успешно обновлен.

Сообщение в журнале: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> renews success.

Описание параметров:

ipv6networkaddr: IPv6-префикс, полученный от делегирующего маршрутизатора.

ipif-name: имя интерфейса DHCPv6-клиента PD.

Описание события: выполняется повторная привязка IPv6-префикса, полученного Информационный от сервера DHCPv6.

Сообщение в журнале: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding.

Описание параметров:

ipv6networkaddr: IPv6-префикс, полученный от делегирующего маршрутизатора.

ipif-name: имя интерфейса DHCPv6-клиента PD.

Описание события: повторная привязка IPv6-префикса, полученного от Информационный делегирующего маршрутизатора, выполнена успешно.

Сообщение в журнале: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> rebinds success.

Описание параметров:

ipv6networkaddr: IPv6-префикс, полученный от делегирующего маршрутизатора.

ipif-name: имя интерфейса DHCPv6-клиента PD.

Описание события: IPv6-префикс, полученный от делегирующего Информационный маршрутизатора, удален.

Сообщение в журнале: The IPv6 prefix <ipv6networkaddr> on interface <intf-name> was deleted.

Описание параметров:

ipv6networkaddr: IPv6-префикс, полученный от делегирующего маршрутизатора.

ipif-name: имя интерфейса DHCPv6-клиента PD.

DHCPv6 Relay

Описание записей журнала	Уровень
Описание события: состояние функции DHCPv6 relay на указанном интерфейсе изменено администратором. Сообщение в журнале: DHCPv6 relay on interface <ipif-name> changed state to [enabled disabled] Описание параметров: <ipif-name>: имя интерфейса DHCPv6 relay agent.	Информационный

DHCPv6 Server

Описание записей журнала	Уровень
Описание события: используется адрес пула сервера DHCPv6. Сообщение в журнале: The address of the DHCPv6 Server pool <pool-name> is used up. Описание параметров: <pool-name>: имя пула сервера DHCPv6.	Информационный
Описание события: количество назначенных IPv6-адресов достигло 4096. Сообщение в журнале: The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to 4096.	Информационный

DULD

Описание записей журнала	Уровень
Описание события: на порту обнаружена потеря связи в одном направлении. Сообщение в журнале: DULD <INTERFACE-ID> is detected as unidirectional link. Описание параметров: INTERFACE-ID: имя интерфейса.	Предупреждение

Dynamic ARP Inspection

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: ARP-запрос (request) или ARP-ответ (response). ip-address: IP-адрес. macaddr: MAC-адрес. vlanid: VLAN ID. interface-id: имя интерфейса.	Предупреждение

ERPS

Описание записей журнала	Уровень
Описание события: произошло событие Manual Switch. Сообщение в журнале: "Manual Switch is issued on node (MAC: <macaddr>, instance <InstanceID>)" Описание параметров: macaddr: MAC-адрес. InstanceID: ID экземпляра.	Предупреждение
Описание события: обнаружено отсутствие сигнала. Сообщение в журнале: "Signal fail detected on node (MAC: <macaddr>, instance <InstanceID>)" Описание параметров: macaddr: MAC-адрес. InstanceID: ID экземпляра.	Предупреждение
Описание события: отсутствие сигнала устранено. Сообщение в журнале: "Signal fail cleared on node(MAC: <macaddr>, instance <InstanceID>)" Описание параметров: macaddr: MAC-адрес. InstanceID: ID экземпляра.	Предупреждение
Описание события: произошло событие Force Switch. Сообщение в журнале: "Force Switch is issued on node (MAC: <macaddr>, instance <InstanceID>)" Описание параметров: macaddr: MAC-адрес. InstanceID: ID экземпляра.	Предупреждение
Описание события: выполнена отмена события. Сообщение в журнале: "Clear command is issued on node (MAC: <macaddr>, instance <InstanceID>)" Описание параметров: macaddr: MAC-адрес. InstanceID: ID экземпляра.	Предупреждение
Описание события: конфликт RPL Owner. Сообщение в журнале: "RPL owner conflicted on the node (MAC: <macaddr>, instance<InstanceID>)" Описание параметров: macaddr: MAC-адрес. InstanceID: ID экземпляра.	Предупреждение

Ethernet OAM

Описание записей журнала	Уровень
Описание события: событие Ethernet OAM dying gasp (удаленно). Сообщение в журнале: OAM dying gasp event received (Port<interface-id>) Описание параметров: interface-id: имя интерфейса.	Предупреждение
Описание события: событие Ethernet OAM dying gasp (локально). Сообщение в журнале: Device encountered an OAM dying gasp event.	Предупреждение
Описание события: событие Ethernet OAM critical (удаленно). Сообщение в журнале: OAM critical event received (Port<interface-id>) Описание параметров: interface-id: имя интерфейса.	Предупреждение
Описание события: событие Ethernet OAM critical (локально). Сообщение в журнале: Device encountered an OAM critical event (Port<interface-id>, <condition>) Описание параметров: interface-id: имя интерфейса. condition: строка, отображающая состояние генерируемых критических событий соединения, например, функция OAM отключена (OAM disable), порт отключен (Port shutdown), соединение на порту прервано (Port link down), перегруженность пакетами (Packet overload).	Предупреждение
Описание события: событие Error symbol period (удаленно). Сообщение в журнале: Errored symbol period event received (Port <interface-id>) Описание параметров: interface-id: имя интерфейса.	Предупреждение
Описание события: событие Error frame. Сообщение в журнале: Errored frame event received(Port <interface-id>) Описание параметров: interface-id: имя интерфейса.	Предупреждение
Описание события: событие Error frame period. Сообщение в журнале: Errored frame period event received(Port <interface-id>) Описание параметров: interface-id: имя интерфейса.	Предупреждение
Описание события: событие Error frame seconds summary. Сообщение в журнале: Errored frame seconds summary event received (Port <interface-id>) Описание параметров: interface-id: имя интерфейса.	Предупреждение

Описание события: запуск опции Remote Loopback.	Предупреждение
Сообщение в журнале: OAM Remote loopback started (Port <interface-id>)	
Описание параметров:	
interface-id: имя интерфейса.	

Описание события: остановка опции Remote Loopback.	Предупреждение
Сообщение в журнале: OAM Remote loopback stopped (Port <interface-id>)	
Описание параметров:	
interface-id: имя интерфейса.	

