



Руководство по командам
Ethernet-коммутаторы
серия QSW-6700



Оглавление

Описание ПО коммутатора	50
Назначение и аудитория	50
Описание продукта	51
1. РАБОТА С ИНТЕРФЕЙСОМ КОМАНДНОЙ СТРОКИ	52
1.1. Синтаксис команд	52
1.2. Условные обозначения команд	52
1.3. Общие значения параметров	53
1.4. Правила наименования unit/slot/port	54
1.5. Использование «No»-формы команд	55
1.6. Выполнение команд "show"	55
1.7. Фильтрация вывода командной строки	55
1.8. Режимы командной строки	57
1.9. Сокращенная форма и автозавершение команд	61
1.10. Сообщения об ошибках CLI	61
1.11. Комбинации клавиш для работы в командной строке	62
1.12. Справка и поддержка в командной строке	63
1.13. Получение доступа к CLI	64
2. КОМАНДЫ БАЗОВОГО КОНФИГУРИРОВАНИЯ КОММУТАТОРА	65
2.1. Команды базового конфигурирования	65
2.1.1. Строка проверки подлинности (authentication line)	65
2.1.2. Баннер (banner)	66
2.1.3. Загрузочный образ (boot img)	66
2.1.4. Конфигурирование загрузки (boot startup-config)	67
2.1.5. Настройка времени (clock set)	68
2.1.6. Конфигурирование (config)	68
2.1.7. Выключение (disable)	69
2.1.8. Включение (enable)	69
2.1.9. Включение пароля (enable password)	70
2.1.10. Окончание (end)	71
2.1.11. Тайм-аут выполнения (exec-timeout)	71
2.1.12. Выход (exit)	72
2.1.13. Справка (help)	72
2.1.14. Имя хоста (hostname)	73
2.1.15. IP-хост (ip host)	73
2.1.16. Хост IPv6 (ipv6 host)	74
2.1.17. Ip http-сервер (ip http server)	74

2.1.18. Логин (login)	75
2.1.19. Пароль (password)	75
2.1.20. Установка уровня привилегий (privilege)	76
2.1.21. Перезапуск (reload)	76
2.1.22. Служба шифрования паролей (service password-encryption)	77
2.1.23. Служба установки размеров окна (service terminal-length)	77
2.1.24. Контакты производителя (sysContact)	78
2.1.25. Адрес производителя (sysLocation)	78
2.1.26. Заводские настройки (set default)	79
2.1.27. Установка пароля в режиме загрузки (set boot password)	79
2.1.28. Настройка (setup)	80
2.1.29. Вывод времени (show clock)	80
2.1.30. Вывод данных об использовании процессора (show cpu usage)	81
2.1.31. Вывод данных о загрузке процессора (show cpu utilization)	81
2.1.32. Вывод данных об использовании памяти (show memory usage)	82
2.1.33. Вывод уровня привилегий (show privilege)	82
2.1.34. Вывод данных об уровне привилегий команды (show privilege mode LINE)	83
2.1.35. Вывод данных для тех. поддержки (show tech-support)	83
2.1.36. Вывод данных о версии (show version)	84
2.1.37. Имя пользователя (username)	84
2.1.38. Уровень HTTP/HTTPS-регистрации 1–15 (web-auth privilege <1-15>)	86
2.1.39. Запись (write)	86
2.1.40. Запись текущей конфигурирования (write running-config)	87
2.2. Команды для Telnet	87
2.2.1. Авторизация команд конфигурирования (aaa authorization config-commands)	87
2.2.2. Выполнение учета (accounting exec)	88
2.2.3. Команда настройки учета (accounting command)	89
2.2.4. Включение аутентификации (authentication enable)	90
2.2.5. Аутентификация с помощью IP access-class (authentication ip access-class)	91
2.2.6. Аутентификация с помощью IPv6 access-class (authentication ipv6 access-class)	91
2.2.7. Аутентификация с помощью логина (authentication line login)	92
2.2.8. Установка безопасного IP-адреса для аутентификации (authentication securityip)	93
2.2.9. Установка безопасного IPv6-адреса для аутентификации (authentication securityipv6)	94



2.2.10. Авторизация (authorization)	95
2.2.11. Команда авторизации через VTY (authorization line vty command)	96
2.2.12. Удаление команды VTY (clear line vty <0-31>)	97
2.2.13. Удаление секретного ключа (crypto key clear rsa)	97
2.2.14. Количество строк на терминале (terminal length)	98
2.2.15. Telnet	98
2.2.16. Включение Telnet-сервера (telnet server enable)	99
2.2.17. Соединение Telnet-сервера (telnet-server max-connection)	100
2.2.18. Число попыток повторной аутентифкации через SSH-сервер	100
2.2.19. Включение SSH-сервера (ssh-server enable)	101
2.2.20. Создание ключа безопасности для хоста (ssh-server host-key create rsa)	101
2.2.21. Соединение SSH-сервера (ssh-server max-connection)	102
2.2.22. Тайм-аут SSH-сервера (ssh-server timeout)	102
2.2.23. Вывод секретного ключа (show crypto key)	103
2.2.24. Вывод SSH-сервера (show ssh-server)	103
2.2.25. Вывод данных о пользователе Telnet (show telnet login)	104
2.2.26. Вывод данных о пользователях (show users)	104
2.2.27. Пользователи (who)	105
2.3. Команды для настройки IP-адресов коммутатора	105
2.3.1. Интерфейс VLAN (interface vlan)	105
2.3.2. IP-адрес (ip address)	106
2.3.3. IPv6-адрес (ipv6 address)	107
2.3.4. Включение ip-адреса BootP-клиента (ip bootp-client enable)	107
2.3.5. Включение ip-адреса DHCP клиента (ip dhcp-client enable)	108
2.4. Команды для настройки протокола SNMP	109
2.4.1. Включение RMON (rmon enable)	109
2.4.2. Вывод объекта oid в частной базе MIB (show private-mib oid)	109
2.4.3. Вывод SNMP (show snmp)	110
2.4.4. Вывод ID системы SNMP (show snmp engineid)	111
2.4.5. Вывод группы SNMP (show snmp group)	111
2.4.6. Вывод MIB SNMP (show snmp mib)	112
2.4.7. Вывод статуса SNMP (show snmp status)	112
2.4.8. Вывод данных о пользователе SNMP (show snmp user)	113
2.4.9. Вывод информации SNMP (show snmp view)	113
2.4.10. Сообщество SNMP-сервера (snmp-server community)	114
2.4.11. Включение SNMP-сервера (snmp-server enable)	115



2.4.12. Включение сообщений прерывания SNMP-сервера (snmp-server enable traps)	115
2.4.13. ID SNMP-сервера (snmp-server engineid)	116
2.4.14. Группа SNMP-сервера (snmp-server group)	117
2.4.15. Хост SNMP-сервера (snmp-server host)	119
2.4.16. Безопасный IP-адрес SNMP-сервера (snmp-server securityip)	120
2.4.17. Включение безопасного IP-адреса SNMP-сервера (snmp-server securityip enable)	121
2.4.18. Источник trap-сообщений SNMP-сервера (snmp-server trap-source)	121
2.4.19. Пользователь SNMP-сервера (snmp-server user)	122
2.4.20. Информация SNMP-сервера (snmp-server view)	123
2.4.21. Включение уведомлений об обновлении порта (switchport updown notification enable)	124
2.5. Команды для обновления коммутатора	125
2.5.1. Копирование (FTP) (copy (FTP))	125
2.5.2. Копирование (FTP) (copy (TFTP))	126
2.5.3. Файлы на FTP-сервере (ftp-dir)	128
2.5.4. Включение FTP-сервера (ftp-server enable)	128
2.5.5. Тайм-аут FTP-сервера (ftp-server timeout)	129
2.5.6. IP-адрес FTP (ip ftp)	129
2.5.7. Вывод FTP (show ftp)	130
2.5.8. Вывод TFTP (show tftp)	130
2.5.9. Включение TFTP-сервера (tftp-server enable)	130
2.5.10. Число попыток передачи данных TFTP (tftp-server retransmission-number)	131
2.5.11. Тайм-аут передачи данных TFTP-сервера (tftp-server transmission-timeout)	131
2.6. Команды для работы с файловой системой	132
2.6.1. Текущее устройство (cd)	132
2.6.2. Копирование (copy)	132
2.6.3. Удаление (delete)	133
2.6.4. Каталог (dir)	134
2.6.5. Текущая директория (pwd)	134
2.6.6. Переименование (rename)	135
3. РУКОВОДСТВО ПО НАСТРОЙКЕ ПОРТОВ	136
3.1. Команды для настройки Ethernet-порта	136
3.1.1. Пропускная способность (bandwidth)	136
3.1.2. Удаление данных интерфейса счетчиков (clear counters interface)	136
3.1.3. Описание (description)	137



3.1.4. Управление потоком (flow control)	137
3.1.5. Режим порта Ethernet (interface ethernet)	138
3.1.6. Петля (Loopback)	138
3.1.7. Интервал сбора статистики скорости порта (Port-rate-statistics interval)	139
3.1.8. Аномалия скорости (rate-violation)	139
3.1.9. Управление действиями при аномалии скорости (rate-violation control)	140
3.1.10. Вывод интерфейса (show interface)	141
3.1.11. Остановка (Shutdown)	142
3.1.12. Скорость и режим дуплекса (speed-duplex)	142
3.1.13. Управление трафиком (storm-control)	143
3.1.14. Управление трафиком (storm-control)	144
3.1.15. Управление фильтрацией (storm-control bypass)	145
3.1.16. Отмена приема пакетов (switchport discard packet)	146
3.1.17. Управление потоком коммутатора (switchport flood-control)	146
3.1.18. Переадресация потока коммутатора (switchport flood-forwarding)	147
3.2. Команды для настройки изоляции портов	148
3.2.1. Изоляция группы портов (isolate-port group)	148
3.2.2. Интерфейс изоляции порта группы (isolate-port group switchport interface)	148
3.2.3. Вывод данных об изоляции порта группы (show isolate-port group)	149
3.3. Команды обнаружения петель в портах	150
3.3.1. Управление обнаружением петель (loopback-detection control)	150
3.3.2. Тайм-аут восстановления после обнаружения петли (loopback-detection control-recovery timeout)	150
3.3.3. Интервал обнаружения петель (loopback-detection interval-time)	151
3.3.4. loopback-detection specified-vlan	151
3.3.5. Вывод данных об обнаружении петель (show loopback-detection)	152
3.4. Команды для настройки функции ULDP	153
3.4.1. Агрессивный режим ULDP (uldp aggressive-mode)	153
3.4.2. Включение ULDP (uldp enable)	153
3.4.3. Интервал приветственных сообщений ULDP (uldp hello-interval)	154
3.4.4. Ручная остановка ULDP (uldp manual-shutdown)	154
3.4.5. Время восстановления ULDP (uldp recovery-time)	155
3.4.6. Сброс ULDP (uldp reset)	155
3.4.7. Вывод данных ULDP (show uldp)	155
3.5. Команды для функции LLDP	156
3.5.1. Очистка удаленных таблиц LLDP (clear lldp remote-table)	156
3.5.2. Включение LLDP (lldp enable)	157



3.5.3. Включение порта LLDP (lldp enable (port))	157
3.5.4. TLV адреса управления LLDP (lldp management-address tlv)	157
3.5.5. Режим LLDP (lldp mode)	158
3.5.6. Множитель времени жизни сообщений LLDP (lldp msgTxHold)	159
3.5.7. Максимальное число записей LLDP (lldp neighbors max-num)	159
3.5.8. Интервал уведомлений LLDP (lldp notification interval)	159
3.5.9. Слишком много уведомлений LLDP (lldp tooManyNeighbors)	160
3.5.10. Задержка передачи LLDP (lldp transmit delay)	160
3.5.11. Опциональный TLV передачи LLDP (lldp transmit optional tlv)	161
3.5.12. Сообщения прерывания LLDP (lldp trap)	161
3.5.13. Интервал отправки LLDP (lldp tx-interval)	162
3.5.14. Вывод данных отладки LLDP (show debugging lldp)	163
3.5.15. Вывод данных LLDP (show lldp)	163
3.5.16. Вывод Ethernet-интерфейса LLDP (show lldp interface ethernet)	164
3.5.17. Вывод данных Ethernet-интерфейса соседних устройств LLDP (show lldp neighbors interface ethernet)	164
3.5.18. Вывод данных трафика LLDP (show lldp traffic)	165
3.6. Команды для настройки канала порта (Port Channel)	166
3.6.1. Интерфейс Port Channel (interface port-channel)	166
3.6.2. Приоритет порта протокола LACP (lacp port-priority)	166
3.6.3. Приоритет системы протокола LACP (lacp system-priority)	166
3.6.4. Тайм-аут LACP (lacp timeout)	167
3.6.5. Балансировка нагрузки (load-balance)	167
3.6.6. Группа портов (port-group)	168
3.6.7. Режим группы портов (port-group mode)	169
3.6.8. Вывод данных группы портов (show port-group)	169
3.7. Настройка MTU	170
3.7.1. MTU (Mtu)	170
3.8. Команды для EFM OAM	171
3.8.1. Удаление данных Ethernet OAM (clear ethernet-oam)	171
3.8.2. Ethernet OAM (ethernet-oam)	171
3.8.3. Верхний порог события ошибочного кадра для Ethernet OAM (ethernet-oam errored-frame threshold high)	172
3.8.4. Нижний порог события ошибочного кадра для Ethernet OAM (ethernet-oam errored-frame threshold low)	172
3.8.5. Диапазон обнаружения ошибочных кадров Ethernet OAM (ethernet-oam errored-frame window)	173
3.8.6. Верхний порог обнаружения события ошибочного кадра для Ethernet OAM (ethernet-oam errored-frame-seconds threshold high)	173



3.8.7. Нижний порог обнаружения события ошибочного кадра для Ethernet OAM (ethernet-oam errored-frame-seconds threshold Low)	174
3.8.8. Окно времени ошибочных кадров Ethernet OAM (ethernet-oam errored-frame-seconds window)	175
3.8.9. Верхнее пороговое значение обнаружения события ошибочного символа Ethernet OAM (ethernet-oam errored-symbol-period threshold High)	175
3.8.10. Нижнее пороговое значение обнаружения события ошибочного символа Ethernet OAM (ethernet-oam errored-symbol-period threshold Low)	176
3.8.11. Период обнаружения ошибочного символа Ethernet OAM (ethernet-oam errored-symbol-period window)	177
3.8.12. Мониторинг соединения Ethernet OAM (ethernet-oam link-monitor)	177
3.8.13. Режим Ethernet OAM (ethernet-oam mode)	178
3.8.14. Интервал Ethernet OAM (ethernet-oam period)	178
3.8.15. Удаленная индикация сбоев Ethernet OAM (ethernet-oam remote-failure)	179
3.8.16. Удаленная петля Ethernet OAM (ethernet-oam remote-loopback)	179
3.8.17. Поддержка обратной петли Ethernet OAM (ethernet-oam remote-loopback supported)	180
3.8.18. Тайм-аут Ethernet OAM (ethernet-oam timeout)	180
3.8.19. Вывод данных Ethernet OAM (show ethernet-oam)	181
3.8.20. Вывод данных о событиях Ethernet OAM (show ethernet-oam events)	181
3.8.21. Вывод данных конфигурирования событий соединения Ethernet OAM (show ethernet-oam link-events-configuration)	183
3.8.22. Вывод состояния петли Ethernet OAM (show ethernet-oam loopback status)	183
3.9. Конфигурирование Port Security	184
3.9.1. Удаление защищенных адресов порта (clear port-security)	184
3.9.2. Вывод данных защиты порта (show port-security)	185
3.9.3. Настройка защиты порта (switchport port-security)	185
3.9.4. Настройка MAC-адреса защиты порта (switchport port-security mac-address)	186
3.9.5. Предельное число защищенных MAC-адресов защиты порта (switchport port-security maximum)	186
3.9.6. Нарушение защиты порта (switchport port-security violation)	187
3.10. Настройка DDM	188
3.10.1. Удаление нарушения порогового значения трансивера (clear transceiver threshold-violation)	188
3.10.2. Вывод данных трансивера (show transceiver)	188
3.10.3. Вывод мониторинга трансивера (show transceiver threshold-violation)	189
3.10.4. Мониторинг трансивера (transceiver-monitoring)	190
3.10.5. Интервал мониторинга трансивера (transceiver-monitoring interval)	190
3.10.6. Порог трансивера (transceiver threshold)	191



3.11. Настройка LLDP-MED	192
3.11.1. Физический адрес (civic location)	192
3.11.2. Данные физического местоположения {description-language province-state city county street locationNum location floor room postal otherInfo}	193
3.11.3. Местоположение ECS (ecs location)	194
3.11.4. Быстрая отправка пакетов LLDP (lldp med fast count)	194
3.11.5. Отправка сообщений прерывания LLDP (lldp med trap)	195
3.11.6. Отправка всеми коммутаторами через LLDP-MED TLV (lldp transmit med tlv all)	195
3.11.7. Пропускная способность LLDP-MED TLV (lldp transmit med tlv capability)	196
3.11.8. Настройка порта для отправки LLDP-MED Extended Power-Via-MDI TLV (lldp transmit med tlv extendPoe)	196
3.11.9. Идентификация местоположения LLDP-MED TLV (lldp transmit med tlv location)	197
3.11.10. Управление реестром отправки LLDP-MED TLV (lldp transmit med tlv inventory)	197
3.11.11. Сетевая политика передачи LLDP-MED TLV (lldp transmit med tlv networkPolicy)	198
3.11.12. Сетевая политика (network policy)	199
3.11.13. Вывод данных LLDP (show lldp)	200
3.11.14. Вывод данных LLDP [Ethernet-интерфейс <IFNAME>] (show lldp [interface ethernet <IFNAME>])	201
3.11.15. Вывод данных соседних устройств LLDP (show lldp neighbors)	201
3.11.16. Вывод данных трафика LLDP (show lldp traffic)	202
3.12. Настройка BPDU-Tunnel	203
3.12.1. Протокол BPDU-Tunnel (bpdu-tunnel-protocol)	203
3.12.2. Группа MAC-адресов протокола BPDU-Tunnel (bpdu-tunnel-protocol group-mac)	204
3.12.3. Протокол MAC-адресов BPDU-Tunnel (bpdu-tunnel-protocol protocol-mac)	205
3.12.4. Ethernet протокола BPDU-Tunnel (bpdu-tunnel-protocol ethernetii)	205
3.12.5. Привязка протокола BPDU-Tunnel (bpdu-tunnel-protocol snap)	206
3.12.6. Протокол LLC BPDU-Tunnel (bpdu-tunnel-protocol llc)	207
3.13. Настройка функции энергосбережения EEE	208
3.13.1. Включение EEE (eee enable)	208
3.14. Команды отключения светодиода (LED) портов	209
3.14.1. Интервал отключения LED (port-led shutoff time-range)	209
4. MAC-АДРЕСА	210
4.1. Таблица MAC-адресов	210



4.1.1. Удаление таблицы коллизий MAC-адресов (clear collision-mac-address-table)	210
4.1.2. Удаление записей динамических адресов в таблице MAC-адресов (clear mac-address-table dynamic)	210
4.1.3. Включение/выключение обучения MAC-адресов (mac-address-learning enable disable)	211
4.1.4. Время старения таблицы MAC-адресов (mac-address-table aging-time)	211
4.1.5. Статические записи / «черные дыры» таблицы MAC-адресов (mac-address-table static blackhole)	212
4.1.6. Статический многоадресный MAC таблицы I2-адресов (I2-address-table static-multicast address)	214
4.1.7. Вывод коллизий таблицы MAC-адресов (show collision-mac-address-table)	215
4.1.8. Вывод таблицы MAC-адресов (show mac-address-table)	215
4.1.9. Вывод записей многоадресной таблицы I2-адресов (show I2-address-table multicast)	216
4.1.10. Удаление статистики MAC-уведомлений (clear mac-notification statistics)	216
4.1.11. Уведомления таблицы MAC-адресов (mac-address-table notification)	217
4.1.12. Размер истории уведомлений таблицы MAC-адресов (mac-address-table notification history-size)	217
4.1.13. Диапазон уведомлений таблицы MAC-адресов (mac-address-table notification interval)	218
4.1.14. Уведомления MAC (mac-notification)	218
4.1.15. Вывод сводной информации MAC-уведомлений (show mac-notification summary)	219
4.1.16. Включение уведомлений прерывания MAC-адреса сервера SNMP (snmp-server enable traps mac-notification)	219
5. VLAN	221
5.1. Команды для настройки сети VLAN	221
5.1.1. Сеть VLAN (vlan)	221
5.1.2. Имя VLAN (name (vlan))	222
5.1.3. Настройка интерфейса (switchport interface)	223
5.1.4. Настройка запрещенной сети VLAN (switchport forbidden vlan)	225
5.1.5. Режим переключения (switchport mode)	227
5.1.6. Нативная сеть VLAN гибридного порта (switchport hybrid native vlan)	228
5.1.7. Разрешенная сеть VLAN гибридного порта (switchport hybrid allowed vlan)	228
5.1.8. Настройка сети доступа VLAN (switchport access vlan)	230
5.1.9. Настройка магистрального порта разрешенной сети VLAN (switchport trunk allowed vlan)	230