Interface

Описание записей журнала	Уровень
Описание события: соединение на порту установлено. Сообщение в журнале: Port <portNum> link up, <link state> Описание параметров: portNum: номер логического порта устройства. Значение должно быть целым числом. link state: например: 100Mbps FULL duplex (100 Мбит/с, режим полного дуплекса).	Информационный
Описание события: соединение на порту прервано. Сообщение в журнале: Port <portNum> link down portNum: номер логического порта устройства. Значение должно быть целым числом.	Информационный

IP Directed Broadcast

Описание записей журнала	Уровень
Описание события: скорость направленных широковещательных рассылок превысила 50 пакетов в секунду в определенной подсети. Сообщение в журнале: IP Directed Broadcast packet rate is high on subnet. [(IP: %s)] Описание параметров: IP: адрес назначения (destination) широковещательной рассылки.	Информационный
Описание события: скорость направленных широковещательных рассылок превысила 100 пакетов в секунду. Сообщение в журнале: IP Directed Broadcast rate is high.	Информационный

LACP

Описание записей журнала	Уровень
Описание события: группа агрегирования (Link Aggregation) включена.	Информационный

Сообщение в журнале: Link Aggregation Group <group_id> link up.

Описание параметров:

group_id: ID включенной группы агрегирования.

Описание события: группа агрегирования (Link Aggregation) отключена.

Информационный

Сообщение в журнале: Link Aggregation Group <group_id> link down.

Описание параметров:

group_id: ID включенной группы агрегирования.

Описание события: member-порт присоединился к группе агрегирования.

Информационный

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.

Описание события: member-порт покинул группу агрегирования.

Информационный

Сообщение в журнале: <ifname> detach from Link Aggregation Group <group_id>.

Описание параметров:

Ifname: имя интерфейса порта, который покинул группу агрегирования.

group_id: ID группы агрегирования, которую покинул порт.

LBD

Описание записей журнала	Уровень
Описание события: обнаружена петля в режиме Port-based Mode. Сообщение в журнале: IfInfo LBD loop occurred. Описание параметров: IfInfo: информация об интерфейсе.	Критический
Описание события: порт вернулся в исходное состояние в режиме Port-based Mode. Сообщение в журнале: IfInfo LBD loop recovered. Описание параметров: IfInfo: информация об интерфейсе.	Критический
Описание события: обнаружена петля в режиме VLAN-based Mode. Сообщение в журнале: IfInfo VID <vlanID> LBD loop occurred. Описание параметров: IfInfo: информация об интерфейсе. vlanID: номер VLAN ID.	Критический
Описание события: порт вернулся в исходное состояние в режиме VLAN-based Mode. Сообщение в журнале: IfInfo LBD loop recovered.	Критический

Описание параметров:

lflInfo: информация об интерфейсе.

vlanID: номер VLAN ID.

Описание события: число VLAN, на которых была обнаружена петля, превысило Критический указанное число.

Сообщение в журнале: Loop VLAN numbers overflow.

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.	Уведомление

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.

Описание события: обнаружен несовместимый набор TLV LLDP-MED.

Уведомление

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.

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:	Предупреждение

username: имя текущего пользователя.

ipaddr: IP-адрес клиента.

Описание события: время сессии Telnet истекло.

Информационный

Сообщение в журнале: Telnet session timed out (Username: <username>, IP: <ipaddr>)

Описание параметров:

username: имя текущего пользователя.

ipaddr: IP-адрес клиента.

Описание события: выполнен выход через Telnet.

Информационный

Сообщение в журнале: Logout through Telnet (Username: <username>, IP: <ipaddr>)

Описание параметров:

username: имя текущего пользователя.

ipaddr: IP-адрес клиента.

Описание события: успешный вход через SSH.

Информационный

Сообщение в журнале: Successful login through SSH (Username: <username>, IP: <ipaddr>)

Описание параметров:

username: имя текущего пользователя.

ipaddr: IP-адрес клиента.

Описание события: не удалось выполнить вход через SSH.

Критический

Сообщение в журнале: Login failed through SSH (Username: <username>, IP: <ipaddr>)

Описание параметров:

username: имя текущего пользователя.

ipaddr: IP-адрес клиента.

Описание события: время сессии SSH истекло.

Информационный

Сообщение в журнале: SSH session timed out (Username: <username>, IP: <ipaddr>)

Описание параметров:

username: имя текущего пользователя.

ipaddr: IP-адрес клиента.

Описание события: выполнен выход через SSH.

Информационный

Сообщение в журнале: Logout through SSH (Username: <username>, IP: <ipaddr>)

Описание параметров:

username: имя текущего пользователя.

ipaddr: IP-адрес клиента.

MAC

Описание записей журнала	Уровень
--------------------------	---------

Описание события: узел успешно прошел аутентификацию на основе MAC. Информационный
Сообщение в журнале: MAC-based Access Control host login success (MAC: <mac-address>, <interface-id>, VID: <vlan-id>)

Описание параметров:

mac-address: MAC-адрес узла.

interface-id: интерфейс, на котором аутентифицирован узел.

vlan-id: ID VLAN, в которой находится узел.

Описание события: время аутентификации узла истекло. Информационный
Сообщение в журнале: MAC-based Access Control host aged out (MAC: <mac-address>, <interface-id>, VID: <vlan-id>)

Описание параметров:

mac-address: MAC-адрес узла.

interface-id: интерфейс, на котором аутентифицирован узел.

vlan-id: ID VLAN, в которой находится узел.

Описание события: узел не прошел аутентификацию. Критический
Сообщение в журнале: MAC-based Access Control host login fail (MAC: <mac-address>, <interface-id>, VID: <vlan-id>)

Описание параметров:

mac-address: MAC-адрес узла.

interface-id: интерфейс, на котором аутентифицирован узел.

vlan-id: ID VLAN, в которой находится узел.

Описание события: количество авторизованных пользователей на устройстве достигло максимального значения. Предупреждение
Сообщение в журнале: MAC-based Access Control enters stop learning state.

Описание события: количество авторизованных пользователей на устройстве вернулось к значению ниже максимального за заданный интервал времени. Предупреждение
Сообщение в журнале: MAC-based Access Control recovers from stop learning state.

Описание события: количество авторизованных пользователей на интерфейсе достигло максимального значения. Предупреждение

Сообщение в журнале: <interface-id> enters MAC-based Access Control stop learning state

Описание параметров:

interface-id: интерфейс, на котором аутентифицирован узел.

Описание события: количество авторизованных пользователей на интерфейсе вернулось к значению ниже максимального за заданный интервал времени. Предупреждение
Сообщение в журнале: <interface-id> recovers from MAC-based Access Control stop learning state.

Описание параметров:

interface-id: интерфейс, на котором аутентифицирован узел.