5.1.10. Настройка магистрального порта нативной сети VLAN (switchport trunk native vlan)	231
5.1.11. Очистка списка разрешений (switchport mode trunk allow-null)	232
5.1.12. Включение отбрасывания VLAN (vlan ingress enable)	233
5.1.13. Включение преобразования тегов VLAN (vlan-translation enable)	234
5.1.14. Трансляция VLAN (vlan-translation)	235
5.1.15. Отбрасывание пакетов при трансляции VLAN (vlan-translation miss drop)	236
5.1.16. Включение туннеля Dot1q (dot1q-tunnel enable)	236
5.1.17. Включение расширения Selective QinQ (dot1q-tunnel selective enable)	237
5.1.18. Отношение Selective QinQ и VLAN (dot1q-tunnel selective s-vlan)	239
5.1.19. Таймер слияния GARP (garp timer join)	240
5.1.20. Таймер удаления GARP (garp timer leave)	241
5.1.21. Таймер удаления всех (leaveAll) GARP (garp timer leaveall)	242
5.1.22. Удаление таймеров GARP (no garp timer)	242
5.1.23. Режим глобальной конфигурации GVRP (gvrp(Global))	243
5.1.24. GVRP порта (gvrp(Port))	244
5.1.25. Частная сеть VLAN (private-vlan)	245
5.1.26. Ассоциация частной VLAN (private-vlan association)	246
5.1.27. Вывод данных туннеля Dot1q (show dot1q-tunnel)	247
5.1.28. Вывод значений таймеров GARP (show garp timer)	247
5.1.29. Вывод данных машин GVRP (show gvrp fsm information)	248
5.1.30. Вывод данных машин в статусе leaveAll (show gvrp leaveAll fsm information)	249
5.1.31. Данные таймера удержания GVRP (show gvrp leavetimer running information)	250
5.1.32. Просмотр портов с включенным GVRP (show gvrp port-member)	250
5.1.33. Вывод данных регистрации VLAN (show gvrp port registered vlan)	251
5.1.34. Данные установленных таймеров GVRP (show gvrp timer running information)	252
5.1.35. Вывод данных портов с зарегистрированной VLAN (show gvrp vlan registered port)	252
5.1.36. Вывод данных VLAN (show vlan)	253
5.1.37. Вывод данных VLAN-трансляции (show vlan-translation)	254
5.1.38. Трансляция VLAN Multi-to-One (vlan-translation n-to-1)	254
5.1.39. Вывод данных о трансляции Multi-to-One VLAN (show vlan-translation n-to-1)	256
5.1.40. Предпочтение динамической VLAN на основе MAC-адресов (dynamic-vlan mac-vlan prefer)	256
5.1.41. Приоритетность подсети VLAN (dynamic-vlan subnet-vlan prefer)	257



5.1.42. Сеть MAC VLAN (mac-vlan vlan)	258
5.1.43. Ассоциация MAC-адреса с VLAN (mac-vlan)	259
5.1.44. Протоколы VLAN (protocol-vlan)	260
5.1.45. Вывод данных о приоритетных динамических VLAN (show dynamic-vlan prefer)	261
5.1.46. Вывод данных VLAN на основе MAC-адресов (show mac-vlan interface)	261
5.1.47. Вывод данных протокола VLAN (show protocol-vlan)	262
5.1.48. Вывод данных подсети VLAN (show subnet-vlan)	262
5.1.49. Вывод интерфейса подсети VLAN (show subnet-vlan interface)	263
5.1.50. subnet-vlan	264
5.1.51. Настройка VLAN на основе MAC-адресов (switchport mac-vlan enable)	265
5.1.52. Настройка подсетей VLAN (switchport subnet-vlan enable)	265
5.1.53. Вывод данных голосовой VLAN (show voice-vlan)	266
5.1.54. Настройки голосовой VLAN (switchport voice-vlan enable)	267
5.1.55. Голосовая VLAN (voice-vlan)	268
5.1.56. Настройка VLAN в качестве голосовой (voice-vlan vlan)	269
6. НАСТРОЙКА ПРОТОКОЛА ANTI-RING	271
6.1. Команды работы с протоколом MSTP	271
6.1.1. Прерывание (abort)	271
6.1.2. Выход (exit)	271
6.1.3. Экземпляры VLAN (instance vlan)	272
6.1.4. Имя (name)	272
6.1.5. Номер версии (revision-level)	273
6.1.6. Протокол STP (spanning-tree)	273
6.1.7. Метрика протокола STP (spanning-tree cost)	274
6.1.8. Использование партнерского порта (spanning-tree digest-snooping)	275
6.1.9. Формат пакета STP (spanning-tree format)	276
6.1.10. Время задержки передачи (spanning-tree forward-time)	277
6.1.11. Время приветствия STP (spanning-tree hello-time)	277
6.1.12. Тип линии «точка-точка» (spanning-tree link-type p2p)	278
6.1.13. Максимальный срок жизни (spanning-tree maxage)	278
6.1.14. Максимальное число хопов (spanning-tree max-hop)	279
6.1.15. Установка режима MSTP (spanning-tree mcheck)	280
6.1.16. Режим STP (spanning-tree mode)	280
6.1.17. Режим конфигурации MSTP (spanning-tree mst configuration)	281
6.1.18. Метрика MSTP (spanning-tree mst cost)	281
6.1.19. Формат метрики MSTP (spanning-tree cost-format)	283
6.1.20. Защита от закольцовывания MSTP (spanning-tree mst loopguard)	283



6.1.21. Приоритет порта (spanning-tree mst port-priority)	284
6.1.22. Приоритет коммутатора MSTP (spanning-tree mst priority)	284
6.1.23. Защита коммутатора (spanning-tree mst rootguard)	285
6.1.24. Режим граничного порта (spanning-tree portfast)	286
6.1.25. Приоритет порта (spanning-tree port-priority)	287
6.1.26. Приоритет коммутатора (spanning-tree priority)	287
6.1.27. Защита корневого порта (spanning-tree rootguard)	288
6.1.28. Режим FLUSH STP (режим глобальной конфигурации) (spanning-tree tcflush (Global mode))	288
6.1.29. Режим FLUSH STP (режим конфигурации порта) (spanning-tree tcflush (Port mode))	289
6.1.30. Максимальное число отправки (spanning-tree transmit-hold-count)	290
6.1.31. Вывод данных текущего региона MSTP (show mst-pending)	290
6.1.32. Вывод данных MSTP (show spanning-tree)	291
6.1.33. Вывод параметров MSTP (show spanning-tree mst config)	293
6.1.34. Процесс MSTP (spanning-tree process)	294
6.1.35. MSTP-процесс 0 (spanning-tree tc-notify process0)	294
6.1.36. Процесс присоединения порта (spanning-tree binding-process)	295
6.1.37. Присоединение общего порта (spanning-tree binding-process link-share)	295
6.2. Команды настройки протокола ERPS	296
6.2.1. Настройка отправки уведомлений ERPS (ethernet tcn-propagation erps to {erps stp})	296
6.2.2. Имя кольца ERPS (erps-ring <ring-name>)	297
6.2.3. Версия (version {v1 v2})	297
6.2.4. Подкольцо открытого типа (open-ring)	298
6.2.5. Виртуальный канал R-APS (raps-virtual-channel {with without})	299
6.2.6. Порт 0 кольца ERPS (erps-ring <ring-name> port0 [port1-none])	299
6.2.7. Порт 1 кольца ERPS (erps-ring <ring-name> port1)	300
6.2.8. Обнаружение неисправности (failure-detect {cc physical-link-or-cc} domain <domain-name> service {< ma-name > number < ma-num > pvlan < vlan-id >} mep <mep-id> rmep<rmep-id>)	301
6.2.9. Экземпляр кольца ERPS (erps-instance <instance-id>)	302
6.2.10. Описание (description)	303
6.2.11. Идентификатор кольца ERPS (ring-id <ring-id>)	303
6.2.12. Роли RPL (rpl {port0 port1} {owner neighbour})	304
6.2.13. Реверсивный режим (non-revertive)	305
6.2.14. Таймер защиты (guard-timer <guard-times>)	305
6.2.15. Таймер задержки (holdoff-timer <holdoff-times>)	306
6.2.16. Таймер WTR (wtr-timer <wtr-times>)	306



6.2.17. Экземпляр защиты (protected-instance)	307
6.2.18. Уровень канала R-APS (raps-mel <level-value>)	307
6.2.19. Управляющая сеть VLAN (control-vlan <vlan-id>)	308
6.2.20. Принудительное переключение (forced-switch {port0 port1})	309
6.2.21. Ручное переключение (manual-switch {port0 port1})	309
6.2.22. Очищение команд (clear command)	310
6.2.23. Вывод данных о кольце ERPS (show erps ring {<ring-name> brief})	311
6.2.24. Вывод данных экземпляра кольца ERPS (show erps instance [ring <ring-name> [instance <instance-id>]])	312
6.2.25. Вывод состояния экземпляра кольца ERPS (show erps status [ring <ring-name> [instance <instance-id>]])	313
6.2.26. Вывод статистики экземпляра кольца ERPS (show erps statistics [ring <ring-name> [instance <instance-id>]])	315
6.2.27. Удаление статистики экземпляра кольца ERPS (clear erps statistics [ring <ring-name> [instance <instance-id>]])	316
7. КАЧЕСТВО ОБСЛУЖИВАНИЯ (QOS)	318
7.1. Команды для настройки качества обслуживания (QOS)	318
7.1.1. Статистика (accounting)	318
7.1.2. Класс (class)	318
7.1.3. Карта классов (class-map)	319
7.1.4. Удаление статистики карт правил (clear mls qos statistics)	320
7.1.5. Отбрасывание (drop)	320
7.1.6. Согласование (match)	321
7.1.7. Значение CoS (mls qos cos)	322
7.1.8. Карта соответствия значений (mls qos map)	323
7.1.9. Пропускная способность очереди (mls qos queue bandwidth)	325
7.1.10. Доверие меткам COS (mls qos trust)	326
7.1.11. Карта правил (Policy-map)	327
7.1.12. Применение карты правил (service-policy input)	328
7.1.13. Применение карты правил на указанном VLAN-интерфейсе (service-policy input vlan)	328
7.1.14. Настройка значений (set)	329
7.1.15. Вывод карты классов (show class-map)	330
7.1.16. Вывод карты правил (show policy-map)	330
7.1.17. Вывод интерфейса QoS (show mls qos interface)	331
7.1.18. Вывод данных о настройках политики (show mls qos in (interface <interface-name> policy) (vlan <vlan-id>))	334
7.1.19. Вывод данных о настройках карт (show mls qos maps)	335
7.1.20. Вывод данных о конфигурировании QOS VLAN (show mls qos vlan)	337



7.1.21. Передача (transmit)	337
7.1.22. Перенаправление на основе трафика (access-group redirect to interface ethernet)	338
7.1.23. Перенаправлении трафика для системы/порта (show flow-based-redirect)	339
7.1.24. Добавление (add)	339
7.1.25. Согласование (match)	340
7.1.26. Карта политики (service-policy)	341
7.1.27. Установка (set)	342
8. КОМАНДЫ ДЛЯ ПРОТОКОЛОВ FORWARD И ARP УРОВНЯ 3	344
8.1. Команды для настройки интерфейса уровня 3	344
8.1.1. Описание (description)	344
8.1.2. Интерфейс VLAN (interface vlan)	344
8.1.3. Удаление интерфейса (no interface IFNAME)	345
8.1.4. Вывод данных маршрутизации (show ip route)	345
8.2. Команды для настройки протоколов IPv4/v6	346
8.2.1. Очищение статистической информации IP-протокола (clear ip traffic)	346
8.2.2. Очищение адресов соседних устройств (clear ipv6 neighbor)	347
8.2.3. IP-адрес (ip address)	347
8.2.4. IPv6-адрес (ipv6 address)	348
8.2.5. Число сообщений оповещения соседних устройств (ipv6 nd dad attempts)	349
8.2.6. Интервал отправки сообщений (ipv6 nd ns-interval)	349
8.2.7. ipv6 neighbor	350
8.2.8. Вывод данных интерфейса VLAN (show ip interface)	351
8.2.9. Вывод данных трафика пакетов IP (show ip traffic)	351
8.2.10. Вывод данных интерфейса IPv6 (show ipv6 interface)	353
8.2.11. Вывод данных маршрутизации IPv6 (show ipv6 route)	355
8.2.12. Вывод данных устройств IPv6 (show ipv6 neighbors)	356
8.2.13. Вывод данных трафика IPv6 (show ipv6 traffic)	357
8.2.14. IP-адрес маршрутизации (ip route)	359
8.3. Команды для настройки ARP	360
8.3.1. Записи ARP (arp)	360
8.3.2. Удаление содержимого таблицы ARP (clear arp-cache)	360
8.3.3. Очищение данных трафика ARP (clear arp traffic)	361
8.3.4. Вывод текущей таблицы ARP (show arp)	361
8.3.5. Вывод трафика сообщений ARP (show arp traffic)	363
8.4. Команды для настройки защиты от arp-сканирования	363



8.4.1. Включение защиты от ARP-сканирования (anti-arpscan enable)	363
8.4.2. Пороговое значение защиты от ARP-сканирования (anti-arpscan port-based threshold)	364
8.4.3. Пороговое значение защиты от ARP-сканирования на основе IP-адресов (anti-arpscan ip-based threshold)	364
8.4.4. Настройка безопасного порта (anti-arpscan trust)	365
8.4.5. Настройка безопасного IP-адреса (anti-arpscan trust ip)	365
8.4.6. Включение автоматического восстановления (anti-arpscan recovery enable)	366
8.4.7. Время автоматического восстановления (anti-arpscan recovery time)	366
8.4.8. Включение регистрации защиты от ARP-сканирования (anti-arpscan log enable)	367
8.4.9. Включение SNMP Trap защиты от ARP-сканирования (anti-arpscan trap enable)	367
8.4.10. Вывод данных защиты от ARP-сканирования (show anti-arpscan)	368
8.5. Команды для настройки защиты от подмены ARP	369
8.5.1. Автоматическое обновление ARP (ip arp-security updateprotect)	369
8.5.2. Автоматическое обучение ARP (ip arp-security learnprotect)	370
8.5.3. Преобразование записей ARP (ip arp-security convert)	370
8.5.4. Удаление записей ARP (clear ip arp dynamic)	370
8.5.5. Удаление записей ND (clear ipv6 nd dynamic)	371
8.6. Команды для настройки защиты ARP (ARP Guard)	371
8.6.1. Настройка ip-адреса (arp-guard ip)	371
8.7. Команды для настройки самообращенных запросов (Gratuitous ARP)	372
8.7.1. Включение самообращенного ARP и настройка интервала обновления (ip gratuitous-arp)	372
8.7.2. Отображение конфигурации самообращенного ARP (show ip gratuitous-arp)	373
8.8. Команды настройки функции контроля динамических ARP (Dynamic ARP Inspection)	373
8.8.1. Включение функции ARP (ip arp inspection)	373
8.8.2. Настройка доверенного порта (ip arp inspection trust)	374
8.8.3. Частота получаемых запросов (ip arp inspection limit-rate)	374
9. DHCP	376
9.1. Команды для настройки DHCP	376
9.1.1. Настройка загрузочного файла (bootfile)	376
9.1.2. Удаление записи привязки IP-адреса (clear ip dhcp binding)	376
9.1.3. Удаление записи обнаруженных конфликтов адресов (clear ip dhcp conflict)	377
9.1.4. Удаление статистики DHCP-сервера (clear ip dhcp server statistics)	377



9.1.5. Настройка идентификатора пользователя (client-identifier)	378
9.1.6. Настройка шлюза по умолчанию (default-router)	378
9.1.7. Настройка DNS-серверов (dns-server)	379
9.1.8. Доменное имя для DHCP-клиентов (domain-name)	379
9.1.9. Аппаратный адрес пользователя (hardware-address)	380
9.1.10. Настройка IP-адреса для пользователя (host)	381
9.1.11. Регистрация конфликтов адресов (ip dhcp conflict logging)	381
9.1.12. Выключение сервисов DHCP на интерфейсе (ip dhcp disable)	382
9.1.13. Удаление динамически распределяемых адресов (ip dhcp excluded-address)	382
9.1.14. Пул DHCP-адресов (ip dhcp pool)	383
9.1.15. Ping-обнаружение конфликтов на DHCP-сервере (ip dhcp conflict ping-detection enable)	383
9.1.16. Количество направляемых ping-пакетов (ip dhcp ping packets)	384
9.1.17. Тайм-аут ping-пакета (ip dhcp ping timeout)	384
9.1.18. Срок аренды адресов пула (lease)	385
9.1.19. Максимальное время аренды адреса (max-lease-time)	386
9.1.20. Адрес WINS-сервера (netbios-name-server)	386
9.1.21. Тип узла для порта (netbios-node-type)	387
9.1.22. Диапазон присваиваемых адресов (network-address)	388
9.1.23. Адрес сервера хранения файла, импортируемого клиентом (next-server)	388
9.1.24. Настройка параметра сети (option)	389
9.1.25. Включение службы DHCP (service dhcp)	390
9.1.26. Вывод информации о привязках (show ip dhcp binding)	390
9.1.27. Вывод информации по конфликтующим адресам (show ip dhcp conflict)	391
9.1.28. Отображение информации состоянии опции (show ip dhcp relay information option)	392
9.1.29. Вывести статистику для DHCP-сервера (show ip dhcp server statistics)	392
9.1.30. Подавление широковещательной рассылки DHCP (ip dhcp broadcast suppress)	394
9.1.31. Настройка VLAN источника и назначения перенаправления (ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist>)	395
9.1.32. Настройка DHCP-relay для перенаправления пакетов (ip forward-protocol udp bootps)	395
9.1.33. Адрес DHCP сервера для перенаправления (ip helper-address)	396
9.1.34. Отображение протокола перенаправления (show ip forward-protocol)	397
9.1.35. Вывод адреса сервера ретрансляции (show ip helper-address)	397
9.1.36. Удаление запись привязки IPv6-адреса (clear ipv6 dhcp binding)	398



9.1.37. Удаление информации о конфликтах ipv6-адресов (clear ipv6 dhcp conflict)	398
9.1.38. Удаление статистики ipv6 DHCP-сервера (clear ipv6 dhcp statistics)	399
9.1.39. DNS-серверы для DHCPv6-клиентов (dns-server)	399
9.1.40. Доменное имя для DHCPv6-клиентов (domain-name)	400
9.1.41. Исключение адреса из раздачи (excluded-address)	400
9.1.42. Настройка IPv6-адреса (ipv6 address)	401
9.1.43. Сконфигурировать клиент назначения префикса (ipv6 dhcp client pd)	402
9.1.44. Назначить требуемый клиентом префикс (ipv6 dhcp client pd hint)	403
9.1.45. Создание пула адресов DHCPv6 (ipv6 dhcp pool)	403
9.1.46. Адрес перенаправления запросов для DHCPv6 relay (ipv6 dhcp relay destination)	404
9.1.47. Включение функции DHCPv6 сервера (ipv6 dhcp server)	405
9.1.48. Настройка общего префикса адресов (ipv6 general-prefix)	405
9.1.49. Пул делегирования префиксов (ipv6 local pool)	406
9.1.50. Конфигурирование времени жизни (lifetime)	407
9.1.51. Настройка пула адресов (network-address)	408
9.1.52. Выдача определенного префикса (prefix-delegation)	409
9.1.53. Пул делегирования префиксов, используемый адресным пулом (prefix-delegation pool)	410
9.1.54. Включение службы DHCPv6 (service dhcpv6)	410
9.1.55. Вывод настроек сервера DHCPv6 (show ipv6 dhcp)	411
9.1.56. Вывод привязки адресов и префиксов службы DHCPv6 (show ipv6 dhcp binding)	411
9.1.57. Вывод всех конфликтов адресов, зарегистрированных сервером DHCPv6 (show ipv6 dhcp conflict)	412
9.1.58. Вывод информации DHCPv6 для интерфейса (show ipv6 dhcp interface)	412
9.1.59. Проверка имени DHCPv6-пула и его параметры (show ipv6 dhcp pool)	413
9.1.60. Статистика DHCPv6-сервера (show ipv6 dhcp statistics)	414
9.1.61. Вывод информации, общей для префикса IPv6-пула (show ipv6 general-prefix)	415
9.1.62. Вывести информацию для DHCPv6 пула префиксов (show ipv6 local pool)	416
9.1.63. Включение добавления опции 82 ретрансляции DHCP (ip dhcp relay information option)	416
9.1.64. Настройка разделителя (ip dhcp relay information option delimiter)	417
9.1.65. Настройка Remote ID опции 82 (ip dhcp relay information option remote-id)	417
9.1.66. Настройка формата Remote ID опции 82 (ip dhcp relay information option remote-id format)	418



9.1.67. Пользовательские параметры remote-id для опции 82 (ip dhcp relay information option self-defined remote-id)	419
9.1.68. Формат представления данных remote-id для опции 82 (ip dhcp relay information option self-defined remote-id format)	420
9.1.69. Пользовательские параметры subscriber-id для опции 82 (ip dhcp relay information option self-defined subscriber-id)	421
9.1.70. Пользовательский формат subscriber-id (ip dhcp relay information option self-defined subscriber-id format)	421
9.1.71. Содержание опции subscriber-id (ip dhcp relay information option subscriber-id)	422
9.1.72. Формат представления данных опции subscriber-id (ip dhcp relay information option subscriber-id format)	423
9.1.73. Политика ретрансляции сообщения (ip dhcp relay information policy)	424
9.1.74. Включение опции 82 DHCP сервера (ip dhcp server relay information enable)	425
9.1.75. Вывод информации о состоянии опции 82 (show ip dhcp relay information option)	425
9.1.76. Установка опции 43 в формате ASCII (option 43 ascii LINE)	426
9.1.77. Задать опцию 43 в формате HEX (option 43 hex WORD)	426
9.1.78. Задать опцию 43 в формате IP-адреса (option 43 ip A.B.C.D)	427
9.1.79. Задать опцию 60 в формате ASCII (option 60 ascii LINE)	427
9.1.80. Задать опцию 60 в формате HEX (option 60 hex WORD)	428
9.1.81. Задать опцию 60 в формате IP-адреса (option 60 ip A.B.C.D)	428
9.1.82. Диапазон адресов адресного пула (address range)	429
9.1.83. Конфигурация класса в пуле адресов (class)	430
9.1.84. Создание dhcpv6 класс (ipv6 dhcp class)	430
9.1.85. Настройка добавления опции 37 (ipv6 dhcp relay remote-id)	431
9.1.86. Включение поддержки опции 37 в DHCPv6-relay (ipv6 dhcp relay remote-id option)	431
9.1.87. Настройка добавления опции 38 в DHCPv6-relay (ipv6 dhcp relay subscriber-id)	432
9.1.88. Включение поддержки опции 38 в DHCPv6-relay (ipv6 dhcp relay subscriber-id option)	433
9.1.89. Выбор разделителя наименований для опции 38 DHCPv6 ретранслятора (ipv6 dhcp relay subscriber-id select delimiter)	433
9.1.90. Поддержка опции 37 в DHCPv6-сервере (ipv6 dhcp server remote-id option)	434
9.1.91. Выбор между опциями 37 и 38 на DHCPv6-сервере (ip dhcp server select relay-forw)	434
9.1.92. Выбор между опциями 37 и 38 на DHCPv6-сервере (ip dhcp server select relay-forw)	435