MSTP Debug Enhancement

Описание записей журнала	Уровень
Описание события: топология изменилась. Сообщение в журнале: Topology changed [([Instance:<InstanceID>] , <portNum> ,MAC: <macaddr>)] Описание параметров: InstanceID: ID экземпляра. portNum: ID порта. macaddr: MAC-адрес.	Уведомление
Описание события: новый корневой мост. Сообщение в журнале: [CIST CIST Regional MSTI Regional] New Root bridge selected([Instance: <InstanceID>],MAC: <macaddr>, Priority :<value>) Описание параметров: InstanceID: ID экземпляра. macaddr: MAC-адрес. value: значение приоритета.	Информационный
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: новый корневой порт. Сообщение в журнале: New root port selected [([Instance:<InstanceID>] , <portNum>)] Описание параметров: InstanceID: ID экземпляра. portNum: ID порта.	Уведомление
Описание события: статус порта Spanning Tree изменился. Сообщение в журнале: Spanning Tree port status change [([Instance:<InstanceID>] , <portNum>)] <old_status> -> <new_status> Описание параметров: InstanceID: ID экземпляра. portNum: ID порта. old_status: предыдущий статус. new_status: новый статус.	Уведомление
Описание события: роль порта Spanning Tree изменилась. Сообщение в журнале: Spanning Tree port role change. [([Instance:<InstanceID>] , <[portNum>)] <old_role> -> <new_role> Описание параметров: InstanceID: ID экземпляра.	Информационный

portNum: ID порта.

old_role: предыдущая роль.

new_role: новая роль.

Описание события: создан экземпляр Spanning Tree.

Информационный

Сообщение в журнале: Spanning Tree instance created. (Instance:<InstanceID>)

Описание параметров:

InstanceID: ID экземпляра.

Описание события: удален экземпляр Spanning Tree.

Информационный

Сообщение в журнале: Spanning Tree instance deleted. (Instance:<InstanceID>)

Описание параметров:

InstanceID: ID экземпляра.

Описание события: версия Spanning Tree изменилась.

Информационный

Сообщение в журнале: Spanning Tree version change.(New version:<new_version>)

Описание параметров:

new_version: новая версия STP.

Описание события: ID конфигурации MST Spanning Tree и revision level изменились. Информационный

Сообщение в журнале: Spanning Tree MST configuration ID name and revision level change (name:<name> revision level <revision_level>).

Описание параметров:

revision_level: новый уровень ревизии.

Описание события: таблица соответствия Spanning Tree MST configuration ID VLAN удалена. Информационный

Сообщение в журнале: Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]).

Описание параметров:

InstanceID: ID экземпляра.

startvlanid- endvlanid: список VLAN.

Описание события: таблица соответствия Spanning Tree MST configuration ID VLAN добавлена. Информационный

Сообщение в журнале: Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]).

Описание параметров:

InstanceID: ID экземпляра.

startvlanid- endvlanid: список VLAN.

Описание события: порту Spanning Tree была присвоена роль альтернативного порта (alternate port) из-за STP Root Guard. Информационный

Сообщение в журнале: Spanning Tree port role change (Instance : <InstanceID>, <portNum>) to alternate port due to the guard root.

Описание параметров:

InstanceID: ID экземпляра.

portNum: ID порта.

Описание события: состояние «blocking» Spanning Tree Loop Guard.

Информационный

Сообщение в журнале: Spanning Tree loop guard blocking(Instance : <InstanceID>, <portNum>)

Описание параметров:

InstanceID: ID экземпляра.

portNum: ID порта.

Peripheral

Описание записей журнала	Уровень
Описание события: вентилятор восстановлен. Сообщение в журнале: Unit <unit-id>, <fan-descr> back to normal Описание параметров: Unit <id>: Unit ID. <fan-descr>: например, Right Fan, Left Fan и т. д.	Критический
Описание события: вентилятор вышел из строя. Сообщение в журнале: Unit <unit-id> <fan-descr> failed. Описание параметров: Unit <id>: ID устройства. <fan-descr>: например, Right Fan, Left Fan и т. д.	Критический
Описание события: датчик температуры показывает критическое значение. Сообщение в журнале: Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree> Описание параметров: Unit <id>: ID устройства. thermal-sensor-descr: описание датчика. degree: текущая температура, отображаемая датчиком.	Предупреждение
Описание события: температура вернулась к нормальному значению. Сообщение в журнале: Unit <unit-id> <thermal-sensor-descr> temperature back to normal Описание параметров: Unit <id>: ID устройства. thermal-sensor-descr: описание датчика. degree: текущая температура, отображаемая датчиком.	Информационный

Описание события: отказ питания. Сообщение в журнале: Unit <unit-id> <power-descr> failed Описание параметров: Unit <id>: ID устройства. power-descr: описание питания.	Критический
Описание события: восстановление питания. Сообщение в журнале: Unit <unit-id> <power-descr> back to normal Описание параметров: Unit <id>: ID устройства. power-descr: описание питания.	Критический
Описание события: состояние External Alarm изменилось. Сообщение в журнале: Unit <unit-id> External Alarm Channel <channelID> :<alarmMsg> Описание параметров: Unit <id>: ID устройства. ChannelID: ID канала. alarmMsg: Alarm Msg.	Критический

Port

Описание записей журнала	Уровень
Описание события: соединение на порту установлено. Сообщение в журнале: Port <port> link up, <nway> Описание параметров: port: номер логического порта. nway: скорость и режим дуплекса соединения.	Информационный
Описание события: соединение на порту прервано. Сообщение в журнале: Port <port> link down Описание параметров: port: номер логического порта.	Информационный

Port Security

Описание записей журнала	Уровень
Описание события: превышено максимальное количество адресов на порту. Сообщение в журнале: MAC address <mac-address> causes port security violation on <interface-id>. Описание параметров: macaddr: недопустимый MAC-адрес. interface-id: имя интерфейса.	Предупреждение

Описание события: превышено максимальное количество адресов в системе. Предупреждение
Сообщение в журнале: Limit on system entry number has been exceeded.

Reboot Schedule

Описание записей журнала	Уровень
Описание события: рекомендованное значение времени для перезагрузки коммутатора.	Критический
Сообщение в журнале: Display "Reboot scheduled in 5 minutes" when the countdown equals 5 minutes. Display "Reboot scheduled in 1 minute" when the countdown equals 1 minute.	

Safeguard

Описание записей журнала	Уровень
Описание события: загрузка CPU превысила верхний порог, коммутатор перешел в режим высокой загрузки.	Предупреждение
Сообщение в журнале: Unit <unit-id>, Safeguard Engine enters EXHAUSTED mode.	
Описание параметров: unit-id: Unit ID.	
Описание события: загрузка CPU снизилась до нижнего порога, коммутатор перешел в нормальный режим.	Информационный
Сообщение в журнале: Unit <unit-id>, Safeguard Engine enters NORMAL mode.	
Описание параметров: unit-id: Unit ID.	

SNMP

Описание записей журнала	Уровень
Описание события: получен запрос SNMP с неверной строкой сообщества.	Информационный
Сообщение в журнале: SNMP request received from <ipaddr> with invalid community string.	
Описание параметров: ipaddr: IP-адрес.	

SSH

Описание записей журнала	Уровень
Описание события: сервер SSH включен.	Информационный
Сообщение в журнале: SSH server is enabled	

Описание события: сервер SSH отключен.
Сообщение в журнале: SSH server is disabled

Информационный

SSL

Описание записей журнала	Уровень
Описание события: успешный вход через Web (SSL). Сообщение в журнале: Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя пользователя, используемое для входа на SSL-сервер. ipaddr: IP-адрес SSL-клиента.	Информационный
Описание события: не удалось выполнить вход через Web (SSL). Сообщение в журнале: Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя пользователя, используемое для входа на SSL-сервер. ipaddr: IP-адрес SSL-клиента.	Предупреждение
Описание события: время сессии Web (SSL) истекло. Сообщение в журнале: Web (SSL) session timed out (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя пользователя, используемое для входа на SSL-сервер. ipaddr: IP-адрес SSL-клиента.	Информационный
Описание события: выполнен выход через Web (SSL). Сообщение в журнале: Logout through Web (SSL) (Username: <username>, IP: <ipaddr>). Описание параметров: username: имя пользователя, используемое для входа на SSL-сервер. ipaddr: IP-адрес SSL-клиента.	Информационный

Stacking

Описание записей журнала	Уровень
Описание события: «горячее» добавление. Сообщение в журнале: Unit: <unitID>, MAC: <macaddr> Hot insertion. Описание параметров: unitID: ID модуля. Macaddr: MAC-адрес.	Информационный
Описание события: «горячее» удаление.	Информационный

Сообщение в журнале: Unit: <unitID>, MAC: <macaddr> Hot removal.

Описание параметров:

unitID: ID модуля.

Macaddr: MAC-адрес.

Описание события: топология стекирования изменилась.

Критический

Сообщение в журнале: Stacking topology is <Stack_TP_TYPE>. Master (Unit <unitID>, MAC:<macaddr>).

Описание параметров:

Stack_TP_TYPE: типы топологии стекирования: Ring (кольцевая), Chain (линейная).

unitID: ID модуля.

Macaddr: MAC-адрес.

Описание события: резервное устройство стало основным.

Информационный

Сообщение в журнале: Backup master changed to master. Master (Unit: <unitID>).

Описание параметров:

unitID: ID модуля.

Описание события: дополнительное устройство стало основным.

Информационный

Сообщение в журнале: Slave changed to master. Master (Unit: <unitID>).

Описание параметров:

unitID: ID модуля.

Описание события: соединение на порту стекирования установлено.

Критический

Сообщение в журнале: Stacking port <portID> link up.

Описание параметров:

portID: ID порта.

Описание события: соединение на порту стекирования прервано.

Критический

Сообщение в журнале: Stacking port <portID> link down.

Описание параметров:

portID: ID порта.

Storm Control

Описание записей журнала	Уровень
--------------------------	---------

Описание события: возникновение шторма.

Предупреждение

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.

Описание события: шторм устранен.

Информационный

Сообщение в журнале: <Broadcast | Multicast | Unicast> storm is cleared on <interface-id>.

Описание параметров:

Broadcast: устранен шторм ширококестательных 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.

Описание события: соединение на порту прервано из-за возникновение шторма. Предупреждение

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 ширококестательных пакетов.

Multicast: интерфейс отключен из-за шторма многоадресных пакетов.

Unicast: интерфейс отключен из-за шторма одноадресных пакетов, включая известные и неизвестные пакеты.

Примечание: журналы будут генерироваться только в том случае, если для действия control установлен режим Shutdown (отключение) для одноадресного трафика, включая как известный, так и неизвестный одноадресный трафик. Действия, отличные режима Shutdown (отключение), такие как Drop (отбрасывание) одноадресного трафика, не будут генерировать журналы.

Telnet

Описание записей журнала	Уровень
Описание события: успешный вход через Telnet.	Информационный
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.	
Описание события: не удалось выполнить вход через Telnet.	Предупреждение
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.

Описание события: выполнен выход через Telnet.	Информационный
--	----------------

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.

Описание события: время сессии Telnet истекло.	Информационный
--	----------------

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.

WAC

Описание записей журнала	Уровень
--------------------------	---------

Описание события: узлу не удалось пройти аутентификацию.	Предупреждение
--	----------------

Сообщение в журнале: WAC unauthenticated user (User Name: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:]portNum>)

Описание параметров:

string: имя пользователя.

ipaddr: IP-адрес.

ipv6address: IPv6-адрес.

macaddr: MAC-адрес.

unitID: Unit ID.

portNum: номер порта.

Описание события: количество авторизованных пользователей на устройстве превысило максимальное значение.	Предупреждение
--	----------------

Сообщение в журнале: WAC enters stop learning state.

Описание события: количество авторизованных пользователей на устройстве через определенный интервал времени вернулось к значению ниже максимального.	Предупреждение
--	----------------

Сообщение в журнале: WAC recovered from stop learning state.

Описание события: узел успешно прошел аутентификацию.	Информационный
---	----------------

Сообщение в журнале: WAC authenticated user (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:] portNum>)

Описание параметров:

string: имя пользователя.

ipaddr: IP-адрес.

ipv6address: IPv6-адрес.

macaddr: MAC-адрес.
unitID: Unit ID.
portNum: номер порта.

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

Приложение В. Записи trap-сообщений

Таблица ниже содержит все возможные записи trap-сообщений и их соответствующие значения, встречающиеся на коммутаторе.

802.1X

Сообщение trap	Описание	OID
esDot1xExtLoggedSuccess	Узел прошел аутентификацию 802.1X. Вариабельные привязки: (1) ifIndex (2) esnaSessionClientMacAddress (3) esnaSessionAuthVlan (4) esnaSessionAuthUserName	1.3.6.1.4.1.17 1.17.30.0.1
esDot1xExtLoggedFail	Узел не прошел аутентификацию 802.1X. Вариабельные привязки: (1) ifIndex (2) esnaSessionClientMacAddress (3) esnaSessionAuthVlan (4) esnaSessionAuthUserName (5) esDot1xExtNotifyFailReason	1.3.6.1.4.1.17 1.17.30.0.2

802.3ah OAM

Сообщение trap	Описание	OID
dot3OamThresholdEvent	Локальное или удаленное устройство превысило заданный порог. Вариабельные привязки: (1) dot3OamEventLogTimestamp (2) dot3OamEventLogOui (3) dot3OamEventLogType (4) dot3OamEventLogLocation (5) dot3OamEventLogWindowHi (6) dot3OamEventLogWindowLo (7) dot3OamEventLogThresholdHi (8) dot3OamEventLogThresholdLo (9) dot3OamEventLogValue (10) dot3OamEventLogRunningTotal (11) dot3OamEventLogEventTotal	1.3.6.1. 2.1.158. 0.1
dot3OamNonThresholdEvent	Локальное или удаленное устройство не превысило заданный порог. Вариабельные привязки: (1) dot3OamEventLogTimestamp	1.3.6.1. 2.1.158. 0.2