9.1.93. Поддержка опции 38 в DHCPv6 сервере (ipv6 dhcp server subscriber-id option)	436
9.1.94. Формат представления данных remote-id опции 37 ретранслирующего агента (ipv6 dhcp snooping information option remote-id format)	436
9.1.95. Формат представления данных subscribe-id для опции 38 DHCPv6 snooping (ipv6 dhcp snooping information option subscriber-id format)	437
9.1.96. Форма добавления опции 37 в DHCPv6 snooping (ipv6 dhcp snooping remote-id)	438
9.1.97. Поддержка опции 37 в DHCPv6 snooping (ipv6 dhcp snooping remote-id option)	438
9.1.98. Политика пересылки пакетов, содержащих опцию 37 (ipv6 dhcp snooping remote-id policy)	439
9.1.99. Форма добавления опции 38 в DHCPv6-snooping (ipv6 dhcp snooping subscriber-id)	440
9.1.100. Поддержка опции 38 в DHCPv6-snooping (ipv6 dhcp snooping subscriber-id option)	440
9.1.101. Политика пересылки пакетов, содержащих опцию 38 (ipv6 dhcp snooping subscriber-id policy)	441
9.1.102. Выбор разделителя наименований для опции 38 DHCPv6 snooping (ipv6 dhcp snooping subscriber-id select delimiter)	442
9.1.103. Поддержка классов для DHCPv6 адресов (ipv6 dhcp use class)	442
9.1.104. Настройка опций, соответствующих классу (remote-id subscriber-id)	443
9.1.105. Вывод конфигурации ретранслятора (show ipv6 dhcp relay option)	444
9.1.106. Просмотр опций DHCPv6 Snooping (show ipv6 dhcp snooping option)	444
9.1.107. Включение ключа шифрования DES для приватных пакетов (enable trustview key)	445
9.1.108. Включение функции DHCP Snooping (ip dhcp snooping)	445
9.1.109. Установить действия защиты (ip dhcp snooping action)	446
9.1.110. Задать число оборонительных операций (ip dhcp snooping action MaxNum)	447
9.1.111. Включение функции привязки DHCP Snooping (ip dhcp snooping binding)	447
9.1.112. Включение функции привязки DOT1X для DHCP Snooping (ip dhcp snooping binding dot1x)	448
9.1.113. Настройка статической привязки (ip dhcp snooping binding user)	448
9.1.114. Включение функции привязки пользователя (ip dhcp snooping binding user-control)	449
9.1.115. Максимальное число пользователей с разрешенным доступом (ip dhcp snooping binding user-control max-user)	450
9.1.116. Включение функции опции 82 DHCP Snooping (ip dhcp snooping information enable)	451
9.1.117. Разрешение передачи DHCP-запросов с недоверенных портов (ip dhcp snooping information option allow-untrusted (replace))	452



9.1.118. Разделитель для параметров суб-опций опции 82 (ip dhcp snooping information option delimiter)	452
9.1.119. Содержание суб-опции remote-id опции 82 (ip dhcp snooping information option remote-id)	453
9.1.120. Настройка пользовательских параметров суб-опции remote-id в опции 82 (ip dhcp snooping information option self-defined remote-id)	453
9.1.121. Формат представления данных заданной пользователем суб-опции remote-id (ip dhcp snooping information option self-defined remote-id format)	454
9.1.122. Настройка пользовательских параметров суб-опции subscriber-id в опции 82 (ip dhcp snooping information option self-defined subscriber-id)	455
9.1.123. Формат представления данных заданной пользователем суб-опции subscriber-id (ip dhcp snooping information option self-defined subscriber-id)	456
9.1.124. Содержание опции subscriber-id опции 82 DHCP snooping (ip dhcp snooping information option subscriber-id)	456
9.1.125. Формат представления данных subscribe-id для опции 82 DHCPv6 snooping (ipv6 dhcp snooping information option subscriber-id format)	457
9.1.126. Предельная скорость поступления сообщений DHCP (ip dhcp snooping limit-rate)	458
9.1.127. Атрибуты безопасности DHCP Snooping для порта (ip dhcp snooping trust)	459
9.1.128. Функция DHCP snooping для VLAN (ip dhcp snooping vlan)	459
9.1.129. Настройка адреса и порта HELPER-сервера (ip user helper-address)	460
9.1.130. Установить на коммутаторе версию 2 частных пакетов (ip user private packet version two)	461
9.1.131. Вывод информации о текущих настройках dhcp snooping (show ip dhcp snooping)	461
9.1.132. Вывод информации о созданных привязках (show ip dhcp snooping binding all)	464
9.1.133. Вывод информации о пакетах от TrustView (show trustview status)	465
9.1.134. Включить функцию option 82 DHCP Snooping (ip dhcp snooping information enable)	465
10. ПРОТОКОЛ МНОГОАДРЕСНОЙ ПЕРЕДАЧИ	467
10.1. Настройка протокола многоадресной передачи IPv4	467
10.1.1. Список доступа (access-list (управление назначением группового трафика))	467
10.1.2. Список доступа (управление источником группового трафика) (access-list (Multicast Source Control))	468
10.1.3. Список доступа для управления назначением (ip multicast destination-control access-group)	469
10.1.4. Список доступа для управления назначением на указанном сегменте (ip multicast destination-control access-group (sip))	470
10.1.5. Список доступа для управления назначением на указанной сети (ip multicast destination-control access-group (vmac))	470



10.1.6. Политика обслуживания группового трафика (ip multicast policy)	471
10.1.7. Управление групповым источником (ip multicast source-control)	472
10.1.8. Управление источником групповых данных (ip multicast source-control access-group)	472
10.1.9. Управление назначением многоадресной рассылки (ip multicast destination-control)	473
10.1.10. Добавление правила profile-id (Список правил управления многоадресной рассылкой) (profile-id (Multicast Destination Control Rule List))	473
10.1.11. Вывод настроек назначения (show ip multicast destination-control)	474
10.1.12. Вывод настроек списка доступа для управления назначением (show ip multicast destination-control access-list)	475
10.1.13. Вывод списка профилей для контроля назначения (show ip multicast destination-control filter-profile-list)	475
10.1.14. Вывести информацию о настройках политики обслуживания группового трафика (show ip multicast policy)	476
10.1.15. Вывод настроек управления групповым трафиком (show ip multicast source-control)	476
10.1.16. Удаление записи о группе в vlan (clear ip igmp snooping vlan)	477
10.1.17. Удаление mrouter-порт в vlan (clear ip igmp snooping vlan <1-4094> mrouter-port)	477
10.1.18. Включение функции IGMP Snooping (ip igmp snooping)	478
10.1.19. Включить функцию IGMP Snooping проху (ip igmp snooping proxy)	478
10.1.20. Настроить igmp snooping на указанном vlan (ip igmp snooping vlan)	479
10.1.21. Включение функции быстрого выхода для VLAN (ip igmp snooping vlan immediate-leave)	479
10.1.22. Включение функции быстрого выхода по mac-адресам (ip igmp snooping vlan <id> immediately-leave mac-based)	480
10.1.23. Установка vlan как маршрутизатор уровня 2 (ip igmp snooping vlan l2-general-querier)	481
10.1.24. Установка адреса источника для маршрутизатора (ip igmp snooping vlan l2-general-querier-source)	481
10.1.25. Настройка версии маршрутизатора (ip igmp snooping vlan l2-general-querier-version)	482
10.1.26. Максимальное число групп и их источников (ip igmp snooping vlan limit)	482
10.1.27. Максимальное количество групп и их источников для интерфейса IFNAME (ip igmp snooping vlan interface (ethernet port-channel) IFNAME limit)	483
10.1.28. Статический порт mrouter на vlan (ip igmp snooping vlan mrouter-port interface)	484
10.1.29. Динамическое добавление Mrouter порта для VLAN (ip igmp snooping vlan mrouter-port learnpim)	484
10.1.30. Задать срок жизни порта mrouter (ip igmp snooping vlan mrpt)	485



10.1.31. Задать интервал отправки запросов (ip igmp snooping vlan query-interval)	485
10.1.32. Максимальный интервал времени ожидания ответа (ip igmp snooping vlan query-mrsp)	486
10.1.33. Задать надежность запроса (ip igmp snooping vlan query-robustness)	486
10.1.34. IP-адрес источника при перенаправлении IGMP сообщений (ip igmp snooping vlan report source-address)	487
10.1.35. Максимальное время ответа на запросы принадлежности (ip igmp snooping vlan specific-query-mrsp)	487
10.1.36. Задать статическую группу на указанном порту vlan (ip igmp snooping vlan static-group)	488
10.1.37. Задать время подавления запроса (ip igmp snooping vlan suppression-query-time)	488
10.1.38. Вывод информации о сконфигурированных параметрах IGMP Snooping (show ip igmp snooping)	489
10.1.39. Удаление записи о группе в указанном vlan (clear ipv6 mld snooping vlan)	491
10.1.40. Удаление порта mrouter в указанном vlan (clear ipv6 mld snooping vlan <1-4094> mrouter-port)	491
10.1.41. Включение функции MLD Snooping (ipv6 mld snooping)	492
10.1.42. Включение MLD Snooping в указанной VLAN (ipv6 mld snooping vlan)	492
10.1.43. Функция быстрого выхода протокола MLD для указанной vlan (ipv6 mld snooping vlan immediate-leave)	493
10.1.44. Установить указанный vlan, как маршрутизатор уровня 2 (ipv6 mld snooping vlan l2-general-querier)	493
10.1.45. Максимальное число групп MLD snooping и их источников (ipv6 mld snooping vlan limit)	494
10.1.46. Установка статического порта mrouter для VLAN (ipv6 mld snooping vlan mrouter-port interface)	495
10.1.47. Получение информации о mrouter-порт на основе пакетов IPv6 PIM (ipv6 mld snooping vlan mrouter-port learnpim6)	495
10.1.48. Настройка срока жизни порта mrouter (ipv6 mld snooping vlan mrpt)	496
10.1.49. Задать интервал отправки запросов (ipv6 mld snooping vlan query-interval)	496
10.1.50. Максимальный интервал времени ожидания ответа (ipv6 mld snooping vlan query-mrsp)	497
10.1.51. Количество MLD Query без ответа до удаления MLD snooping для VLAN (ipv6 mld snooping vlan query-robustness)	497
10.1.52. Задать в указанном порту VLAN статическую группу (ipv6 mld snooping vlan static-group)	498
10.1.53. Задать время подавления запроса (ipv6 mld snooping vlan suppression-query-time)	498
10.1.54. Вывод настроек MLD Snooping (show ipv6 mld snooping)	499



10.1.55. Включение функции Multicast VLAN на VLAN (multicast-vlan)	501
10.1.56. Ассоциация VLAN с Multicast VLAN (multicast-vlan association)	502
10.1.57. Ассоциация Multicast VLAN с интерфейсом (multicast-vlan association interface)	502
10.1.58. Выбор режима работы Multicast VLAN (multicast-vlan mode)	503
10.1.59. Связь с Multicast Vlan на порте коммутатора (switchport association multicast-vlan)	504
10.2. Команды настройки IGMP	505
10.2.1. Вывод информации таблицы маршрутизации многоадресной рассылки (show ip mroute)	505
10.2.2. Вывод таблицы многоадресной маршрутизации ipv6 (show ipv6 mroute)	506
10.2.3. Удаление IGMP-групп (clear ip igmp group)	507
10.2.4. Включить режим отладки (debug igmp event)	508
10.2.5. Отладка IGMP пакетов (debug igmp packet)	508
10.2.6. Список доступа к интерфейсу IGMP (ip igmp access-group)	509
10.2.7. Группы, поддерживающие немедленный выход на интерфейсе (ip igmp immediate-leave)	509
10.2.8. Подключение интерфейса к группе (ip igmp join-group)	510
10.2.9. Значение интервала запросов последнего участника (ip igmp last-member-query-interval)	511
10.2.10. Максимальное количество разрешённых состояний IGMP (ip igmp limit)	511
10.2.11. Интервал запросов IGMP (ip igmp query-interval)	512
10.2.12. Максимальное время отклика на запрос IGMP (ip igmp query-max-response-time)	513
10.2.13. Тайм-аут запроса IGMP (ip igmp query-timeout)	513
10.2.14. Значение устойчивости IGMP-запроса (ip igmp robust-variable)	514
10.2.15. Статическая принадлежность интерфейса группе (ip igmp static-group)	514
10.2.16. Установка версии IGMP на интерфейсе (ip igmp version)	515
10.2.17. Вывод информации о IGMP-группах (show ip igmp groups)	516
10.2.18. Вывод информации о IGMP на интерфейсе (show ip igmp interface)	518
10.3. Настройка протокола PIM-DM	518
10.3.1. Отладка таймера активности источника PIM (debug pim timer sat)	518
10.3.2. Отладка таймера обновления состояний (debug pim timer srt)	519
10.3.3. Создание статического multicast-маршрута (ip mroute)	519
10.3.4. Настройка границ BSR (ip pim bsr-border)	520
10.3.5. Уплотнённый режим (ip pim dense-mode)	521
10.3.6. Настройка приоритета выбора назначенного маршрутизатора (ip pim dr-priority)	521
10.3.7. Исключение опции GenId (ip pim exclude-genid)	522



10.3.8. Время сохранения информации о сообщениях Hello (ip pim hello-holdtime)	522
10.3.9. Интервал отправки hello-пакетов (ip pim hello-interval)	523
10.3.10. Многоадресная маршрутизация для протокола PIM (ip pim multicast-routing)	524
10.3.11. Настройка фильтрации соседей PIM (ip pim neighbor-filter)	524
10.3.12. Границы управления и ACL для протокола PIM (ip pim scope-border)	525
10.3.13. Установка интервала сообщений SRM (ip pim state-refresh origination-interval)	525
10.3.14. Вывод информации PIM для интерфейса (show ip pim interface)	526
10.3.15. Вывод уплотненного режима многоадресной маршрутизации (show ip pim mroute dense-mode)	527
10.3.16. Вывод информации о соседних устройствах PIM (show ip pim neighbor)	529
10.3.17. Вывод информации о следующих хопах multicast-групп (show ip pim nexthop)	530
10.4. Настройка протокола PIM-SM	531
10.4.1. Удаление информации о точках встречи (clear ip pim bsr rp-set)	531
10.4.2. Отладка событий PIM (debug pim event)	531
10.4.3. Отладка кеша PMI (debug pim mfc)	531
10.4.4. Отладка базы информации управления PIM (debug pim mib)	532
10.4.5. Отладка nexthop в PIM (debug pim nexthop)	532
10.4.6. Отладка менеджера сетевых служб PIM (debug pim nsm)	533
10.4.7. Отладка пакета PIM (debug pim packet)	533
10.4.8. Просмотр информации о статусе PIM (debug pim state)	534
10.4.9. Информация об отладке пакета PIM (debug pim packet)	534
10.4.10. Статический многоадресный трафик (ip mroute)	535
10.4.11. Кеширование многоадресного маршрута (ip multicast unresolved-cache aging-time)	536
10.4.12. Фильтрация пакетов Register (ip pim accept-register)	536
10.4.13. Настройка границ BSR (ip pim bsr-border)	537
10.4.14. Назначения роли Candidate BSR маршрутизатору (ip pim bsr-candidate)	537
10.4.15. Подсчет контрольной суммы пакета Register (ip pim cisco-register-checksum)	538
10.4.16. Настройка приоритета для выбора назначенного маршрутизатора (ip pim dr-priority)	539
10.4.17. Исключение опции GenId (ip pim exclude-genid)	539
10.4.18. Время сохранения информации о сообщениях Hello (ip pim hello-holdtime)	540
10.4.19. Интервал отправки hello-пакетов (ip pim hello-interval)	541



10.4.20. Игнорирование приоритета RP в RP-Set (ip pim ignore-rp-set-priority)	541
10.4.21. Интервал между сообщениями join/prune (ip pim jp-timer)	542
10.4.22. Многоадресная маршрутизация для протокола PIM (ip pim multicast-routing)	542
10.4.23. Настройка фильтрации соседей PIM (ip pim neighbor-filter)	543
10.4.24. Ограничение скорости отправки пакета Register (ip pim register-rate-limit)	543
10.4.25. Обнаружение доступности пакета Register (ip pim register-rp-reachability)	544
10.4.26. Настройка адреса источника пакета Register (ip pim register-source)	544
10.4.27. Настройка времени подавления пакета Register (ip pim register-suppression)	545
10.4.28. Настройка статических адресов RP (ip pim rp-address)	546
10.4.29. Назначение роли RP Candidate (ip pim rp-candidate)	546
10.4.30. Настройка времени keep-alive для регистрационных сообщений (ip pim rp-register-kat)	547
10.4.31. Границы управления и ACL для протокола PIM (ip pim scope-border)	548
10.4.32. Включение PIM для работы в разреженном режиме (ip pim sparse-mode)	548
10.4.33. Вывод информации о BSR (show ip pim bsr-router)	549
10.4.34. Вывод информации о конфигурации для PIM на интерфейсе (show ip pim interface)	550
10.4.35. Вывод таблицы маршрутизации PIM-SM (show ip pim mroute sparse-mode)	550
10.4.36. Вывод информации о соседних устройствах PIM (show ip pim neighbor)	552
10.4.37. Вывод информации о следующих хопх PIM (show ip pim nexthop)	553
10.4.38. Вывод адреса RP для указанной группы (show ip pim rp-hash)	554
10.4.39. Вывод точек встреч и привязок групп к RP (show ip pim rp mapping)	554
10.5. Настройка протокола PIM-SSM	555
10.5.1. Диапазон многоадресной рассылки PIM-SSM (ip multicast ssm)	555
10.6. PIM-IM6	556
10.6.1. Отладка сообщений таймера активности источника IPv6 PIM (debug ipv6 pim timer sat)	556
10.6.2. Отладка для получения информации о таймере обновления ipv6 pim (debug ipv6 pim timer srt)	556
10.6.3. Создание статического многоадресного маршрута IPv6 (ipv6 mroute)	557
10.6.4. Настройка границ PIM6 BSR (ipv6 pim bsr-border)	557
10.6.5. Функция многоадресной маршрутизации IPv6 в уплотненном режиме (ipv6 pim dense-mode)	558



10.6.6. Значения приоритета назначенного маршрутизатора на интерфейсе (ipv6 pim dr-priority)	558
10.6.7. Исключить опцию GenId на интерфейсе (ipv6 pim exclude-genid)	559
10.6.8. Время сохранения информации о сообщениях Hello для IPv6 PIM (ipv6 pim hello-holdtime)	559
10.6.9. Интервал отправки hello-сообщений для PIM IPv6 (ipv6 pim hello-interval)	560
10.6.10. Многоадресная маршрутизация для IPv6, протокол PIM (ipv6 pim multicast-routing)	561
10.6.11. Настройка фильтрации соседей для PIM IPv6 (ipv6 pim neighbor-filter)	561
10.6.12. Границы управления и ACL для протокола PIM IPv6 (ipv6 pim scope-border)	562
10.6.13. Установка интервала SRM в PIM IPv6 (ipv6 pim state-refresh origination-interval)	562
10.6.14. Вывод конфигурации PIM на интерфейсе (show ipv6 pim interface)	563
10.6.15. Вывод уплотненного режима многоадресной маршрутизации PIM IPv6 (show ipv6 pim mroute dense-mode)	564
10.6.16. Вывод информации о соседних устройствах PIM для PIMv6 (show ipv6 pim neighbor)	566
10.6.17. Вывод информации о следующих хопах multicast-групп для PIMv6 (show ipv6 pim nexthop)	566
10.7. PIM-SM6	567
10.7.1. Удалить информацию о точках встречи для PIMv6 (clear ipv6 pim bsr rp-set)	567
10.7.2. Отладка событий PIM для PIMv6 (debug ipv6 pim event)	568
10.7.3. Отладка pim mfc (debug ipv6 pim mfc)	568
10.7.4. Отладка базы информации управления PIM для PIMv6 (debug ipv6 pim mib)	569
10.7.5. Отладка для pim nexthop (debug ipv6 pim nexthop)	569
10.7.6. Отладка менеджера сетевых служб PIM для IPv6 PIM (debug ipv6 pim nsm)	569
10.7.7. Отладка пакета pim (debug ipv6 pim packet)	570
10.7.8. Просмотр информации о статусе PIM для PIMv6 (debug ipv6 pim state)	570
10.7.9. Отладка пакетов pim (debug ipv6 pim packet)	571
10.7.10. Статический многоадресный маршрут для PIMv6 (ipv6 mroute)	572
10.7.11. Кеширование многоадресного маршрута для PIMv6 (ipv6 multicast unresolved-cache aging-time)	572
10.7.12. Фильтрация пакетов Register для IPv6 PIM (ipv6 pim accept-register)	573
10.7.13. Настройка пограничного BSR для IPv6 PIM (ipv6 pim bsr-border)	573
10.7.14. Назначение роли Candidate BSR маршрутизатору для PIMv6 (ipv6 pim bsr-candidate)	574