- (2) dot3OamEventLogOui
- (3) dot3OamEventLogType
- (4) dot3OamEventLogLocation
- (5) dot3OamEventLogEventTotal

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
esBpduProtectionAttackOccur	Атака BPDU на интерфейсе. Вариабельные привязки: (1) ifIndex (2) esBpduProtectionIfCfgMode	1.3.6.1.4.1.17 1.17.47.0.1
esBpduProtectionAttackRecover	Атака BPDU на интерфейсе устранена. Вариабельные привязки: (1) ifIndex	1.3.6.1.4.1.17 1.17.47.0.2

CFM

Сообщение trap	Описание	OID
dot1agCfmFaultAlarm	Обнаружена ошибка подключения. Вариабельные привязки: (1) dot1agCfmMepHighestPrDefect	1.3.111.2.802. 1.1.8.0.1

Расширение CFM

Сообщение trap	Описание	OID
dCfmAisOccurred	Локальная MEP перешла в статус AIS. Вариабельные привязки: (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMepIdentifier	1.3.6.1.4.1.17 1.14.86.0.1

dCfmAisCleared	Локальная MEP вышла из статуса AIS. Вариабельные привязки: (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMeplIdentifier	1.3.6.1.4.1.17 1.14.86.0.2
dCfmLockOccurred	Локальная MEP перешла в состояние «lock». Вариабельные привязки: (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMeplIdentifier	1.3.6.1.4.1.17 1.14.86.0.3
dCfmLockCleared	Локальная MEP вышла из состояния «lock». Вариабельные привязки: (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMeplIdentifier	1.3.6.1.4.1.17 1.14.86.0.4

DDM

Сообщение trap	Описание	OID
esDdmAlarmTrap	Возникновение проблем уровня alarm или возвращение к нормальному состоянию после устранения данных проблем. Трар-сообщение об устранении проблем будет отправлено, если текущее значение выше заданного нижнего порога alarm или ниже заданного верхнего порога alarm. Вариабельные привязки: (1) esDdmNotifyInfoIdxIndex, (2) esDdmNotifyInfoComponent (3) esDdmNotifyInfoAbnormalLevel (4) esDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.17 1.17.72.0.1
esDdmWarningTrap	Возникновение проблем уровня warning или возвращение к нормальному состоянию после устранения данных проблем. Вариабельные привязки: (1) esDdmNotifyInfoIdxIndex, (2) esDdmNotifyInfoComponent (3) esDdmNotifyInfoAbnormalLevel (4) esDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.17 1.17.72.0.2

DHCP Server Screen Prevention

Сообщение trap	Описание	OID
esDhcpFilterAttackDetected	Если функция DHCP Server Screen включена, 1.3.6.1.4.1.17 trap-сообщения будут отправлены при получении 1.17.133.0.1 каждого пакета ложного DHCP-сервера. Вариабельные привязки: (1) esDhcpFilterLogBufServerIpAddr (2) esDhcpFilterLogBufClientMacAddr (3) esDhcpFilterLogBufferVlanId (4) esDhcpFilterLogBufferOccurTime	

ERPS

Сообщение trap	Описание	OID
esErpsFailedetectedNotif	Обнаружено отсутствие сигнала. Trap-сообщение об отсутствии сигнала будет отправлено, если 1.3.6.1.4.1.17 ранее параметр esErpsNotificationEnabled был 1.17.78.0.1 включен.	
esErpsFailureClearedNotif	Отсутствие сигнала устранено. Trap-сообщение об устранении отсутствия сигнала будет отправлено, если 1.3.6.1.4.1.17 ранее параметр esErpsNotificationEnabled был 1.17.78.0.2 включен.	
esErpsRPLOwnerConflictNotif	Конфликт RPL Owner. Trap-сообщение о конфликте RPL Owner будет отправлено, если 1.3.6.1.4.1.17 ранее параметр esErpsNotificationEnabled был 1.17.78.0.3 включен.	

ErrDisable

Сообщение trap	Описание	OID
esErrDisNotifyPortDisabledAssert	Порт перешел в состояние error-disabled. Вариабельные привязки: (1) esErrDisNotifyInfoPortIfIndex (2) esErrDisNotifyInfoReasonID	1.3.6.1.4.1.17 1.17.45.0.1
esErrDisNotifyPortDisabledClear	Порт возвращается в исходное состояние по истечении определенного интервала времени. Вариабельные привязки: (1) esErrDisNotifyInfoPortIfIndex (2) esErrDisNotifyInfoReasonID	1.3.6.1.4.1.17 1.17.45.0.2
esErrDisNotifyVlanDisabledAssert	VLAN перешла в состояние error-disabled. Вариабельные привязки:	1.3.6.1.4.1.17 1.17.45.0.3

	(1) esErrDisNotifyInfoPortIfIndex (2) esErrDisNotifyInfoReasonID (3) esErrDisNotifyInfoLoopDetectedVID
esErrDisNotifyVlanDisabledClear	VLAN, в котором была обнаружена петля, 1.3.6.1.4.1.17 возвращается в исходное состояние по истечении 1.17.45.0.4 определенного интервала времени. Вариабельные привязки: (1) esErrDisNotifyInfoPortIfIndex (2) esErrDisNotifyInfoReasonID (3) esErrDisNotifyInfoLoopDetectedVID

Gratuitous ARP

Сообщение trap	Описание	OID
esIpExtGratuitousARPTrip	Обнаружен конфликт IP-адреса. Вариабельные привязки: (1) esIpExtGratuitousARPIpAddr (2) esIpExtGratuitousARPMacAddr (3) esIpExtGratuitousARPPortNumber (4) esIpExtIfCfgIfIndex	1.3.6.1.4.1.17 1.17.75.0.1

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.	1.3.6.1.6.3.1.1 .5.4

Вариабельные привязки:

- (1) ifIndex,
- (2) if AdminStatus
- (3) ifOperStatus

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
esLbdLoopOccurred	Обнаружена петля. Вариабельные привязки: (1) esLbdNotifyInfolIndex	1.3.6.1.4.1.17.1.17.46.0.1
esLbdLoopRestart	Порт возвращается в исходное состояние по истечении определенного интервала времени. Вариабельные привязки: (1) esLbdNotifyInfolIndex	1.3.6.1.4.1.17.1.17.46.0.2
esLbdVlanLoopOccurred	Обнаружена петля в режиме LBD VLAN-Based. Вариабельные привязки: (1) esLbdNotifyInfolIndex (2) esLbdNotifyInfoVlanId	1.3.6.1.4.1.17.1.17.46.0.3
esLbdVlanLoopRestart	Порт возвращается в исходное состояние в режиме LBD VLAN-based по истечении определенного интервала времени. Вариабельные привязки: (1) esLbdNotifyInfolIndex (2) esLbdNotifyInfoVlanId	1.3.6.1.4.1.17.1.17.46.0.4

LLDP-MED

Сообщение trap	Описание	OID
lldpRemTablesChange	Значение lldpStatsRemTableLastChangeTime изменилось.	1.0.8802.1.1.2.0.0.1

Вариабельные привязки:

- (1) IldpStatsRemTablesInserts
- (2) IldpStatsRemTablesDeletes
- (3) IldpStatsRemTablesDrops
- (4) IldpStatsRemTablesAgeouts

IldpXMedTopologyChangeDetected	Обнаружено изменение в топологии: к порту было подключено новое устройство, удаленное устройство было отключено или было отключено с дальнейшим подключением к другому порту.	1.0.8808.1.1.2 .1.5.4795.0.1
--------------------------------	---	---------------------------------

Вариабельные привязки:

- (1) IldpRemChassisIdSubtype
- (2) IldpRemChassisId
- (3) IldpXMedRemDeviceClass

MAC-based Access Control

Сообщение trap	Описание	OID
esMacAuthLoggedSuccess	Узел успешно прошел аутентификацию на основе MAC. Вариабельные привязки: (1) ifIndex, (2) esnaSessionClientMacAddress (3) esnaSessionAuthVlan	1.3.6.1.4.1.17 1.17.153.0.1
esMacAuthLoggedFai	Узел не прошел аутентификацию на основе MAC. Вариабельные привязки: (1) ifIndex, (2) esnaSessionClientMacAddress (3) esnaSessionAuthVlan	1.3.6.1.4.1.17 1.17.153.0.2
esMacAuthLoggedAgesOut	Время аутентификации узла истекло. (1) ifIndex, (2) esnaSessionClientMacAddress (3) esnaSessionAuthVlan	1.3.6.1.4.1.17 1.17.153.0.3

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	1.3.6.1.4.1.17

VLAN ID. 1.14.3.0.2
Вариабельные привязки:
(1) dL2FdbMacChangeNotifyInfoWithVID

MSTP

Сообщение trap	Описание	OID
newRoot	Новый корень Spanning Tree. Тrap-сообщение будет отправлено мостом сразу же после его назначения в качестве нового корня. По истечении таймера Topology Change мост немедленно будет назначен корнем. Отправка данного trap-сообщения является опциональной.	1.3.6.1.2.1.17.0.1
topologyChange	Мост отправляет trap-сообщение, когда какой-то из его настроенных портов переходит из состояния learning в состояние forwarding или из состояния forwarding в состояние blocking. Данное trap-сообщение не отправляется повторно. Отправка данного trap-сообщения является опциональной.	1.3.6.1.2.1.17.0.2

Peripheral

Сообщение trap	Описание	OID
dEntityExtFanStatusChg	Вентилятор вышел из строя. Данное trap-сообщение отправляется Commander Switch. Уведомление dEntityExtEnvFanStatus может быть «fault», а при восстановлении вентилятора – «ok». Вариабельные привязки: (1) dEntityExtEnvFanUnitId (2) dEntityExtEnvFanIndex (3) dEntityExtEnvFanStatus	1.3.6.1.4.1.17.1.14.5.0.1
dEntityExtThermalStatusChg	Датчик температуры показывает критическое значение. Данное trap-сообщение отправляется Commander Switch. Уведомление dEntityExtEnvTempStatus может быть «abnormal», а при возвращении температуры к нормальному значению – «ok». 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	1.3.6.1.4.1.17

модуля питания. Данное trap-сообщение 1.14.5.0.3 отправляется Commander Switch.

Вариабельные привязки:

- (1) dEntityExtEnvPowerUnitId
- (2) dEntityExtEnvPowerIndex
- (3) dEntityExtEnvPowerStatus

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
esPoelfPowerDeniedNotification	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
esPoelfPowerOverLoadNotification	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	1.3.6.1.4.1.171.14.24.0.2
esPoelfPowerShortCircuitNotification	Состояние диаграммы статуса PSE – ERROR_DELAY_SHORT. Между отправкой уведомлений одним и тем же	1.3.6.1.4.1.171.14.24.0.3

экземпляром параметра должно пройти
не менее 500 миллисекунд.

Вариабельные привязки:

(1) pethPsePortShortCounter

Port Security

Сообщение trap	Описание	OID
esPortSecMacAddrViolation	Если отправка trap-сообщений Port Security включена, trap-сообщения будут отправлены при обнаружении недопустимых MAC-адресов. Вариабельные привязки: (1) ifIndex, (2) esPortSecIfCurrentStatus (3) esPortSecIfViolationMacAddress	1.3.6.1.4.1.17 1.17.8.0.1

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

Reboot Schedule

Сообщение trap	Описание	OID
agentRebootIn5Min	Значение таймера Countdown достигло 5 минут.	1.3.6.1.4.1.17 1.14.170.0.1
agentRebootIn1Min	Значение таймера Countdown достигло 1 минуты.	1.3.6.1.4.1.17 1.14.170.0.2

RMON

Сообщение trap	Описание	OID
----------------	----------	-----

risingAlarm	Запись уровня alarm превысила заданный верхний порог. Вариабельные привязки: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16. 0.1
-------------	---	------------------------

fallingAlarm	Запись уровня alarm снизилась до заданного нижнего порога. Вариабельные привязки: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16. 0.2
--------------	---	------------------------

Safeguard

Сообщение trap	Описание	OID
esSafeguardChgToExhausted	Нормальный режим работы системы изменился на режим высокой загрузки. Вариабельные привязки: (1) esSafeguardEngineCurrentMode	1.3.6.1.4.1.17 1.17.19.1.1.0. 1
esSafeguardChgToNormal	Режим высокой загрузки системы изменился на нормальный режим. Вариабельные привязки: (1) esSafeguardEngineCurrentMode	1.3.6.1.4.1.17 1.17.19.1.1.0. 2

SIM

Сообщение trap	Описание	OID
esSingleIPMSColdStart	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление о «холодном» старте. Вариабельные привязки: (1) esSingleIPMSMacAddrSingleIPMSMacAddr	1.3.6.1.4.1.17 1. 17.225.0.0.11
esSingleIPMSWarmStart	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление о «горячем»	1.3.6.1.4.1.17 1. 17.225.0.0.12

старте.