10.7.15. Подсчет контрольной суммы пакета Register в IPv6 PIM (ipv6 pim cisco-register-checksum)	575
10.7.16. Настройка приоритета для выбора назначенного маршрутизатора в IPv6 PIM (ipv6 pim dr-priority)	575
10.7.17. Исключение опции GenId в IPv6 PIM (ipv6 pim exclude-genid)	576
10.7.18. Время сохранения информации о сообщениях Hello для IPv6 PIM (ipv6 pim hello-holdtime)	576
10.7.19. Интервал отправки hello-пакетов для PIMv6 (ipv6 pim hello-interval)	577
10.7.20. Игнорирование приоритета RP в RP-Set для IPv6 PIM (ipv6 pim ignore-rp-set-priority)	578
10.7.21. Интервал между сообщениями join/prune PIMv6 (ipv6 pim jp-timer)	578
10.7.22. Многоадресная маршрутизация для IPv6 PIM (ipv6 pim multicast-routing)	579
10.7.23. Настройка фильтрации соседей в IPv6 PIM (ipv6 pim neighbor-filter)	579
10.7.24. Ограничение скорости отправки пакета Register для IPv6 PIM (ipv6 pim register-rate-limit)	580
10.7.25. Обнаружение доступности пакета Register для IPv6 PIM (ipv6 pim register-rp-reachability)	581
10.7.26. Настройка адреса источника пакета Register в PIMv6 (ipv6 pim register-source)	581
10.7.27. Настройка времени подавления пакета Register IPv6 PIM (ipv6 pim register-suppression)	582
10.7.28. Настройка статических адресов RP для IPv6 PIM (ipv6 pim rp-address)	582
10.7.29. Назначение роли RP Candidate маршрутизатору в IPv6 PIM (ipv6 pim rp-candidate)	583
10.7.30. Настройка времени keep-alive для регистрационных сообщений в PIMv6 (ipv6 pim rp-register-kat)	584
10.7.31. Границы управления и ACL для IPv6 PIM (ipv6 pim scope-border)	584
10.7.32. Включение PIM-SM на интерфейсе (ipv6 pim sparse-mode)	585
10.7.33. Вывод информации о BSR для IPv6 PIM (show ipv6 pim bsr-router)	585
10.7.34. Вывод информации PIM для IPv6 PIM (show ipv6 pim interface)	586
10.7.35. Вывод таблицы маршрутизации IPv6 PIM-SM multicast (show ipv6 pim mroute sparse-mode)	587
10.7.36. Вывод информации о соседних устройствах IPv6 PIM (show ipv6 pim neighbor)	589
10.7.37. Вывод информации о следующих хопх IPv6 PIM (show ipv6 pim nexthop)	590
10.7.38. Вывод адреса RP для указанной группы PIMv6 (show ipv6 pim rp-hash)	591
10.7.39. Вывод точек встреч и привязок групп к RP IPv6 PIM (show ipv6 pim rp mapping)	591
10.8. Настройка протокола PIM-SSM6	592



10.8.1. Настройка диапазона адресов многоадресной SSM-группы (ipv6 pim ssm)	592
10.9. Anycast RP V4	593
10.9.1. Отладка адресации Anycast RP в PIM (debug pim anycast-rp)	593
10.9.2. Подключение адресации Anycast RP в PIM (ip pim anycast-rp)	593
10.9.3. Настройка адресов точек встречи Anycast RP в PIM (ip pim anycast-rp)	594
10.9.4. Личный адрес маршрутизатора для Anycast адресации в PIM (ip pim anycast-rp self-rp-address)	595
10.9.5. Назначение роли RP Candidate в PIM (ip pim rp-candidate)	596
10.9.6. Вывод отладочных сообщений PIM (show debugging pim)	596
10.9.7. Вывод первого хопа Anycast RP в PIM (show ip pim anycast-rp first-hop)	597
10.9.8. Вывод не первого хопа Anycast RP в PIM (show ip pim anycast-rp non-first-hop)	597
10.9.9. Вывод статуса Anycast RP (show ip pim anycast-rp status)	598
10.10. Anycast RP V6	599
10.10.1. Отладка адресации Anycast RP в IPv6 PIM (debug ipv6 pim anycast-rp)	599
10.10.2. Подключение адресации Anycast RP в IPv6 PIM (ipv6 pim anycast-rp)	600
10.10.3. Настройка адресов точек встречи Anycast RP в IPv6 PIM (ipv6 pim anycast-rp)	600
10.10.4. Личный адрес маршрутизатора для Anycast адресации в IPv6 PIM (ipv6 pim anycast-rp self-rp-address)	601
10.10.5. Назначение роли RP Candidate в IPv6 PIM (ipv6 pim rp-candidate)	602
10.10.6. Вывод отладочных сообщений IPv6 PIM (show debugging ipv6 pim)	603
10.10.7. Вывод первого хопа Anycast RP в IPv6 PIM (show ipv6 pim anycast-rp first-hop)	603
10.10.8. Вывод не первого хопа Anycast RP в IPv6 PIM (show ipv6 pim anycast-rp non-first-hop)	604
10.10.9. Вывод статуса Anycast RP в IPv6 PIM (show ipv6 pim anycast-rp status)	604
11. КОМАНДЫ ДЛЯ НАСТРОЙКИ ФУНКЦИИ БЕЗОПАСНОСТИ	606
11.1. Команды для настройки списков доступа (ACL)	606
11.1.1. Настройка временного диапазона (absolute-periodic/periodic)	606
11.1.2. Абсолютный временной диапазон (absolute start)	607
11.1.3. Нумерованное расширенное правило доступа (access-list (ip extended))	608
11.1.4. Нумерованный список доступа для IP-адресов (access-list (ip standard))	611
11.1.5. Расширенный нумерованный ACL для MAC-адресов (access-list (mac extended))	612
11.1.6. Нумерованное расширенное правило списка доступа MAC-IP ACL (access-list(mac-ip extended))	613
11.1.7. Стандартное нумерованное правило ACL для MAC-адресов (access-list (mac standard))	617



11.1.8. Очистить статистику пакетов (clear access-group statistic)	617
11.1.9. Межсетевой экран (firewall)	618
11.1.10. Расширенный список доступа для IP-адресов (ip access extended)	618
11.1.11. Стандартный список доступа для IP-адресов (ip access standard)	619
11.1.12. Стандартный нумерованный список доступа для IP-адресов (ipv6 access-list)	619
11.1.13. Стандартный список доступа для IPv6-адресов (ipv6 access standard)	620
11.1.14. Расширенный список доступа для IPv6-адресов (ipv6 access extended)	621
11.1.15. Список доступа, привязанный к порту ({ip ipv6 mac mac-ip} access-group)	621
11.1.16. Список доступа ACL с именем для MAC-адресов и его настройка (mac access extended)	622
11.1.17. Список доступа ACL с именем для MAC-IP-адресов и его настройка (mac-ip access extended)	623
11.1.18. Правило управления доступом для расширенного списка IP-адресов (permit deny (ip extended))	624
11.1.19. Правило управления доступом для стандартных IP-адресов (permit deny(ip standard))	626
11.1.20. Правило управления доступом для расширенного списка IPv6-адресов (permit deny (ipv6 extended))	626
11.1.21. Правило управления доступом для стандартных IPv6-адресов (permit deny (ipv6 standard))	628
11.1.22. Правило управления доступом для расширенного списка MAC-адресов (permit deny (mac extended))	629
11.1.23. Правило управления доступом для стандартных MAC-адресов (permit deny (mac-ip extended))	631
11.1.24. Просмотр созданных списков доступа (show access-lists)	635
11.1.25. Просмотр привязки списков доступа ACL к портам (show access-group)	635
11.1.26. Просмотр межсетевого экрана (show firewall)	636
11.1.27. Просмотр настроек списка доступа ACL IPv6 (show ipv6 access-lists)	636
11.1.28. Просмотр информации о временных диапазонах (show time-range)	637
11.1.29. Работа с временными диапазонами (time-range)	638
11.2. Конфигурация правила Self-Defined ACL (определяемый список ACL)	638
11.2.1. Создание окна смещения для правила (userdefined-access-list standard offset)	638
11.2.2. Создание правила для self-defined ACL (userdefined-access-list standard)	640
11.2.3. Настройка определяемого списка ACL в порту (userdefined access-group)	641
11.2.4. Назначение ACL на VLAN (vACL userdefined access-group)	641



11.3. Команды для настройки протокола 802.1X	642
11.3.1. Добавление MAC-адреса в таблицу фильтруемых адресов dot1x (dot1x accept-mac)	642
11.3.2. Передача аутентификационных данных протокола EAP (dot1x eap-enable)	643
11.3.3. Включение функции 802.1x (dot1x enable)	644
11.3.4. Функция транзитной пересылки на порту (dot1x ipv6 passthrough)	644
11.3.5. Гостевой VLAN на порту (dot1x guest-vlan)	645
11.3.6. Функция фильтрации dot1x адресов (dot1x macfilter enable)	646
11.3.7. Гостевой VLAN на основе MAC-аутентификации (dot1x macbased guest-vlan)	647
11.3.8. Удаление пользователя, прошедшего сертификацию, если dot1x не работает (dot1x macbased port-down-flush)	648
11.3.9. Число запросов EAP/кадров MD5 до повторной аутентификации (dot1x max-req)	648
11.3.10. Разрешенное перемещение пользователя (dot1x user allow-movement)	649
11.3.11. Настройка общедоступного ресурса 802.1x (dot1x user free-resource)	649
11.3.12. Максимальное число пользователей с доступом к порту при управлении на основе MAC-адреса (dot1x max-user macbased)	650
11.3.13. Максимальное число пользователей с доступом к порту при управлении на основе пользователей (dot1x max-user userbased)	650
11.3.14. Включение режима аутентификации единственного пользователя на порту (dot1x portbased mode single-mode)	651
11.3.15. Задать состояние аутентификации 802.1x (dot1x port-control)	652
11.3.16. Метод управления доступом к указанному интерфейсу (dot1x port-method)	652
11.3.17. Принудительная аутентификация с использованием частного протокола аутентификации 802.1x (dot1x privateclient enable)	654
11.3.18. Включить защиту частного клиента (dot1x privateclient protect enable)	654
11.3.19. Повторная аутентификация реального времени (dot1x re-authenticate)	655
11.3.20. Периодическая аутентификация клиентской системы (dot1x re-authentication)	655
11.3.21. Время бездействия при сбое аутентификации клиентской системы (dot1x timeout quiet-period)	656
11.3.22. Интервал времени для повторной аутентификации клиентской системы (dot1x timeout re-authperiod)	656
11.3.23. Повторная передача запроса/кадра идентичности EAP (dot1x timeout tx-period)	657
11.3.24. Включение функции dot1x (dot1x unicast enable)	657
11.3.25. Вывод информации о параметрах dot1x (show dot1x)	658
11.4. Команды ограничения количества MAC- и IP-адресов на порту и VLAN	659



11.4.1. Максимальное количество ARP записей на интерфейсе (ip arp dynamic maximum)	659
11.4.2. Максимальное количество ND записей на интерфейсе (ipv6 nd dynamic maximum)	659
11.4.3. Просмотр текущего количества ARP записей (show arp-dynamic count)	660
11.4.4. Просмотр текущего количества MAC-адресов (show mac-address dynamic count)	661
11.4.5. Просмотр текущего количества ND записей (show nd-dynamic count)	661
11.4.6. Включить функцию ограничения количества динамических ARP записей (switchport arp dynamic maximum)	662
11.4.7. Включить функцию ограничения количества динамических MAC-адресов (switchport mac-address dynamic maximum)	663
11.4.8. Задать действие при нарушении безопасности (switchport mac-address violation)	663
11.4.9. Включить функцию ограничения количества динамических ND- записей (switchport nd dynamic maximum)	664
11.4.10. Задать максимальное количество MAC-адресов (vlan mac-address dynamic maximum)	665
11.5. Команды для настройки управления доступом (AM)	666
11.5.1. Включить функцию AM (am enable)	666
11.5.2. Включить функцию AM на порту (am port)	666
11.5.3. Настроить записи в IP-таблице (am ip-pool)	667
11.5.4. Настроить MAC-IP в таблице разрешения доступа AM (am mac-ip-pool)	667
11.5.5. Удалить записи таблицы AM (no am all)	668
11.5.6. Просмотр информации о настроенной функции AM (show am)	668
11.6. Конфигурация функций предотвращения атак	669
11.6.1. Функция предотвращения атаки IP-spoofing (dosattack-check srcip-equal-dstip enable)	669
11.6.2. Функция предотвращения атаки TCP unauthorized label (dosattack-check tcp-flags enable)	669
11.6.3. Функция предотвращения атаки подмены порта (dosattack-check srcport-equal-dstport enable)	670
11.7. Команды для настройки протокола TACACS+	671
11.7.1. Параметры обращения к серверу TACACS+ (tacacs-server authentication host)	671
11.7.2. Задать ключ сервера TACACS+ (tacacs-server key)	672
11.7.3. Настроить IP-адрес источника для отправляемых TACACS+ пакетов (tacacs-server nas-ipv4)	672
11.7.4. Время таймера для сервера TACACS+ (tacacs-server timeout)	673
11.8. Команды для настройки протокола RADIUS	674
11.8.1. Включить функцию AAA (aaa enable)	674

11.8.2. Включить учет сетевых сервисов (aaa-accounting enable)	674
11.8.3. Обновление информации учета сетевых сервисов (aaa-accounting update)	675
11.8.4. Задать IP-адрес источника для отправляемых пакетов RADIUS (radius nas-ipv4)	675
11.8.5. Задать IPv6-адрес источника для отправляемых пакетов RADIUS (radius nas-ipv6)	676
11.8.6. Настроить параметры RADIUS-сервера для учета (radius-server accounting host)	677
11.8.7. Настроить параметры RADIUS-сервера для аутентификации (radius-server authentication host)	678
11.8.8. Время восстановления RADIUS-сервера после выключения (radius-server dead-time)	679
11.8.9. Ключ для RADIUS-сервера (radius-server key)	680
11.8.10. Число попыток повторной передачи пакетов аутентификации (radius-server retransmit)	680
11.8.11. Время таймера RADIUS-сервера (radius-server timeout)	681
11.8.12. Интервал отправки сообщений обновления информации учета сервисов (radius-server accounting-interim-update timeout)	682
11.8.13. Просмотр информации об аутентифицированных пользователях (show aaa authenticated-user)	683
11.8.14. Просмотр информации о проходящих аутентификацию пользователях (show aaa authenticating-user)	683
11.8.15. Просмотр информации коммутатора как RADIUS-клиента (show aaa config)	684
11.8.16. Статистика аутентифицированных пользователей RADIUS (show radius authenticated-user count)	684
11.8.17. Статистика аутентифицируемых пользователей RADIUS (show radius authenticating-user count)	685
11.8.18. Статистика пользователей RADIUS-аутентификации (show radius count)	685
11.9. Команды для настройки SSL	686
11.9.1. Управление коммутатором через защищенное подключение (ip http secure-server)	686
11.9.2. Порт защищенного подключения (ip http secure-port)	686
11.9.3. Метод шифрования для SSL (ip http secure- ciphersuite)	687
11.9.4. Просмотр информации о конфигурации SSL (show ip http secure-server status)	688
11.10. Конфигурация IPv6 RA Security	688
11.10.1. Активация функции RA Security (ipv6 security-ra enable)	688
11.10.2. Включить функцию IPv6 RA Security на порту (ipv6 security-ra enable)	689



11.10.3. Отобразить информацию о функции IPv6 RA Security на интерфейсе (show ipv6 security-ra)	689
11.11. Команды для настройки MAB	690
11.11.1. Методы аутентификации MAB (authentication mab)	690
11.11.2. Удаление информации о привязках MAB (clear mac-authentication-bypass binding)	691
11.11.3. Максимальное количество привязок MAB (mac-authentication-bypass binding-limit)	691
11.11.4. Включение функции MAB глобально и на порту (mac-authentication-bypass enable)	692
11.11.5. Гостевой vlan для MAB аутентификации (mac-authentication-bypass guest-vlan)	692
11.11.6. Функция обнаружения атаки GARP-spoofing (mac-authentication-bypass spoofing-garp-check)	693
11.11.7. Время восстановления состояния порта (mac-authentication-bypass timeout linkup-period)	694
11.11.8. Время обнаружения не подключенных пользователей и удаления записи MAB (mac-authentication-bypass timeout offline-detect)	694
11.11.9. Период тишины MAB привязок (mac-authentication-bypass timeout quiet-period)	695
11.11.10. Интервал повторной аутентификации при неудачной аутентификации (mac-authentication-bypass timeout reauth-period)	695
11.11.11. Период до удаления привязок после отключения MAB-порта (mac-authentication-bypass timeout stale-period)	696
11.11.12. Метод MAB-аутентификации (mac-authentication-bypass username-format)	697
11.11.13. Просмотр информации о MAB-аутентификации (show mac-authentication-bypass)	697
11.12. Команды для настройки PPPoE Intermediate Agent	698
11.12.1. Включить PPPoE intermediate agent глобально (pppoe intermediate-agent)	698
11.12.2. Включить PPPoE intermediate agent на порту (pppoe intermediate-agent (Port))	699
11.12.3. Идентификатор узла доступа для порта (pppoe intermediate-agent circuit-id)	699
11.12.4. Разделитель полей в идентификаторе (pppoe intermediate-agent delimiter)	700
11.12.5. Задать формат представления (pppoe intermediate-agent format)	700
11.12.6. Задать идентификатор (pppoe intermediate-agent remote-id)	701
11.12.7. Выбрать порт в качестве доверенного (pppoe intermediate-agent trust)	701
11.12.8. Задать собственный формат идентификатора узла доступа (pppoe intermediate-agent type self-defined circuit-id)	702



11.12.9. Задать собственный формат идентификатора удаленного хоста (pppoe intermediate-agent type self-defined remoteid)	703
11.12.10. Настроить идентификатор узла доступа (pppoe intermediate-agent type tr-101 circuit-id access-node-id)	703
11.12.11. Разделитель каждого параметра (pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter)	704
11.12.12. Удаление vendor-тега из пакета PPPoE (pppoe intermediate-agent vendor-tag strip)	705
11.12.13. Просмотр идентификатора узла доступа (show pppoe intermediate-agent access-node-id)	706
11.12.14. Просмотр конфигурации разделителя опций (show pppoe intermediate-agent identifier-string option delimiter)	706
11.12.15. Просмотр настроек PPPoE Intermediate Agent (show pppoe intermediate-agent info)	707
11.13. Команды для конфигурации VLAN-ACL	707
11.13.1. Очистка статистики VLAN-ACL (clear vac1 statistic vlan)	707
11.13.2. Просмотр конфигурации и статистики (show vac1 vlan)	708
11.13.3. Применить IP-ACL на на входящее направление трафика на VLAN (vac1 ip access-group)	710
11.13.4. Применить IPv6 ACL на на входящее направление трафика на VLAN (vac1 ipv6 access-group)	710
11.13.5. Применить MAC ACL на на входящее направление трафика на VLAN (vac1 mac access-group)	711
11.13.6. Применить MAC-IP ACL на на входящее направление трафика на VLAN (vac1 mac-ip access-group)	712
11.14. Конфигурация SAVI	713
11.14.1. Задать префикс вручную (ipv6 cps prefix)	713
11.14.2. Включить функцию проверки префикса (ipv6 cps prefix check enable)	713
11.14.3. Назначить доверенный порт DHCPv6 Snooping (ipv6 dhcp snooping trust)	714
11.14.4. Назначить доверенный порт ND Snooping (ipv6 nd snooping trust)	714
11.14.5. Метод проверки при обнаружении конфликта записей (savi check binding)	715
11.14.6. Включить функцию SAVI (savi enable)	716
11.14.7. Задать лимит записей SAVI для порта (savi ipv6 binding num)	716
11.14.8. Создать запись в таблице SAVI (savi ipv6 check source binding)	717
11.14.9. Контроль проверки подлинности (savi ipv6 check source ip-address mac-address)	718
11.14.10. Задать метод обнаружения SAVI (savi ipv6 {dhcp-only slaac-only dhcp-slaac} enable)	718
11.14.11. Максимальное количество записей с одним MAC (savi ipv6 mac-binding-limit)	719



11.14.12. Время обнаружения записи в таблице SAVI (savi max-dad-dalay)	719
11.14.13. Время повторного обнаружения динамической записи (savi max-dad-prepare-delay)	720
11.14.14. Время жизни для записи SLAAC (savi max-slaac-life)	720
11.14.15. Время хранения записи в таблице SAVI (savi timeout bind-protect)	721
11.14.16. Просмотр записи в таблице SAVI (show savi ipv6 check source binding)	721
12. КОМАНДЫ ДЛЯ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ	723
12.1. Команды для настройки MRPP	723
12.1.1. Задать виртуальный VLAN ID для кольца MRPP (control-vlan)	723
12.1.2. Удалить статистику принимаемых и передаваемых пакетов MRPP (clear mrpp statistics)	723
12.1.3. Включить сконфигурированное кольцо MRPP (enable)	724
12.1.4. Создать домен ERPP (errp domain)	724
12.1.5. Таймер получения пакетов Hello в первичном узле (fail-timer)	725
12.1.6. Таймер передачи пакетов Hello из первичного узла (hello-timer)	725
12.1.7. Включить режим совместимости с EARS (mrpp eaps compatible)	726
12.1.8. Включить модуль протокола MRPP (mrpp enable)	726
12.1.9. Включить режим совместимости с ERPP (mrpp errp compatible)	727
12.1.10. Установить интервал опроса MRPP (mrpp poll-time)	727
12.1.11. Создать кольцо MRPP и войти в режим настройки (mrpp ring)	728
12.1.12. Задать первичный порт кольца MRPP (mrpp ring primary-port)	728
12.1.13. Задать вторичный порт кольца MRPP (mrpp ring secondary-port)	729
12.1.14. Задать тип узла кольца MRPP (node-mode)	729
12.1.15. Просмотр настроек кольца MRPP (show mrpp)	730
12.1.16. Просмотр статистики кольца MRPP (show mrpp statistics)	730
12.2. Команды для настройки ULPP	731
12.2.1. Очистить счетчики flush-пакетов на интерфейсе (clear ulpp flush counter interface)	731
12.2.2. Задать управляющий VLAN (control vlan)	731
12.2.3. Задать описание для ULPP группы (description)	732
12.2.4. Включить/выключить функцию отправки flush пакета для обновления ARP-таблицы (flush {enable disable} arp)	732
12.2.5. Включить/выключить функцию отправки flush пакета для обновления MAC-таблицы (flush {enable disable} mac)	733
12.2.6. Включить/выключить функцию отправки flush пакета для удаления MAC из MAC-VLAN (flush {enable disable} mac-vlan)	733
12.2.7. Время задержки приоритетного переключения (preemption delay)	734
12.2.8. Режим приоритетного переключения (preemption mode)	734