Вариабельные привязки:

(1) esSingleIPMSMacAddr

esSingleIPMSLinkDown	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление о прерванном соединении.	1.3.6.1.4.1.17 1. 17.225.0.0.13
	Вариабельные привязки: (1) esSingleIPMSMacAddr (2) ifIndex	
esSingleIPMSLinkUp	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление об установленном соединении.	1.3.6.1.4.1.17 1. 17.225.0.0.14
	Вариабельные привязки: (1) esSingleIPMSMacAddr (2) ifIndex	
esSingleIPMSAuthFail	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление об ошибке аутентификации.	1.3.6.1.4.1.17 1. 17.225.0.0.15
	Вариабельные привязки: (1) esSingleIPMSMacAddr	
esSingleIPMSnewRoot	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление о новом корне.	1.3.6.1.4.1.17 1. 17.225.0.0.16
	Вариабельные привязки: (1) esSingleIPMSMacAddr	
esSingleIPMSTopologyChange	Данное trap-сообщений будет отправлено Commander Switch, если участником его группы было сгенерировано уведомление об изменении топологии.	1.3.6.1.4.1.17 1. 17.225.0.0.17
	Вариабельные привязки: (1) esSingleIPMSMacAddr	
esSingleIPMSrisingAlarm	Данное trap-сообщений будет отправлено Commander Switch указанному узлу, если участником его группы было сгенерировано уведомление о превышении уровня alarm.	1.3.6.1.4.1.17 1. 17.225.0.0.18
	Вариабельные привязки: (1) esSingleIPMSTrapMacAddr	
esSingleIPMSfallingAlarm	Данное trap-сообщений будет отправлено	1.3.6.1.4.1.17

	Commander Switch указанному узлу, если 1.17.225.0.0.19 участником его группы было сгенерировано уведомление о снижении уровня alarm. Вариабельные привязки: (1) esSingleIpMSTrapMacAddr
esSingleIpMSmacNotification	Данное trap-сообщений будет отправлено 1.3.6.1.4.1.17 Commander Switch указанному узлу, если 1.17.225.0.0.20 участником его группы было сгенерировано уведомление об изменении MAC-адреса. Вариабельные привязки: (1) esSingleIpMSTrapMacAddr (2) esSingleIpMSTrapMessage
esSingleIpMSPortTypeChange	Данное trap-сообщений будет отправлено 1.3.6.1.4.1.17 Commander Switch указанному узлу, если 1.17.225.0.0.21 участником его группы было сгенерировано уведомление об изменении типа порта. Вариабельные привязки: (1) esSingleIpMSTrapMacAddr (2) ifIndex (3) esSingleIpMSTrapMessage
esSingleIpMSPowerStatusChg	Данное trap-сообщений будет отправлено 1.3.6.1.4.1.17 Commander Switch указанному узлу, если 1.17.225.0.0.22 участником его группы было сгенерировано уведомление об изменении статуса питания. Вариабельные привязки: (1) esSingleIpMSTrapMacAddr (2) esSingleIpMSTrapMessage
esSingleIpMSPowerFailure	Данное trap-сообщений будет отправлено 1.3.6.1.4.1.17 Commander Switch указанному узлу, если 1.17.225.0.0.23 участником его группы было сгенерировано уведомление о сбое подачи питания. Вариабельные привязки: (1) esSingleIpMSTrapMacAddr (2) esSingleIpMSTrapMessage
esSingleIpMSPowerRecover	Данное trap-сообщений будет отправлено 1.3.6.1.4.1.17 Commander Switch указанному узлу, если 1.17.225.0.0.24 участником его группы было сгенерировано уведомление о восстановлении подачи питания. Вариабельные привязки: (1) esSingleIpMSTrapMacAddr (2) esSingleIpMSTrapMessage

Stacking

Сообщение trap	Описание	OID
esStackTPChangeNotification	Изменение топологии стекирования. Вариабельные привязки: (1) esStackNotifyInfoTopologyType (2) esStackNotifyInfoBoxId (3) esStackInfoMacAddr	1.3.6.1.4.1.17 1.17.9.0.4

Start

Сообщение trap	Описание	OID
coldStart	Повторная инициализация SNMPv2-устройства в роли агента и возможное изменение его настроек.	1.3.6.1.6.3.1.1 .5.1
warmStart	Повторная инициализация SNMPv2-устройства в роли агента с неизменной конфигурацией.	1.3.6.1.4.1.17 1.14.9.0.2

Storm Control

Сообщение trap	Описание	OID
esStormCtrlOccurred	Данное trap-сообщение будет отправлено, если значение параметра esStormCtrlNotifyEnable – «stormOccurred» или «both», а также при возникновении шторма. Вариабельные привязки: (1) ifIndex, (2) esStormCtrlNotifyTrafficType	1.3.6.1.4.1.17 1.17.25.0.1
esStormCtrlStormCleared	Данное trap-сообщение будет отправлено, если значение параметра esStormCtrlNotifyEnable – «stormCleared» или «both», а также при устранении шторма. Вариабельные привязки: (1) ifIndex, (2) esStormCtrlNotifyTrafficType	1.3.6.1.4.1.17 1.14.25.0.2

Примечание: trap-сообщения будут генерироваться только в том случае, если для действия control установлен режим Shutdown (отключение) для одноадресного трафика, включая как известный, так и неизвестный одноадресный трафик. Действия, отличные режима Shutdown (отключение), такие как Drop (отбрасывание) одноадресного трафика, не будут генерировать trap-сообщения.

System File

Сообщение trap	Описание	OID
----------------	----------	-----

dsfUploadImage	Пользователь успешно выгрузил файл образа.	1.3.6.1.4.1.17 1.14.14.0.1
dsfDownloadImage	Пользователь успешно загрузил файл образа.	1.3.6.1.4.1.17 1.14.14.0.2
dsfUploadCfg	Пользователь успешно выгрузил конфигурационный файл.	1.3.6.1.4.1.17 1.14.14.0.3
dsfDownloadCfg	Пользователь успешно загрузил конфигурационный файл.	1.3.6.1.4.1.17 1.14.14.0.4
dsfSaveCfg	Пользователь успешно сохранил конфигурационный файл.	1.3.6.1.4.1.17 1.14.14.0.5

Upload/Download

Сообщение trap	Описание	OID
agentFirmwareUpgrade	Завершение процесса обновления ПО через SNMP. Вариабельные привязки: (1) swMultilImageVersion	1.3.6.1.4.1.17 1.12.1.7.2.0.7
agentCfgOperCompleteTrap	Настройки полностью сохранены, выгружены или загружены. Вариабельные привязки: (1) unitID (2) agentCfgOperate (3) agentLoginUserName	1.3.6.1.4.1.17 1.12.1.7.2.0.9

VRRP

Сообщение trap	Описание	OID
vrrpTrapNewMaster	Переход устройства в режим Master. Вариабельные привязки: (1) vrrpOperMasterIpAddr	1.3.6.1.2.1.68. 0.1
vrrpTrapAuthFailure	Маршрутизатором был получен пакет, ключ аутентификации или тип аутентификации которого конфликтует с ключом аутентификации или типом аутентификации этого маршрутизатора. Отправка данного trap-сообщения является опциональной. Вариабельные привязки: (1) vrrpTrapPacketSrc	1.3.6.1.2.1.68. 0.2

(2) vrrpTrapAuthErrorType

WAC

Сообщение trap	Описание	OID
esWebAuthLoggedSuccess	Узел успешно прошел Web-аутентификацию. Вариабельные привязки: (1) ifIndex (2) esnaSessionAuthVlan (3) esnaSessionClientMacAddress (4) esnaSessionClientAddrType (5) esnaSessionClientAddress (6) esnaSessionAuthUserName	1.3.6.1.4.1.17 1.17.154.0.1
esWebAuthLoggedFail	Узлу не удалось пройти аутентификацию. Вариабельные привязки: (1) ifIndex (2) esnaSessionAuthVlan (3) esnaSessionClientMacAddress (4) esnaSessionClientAddrType (5) esnaSessionClientAddress (6) esnaSessionAuthUserName	1.3.6.1.4.1.17 1.17.154.0.2

Приложение Г. Назначение атрибутов RADIUS

На коммутаторах DMS-3130 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 производителя	для Описание	Значение	Использование
Vendor-ID	Определяет производителя	171 (DLINK)	Обязательно
Vendor-Type	Определяет атрибут	1	Обязательно
Attribute-Specific Field	Используется для назначения уровня привилегии пользователя для работы с коммутатором	Диапазон (1-15)	Обязательно

Если пользователь сконфигурировал атрибут уровня привилегии на RADIUS-сервере (например, уровень 15) и аутентификация Console, Telnet, SSH и Web прошла успешно, устройство назначит уровень привилегии пользователю в соответствии со значением на RADIUS-сервере. Однако если пользователь не сконфигурировал атрибут уровня привилегии и аутентификация проходит успешно, устройство не назначит пользователю уровень привилегии. Если атрибут уровня привилегии установлен на значение ниже минимального поддерживаемого значения или выше максимального поддерживаемого значения, уровень привилегии игнорируется.

Для того чтобы RADIUS-сервер назначил **входящую/исходящую полосу пропускания**, необходимо сконфигурировать соответствующие параметры на сервере. В таблице ниже приведены параметры для полосы пропускания.

Атрибуты для производителя (Vendor-Specific Attributes):

Атрибут производителя	для 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 Unit (Kbits) полосы пропускания порта	Обязательно
--------------------------	---	-------------

Если пользователь сконфигурировал атрибут полосы пропускания на RADIUS-сервере (например, входящая полоса пропускания 1000 кбит/с) и аутентификация 802.1X прошла успешно, устройство назначит полосу пропускания пользователю в соответствии со значением на RADIUS-сервере. Однако если пользователь не сконфигурировал атрибут полосы пропускания и аутентификация проходит успешно, устройство не назначит пользователю полосу пропускания. Если атрибут полосы пропускания установлен на «0», для эффективной полосы пропускания будет установлен параметр no_limited. Если атрибут полосы пропускания установлен на значение ниже нуля или выше максимального поддерживаемого значения, полоса пропускания игнорируется.

Для того чтобы RADIUS-сервер назначил **приоритет по умолчанию 802.1p**, необходимо сконфигурировать соответствующие параметры на сервере. В таблице ниже приведены параметры для приоритета 802.1p.

Атрибуты для производителя (Vendor-Specific Attributes):

Атрибут производителя	Описание	Значение	Использование
Vendor-ID	Определяет производителя	171 (DLINK)	Обязательно
Vendor-Type	Определяет атрибут	4	Обязательно
Attribute-Specific Field	Используется для назначения приоритета по умолчанию 802.1p порта	0-7	Обязательно

Если пользователь сконфигурировал атрибут приоритета 802.1p на RADIUS-сервере (например, приоритет 7) и аутентификация 802.1X или на основе MAC прошла успешно, устройство назначит порту приоритет по умолчанию в соответствии со значением на RADIUS-сервере. Однако если пользователь не сконфигурировал атрибут приоритета и аутентификация проходит успешно, устройство не назначит порту приоритет. Если атрибут приоритета на RADIUS-сервере установлен на значение вне диапазона (>7), он не будет установлен на устройстве.

Для того чтобы RADIUS-сервер назначил **VLAN**, необходимо сконфигурировать соответствующие параметры на сервере. Для назначения VLAN RFC 3580 определяет следующие атрибуты в пакетах RADIUS.

Параметры для VLAN:

RADIUS Attribute	Tunnel Description	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 A string (VID)	Обязательно

Ниже показана краткая информация о формате атрибута Tunnel-Private-Group-ID:

[illegible]

В таблице ниже приведено описание поля Tag, которое отличается от RFC 2868:

Значение поля Tag	Формат строки поля
0x01	Имя VLAN (ASCII)
0x02	VLAN ID (ASCII)
Другие (0x00, 0x03 ~ 0x1F, >0x1F)	При получении строки настройки VLAN коммутатор сначала будет проверять все существующие VLAN ID и выберет подходящий, который станет идентификатором данной VLAN. Если подходящий VLAN ID отсутствует, коммутатор будет проверять доступные имена VLAN.

Примечание: поле тега больше 0x1F распознается как первый октет следующего поля.

Если пользователь сконфигурировал атрибут VLAN на RADIUS-сервере (например, VID 3) и аутентификация 802.1X, WAC или на основе MAC прошла успешно, порт будет назначен VLAN 3. Однако если пользователь не сконфигурировал атрибуты VLAN, порт, который не является членом Guest VLAN, будет храниться в текущей аутентификации VLAN, а порт, являющийся членом Guest VLAN, будет назначен в исходную VLAN.

Для того чтобы RADIUS-сервер назначил **ACL**, необходимо сконфигурировать соответствующие параметры на сервере. В таблице ниже приведены параметры для ACL.

Параметры для производителя (Vendor-Specific Attributes):

Атрибут производителя	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)»**.

Приложение Д. Поддержка атрибутов IETF RADIUS

Для атрибутов RADIUS существуют определенные детали аутентификации, авторизации и конфигурации для запросов и ответов. В данном разделе приведен список атрибутов RADIUS, которые в данный момент поддерживает коммутатор.

Атрибуты RADIUS поддерживаются стандартом IETF и Vendor-Specific Attribute (VSA). VSA позволяет вендорам создавать собственные дополнительные атрибуты RADIUS. Для подробной информации о VSA D-Link обратитесь к **Приложению Г, «Назначение атрибутов RADIUS»**.

Атрибуты RADIUS стандарта IETF определены в RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support и RFC 2869 RADIUS Extensions.

Список атрибутов IETF RADIUS, поддерживаемых коммутатором 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