12.2.9. Обозначить VLAN, защищаемые ULPP группой (protect vlan-reference-instance)	735
12.2.10. Просмотр статистики о переданных и полученных flush-пакетах (show ulpp flush counter interface)	735
12.2.11. Просмотр информации о порте, получившем flush-пакет (show ulpp flush-receive-port)	736
12.2.12. Просмотр информации о сконфигурированных ULPP группах (show ulpp group)	736
12.2.13. Задать список управляющих VLAN, принимающих flush-пакеты (ulpp control vlan)	737
12.2.14. Включить/выключить функцию приема flush-пакета для обновления ARP-таблицы на порту (ulpp flush {enable disable} arp)	738
12.2.15. Включить/выключить функцию отправки flush пакета для обновления MAC-таблицы на порту (ulpp flush {enable disable} mac)	738
12.2.16. Включить/выключить функцию отправки flush пакета для удаления MAC из MAC-VLAN на порту (ulpp flush {enable disable} mac-vlan)	739
12.2.17. Создать ULPP группу (ulpp group)	739
12.2.18. Определение master-порта и slave-порта в группе (ulpp group {master slave})	740
12.3. Команды для настройки ULSM	740
12.3.1. Просмотр сконфигурированных ULSM групп (show ulsm group)	740
12.3.2. Создать ULSM группу (ulsm group)	741
12.3.3. Задать порт исходящей/нисходящей связи ULSM-группы (ulsm group {uplink downlink})	741
13. КОМАНДЫ ДЛЯ НАСТРОЙКИ ЗЕРКАЛИРОВАНИЯ ПОРТОВ	742
13.1. Команды для настройки зеркалирования портов	742
13.1.1. Задать интерфейс-источник зеркалирования (monitor session source interface)	742
13.1.2. Список доступа для управления источником порта зеркалирования (monitor session source interface access-list)	743
13.1.3. Задать интерфейс назначения зеркалирования (monitor session destination interface)	744
13.1.4. Просмотр информации о сессии зеркалирования (show monitor)	744
13.2. Команды для настройки протокола sFlow	745
13.2.1. Идентификатор агента sFlow (sflow agent-address)	745
13.2.2. Анализатор sFlow (sflow analyzer)	745
13.2.3. Интервал сбора статистики sFlow (sflow counter-interval)	746
13.2.4. Настроить максимальную длину группы выборок sFlow (sflow data-len)	746
13.2.5. Адрес и порт назначения для отправки данных sFlow (sflow destination)	747
13.2.6. Настроить длину заголовка пакета, копируемого в sFlow (sflow header-len)	747



13.2.7. Задать приоритет sFlow прокси (sflow priority)	748
13.2.8. Настроить частоту дискретизации (sflow rate)	748
13.2.9. Просмотр информации о работе sFlow (show sflow)	749
13.3. Команды конфигурирования RSPAN	751
13.3.1. Настройка RSPAN VLAN (remote-span)	751
13.3.2. Задать удаленный VLAN для мониторинговой сессии (monitor session remote vlan)	751
13.3.3. Настройка порта-отражателя (monitor session reflector-port)	752
14. КОМАНДЫ ДЛЯ УПРАВЛЕНИЯ СЕТЕВЫМ ВРЕМЕНЕМ	753
14.1. Команды для настройки SNTP	753
14.1.1. Задать часовой пояс (clock timezone)	753
14.1.2. Задать интервал синхронизации SNTP (sntp polltime)	753
14.1.3. Указать сервер времени как источник синхронизации (sntp server)	754
14.1.4. Просмотр текущих настроек SNTP (show sntp)	754
14.2. Команды для настройки NTP	755
14.2.1. Фильтрация по списку доступа при работе коммутатора в режиме NTP-сервера (ntp access-group)	755
14.2.2. Включить функцию аутентификации NTP (ntp authenticate)	755
14.2.3. Ключ NTP-аутентификации (ntp authentication-key)	756
14.2.4. Задать поддерживаемые broadcast и multicast NTP серверы (ntp broadcast server count)	756
14.2.5. Включить функцию NTP в порту (ntp disable)	757
14.2.6. Включить или выключить функцию NTP в глобальном режиме (ntp enable)	757
14.2.7. Настроить прием IPv6 multicast NTP пакетов на интерфейсе (ntp ipv6 multicast client)	757
14.2.8. Настроить интерфейс для приема multicast NTP пакетов (ntp multicast client)	758
14.2.9. Указать в NTP-сервер (ntp server)	758
14.2.10. Период отправки NTP-клиентом пакетов запроса (ntp syn-interval)	759
14.2.11. Задать безопасный ключ (ntp trusted-key)	760
14.2.12. Просмотр информации о статусе и конфигурации NTP (show ntp status)	760
14.2.13. Просмотр информации о сеансах NTP (show ntp session)	761
15. ДИАГНОСТИКА И КОНТРОЛЬ СОСТОЯНИЯ УСТРОЙСТВА	762
15.1. Команды Show	762
15.1.1. Очистить историю команд пользователей (clear history all-users)	762
15.1.2. Очистить системный журнал (clear logging)	762
15.1.3. Максимальное число хранимых в истории команд (history all-users max-length)	762



15.1.4. Настройка журнала хоста канала вывода (logging)	763
15.1.5. Запись в журнал вводимых команд (logging executed-commands)	764
15.1.6. Задать сообщению порядковый номер (logging loghost sequence-number)	764
15.1.7. Задать адрес источника при отправке логов (logging source-ip)	765
15.1.8. Отправка пакета запроса ICMP устройству и проверка связи на обеих сторонах (ping)	765
15.1.9. Проверка связи с сетью назначения (ping6)	767
15.1.10. Просмотр файлов загрузки (show boot-files)	769
15.1.11. Просмотр информации о файлах, хранящихся во флеш-памяти (show flash)	770
15.1.12. Просмотр введенных пользователем команды в хронологическом порядке (show history)	770
15.1.13. Просмотр информации о истории действий всех пользователей (show history all-users)	771
15.1.14. Просмотр детальной информации о канале буфера системных сообщений (show logging buffered)	772
15.1.15. Отображение статуса логирования действий пользователя (show logging executed-commands state)	772
15.1.16. Просмотр детальной информации о сообщениях модуля MSTP (show logging source)	773
15.1.17. Просмотр параметров текущей конфигурации коммутатора (show running-config)	773
15.1.18. Просмотр параметров конфигурации при текущем режиме пользователя (show running-config current-mode)	774
15.1.19. Отобразить текущую загрузочную конфигурацию (show startup-config)	774
15.1.20. Отобразить информацию о VLAN принадлежащих к интерфейсу (show switchport interface)	775
15.1.21. Отображение информации о текущих TCP-сессиях (show tcp)	775
15.1.22. Отобразить информацию о текущих TCP сессиях (show tcp ipv6)	776
15.1.23. Просмотр текущих telnet-сессий к коммутатору (show telnet login)	777
15.1.24. Отобразить информацию о текущих UDP сессиях (show udp)	777
15.1.25. Отобразить информацию о текущих UDP сессиях (show udp ipv6)	778
15.1.26. Просмотр версии коммутатора (show version)	779
15.1.27. Проверка маршрута прохождения пакетов через сеть (traceroute)	779
15.1.28. Проверка маршрута прохождения пакетов через сеть (traceroute6)	780
15.1.29. Перегрузка коммутатора (reload after)	781
15.1.30. Отмена перезагрузки коммутатора (reload cancel)	782
15.1.31. Просмотр времени, на которое назначена перезагрузка (show reload)	782
15.1.32. Очистить статистику пакетов, принятых в CPU (clear cpu-rx-stat protocol)	783



15.1.33. Задать максимальную скорость приема пакетов для указанного типа протокола (cpu-rx-ratelimit protocol)	783
15.1.34. Задать для CPU максимальную скорость приема пакетов (cpu-rx-ratelimit total)	784
15.1.35. Просмотр статистики принятых CPU пакетов протокола указанного типа (show cpu-rx protocol)	784
16. КОНФИГУРАЦИЯ ПРОТОКОЛОВ МАРШРУТИЗАЦИИ	786
16.1. Команды протокола RIP	786
16.1.1. Время действия ключа аутентификации (accept-lifetime)	786
16.2. Команды протокола OSPF.	787
16.2.1. Включить аутентификацию для OSPF области (area authentication)	787
16.2.2. Стоимость для маршрута по умолчанию, отправляемого в стабильную область (area default-cost)	788
16.2.3. Настройка фильтрации в области (area filter-list)	788
16.2.4. Определение области как области NSSA (area nssa)	789
16.2.5. Формирование суммарного префикса для области OSPF (area range)	790
16.2.6. Определение области как тупиковой (area stub)	791
16.2.7. Формирование виртуального соединения для обмена LSA (area virtual-link)	791
16.2.8. Параметр для вычисления метрики протокола OSPF (auto-cost reference-bandwidth)	792
16.2.9. Установка выбора расчета цены маршрута согласно RFC1583 (compatible rfc1583)	793
16.2.10. Удаление всех процессов OSP (clear ip ospf process)	794
16.2.11. Генерация внешнего маршрута по умолчанию в область OSPF (default-information originate)	794
16.2.12. Установка значений метрики по умолчанию для OSPF (default-metric)	795
16.2.13. Определение административных расстояний маршрутов в OSPF (distance)	795
16.2.14. Фильтрация обновлений маршрута (distribute-list)	796
16.2.15. Политика фильтрации (filter-policy)	797
16.2.16. Принадлежность хоста к области (host area)	798
16.2.17. Настройка параметров ospf аутентификации на интерфейсе (ip ospf authentication)	798
16.2.18. Задать пароль аутентификации OSPF (ip ospf authentication-key)	799
16.2.19. Стоимость пересылки данных через интерфейс (ip ospf cost)	800
16.2.20. Фильтр базы данных LSA для конкретного интерфейса (ip ospf database-filter)	800
16.2.21. Интервал ожидания отклика до объявления соседнего устройства недоступным (ip ospf dead-interval)	801
16.2.22. Запрет обработки OSPF пакетов на интерфейсе (ip ospf disable all)	801

16.2.23. Интервал между пакетами hello на интерфейсе (ip ospf hello-interval)	802
16.2.24. Парегистрировать ключ для аутентификации OSPF (ip ospf message-digest-key)	803
16.2.25. Размер MTU для OSPF (ip ospf mtu)	803
16.2.26. Игнорировать эту проверку MTU (ip ospf mtu-ignore)	804
16.2.27. Задать тип сети OSPF (ip ospf network)	804
16.2.28. Задать приоритет маршрутизатора (ip ospf priority)	805
16.2.29. Интервал между повторными передачами объявлений о состоянии связи (ip ospf retransmit-interval)	806
16.2.30. Предполагаемое время для отправки пакета LSA (ip ospf transmit-delay)	806
16.2.31. Создание ключа в ключевой цепочке (key)	807
16.2.32. Цепочка ключей (key chain)	808
16.2.33. Отправка сообщений об изменении состояния для протокола OSPF (log-adjacency-changes detail)	808
16.2.34. Максимальное количество одновременно обрабатываемых сообщений обмена базами данных (max-concurrent-dd)	809
16.2.35. Указание соседа по протоколу OSPF (neighbor)	809
16.2.36. Определение OSPF области (network area)	810
16.2.37. Тип пограничного маршрутизатора (ospf abr-type)	811
16.2.38. ID маршрутизатора для процессов OSPF (ospf router-id)	811
16.2.39. Ограничить количество LSA, получаемых маршрутизатором (overflow database)	812
16.2.40. Максимальное количество LSA от внешних автономных систем (overflow database external)	813
16.2.41. Отключить отправку обновлений маршрутизации (passive-interface)	813
16.2.42. Перераспределение маршрутов (redistribute)	814
16.2.43. Перераспределение маршрутов OSPF (redistribute ospf)	815
16.2.44. Включение процесса маршрутизации OSPF (router ospf)	815
16.2.45. Создание суммированных адресов (summary-address)	816
16.2.46. Время выполнения вычислений кратчайшего пути (timers spf)	816
16.2.47. Просмотр общей информации о процессах маршрутизации OSPF (show ip ospf)	817
16.2.48. Просмотр внутренней таблицы маршрутизации OSPF для граничных маршрутизаторов (show ip ospf border-routers)	818
16.2.49. Просмотр информации о базе данных OSPF (show ip ospf database)	819
16.2.50. Просмотр информации об интерфейсе для OSPF (show ip ospf interface)	820
16.2.51. Просмотр информации о соседних узлах (show ip ospf neighbor)	821
16.2.52. Просмотр информации о перераспределении в OSPF (show ip ospf redistribute)	822



16.2.53. Просмотр сводной информации о маршрутах в OSPF (show ip ospf route)	823
16.2.54. Просмотр виртуальных соединений с другими маршрутизаторами OSPF (show ip ospf virtual-links)	824
16.2.55. Просмотр подробной информации о маршрутизации (show ip route process-detail)	824
16.2.56. Просмотр статуса и параметров протоколов маршрутизации (show ip protocols)	825
16.2.57. Параметры отладки и устранения неполадок событий OSPF (debug ospf events)	826
16.2.58. Параметры отладки состояний IFSM в OSPF (debug ospf ifsm)	827
16.2.59. Параметры отладки объявлений о состоянии канала (debug ospf lsa)	827
16.2.60. Параметры отладки состояний NFSM (debug ospf nfsm)	828
16.2.61. Параметры отладки, относящиеся к NSM в OSPF (debug ospf nsm)	828
16.2.62. Параметры отладки пакетов OSPF (debug ospf packet)	829
16.2.63. Параметры отладки процесса расчета маршрута (debug ospf route)	829
16.2.64. Параметры отладки отправленных сообщений перераспределения (debug ospf redistribute message send)	830
16.2.65. Параметры отладки полученных сообщений о перераспределении маршрута (debug ospf redistribute route receive)	830
16.2.66. Поддержка мягкого перезапуска соседних маршрутизаторов (capability restart graceful)	831
16.2.67. Параметры отладки мягкого перезапуска на OSPF (debug ospf events gr)	831
16.2.68. Период отсрочки мягкого перезапуска (ospf graceful-restart grace-period)	832
16.2.69. Поведение помощника для мягкого перезапуска (ospf graceful-restart helper max-grace-period)	832
16.2.70. Запрет роли помощника для маршрутизатора (ospf graceful-restart helper never)	833
16.2.71. Просмотр состояния мягкого перезапуска OSPF протокола (show ip ospf graceful-restart)	833
16.3. Команды для протокола BGP	835
16.3.1. Настройка агрегированных элементов BGP таблиц (aggregate-address)	835
16.3.2. Выполнение агрегации на следующем узле (bgp aggregate-nexthop-check)	836
16.3.3. Сравнение MED для маршрутов от соседних узлов из различных автономных систем (bgp always-compare-med)	836
16.3.4. Метод ASDOT для записи AC (bgp asnotation asdot)	837
16.3.5. Предотвращение учета as-path в алгоритме выбора маршрута (bgp bestpath as-path ignore)	837



16.3.6. Сравнение длины пути конфедерации AC (bgp bestpath compare-confed- aspath)	838
16.3.7. Сравнение идентификаторов маршрутизаторов для одинаковых путей BGP (bgp bestpath compare-routerid)	838
16.3.8. Сравнение атрибута MED при выборе путей (bgp bestpath med)	839
16.3.9. Пересылка маршрутов от клиента к клиенту (bgp client-to-client reflection)	839
16.3.10. Настройка идентификатора кластера (bgp cluster-id)	840
16.3.11. Идентификатор BGP конфедерации (bgp confederation identifier)	841
16.3.12. Определение участников конфедерации (bgp confederation peers)	841
16.3.13. Подавление маршрутов в BGP (bgp dampening)	842
16.3.14. Параметры BGP по умолчанию (bgp default)	843
16.3.15. Сравнение MED, анонсируемой разными узлами в общей автономной системе (bgp deterministic-med)	843
16.3.16. Принудительная подстановка номеров AC (bgp enforce-first-as)	844
16.3.17. Немедленный сброс сеанса BGP (bgp fast-external-failover)	844
16.3.18. Включить входной фильтр маршрутов (bgp inbound-route-filter)	845
16.3.19. Максимальное количество маршрутизаторов в процессе BGP (bgp inbound-max-route-num)	845
16.3.20. Запись сообщений об изменении состояния соседних устройств без включения отладки BGP (bgp log-neighbor-changes)	846
16.3.21. Проверка маршрутов на наличие префикса в таблице маршрутизации (bgp network import-check)	846
16.3.22. Установить выбор пути, совместимого с RFC 1771 (bgp rfc1771-path- select)	847
16.3.23. Строгое выполнение протокола RFC 1771 (bgp rfc1771-strict)	847
16.3.24. Настройка ID-маршрутизатора вручную (bgp router-id)	848
16.3.25. Интервалы сканирования маршрутизаторов BGP (bgp scan-time)	848
16.3.26. Сброс соединения BGP (clear ip bgp)	849
16.3.27. Удаление информации о подавленных маршрутах (clear ip bgp dampening)	849
16.3.28. Удалить статистику нестабильностей BGP (clear ip bgp flap-statistics)	850
16.3.29. Установка административной дистанции маршрутов для указанного префикса (distance)	851
16.3.30. Установка административной дистанции для маршрутов BGP (distance bgp)	851
16.3.31. Создать список доступа к пути автономной системы (AC) BGP (ip as- path access-list)	852
16.3.32. Список сообществ (ip community-list)	852
16.3.33. Расширенный список сообществ (ip extcommunity-list)	853



16.3.34. Разрешение на обмен маршрутами с соседним узлом (neighbor activate)	854
16.3.35. Минимальный интервал между отправкой обновлений маршрутизации BGP (neighbor advertisement-interval)	855
16.3.36. Анонсирование префиксов, содержащих дублирующиеся номера автономных систем (neighbor allowas-in)	855
16.3.37. Передача соседнему устройству неизменных атрибутов (neighbor attribute-unchanged)	856
16.3.38. Анонсирование возможностей обновления (neighbor capability)	857
16.3.39. Анонсирование возможностей обновления ORF (neighbor capability orf prefix-list)	858
16.3.40. Определение наличия и решение для устранения коллизий (neighbor collide-established)	859
16.3.41. Отправка соседнему узлу маршрута по умолчанию от локального маршрутизатора (neighbor default-originate)	859
16.3.42. Описание соседнего маршрутизатора (neighbor description)	860
16.3.43. Фильтрация обновлений от конкретного соседа BGP (neighbor distribute-list)	861
16.3.44. Не выполнение согласований (neighbor dont-capability-negotiate)	861
16.3.45. Предоставление участия в динамической маршрутизации узлам, не соединенным напрямую (neighbor ebgp-multihop)	862
16.3.46. Принудительно установить многохоповые переходы (neighbor enforce-multihop)	863
16.3.47. Настройка фильтра BGP (neighbor filter-list)	864
16.3.48. Интерфейс соседнего устройства (neighbor interface)	864
16.3.49. Установка максимального числа префиксов, принимаемых узлом (neighbor maximum-prefix)	865
16.3.50. Настроить маршрутизатор как следующий узел для соседнего BGP (neighbor next-hop-self)	866
16.3.51. Переопределение результата согласования возможностей (neighbor override-capability)	866
16.3.52. Предписание маршрутизатору не инициировать соединение (neighbor passive)	867
16.3.53. Создание группы пиров (neighbor peer-group (Creating))	868
16.3.54. Управление членами группы пиров (neighbor peer-group (Configuring group members))	868
16.3.55. Порт для соседнего узла (neighbor port)	869
16.3.56. Применение префиксного списка для фильтрации обновлений от узла (neighbor prefix-list)	869
16.3.57. Номер автономной системы соседнего узла BGP (neighbor remote-as)	870
16.3.58. Исключение частных АС из обновлений (neighbor remove-private-AS)	871
16.3.59. Применение карты маршрута (neighbor route-map)	871



16.3.60. Настройка маршрутизатора в качестве отражателя маршрутов BGP и указанного соседа в качестве его клиента (neighbor route-reflector-client)	872
16.3.61. Настроить соседний узел как клиент сервера маршрутизации (neighbor route-server-client)	873
16.3.62. Отправка соседним узлам BGP атрибутов сообщества (neighbor send-community)	873
16.3.63. Отключение соседнего маршрутизатора (neighbor shutdown)	874
16.3.64. Сохранение полученных маршрутных обновлений на локальном маршрутизаторе (neighbor soft-reconfiguration inbound)	875
16.3.65. Строгое соответствие возможностям узла (neighbor strict-capability-match)	875
16.3.66. Установка таймера для определенного BGP узла (neighbor timers)	876
16.3.67. Таймер подключения BGP (neighbor timers connect)	877
16.3.68. Выборочная передача маршрутов определенному узлу BGP (neighbor unsuppress-map)	877
16.3.69. Источник для обновлений BGP (neighbor update-source)	878
16.3.70. Применение конкретной версии BGP (neighbor version 4)	879
16.3.71. Определение веса для маршрутов от указанного узла (neighbor weight)	879
16.3.72. Анонсирование сетей в процессе маршрутизации BGP (network (BGP))	880
16.3.73. Перераспределение входящих маршрутов в BGP (redistribute (BGP))	880
16.3.74. Перераспределять маршруты OSPF (redistribute ospf)	881
16.3.75. Запуск процесса BGP (router bgp)	882
16.3.76. Глобальная настройка таймеров для BGP (timers bgp)	882
16.3.77. Просмотр информации о сети BGP (show ip bgp)	883
16.3.78. Просмотр информации об атрибутах сети BGP (show ip bgp attribute-info)	884
16.3.79. Просмотр маршрутов, принадлежащих определённым сообществам BGP (show ip bgp community)	884
16.3.80. Просмотр информации о сообществе BGP (show ip bgp community-info)	885
16.3.81. Просмотр маршрутов, соответствующих списку сообществ (show ip bgp community-list)	885
16.3.82. Просмотр информации о подавленных маршрутах (show ip bgp dampening)	886
16.3.83. Просмотр маршрутов, соответствующих списку фильтрации (show ip bgp filter-list)	887
16.3.84. Просмотр маршрутов с несогласованными путями AC (show ip bgp inconsistent-as)	888
16.3.85. Просмотр информации о распространении маршрутов (show ip bgp neighbors)	889



16.3.86. Просмотр путей BGP (show ip bgp paths)	890
16.3.87. Просмотр маршрутов, соответствующих списку префиксов (show ip bgp prefix-list)	890
16.3.88. Просмотр маршрутов BGP, содержащих указанное регулярное выражение (show ip bgp quote-regexp)	891
16.3.89. Просмотр информации о перераспределении из внешних процессов (show ip bgp redistribute)	892
16.3.90. Просмотр информации о соседних устройствах (show ip bgp neighbors)	892
16.3.91. Просмотр маршрутов BGP, содержащих указанное регулярное выражение (show ip bgp regexp)	893
16.3.92. Просмотр маршрутов BGP, входящих в указанную карту маршрутов (show ip bgp route-map)	893
16.3.93. Отображение статуса сканирования BGP (show ip bgp scan)	894
16.3.94. Просмотр сводной информации о BGP (show ip bgp summary)	895
16.3.95. Просмотр информации о виде BGP (show ip bgp view)	896
16.3.96. Просмотр информации о соседних узлах указанного экземпляра BGP (show ip bgp view neighbors)	897
16.3.97. Параметры отладки для протокола BGP (debug bgp)	897
16.3.98. Параметры отладки отправленных сообщений перераспределения (debug bgp redistribute message send)	898
16.3.99. Параметры отладки полученных сообщений о перераспределении маршрута (debug bgp redistribute route receive)	898
16.3.100. Включить возможность мягкого перезапуска BGP (bgp graceful-restart)	899
16.3.101. Время ожидания для восстановления узла при мягком перезапуске (bgp graceful-restart restart-time)	899
16.3.102. Время хранения пути при мягком перезапуске (bgp graceful-restart stale-path-time)	900
16.3.103. Установка таймера до выбора маршрута для перезапускаемого узла (bgp selection-deferral-time)	900
16.3.104. Поддержка мягкого перезапуска на соседнем узле (neighbor capability graceful-restart)	901
16.3.105. Время перезапуска для соседних узлов (neighbor restart-time)	901
16.4. Команды протокола RIP	902
16.4.1. Удаление записей из таблицы маршрутизации (clear ipv6 rip route)	902
16.4.2. Анонс маршрута по умолчанию в RIP (default-information originate)	903
16.4.3. Метрика по умолчанию (default-metric)	903
16.4.4. Административная дистанция (distance)	904
16.4.5. Фильтрация обновлений маршрута (distribute-list)	904
16.4.6. Параметры отладки для RIPv6 (debug ipv6 rip)	905



16.4.7. Параметры отладки отправленных сообщений перераспределения маршрута (debug ipv6 rip redistribute message send)	906
16.4.8. Параметры отладки полученных сообщений о перераспределении маршрута (debug ipv6 rip redistribute route receive)	907
16.4.9. Агрегированные адреса (ipv6 rip aggregate-address)	907
16.4.10. Расщепление горизонта (ipv6 rip split-horizon)	908
16.4.11. Включение маршрутизации RIPv6 на интерфейсе (ipv6 router rip)	909
16.4.12. Указание соседнего маршрутизатора (neighbor)	909
16.4.13. Смещения к входящим и исходящим метрикам (offset-list)	910
16.4.14. Отключение отправки обновлений маршрутизации (passive-interface)	911
16.4.15. Перераспределение информации о маршрутизации из других протоколов (redistribute)	911
16.4.16. Перераспределение в OSPF (redistribute ospf)	912
16.4.17. Маршрут (route)	912
16.4.18. Включение процесса маршрутизации RIPv6 (router ipv6 rip)	913
16.4.19. Просмотр статуса для событий и пакетов RIPv6 (show debugging ipv6 rip)	913
16.4.20. Просмотр информации об интерфейсах RIPv6 (show ipv6 rip interface)	914
16.4.21. Просмотр настроек перераспределения (show ipv6 rip redistribute)	915
16.4.22. Просмотр таблицы маршрутизации RIPv6 (show ipv6 protocols rip)	915
16.4.23. Просмотр маршрутов RIPv6 (show ipv6 rip)	916
16.4.24. Просмотр информации о базе данных IPv6 RIPv6 (show ipv6 rip database)	917
16.4.25. Просмотр агрегирования (show ipv6 rip aggregate)	917
16.4.26. Настройка таймеров маршрутизации RIPv6 (timers basic)	918
16.5. Команды OSPFv3	919
16.5.1. Стоимость маршрута по умолчанию (area default-cost)	919
16.5.2. Настройка диапазона адресов OSPF (area range)	919
16.5.3. Задание тупиковой области OSPF (area stub)	920
16.5.4. Создание виртуального соединения для обмена LSA (area virtual-link)	921
16.5.5. Модели пограничного маршрутизатора (abr-type)	922
16.5.6. Метрики для перераспределённых маршрутов (default-metric)	922
16.5.7. Параметры отладки событий OSPF (debug ipv6 ospf events)	923
16.5.8. Параметры отладки состояний IFSM в OSPF (debug ipv6 ospf ifsm)	923
16.5.9. Параметры отладки для LSA (debug ipv6 ospf lsa)	924
16.5.10. Параметры отладки состояний NFSM в OSPF (debug ipv6 ospf nfsm)	924
16.5.11. Параметры отладки состояний NSM в OSPF (debug ipv6 ospf nsm)	925
16.5.12. Параметры отладки для обмена пакетами (debug ipv6 ospf packet)	925



16.5.13. Параметры отладки отправленных сообщений перераспределения (debug ipv6 ospf redistribute message send)	926
16.5.14. Параметры отладки полученных сообщений о перераспределении маршрута (debug ipv6 ospf redistribute route receive)	926
16.5.15. Параметры отладки событий IPv6 маршрутизации (debug ipv6 ospf route)	927
16.5.16. Стоимость отправки пакета на интерфейсе (ipv6 ospf cost)	927
16.5.17. Интервал ожидания отклика до объявления соседнего устройства недоступным (ipv6 ospf dead-interval)	928
16.5.18. Отобразить данные о каждом маршруте в одной строке (ipv6 ospf display route single-line)	928
16.5.19. Задать интервал между пакетами hello (ipv6 ospf hello-interval)	929
16.5.20. Приоритет маршрутизатора для определения назначенного маршрутизатора (ipv6 ospf priority)	930
16.5.21. Интервал между повторными передачами пакетов обновлений состояния канала связи (ipv6 ospf retransmit-interval)	930
16.5.22. Предполагаемое время для отправки пакета LSA (ipv6 ospf transmit-delay)	931
16.5.23. Разрешение процесса OSPFv3 на интерфейсе (ipv6 router ospf)	932
16.5.24. Максимальное количество одновременно обрабатываемых сообщений обмена базами данных (max-concurrent-dd)	933
16.5.25. Отключение отправки обновлений (passive-interface)	933
16.5.26. Перераспределение маршрутов (redistribute)	934
16.5.27. Перераспределение маршрутов OSPF (redistribute ospf)	935
16.5.28. Идентификатор маршрутизатора (router-id)	935
16.5.29. Настройка процесса маршрутизации OSPF (router ipv6 ospf)	936
16.5.30. Просмотр общей информации о процессах маршрутизации OSPFv3 (show ipv6 ospf)	936
16.5.31. Просмотр базы данных OSPFv3 (show ipv6 ospf database)	937
16.5.32. Просмотр интерфейсов, где включен протокол OSPFv3 (show ipv6 ospf interface)	939
16.5.33. Просмотр состояния смежности с соседними маршрутизаторами (show ipv6 ospf neighbor)	941
16.5.34. Просмотр маршрута (show ipv6 ospf route)	942
16.5.35. Просмотр информации о перераспределении в OSPF (show ipv6 ospf redistribute)	943
16.5.36. Просмотр информации о топологии маршрутизации OSPFv3 (show ipv6 ospf topology)	944
16.5.37. Просмотр информации о виртуальных соединениях (show ipv6 ospf virtual-links)	944
16.5.38. Просмотр подробной информации о маршрутизации (show ipv6 route process-detail)	945



16.5.39. Время выполнения вычислений кратчайшего пути (timers spf)	946
16.6. Команды MBGP4+	946
16.6.1. Параметры отладки отправленных сообщений перераспределения (debug ipv6 bgp redistribute message send)	946
16.6.2. Параметры отладки полученных сообщений о перераспределении маршрута (debug ipv6 bgp redistribute route receive)	947
16.6.3. Перераспределение маршрутов в OSPF (redistribute ospf (MBGP4+))	947
16.6.4. Просмотр перераспределения (show ipv6 bgp redistribute)	948
17. ОБЩАЯ ИНФОРМАЦИЯ	949
17.1. Гарантия и сервис	949
17.2. Техническая поддержка	949
17.3. Электронная версия документа	949



Об этом документе

Описание ПО коммутатора

Описание ПО коммутатора

Программное обеспечение коммутатора выполняет две функции:

- Обеспечивает различные возможности коммутации фреймов, основываясь на содержащейся в них информации 2,3 и 4 уровней OSI.
- Предоставляет сетевому администратору возможности для мониторинга и конфигурирования.

Назначение и аудитория

В этом документе описывается интерфейс командной строки (CLI), используемый для настройки и мониторинга работы программного обеспечения коммутатора. Доступ к командной строке можно получить при помощи прямого подключения к последовательному порту коммутатора либо по Telnet или SSH через удаленное подключение.

Этот документ предназначен для системных администраторов, настраивающих и эксплуатирующих коммутаторы QTECH. Документ содержит описание конфигурации ПО коммутатора.

Предполагается, что читатель понимает базовые принципы работы программного обеспечения коммутатора и ознакомлен с техническими характеристиками соответствующего устройства. Также предполагается, что читатель обладает базовыми знаниями о технологии Ethernet и пониманием механизмов работы компьютерных сетей.

Пожалуйста, ознакомьтесь с техническим описанием коммутаторов. Техническое описание содержит информацию о характерных для конкретных коммутаторов функциях маршрутизации, коммутации, SNMP, настроек, управления и других функциях. Некоторые функции не поддерживаются в определенных моделях коммутаторов.



Описание продукта

Развитие сетевых технологий перевело коммутацию Fast Ethernet и Gigabit Ethernet из класса магистральных приложений уровня high-end в разряд недорогих потребительских решений. Стоимость решений продолжает снижаться, и в то же время повышается производительность и расширяется набор доступных функций. Устройства, способные осуществлять коммутацию уровней 2, 3 и 4 OSI, становятся все более востребованы. Программное обеспечение коммутатора обеспечивает гибкое решение для этих все возрастающих потребностей.

Точные функциональные возможности каждого сетевого устройства, на котором работает базовое ПО коммутатора, отличаются в зависимости от модели. В любом случае, ПО включает в себя набор функций для управления как самим коммутатором, так и сетью. Вы можете управлять ПО одним из следующих трех способов:

- Интерфейс командной строки (CLI)
- Simple Network Management Protocol (SNMP)
- Веб-интерфейс

Каждый из данных способов позволяет работать как локально, так и удалённо, используя механизмы управления по внутреннему или по вспомогательному каналу. Управление основывается на стандартах, с параметрами конфигурации и приватной MIB, обеспечивающими возможность управления функциями, не полностью описанными в публичных MIB.



1. РАБОТА С ИНТЕРФЕЙСОМ КОМАНДНОЙ СТРОКИ

Интерфейс командной строки (CLI) представляет собой средство конфигурирования и мониторинга состояния системы, основанное на текстовых командах. Доступ к командной строке можно получить при помощи прямого подключения к последовательному (консольному) порту, либо при помощи удалённого логического соединения посредством Telnet или SSH.

1.1. Синтаксис команд

Команда — это одно или несколько слов, за которыми могут следовать один или несколько параметров. Параметры могут быть обязательными или необязательными.

Некоторые команды, например, `show network` или `clear vlan`, не требуют указания параметров. С другими командами, такими как `network parms`, требуется указать обязательный параметр. Параметры следует указывать в строгом порядке. Сначала указываются обязательные параметры, затем – необязательные. Ниже приведен пример, иллюстрирующий синтаксис команды `network parms`:

`network parms ipaddr netmask [gateway]`

- `network parms` — это имя команды.
- `ipaddr` и `netmask` — это параметры, вместо которых необходимо ввести нужные значения, после ввода ключевых слов команды.
- `[gateway]` — это необязательный параметр. Вы можете указать его значение, а можете не указывать.

Справочник команд содержит все команды, вместе с именем команды и кратким описанием её работы. Описание каждой команды содержит следующую информацию:

- Формат — показывает ключевые слова команды, а также необходимые и необязательные параметры.
- Режим — указывается режим CLI, необходимый для исполнения команды.
- По умолчанию — указываются значения по умолчанию, если таковые имеются, для данной команды.

Команды `show` содержат также описание информации, которую данная команда может вывести на экран.

1.2. Условные обозначения команд

Параметры команд могут включать в себя обязательные значения, необязательные значения либо одно из ключевых слов. Параметры указываются в строгом порядке. Таблица 1 описывает условные обозначения, принятые в данном документе для разграничения значений различных типов.

Таблица 1 – Обозначение

Символ	Пример	Описание
<code>[]</code> квадратные скобки	<code>[value]</code>	Необязательный параметр



Символ	Пример	Описание
<i>Курсив</i>	value или [value]	Значение переменной. Текст, выделенный курсивом, необходимо заменить на нужное значение, которое может представлять собой строку текста или число
{ } фигурные скобки	{choice1 choice2}	Необходимо выбрать один из перечисленных параметров
вертикальная черта	choice1 choice2	Разделяет взаимоисключающие варианты
[{ }] фигурные скобки внутри квадратных	[{choice1 choice2}]	Выбор одного из необязательных параметров

1.3. Общие значения параметров

Значения параметров могут представлять собой строку текста или число. Если в составе текстового значения параметра присутствует пробел - заключите значение в кавычки. Например, выражение "System Name with Spaces" заставляет систему принять значение с пробелами. Определяемые пользователем значения не могут представлять собой пустую строку (""). Таблица 2 описывает общие значения параметров и различные типы форматирования.

Таблица 2 – Описание параметров

Параметры	Описание
ipaddr	Действительный IP-адрес. IP-адрес вводится в одном из следующих форматов: (32 бита) (8.24 бита) (8.8.16 бит) a.b.c.d (8.8.8.8) В дополнение к этим форматам, командная строка принимает десятичный, шестнадцатеричный и восьмеричный форматы, через следующие форматы ввода (где n - любое действительное шестнадцатеричное, восьмеричное или десятичное число): 0xn (командная строка принимает шестнадцатеричный формат). 0n (командная строка принимает восьмеричный формат с нулями). n (командная строка принимает десятичный формат)



Параметры	Описание
Адрес IPv6	FE80:0000:0000:0000:020F:24FF:FEBF:DBCB, или FE80:0:0:0:20F:24FF:FEBF:DBCB, или FE80::20F24FF:FEBF:DBCB, или FE80:0:0:0:20F:24FF:128:141:49:32 Дополнительные сведения см. в RFC 3513
Интерфейс или unit/slot/port	Номера слота и порта разделяются косой чертой. Например, 0/1 обозначает номер слота 0 и номер порта 1
Логический интерфейс	Представляет собой логические номера слота и порта. Это применимо в случае агрегированных каналов (LAG). Вы можете использовать логический unit/slot/port для настройки агрегированного канала
Строки символов	Используйте двойные кавычки для обозначения строки символов, например, "System name with Spaces". Пустая строка ("") недопустима

1.4. Правила наименования unit/slot/port

ПО коммутатора обращается к физическим объектам, таким как платы и порты, с использованием правила unit/slot/port. Данное правило применяется и для идентификации логических объектов, например, интерфейсов агрегированного канала.

Номер слота может означать одно из двух, в зависимости от случая применения. В случае с физическим портом он указывает на плату, содержащую данный порт. В случае с логическим портом и портом CPU он также идентифицирует тип интерфейса или порт.

Таблица 3 – Типы слотов

Тип слота	Описание
Нумерация физических слотов	Нумерация физических слотов начинается с нуля и заканчивается номером последнего нумеруемого порта на устройстве
Нумерация логических слотов	Логические слоты немедленно следуют за физическими слотами и идентифицируют агрегированные каналы (LAG) или интерфейсы маршрутизатора. Значение номера логического слота зависит от типа логического интерфейса и может отличаться от платформы к платформе
Нумерация слотов CPU	Слоты CPU немедленно следуют за логическими слотами



Порт идентифицирует конкретный физический порт или логический интерфейс, управление которыми осуществляется, на данном слоте.

Таблица 4 – Типы портов

Тип порта	Описание
Физические порты	Физические порты для всех слотов нумеруются последовательно, начиная с единицы. Например, порт 1 в слоте 0 (внутренний порт) для отдельно стоящего (не состоящего в стеке) коммутатора) будет иметь номер 1/0/1, порт 2 - 1/0/2, порт 3 - 1/0/3, и так далее
Логические интерфейсы	Интерфейсы агрегированного канала (или группы каналов) представляют собой логические интерфейсы, которые используются только для функции моста. VLAN-интерфейс используется только для функций маршрутизации. Loopback-интерфейсы являются логическими интерфейсами, постоянно находящиеся в рабочем состоянии. Туннельные интерфейсы – это логические линки точка-точка, пересылающие инкапсулированные пакеты
Порты CPU	Порты CPU используются драйвером либо другим физическим объектом, расположенным на физических слотах

ПРИМЕЧАНИЕ: в командной строке loopback-интерфейсы и туннельные интерфейсы не используют формат unit/slot/port. Для выделения loopback-интерфейса используете loopback ID. Для выделения туннельного интерфейса используйте tunnel ID.

1.5. Использование «No»-формы команд

Ключевое слово «no» позволяет использовать специальную форму существующей команды (и не является командой самостоятельно). Почти каждая команда конфигурации имеет форму «no». В общем случае команда с ключевым словом «no» делает противоположное этой же команде без ключевого слова «no», либо возвращает значение по умолчанию. Например, команда no shutdown отменяет выключение интерфейса. Используйте команду без ключевого слова «no», чтобы повторно включить отключенный функционал или включить функционал, выключенный по умолчанию. «No» – форму имеют только конфигурационные команды.

1.6. Выполнение команд "show"

Все команды «show» можно вызвать в любом режиме (режиме Global Configuration, Interface Configuration, VLAN Configuration и т.п.). Команды «show» выводят информацию об определенном параметре системы, его состоянии, текущей конфигурации и статистике. Ранее команды «show» могли быть выполнены только в режимах User EXEC и Privileged EXEC.

1.7. Фильтрация вывода командной строки

Многие команды «show» выдают пользователю значительное количество информации. Это может показаться слишком запутанным и сложным для восприятия. Функция



фильтрации выдачи позволяет пользователю указывать определенные аргументы, что помогает пользователю легче найти нужную информацию.

Главные функции фильтрации выдачи командной строки:

- Постраничная разбивка страниц
 - Поддерживается включение/отключение разбивки выдачи по страницам для всех команд «show». Если функция отключена, вывод отображается единым блоком. Если функция включена, вывод отображается страница за страницей таким образом, что информация не прокручивается на экране до тех пор, пока пользователь не нажмёт клавишу для продолжения. В конце каждой страницы отображается следующая подсказка: --More-- or (q)uit
 - Клавиши, используемые при включенной функции постраничной разбивки: Return (Enter) осуществляет отображение новой строки, q или Q отключают постраничную разбивку, любая другая клавиша переводит на следующую страницу. Переназначить функции на другие клавиши нельзя.

ПРИМЕЧАНИЕ: хотя некоторые команды «show» сами по себе поддерживают постраничную разбивку, принцип разбивки может отличаться для различных команд этого типа.

- Фильтрация вывода
 - “Grep” – подобные команды, модифицирующие вывод таким образом, что пользователь видит лишь желаемый контент.
- Фильтрация, показывающая только те строки, которые содержат совпадения с заданным значением.
- Фильтрация, скрывающая из выдачи строки, которые содержат совпадения с заданным значением.
- Фильтрация, показывающая только те строки, которые содержат совпадения с заданным значением, и следующие за ними.
- Фильтрация, показывающая только указанные разделы содержимого (например, “interface 0/1”) с настраиваемым разделителем конца раздела.
- Фильтрация по текстовому значению не чувствительна к регистру.
- Разбивка на страницы (в случае, если она включена) также применяется к отфильтрованной выдаче.

Пример: в данном примере рассматривается использование ключевых слов, фильтрующих вывод командной строки, в применении к одной из команд «show».

(Switch) #show running-config ?

<cr>	Press enter to execute the command.
	Output filter options.
<scriptname>	Script file name for writing active configuration.
all	Show all the running configuration on the switch.
interface	Display the running configuration for specified interface on the switch.

(Switch) #show running-config | ?



begin	Begin with the line that matches
exclude	Exclude lines that matches
include	Include lines that matches
section	Display portion of lines

1.8. Режимы командной строки

В командной строке команды сгруппированы в различные режимы, в зависимости от выполняемых функций. Каждый режим поддерживает определенный компонент ПО. Команды определенного режима не доступны до тех пор, пока соответствующий режим не будет задействован (единственное отключение - команды режима User EXEC, которые могут выполняться и в режиме Privileged EXEC).

В каждом из режимов интерфейс выглядит несколько иначе, что позволяет мгновенно определить текущий режим. Таблица 5 содержит описания режимов и их визуальных различий.

ПРИМЕЧАНИЕ: набор командных режимов, доступных на конкретном коммутаторе, может отличаться, в зависимости от версии установленного ПО.

Таблица 5 – Режимы командной строки

Режим команд	Вид	Описание
User EXEC	Switch>	Содержит ограниченный набор команд для просмотра базовой системной информации
Privileged EXEC	Switch#	Позволяет выполнение любой команды EXEC, войти в режимы VLAN Config и Global Config
Global Config	Switch (Config)#	Содержит команды общей настройки и позволяет модифицировать уже работающую конфигурацию
VLAN config	Switch (Vlan)#	Содержит команды конфигурации VLAN

Interface Config	Switch (Interface unit/slot/port)# Switch (Interface Loopback id)# Switch (Interface Tunnel id)# Switch (Interface unit/slot/port(start range)- unit/slot/port(end range))# Switch (Interface lag lag-intfnum)# Switch (Interface vlan vlan-id)#	Управление работой интерфейса. Так же дает доступ к командам настройки виртуальных интерфейсов маршрутизации. Используйте данный режим, для настройки физического порта или заданного логического интерфейса. Так же в данном режиме вы можете настраивать диапазон интерфейсов. Например:



		Switch (Interface 1/0/1-1/0/4) # Переход в режим конфигурации интерфейса LAG Переход в режим конфигурации VLAN для указанного VLAN ID
Line Console	Switch (config- line)#	Содержит команды для настройки консольного интерфейса, в том числе настройки аутентификации
Line SSH	Switch (config- ssh)#	Содержит команды для настройки протокола SSH, в том числе настройки аутентификации
Line Telnet	Switch (config- telnet)#	Содержит команды для настройки протокола Telnet, в том числе настройки аутентификации
AAA IAS User config	Switch (Config-IAS- User)#	Позволяет настроить пользовательский пароль в базе IAS
Policy Map Config	Switch (Config- policy-map)#	Содержит команды настройки карты политик QoS
Policy Class Config	Switch (Config- policy-class-map)#	Режим создания, удаления и настройки карты политик классов. Команды отбора по классам классов работают как с общими критериями, так и с критериями уровней 2 и 3
Class Map Config	Switch (Config- class-map)#	Режим включает команды настройки карты классов QoS
Radius Dynamic Authorization Config	(Config-radius-da)	Режим настройки динамической авторизации RADIUS
MAC Access-list Config	Switch (Config-mac- access-list)#	Позволяет создать список доступа с фильтрацией по MAC, а также войти в режим конфигурации, содержащий команды, относящиеся к спискам такого рода
TACACS Config	Switch (Tacacs)#	Содержит команды для настройки сервера TACACS



DHCP Pool Config	Switch (Config dhcp-pool)#	Содержит команды настройки пула IP-адресов DHCP
Support Mode	Switch (Support)#	Обеспечивает доступ к командам поддержки (режим должен использоваться только специалистами службы технической поддержки производителя, так как неправильное использование может стать причиной некорректной работой системы и/или прекращения гарантийных обязательств)

Таблица 6 описывает процедуру входа в каждый режим и выхода из него.

Таблица 6 – Режимы командной строки, вход и выход

Режим команд	Вид	Описание
User EXEC	Первый уровень доступа	Для выхода введите logout
Privileged EXEC	В режиме User EXEC введите enable	Для выхода в режим User EXEC введите exit или нажмите Ctrl-Z
Global Config	В режиме Privileged EXEC введите configure	Для выхода в режим Privileged EXEC введите exit или нажмите Ctrl-Z
VLAN Config	В режиме Privileged EXEC введите vlan database	Для выхода в режим Privileged EXEC введите exit, или нажмите Ctrl-Z
Interface Config	В режиме Global Config введите: interface unit/slot/port, либо interface loopback id, либо interface tunnel id interface unit/slot/port(start range)-unit/slot/port(endrange) interface lag lag-intf-num interface vlan vlan-id	Для выхода в режим Global Config введите exit. Для выхода в режим Privileged EXEC введите exit или нажмите Ctrl-Z



Режим команд	Вид	Описание
Line Console	В режиме Global Config введите line console:	Для выхода в режим Global Config введите exit. Для выхода в режим Privileged EXEC нажмите Ctrl-Z
Line SSH	В режиме Global Config введите line ssh:	Для выхода в режим Global Config введите exit. Для выхода в режим Privileged EXEC нажмите Ctrl-Z
Line Telnet	В режиме Global Config введите line telnet:	Для выхода в режим глобальной конфигурации введите exit. Для выхода в режим Privileged EXEC нажмите Ctrl-Z
AAA IAS User Config	В режиме Global Config введите aaa ias-user username name	Для выхода в режим Global Config введите exit. Для выхода в режим Privileged EXEC нажмите Ctrl-Z
Mail Server Config	В режиме Global Config введите mail-server address	Для выхода в режим Global Config введите exit. Для выхода в режим Privileged EXEC нажмите Ctrl-Z
Policy-Map Config	В режиме Global Config введите policy-map	Для выхода в режим Global Config введите exit. Для выхода в режим Privileged EXEC нажмите Ctrl-Z
Policy-Class-Map Config	В режиме Policy Map введите class	Для выхода в режим Policy Map введите exit. Для выхода в режим Privileged EXEC нажмите Ctrl-Z
Class-Map Config	В режиме Global Config введите class-map "class-map"	Для выхода в режим Global Config введите exit. Для выхода в режим Privileged EXEC нажмите Ctrl-Z
MAC Access-list Config	В режиме Global Config введите mac access-list extended name	Для выхода в режим Global Config введите exit. Для выхода в режим Privileged EXEC нажмите Ctrl-Z



Режим команд	Вид	Описание
TACACS Config	В режиме Global Config введите tacacs-server host ip-addr, где ip-addr – это IP-адрес TACACS-сервера вашей сети	Для выхода в режим Global Config введите exit. Для выхода в режим Privileged EXEC нажмите Ctrl-Z
DHCP Pool Config	В режиме Global Config введите ip dhcp pool pool-name	Для выхода в режим Global Config введите exit. Для выхода в режим Privileged EXEC нажмите Ctrl-Z
Support Mode	В режиме Privileged EXEC введите support. ПРИМЕЧАНИЕ: команда support доступна только после предварительного выполнения команды techsupport enable	Для выхода в режим Privileged EXEC введите exit или нажмите Ctrl-Z

1.9. Сокращенная форма и автозавершение команд

Автозавершение команд заканчивает написание команды при вводе достаточного количества

символов, позволяющих однозначно идентифицировать ключевое слово. После того как вы ввели достаточно букв, нажмите клавишу пробел или TAB для завершения слова.

Сокращенная форма позволяет выполнить команду после ввода достаточного количества символов, позволяющих однозначно ее идентифицировать. Перед выполнением команды необходимо ввести все обязательные для нее ключевые слова и параметры.

1.10. Сообщения об ошибках CLI

Ввод команды, которую система не может выполнить, вызывает сообщение об ошибке. Таблица 7 описывает наиболее распространенные сообщения об ошибках интерфейса командной строки.



Таблица 7 – Сообщения об ошибках CLI

Текст сообщения	Описание
% Invalid input detected at '^' marker	Указывает на ввод неверной или недоступной команды. Символ карет (^) показывает, где именно обнаружен некорректный текст. Это же сообщение появляется, если какой-то из параметров или значений не распознаётся
Command not found / Incomplete command. Use ? to list commands	Указывает на отсутствие обязательных ключевых слов или значений
Ambiguous command	Оповещает о том, что введенных символов недостаточно для однозначной идентификации команды

1.11. Комбинации клавиш для работы в командной строке

В таблице 8 приведены комбинации клавиш, которые можно использовать для редактирования команд или увеличения скорости ввода команд. Вы также можете получить доступ к этому списку из интерфейса командной строки, введя help в режимах User или Privileged EXEC.

Таблица 8 – Клавиатурные сокращения командной строки

Сочетание клавиш	Описание
DEL или BACKSPACE	Удалить предыдущий символ
Ctrl-A	Перейти к началу строки
Ctrl-E	Перейти в конец строки
Ctrl-F	Перейти на один символ вперед
Ctrl-B	Перейти на один символ назад
Ctrl-D	Удаление текущего символа
Ctrl-U, X	Удалить начало строки
Ctrl-K	Удалить конец строки
Ctrl-W	Удалить предыдущее слово



Сочетание клавиш	Описание
Ctrl-T	Поменять местами текущий и следующий символы
Ctrl-P	Перейти к предыдущей строке в буфере истории
Ctrl-R	Заменить или вставить строку
Ctrl-N	Перейти к следующей строке в буфере истории
Ctrl-Y	Напечатать последний удаленный символ
Ctrl-Q	Включить последовательный поток
Ctrl-S	Отключить последовательный поток
Ctrl-Z	Выйти в предшествующий режим командной строки
Tab, пробел	Автозавершение команды
Exit	Возвращение в предыдущий режим
?	Список доступных команд, ключевых слов или параметров

1.12. Справка и поддержка в командной строке

Введите вопросительный знак (?) в командной строке для отображения списка доступных команд в текущем режиме.

(switch) >?

enable	Enter into user privilege mode
help	Display help for various special keys
logout	Exit this session. Any unsaved changes are lost
password	Change an existing user's password
ping	Send ICMP echo packets to a specified IP address
quit	Exit this session. Any unsaved changes are lost
show	Display Switch Options and Settings
telnet	Telnet to a remote host

Введите вопросительный знак (?) после слова, чтобы увидеть доступные для него параметры или ключевые слова.



(switch) #network ?

ipv6	Configure IPv6 parameters for system network
javamode	Enable/Disable
mac-address	Configure MAC Address
mac-type	Select the locally administered or burnedin MAC address
mgmt_vlan	Configure the Management VLAN ID of the switch
parms	Configure Network Parameters of the device
protocol	Select DHCP, BootP, or None as the network config protocol

Если справочная информация содержит параметр, заключенный в угловые скобки, необходимо заменить его на значение.

(Switch) #network parms ?

<ipaddr> Enter the IP Address.
none Reset IP address and gateway on management interface

Если у команды нет дополнительных ключевых слов и параметров, либо если параметры не являются обязательными, вы увидите следующее сообщение:

<cr> Press Enter to execute the command

Можно также ввести знак вопроса (?) после ввода одного или нескольких символов в слове, чтобы вывести список доступных команд или параметров, которые начинаются с введенной последовательности символов, как показано в следующем примере:

```
(switch) #show m?
mac
mail-server          mac-addr-table mbuf      mac-address-table monitor
```

1.13. Получение доступа к CLI

Доступ к командной строке можно получить при помощи прямого подключения к консольному порту, либо при помощи удалённого соединения посредством протоколов Telnet или SSH.

Для первоначального подключения, вы должны использовать прямое подключение к консольному порту. Вы не можете получить доступ к удаленной системе, в системе не настроены IP-адрес, маска подсети и шлюз по умолчанию. Вы можете ввести эти настройки вручную, либо получить их с сервера BOOTP или DHCP в вашей сети.



2. КОМАНДЫ БАЗОВОГО КОНФИГУРИРОВАНИЯ КОММУТАТОРА

2.1. Команды базового конфигурирования

2.1.1. Строка проверки подлинности (authentication line)

Команда	authentication line {console vty web} login {local radius tacacs} no authentication line {console vty web} login	
Параметр	console	Подключение к коммутатору через последовательный консольный порт
	vtty	Подключение к коммутатору через удаленный терминал (SSH или Telnet)
	web	Подключение к коммутатору через HTTP/HTTPS
Состояние по умолчанию	Настройки для авторизации через консоль отсутствуют. По умолчанию для подключения через удаленный терминал и HTTP/HTTPS подключена локальная идентификация	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда позволяет настроить методы аутентификации входа пользователей через консольный порт, удаленный терминал и веб-интерфейс соответственно. Способами аутентификации могут быть Local, RADIUS и TACACS как отдельно, так и в комбинации. Если задана комбинация методов, выбор предпочтительного метода выполняется слева направо. Если пользователь уже прошел проверку подлинности, менее предпочтительный способ аутентификации будет проигнорирован. Если проверка подлинности пройдена, пользователь сможет войти в систему. Перед использованием аутентификации RADIUS необходимо настроить функцию AAA и сервер RADIUS. Если локальная аутентификация установлена без настройки локальных пользователей, пользователи смогут подключаться к коммутатору через консоль. Поддерживаются следующие методы аутентификации. Local: используется локальная база данных пользователей. Tacacs: для аутентификации используется список удаленных серверов Tacas. Radius: для аутентификации используется список удаленных серверов RADIUS.	



	"no" в начале команды восстанавливает метод аутентификации по умолчанию
Пример	Установить для входа Telnet и ssh метод аутентификации Local и RADIUS. Switch(config)# authentication line vty login local radius lists

2.1.2. Баннер (banner)

Команда	banner motd<LINE> no banner motd	
Параметр	<LINE>	Информация, отображаемая при успешной аутентификации, ограничение по длине от 1 до 100 символов
Состояние по умолчанию	При успешной аутентификации информация не отображается	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда используется для настройки информации, отображаемой при успешной аутентификации пользователя через консоль или telnet; "no" в начале команды задает отсутствие отображаемой информации при успешной аутентификации	
Пример	Настроить появление на экране сообщения "Welcome (Добро пожаловать)" после успешной аутентификации. Switch(config)# banner motd Welcome	

2.1.3. Загрузочный образ (boot img)

Команда	boot img {primary backup}	
	primary	исходная запись в файле img
	backup	вторая запись в файле img
Состояние по умолчанию	Заводская настройка по умолчанию определяет только первый файл IMG образа ПО pos.img на Flash-памяти, без второго IMG-файла образа ПО	
Режим	Привилегированный режим	



Руководство по использованию	Эта команда используется для выбора первого или второго образа программного обеспечения, который будет использоваться при загрузке коммутатора. Первый и второй img-файлы могут использовать только файлы .img, хранящиеся в коммутаторе. Расширение имени файла должно быть .img. Полная длина пути к файлу не должна превышать 128 символов, а имя файла – 80 символов
Пример	Установить в качестве второго загрузочного файла образа ПО, используемого при следующей загрузке коммутатора. Switch#boot img backup

2.1.4. Конфигурирование загрузки (boot startup-config)

Команда	boot startup-config {NULL <file-url>}	
Параметр	NULL	При следующей перезагрузке применяются заводские настройки по умолчанию
	<file-url>	Полный путь к CFG-файлу, используемому при следующей загрузке
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Команда позволяет сконфигурировать CFG-файл, который будет использоваться при следующей загрузке коммутатора. При конфигурировании CFG-файла для следующей загрузки можно использовать только файл .cfg, хранящийся в коммутаторе. Путь к файлу состоит из трех частей: префикса устройства в качестве корневого каталога (flash: /), подкаталога и имени файла. Между частями не должно быть пробелов. Расширение имени файла должно быть .cfg. Полная длина пути к файлу не должна превышать 128 символов, а имя файла – 80 символов	
Пример	Установить flash: / startup.cfg в качестве CFG-файла, используемого при следующей загрузке коммутатора. Switch# boot startup-config flash: / startup.cfg	



2.1.5. Настройка времени (clock set)

Команда	clock set <HH: MM: SS> <YYYY.MM.DD>	
Параметр	<HH: MM: SS>	Время, часы (HH), применяемый диапазон от 0 до 23, минуты (MM) и секунды (SS) от 0 до 59
	<YYYY.MM.DD>	Год, месяц и дата; диапазон значений: год (YYYY) от 1970 до 2038, месяц (MON) от 1 до 12, день (DD) от 1 до 31
Состояние по умолчанию	По умолчанию при первом запуске устанавливается значение 2006.1.1 0: 0: 0	
Режим	Привилегированный режим	
Руководство по использованию	Команда позволяет настроить системное время и дату на коммутаторе. Коммутатор не может продолжать отсчет времени при выключенном питании, поэтому в условиях, где требуется точное время, необходимо сначала установить текущую дату и время	
Пример	Установить текущую дату и время коммутатора на 01.08.2024 23:00:00 Switch#clock set 23:0:0 2024.8.1	

2.1.6. Конфигурирование (config)

Команда	config [terminal]
Параметр	[terminal] обозначает конфигурирование терминала
Состояние по умолчанию	Не задано
Режим	Привилегированный режим
Руководство по использованию	Эта команда используется для перехода из привилегированного режима в режим глобальной конфигурации "config"
Пример	Войти в Режим глобальной конфигурации "config" из режима управления "admin". Switch#config



2.1.7. Выключение (disable)

Команда	disable	
Параметр	none	Отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Эта команда используется для перехода из привилегированного режима обратно в режим обычного пользователя	
Пример	Выход из привилегированного режима в режим обычного пользователя. Switch#disable Switch>	

2.1.8. Включение (enable)

Команда	enable [<1-15>]	
Параметр	[<1-15>]	Уровень прав пользователя
Состояние по умолчанию	Не задано	
Режим	Режим пользователя/Привилегированный режим	
Руководство по использованию	Команда предназначена для перехода из режима пользователя в привилегированный режим, либо для смены уровня привилегий у текущего пользователя. Для предотвращения несанкционированного доступа пользователей, не являющихся администраторами, при входе в привилегированный режим из режима пользователя требуется аутентификация пользователя (т.е. необходимо ввести пароль пользователя Admin). Если пароль администратора введен правильно, пользователю будет разрешен вход в привилегированный режим; если пароль администратора введен неправильно 3 раза подряд, сохранится режим пользователя. При изменении привилегий пользователей с низкого уровня на высокий необходимо подтвердить подлинность пароля соответствующего уровня. Для установки пароля пользователя admin в режиме глобальной конфигурации используйте команду "enable password"	



Пример	Вход в режим управления из режима пользователя. Switch>enable Switch#

2.1.9. Включение пароля (enable password)

Команда	enable password [level <1-15>] [0 7] <password> no enable password [level <1-15>]	
Параметр	[level <1-15>]	Используется для указания уровня привилегий, по умолчанию уровень равен 15
	[0 7]	Если в настройках пароля ввести значение 0, пароль не будет зашифрован; Если в настройках пароля ввести параметр 7, пароль будет зашифрован
	<password>	пароль пользователя
Состояние по умолчанию	По умолчанию поле пароля не заполнено	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет установить пароль, который используется для входа в привилегированный режим из режима пользователя. Установка этого пароля предотвращает несанкционированный доступ к режиму администратора. Рекомендуется устанавливать пароль во время первоначальной настройки коммутатора. Кроме того, если администратору на продолжительное время необходимо покинуть терминал, рекомендуется использовать команду "exit". Команда "no enable password" удаляет пароль	
Пример	Настроить команду для обычных пользователей для входа в привилегированный режим по правилу в качестве теста. Switch(config)#enable password 0 test	



2.1.10. Окончание (end)

Команда	End	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Все режимы за исключением режимов пользователь/администратор	
Руководство по использованию	Эта команда используется для настройки команды входа в привилегированный режим для обычных пользователей по правилу в качестве теста	
Пример	Выход из режима VLAN и возврат в привилегированный режим. Switch(config-vlan1)#end Switch#	

2.1.11. Тайм-аут выполнения (exec-timeout)

Команда	exec-timeout <minutes> [<seconds>] no exec-timeout	
Параметр	<minutes>	значение времени в минутах, находится в диапазоне от 0 до 35791
	[<seconds>]	значение времени в секундах, находится в диапазоне от 0 до 59
Состояние по умолчанию	По умолчанию время ожидания составляет 10 минут	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда используется для установки периода ожидания выхода из привилегированного режима. Для повторного входа в привилегированный режим, если выход осуществлен по таймауту, необходимо ввести код администратора и пароль. Если значение времени ожидания равно 0, таймер отключается. Команда "no exec-timeout" восстанавливает значение по умолчанию	
Пример	Установить значение времени ожидания привилегированного режима на 5 минут 30 секунд. Switch(config)#exec-timeout 5 30	



2.1.12. Выход (exit)

Команда	Exit	
Параметр	none	Отсутствует
Состояние по умолчанию	Не задано	
Режим	Все режимы	
Руководство по использованию	Выход из текущего режима в нижестоящий режим	
Пример	Выйти из режима глобальной конфигурации в предыдущий режим Switch(config)#exit Switch#	

2.1.13. Справка (help)

Команда	Help	
Параметр	none	Отсутствует
Состояние по умолчанию	Не задано	
Режим	Все режимы	
Руководство по использованию	Мгновенная интерактивная справка, предоставляемая коммутатором. По команде Help отображается информация обо всей справочной системе, включая полную и краткую справку. Пользователь может в любое время ввести '?' и получить интерактивную справку	
Пример	Получить справку в глобальном режиме. Switch(config)#help CLI (интерфейс командной строки) предоставляет расширенную функцию помощи. Когда необходимо получить справочную информацию, в любое время введите в командной строке символ '?'. Если нет подходящих элементов, список инструкций будет пуст, необходимо выполнять резервирование до тех пор, пока при вводе символа '?' не появятся все доступные варианты	



2.1.14. Имя хоста (hostname)

Команда	hostname <hostname> no hostname	
Параметр	<hostname>	строка пояснительной информации, допускается до 64 символов
Состояние по умолчанию	Приглашения по умолчанию относятся к коммутатору	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет установить приглашение в интерфейсе командной строки коммутатора. "no" в начале команды отменяет конфигурирование	
Пример	Задать подсказку "QTECH". Switch(config)#hostname QTECH QTECH(config)#	

2.1.15. IP-хост (ip host)

Команда	ip host <hostname> <ip_addr> no ip host {<hostname> all}	
Параметр	<hostname>	строка подсказки, допускается до 64 символов
	<ip_addr>	соответствующий IP-адрес для хоста в десятично-точечной записи
	all	все имена хостов
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет настроить соотнесение между хостом и IP-адресом. Установка связи между хостом и IP-адресом может использоваться в таких командах, как "ping <host>". Команда "no ip host" удаляет соотнесение	
Пример	Установить IP-адрес узла с именем "qtech" на 200.121.1.1. Switch(config)#ip host qtech 200.121.1.1	



2.1.16. Хост IPv6 (ipv6 host)

Команда	ipv6 host <hostname> <ipv6_addr> no ipv6 host { <hostname> all}	
Параметр	<hostname>	строка подсказки, допускается до 64 символов
	<ipv6_addr>	соответствующий IPv6-адрес хоста в десятично-точечной записи
	all	все имена хостов
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет настроить соотнесение между хостом и IPv6-адресом. Установка связи между хостом и адресом IPv6 может использоваться в таких командах, как "traceroute6 <host>". Команда "no ip host" удаляет соотнесение	
Пример	Установить IPv6-адрес узла с именем "qtech" на 200:1:2:3::1. Switch(config)#ipv6 host qtech 2001:1:2:3::1	

2.1.17. Ip http-сервер (ip http server)

Команда	ip http server no ip http server	
Параметр	none	отсутствует
Состояние по умолчанию	Включено	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Данной командой включается http-сервер на контроллере. Команда "no ip http server" отключает http-сервер	
Пример	Включить функцию http-сервера и конфигурирования. Switch(config)#ip http server	



2.1.18. Логин (login)

Команда	login no login	
Параметр	none	отсутствует
Состояние по умолчанию	Авторизация по логину отсутствует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	При применении данной команды, пользователи должны ввести пароль, установленный командой password, чтобы войти через консоль. Команда "no login" отменяет ограничение по авторизации	
Пример	Подключить пароль Switch(config)#login	

2.1.19. Пароль (password)

Команда	password [0 7] <password> no password	
Параметр	[0 7]	Если при установке пароля введен параметр 0, пароль задается в открытой форме; если введен параметр 7, пароль задается в зашифрованной форме;
	<password>	пароль пользователя
Состояние по умолчанию	По умолчанию поле пароля не заполнено	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда для установки пароля для входа в обычный пользовательский режим на консоли. Команда "no password" удалит этот пароль	
Пример	Настроить пароль для входа в режим обычного пользователя, как тестовый, в открытой форме. Switch(config)#password 0 test	



2.1.20. Установка уровня привилегий (privilege)

Команда	privilege mode level <1-15> LINE no privilege mode level <1-15> LINE	
Параметр	mode	Режим регистра команды, 'Tab' или '?' ' позволяет показать все регистровые режимы
	<1-15>	Уровни привилегий от 10 до 15
	LINE	Команды, которые необходимо задать; поддерживается сокращение команд
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	С помощью данной команды производится установка уровня разрешений для определенной команды. Функция не изменяет саму команду. Строка LINE должна содержать полный формат команды; формат сокращений используется для тех команд, которые могут быть успешно проанализированы. Уровень команды NO может быть установлен опционально, это не влияет на результат. При использовании команды NO строка LINE должна быть настроенной командной строкой. Если это командная строка с параметрами, параметры должны соответствовать команде set. "no" перед началом команды возвращает уровень привилегий по умолчанию	
Пример	Изменить уровень команды show ip route на 5. Восстановить исходный уровень команды show ip route. Switch(config)#privilege exec level 5 show ip route Switch(config)#no privilege exec level 5 show ip route	

2.1.21. Перезапуск (reload)

Команда	reload	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	



Режим	Привилегированный режим
Руководство по использованию	Команда может применяться для непрерывного перезапуска коммутатора
Пример	Горячий перезапуск коммутатора Switch(config)#reload

2.1.22. Служба шифрования паролей (service password-encryption)

Команда	service password-encryption no service password-encryption	
Параметр	none	отсутствует
Состояние по умолчанию	По умолчанию в системе нет службы шифрования паролей	
Режим	Режим глобальной конфигурации	
Руководство по использованию	При выполнении этой команды текущие незашифрованные (открытые) пароли, а также пароли, установленные командами password, enable password, ip ftp и username, будут зашифрованы. Команда "no service password-encryption" отменяет эту функцию, однако зашифрованные пароли остаются неизменными	
Пример	Зашифровать системные пароли. Switch(config)#service password-encryption	

2.1.23. Служба установки размеров окна (service terminal-length)

Команда	service terminal-length <0-512> no service terminal-length	
Параметр	<0-512>	Столбцы символов, отображаемых на каждом экране vty, в диапазоне от 0 до 512
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда задает столбец символов, отображаемых на каждом экране терминала. Столбцы символов, отображаемые на каждом экране клиента telnet.ssh и консоли, будут соответствовать этой конфигурирования. Команда “no service terminal-length” отключает реакцию на изменение размеров окна
Пример	Установить число потоков vty равным 20. Switch(config)#service terminal-length 20

2.1.24. Контакты производителя (sysContact)

Команда	sysContact <LINE> no sysContact	
Параметр	<LINE>	строка символов подсказки, диапазон от 0 до 255 символов
Состояние по умолчанию	По умолчанию установлены заводские настройки	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет указать контактную информацию производителя устройства. По команде “no sysContact” выполняется возврат к заводским настройкам	
Пример	Задать контакты производителя для проверки. Switch(config)#sysContact test	

2.1.25. Адрес производителя (sysLocation)

Команда	sysLocation<LINE> no sysLocation	
Параметр	<LINE>	строка символов подсказки, диапазон от 0 до 255 символов
Состояние по умолчанию	По умолчанию установлены заводские настройки	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Позволяет указать адрес производителя устройства. По команде “no sysLocation” выполняется возврат к заводским настройкам
Пример	Задать адрес производителя для проверки. Switch(config)#sysLocation test

2.1.26. Заводские настройки (set default)

Команда	set default	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Восстанавливает на коммутаторе заводские настройки. Все настройки, сделанные пользователем, будут стерты. После перезагрузки коммутатора, приглашение командной строки примет вид, который был при первом включении питания коммутатора. Примечание: Для сохранения результатов после применения этой команды следует ввести команду "write (запись)". После перезапуска коммутатор вернется к заводским настройкам	
Пример	Восстановить заводские настройки и перезапустить устройство. Switch#set default Are you sure? [Y/N] = y Switch#write Switch#reload	

2.1.27. Установка пароля в режиме загрузки (set boot password)

Команда	set boot password no set boot password	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда позволяет в режиме образа ПО настроить пароль для последующих входов в режим загрузчика bootrom; в режиме глобальной конфигурации введите эту команду и пароль в соответствии с подсказками и подтвердите успешное завершение конфигурирования. ПРИМЕЧАНИЕ: длина пароля составляет от 3 до 3. "no" в начале команды сбрасывает пароль
Пример	Установить пароль при входе в режим загрузки. <pre>Switch(config)#set boot password</pre> New password : ***** Confirm password : ***** Set password success!

2.1.28. Настройка (setup)

Команда	setup	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	После входа с помощью этой команды в режим настройки коммутатора может быть выполнено конфигурирование IP-адресов и т. п.	
Пример	Войти в режим настройки. <pre>Switch#setup</pre>	

2.1.29. Вывод времени (show clock)

Команда	show clock	
Параметр	none	Отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	



Руководство по использованию	Команда выводит на экран время системы
Пример	Вывести на экран время системы. Switch#show clock Current time is TUE AUG 22 11 : 00 : 01 2024

2.1.30. Вывод данных об использовании процессора (show cpu usage)

Команда	show cpu usage [<slotno>]	
Параметр	[<slotno>]	задает слоты
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим и Режим глобальной конфигурации	
Руководство по использованию	Команда выводит на экран загрузку процессора за последние 5 секунд, 30 секунд, 5 минут и с момента старта устройства. Параметр slotno, который используется для отображения уровня использования ЦП картой в указанном слоте применим только для модульного коммутатора, если параметр отсутствует, то по умолчанию используется текущая карта	
Пример	Показать текущий уровень загруженности процессора. Switch#show cpu usage Last 5 second CPU IDLE: 87% Last 30 second CPU IDLE: 89% Last 5 minute CPU IDLE: 89% From running CPU IDLE: 89%	

2.1.31. Вывод данных о загрузке процессора (show cpu utilization)

Команда	show cpu utilization	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	



Руководство по использованию	Эта команда используется для вывода на экран уровня загрузки процессора за последние 5 секунд, 30 секунд и 5 минут
Пример	Отобразить текущую загрузку процессора Switch#show cpu utilization Last 5 second CPU USAGE: 9% Last 30 second CPU USAGE: 11% Last 5 minute CPU USAGE: 11% From running CPU USAGE: 11%

2.1.32. Вывод данных об использовании памяти (show memory usage)

Команда	show memory usage [<slotno>]	
Параметр	[<slotno>]	задает слоты
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Выводит на экран информацию о использовании оперативной памяти. Параметр slotno, который используется для отображения уровня использования памяти в указанном слоте применим только для модульного коммутатора, если параметр отсутствует, то по умолчанию используется текущая карта	
Пример	Вывести на экран информацию о использовании оперативной памяти. Switch#show memory usage The memory total 128 MB, free 58914872 bytes, usage is 56.10%	

2.1.33. Вывод уровня привилегий (show privilege)

Команда	show privilege	
Параметр	none	Отсутствует
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда показывает текущий уровень привилегий пользователя
Пример	Показать текущий уровень привилегий пользователя. Switch(config)#show privilege Current privilege level is 15

2.1.34. Вывод данных об уровне привилегий команды (show privilege mode LINE)

Команда	show privilege mode LINE	
Параметр	mode	режим регистра команды, 'Tab' или '?' ' позволяет показать все регистровые режимы
	LINE	Команды, которые необходимо задать; поддерживается сокращение команд
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим/ Режим глобальной конфигурации	
Руководство по использованию	Показывает уровень заданной команды. LINE должна быть полным форматом команды; формат сокращений используется для команд, которые могут быть успешно проанализированы. Команды с половинчатой формулировкой, ложные команды записи и команды с аббревиатурой не могут быть успешно проанализированы, их уровень не может быть показан	
Пример	Показать уровень привилегий команды. Switch(config)#show privilege exec show ip route The command : show ip route Privilege is : 15	

2.1.35. Вывод данных для тех. поддержки (show tech-support)

Команда	show tech-support [no-more]	
Параметр	[no-more]	позволяет вывести всю необходимую информацию на экран сразу же, не подключая пользователя через "more"



Состояние по умолчанию	Не задано
Режим	Привилегированный режим/Режим глобальной конфигурации
Руководство по использованию	Команда применяется для сбора соответствующей информации при сбоях в работе коммутатора. Отображает оперативную информацию и статус задачи коммутатора. Персонал службы технической поддержки может использовать эту команду для контроля правильности работы коммутатора
Пример	Вывести на экран информацию о работе коммутатора, информацию о состоянии задач. Switch#show tech-support

2.1.36. Вывод данных о версии (show version)

Команда	show version	
Параметр	none	Отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим/Режим глобальной конфигурации	
Руководство по использованию	Команда показывает текущую версию аппаратных и программных средств коммутатора	
Пример	Показать версию коммутатора Switch#show version	

2.1.37. Имя пользователя (username)

Команда	username <username> [privilege <privilege>] [password [0 7]<password>] no username <username>	
Параметр	<username>	имя пользователя, диапазон не должен превышать 32 символа
	<privilege>	максимальный уровень привилегий для доступа к командам, определяющий те из них, которые разрешено выполнять пользователю



	[0 7]	Если ввести опцию 0, пароль шифроваться не будет; если при установке пароля ввести опцию 7, то пароль будет зашифрован (используется 32-битный пароль, зашифрованный с помощью MD5)
	<password>	пароль пользователя
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет установить имя пользователя для локального входа в систему и пароль, соответствующий уровень привилегий. С помощью этой команды можно настроить не более 16 локальных пользователей, а максимальная длина пароля должна быть не менее 32. Пользователь может войти в систему под своим именем и приоритетом после того, как команда установлена, перед тем как задать команду "authentication line console login local", необходимо убедиться, что у одного пользователя настроен уровень привилегий 15, для того чтобы войти в коммутатор и вносить изменения в конфигурирование в привилегированном и глобальном режимах. Если нет настроенных локальных пользователей с уровнем привилегий 15, а для метода входа в консоль определена только локальная аутентификация, вход может выполняться без какой-либо аутентификации. При использовании метода HTTP для входа в коммутатор только пользователи с уровнем привилегий 15 могут войти, пользователям с уровнем привилегий, отличным от 15, будет отказано. "no" перед началом команды удаляет пользователя	
Пример	Настроить учетную запись администратора с именем admin, с уровнем привилегий 15. Кроме того, создать двух обычных пользователей с уровнем привилегий 1. После этого включить локальную аутентификацию. <pre>Switch(config)#username admin privilege 15 password 0 admin Switch(config)#username user1 privilege 1 password 7 4a7d1ed414474e4033ac29ccb8653d9b Switch(config)# username user2 password 0 user2 Switch(config)# authentication line console login local</pre>	



2.1.38. Уровень HTTP/HTTPS-регистрации 1–15 (web-auth privilege <1-15>)

Команда	web-auth privilege <1-15> no web-auth privilege	
Параметр	<1-15>	задает уровень регистрации в коммутаторе через HTTP/HTTPS, диапазон от 1 до 15
Состояние по умолчанию	По умолчанию задан уровень 15	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать уровень регистрации в коммутаторе через HTTP/HTTPS. После настройки уровня входа в коммутатор по через HTTP/HTTPS, только пользователь с уровнем, равным или превышающим его, сможет войти в коммутатор по через HTTP/HTTPS	
Пример	Настроить уровень регистрации в коммутаторе по HTTP равным 10. Switch(config)# web-auth privilege 10	

2.1.39. Запись (write)

Команда	Write	
Параметр	none	Отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	С помощью этой команды, изменения, внесенные в конфигурирование, могут быть сохранены во флеш-памяти. После настройки нужных функций необходимо сохранить изменения в указанном файле конфигурирования, чтобы система могла автоматически вернуться к сохраненным настройкам в случае неожиданного выключения или сбоя питания. Равнозначна команде "copy running-config startup-config"	
Пример	Сохранить текущую конфигурацию. Switch#write	



2.1.40. Запись текущей конфигурирования (write running-config)

Команда	write running-config [<startup-config-file-name>]	
Параметр	[<startup-config-file-name>]	полный путь к файлу cfg
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Команда позволяет сохранить текущую выполняемую конфигурирование в виде файла .cfg на флеш-память. Путь к файлу состоит из двух частей: префикса устройства, используемого в качестве корневого каталога (flash:/) / и имени файла. Между частями не должно быть пробелов. Расширение имени файла должно быть .cfg. Длина полного пути к файлу не должна превышать 128 символов, а имя файла не может быть длиннее 80 символов	
Пример	Сохранить текущую конфигурирование в файле .cfg с именем 123. Switch#write running-config 123.cfg	

2.2. Команды для Telnet

2.2.1. Авторизация команд конфигурирования (aaa authorization config-commands)

Команда	aaa authorization config-commands no aaa authorization config-commands	
Параметр	none	отсутствует
Состояние по умолчанию	Отключено	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда подключает функцию проверки разрешения на установку команд для пользователя, входящего в систему с VTY (вход с помощью Telnet и SSH). Только добавления этой команды и установки метода проверки полномочий, будет выполняться запрос авторизации при выполнении определенных команд. "no" перед началом команды отключает эту функцию	



Пример	Включить функцию авторизации команд VTY. Switch(config)#aaa authorization config-commands

2.2.2. Выполнение учета (accounting exec)

Команда	accounting line {console vty} exec {start-stop stop-only none} method1 [method2...] no accounting line {console vty} exec	
Параметр	console	вход в систему через последовательный порт (COM-порт)
	vtu	вход в систему через telnet или ssh
	start-stop	отправлять сигнал начала учета или остановки учета, когда пользователь входит в систему или выходит из нее
	stop-only	отправлять запрос остановки учета только при выходе пользователя из системы
	none	не отправлять сигналы начала или остановки учета
	method	список методов учета, поддерживает только ключевое слово tacacs; tacacs использует удаленный сервер TACACS+ для подсчета
Состояние по умолчанию	По умолчанию учет не ведется	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет настроить список методов учета пользователей, входящих в систему через VTY (вход с помощью Telnet и SSH) и Console. Вход с помощью console и vty позволяет задать соответствующий способ учета, в настоящее время поддерживается учет TACACS+. "no" перед началом команды восстанавливает метод учета по умолчанию	
Пример	Настроить учет входа в систему с помощью метода telnet. Switch(config)#accounting line vty exec start-stop tacacs	



2.2.3. Команда настройки учета (accounting command)

Команда	accounting line {console vty} command <1-15> {start-stop stop-only none} method1 [method2...] no accounting line {console vty} command <1-15>	
Параметр	console	вход в систему через последовательный порт (COM-порт)
	vty	вход в систему через telnet или ssh
	command <1-15>	уровень учета команды
	start-stop	отправлять сигнал начала учета или остановки учета, когда пользователь входит в систему или выходит из нее
	stop-only	отправлять запрос остановки учета только при выходе пользователя из системы
	отсутствует	не отправлять сигналы начала или остановки учета
	method	список методов учета, поддерживает только ключевое слово tacacs; tacacs использует удаленный сервер TACACS+ для подсчета
Состояние по умолчанию	По умолчанию метод учета не установлен	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет настроить список методов учета команд с помощью VTY (вход с помощью Telnet и SSH) и Console. "no" перед началом команды восстанавливает метод учета по умолчанию. Вход с помощью console и vty позволяет задать соответствующий способ учета, в настоящее время поддерживается только учет TACACS+. Записывается только информация об остановке учета, независимо от настройки start-stop или stop-only. "no" перед началом команды восстанавливает метод учета по умолчанию	



Пример	Настроить методы учета вводимых команд для входа в систему через telnet, уровень команд 15. Switch(config)#authorization line vty command 15 start-stop tacacs

2.2.4. Включение аутентификации (authentication enable)

Команда	authentication enable method1 [method2...] no authentication enable	
Параметр	method	перечень методов аутентификации, должен указываться среди ключевых слов local, tacacs и radius local: для аутентификации используется локальная база данны tacacs: используется список удаленного сервера TACACS+ для аутентификации radius: аутентификация с помощью удаленного RADIUS-сервера
Состояние по умолчанию	По умолчанию включена локальная аутентификация	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет настроить список разрешенных методов аутентификации. Может быть выбрана локальная аутентификация, аутентификация по протоколам RADIUS, TACACS, либо любая комбинация этих трех методов аутентификации. Если задана комбинация методов аутентификации, выбор предпочтительного метода выполняется слева направо. Если пользователь уже прошел проверку подлинности, менее предпочтительный метод проверки подлинности будет проигнорирован. Если пользователь получил ответ от соответствующего протокола (о том, что он допущен или отвергнут), то не будет предпринята попытки применения следующего метода (исключение из этого правила: если локальная аутентификация была безуспешна, будет предпринята попытка применить следующий метод аутентификации). Если ответ от протокола аутентификации не получен, будет предпринята попытка использовать следующий метод аутентификации. Для того, чтобы можно было использовать метод RADIUS, предварительно должны быть сконфигурированы функции AAA RADIUS-сервера. Для того, чтобы можно было использовать метод TACACS, предварительно должен быть сконфигурирован TACACS-сервер.	



	"no" перед началом команды восстанавливает способ аутентификации по умолчанию
Пример	Настроить разрешенные методы аутентификации tacacs и local. Switch(config)#authentication enable tacacs local

2.2.5. Аутентификация с помощью IP access-class (authentication ip access-class)

Команда	authentication ip access-class {<num-std> <name>} no authentication ip access-class	
Параметр	<num-std>	номер класса доступа для standard numeric ACL, в диапазоне от 1 до 99
	<name>	наименование класса доступа для standard ACL, длина строки символов варьируется от 1 до 32
Состояние по умолчанию	По умолчанию нет привязки ACL к службам Telnet/SSH/Web	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет привязать standard IP ACL к аутентификации через Telnet/SSH/Web. "no" перед началом команды отменит привязку ACL	
Пример	Привязать standard IP ACL к классу доступа access-class 1. Switch(config)#authentication ip access-class 1 in	

2.2.6. Аутентификация с помощью IPv6 access-class (authentication ipv6 access-class)

Команда	authentication ipv6 access-class {<num-std> <name>} no authentication ipv6 access-class	
Параметр	<num-std>	номер класса доступа для standard numeric ACL, в диапазоне 500-599
	<name>	имя класса доступа для стандартного ACL, длина строки от 1 до 32 символов
Состояние по умолчанию	По умолчанию нет привязки ACL к службам Telnet/SSH/Web	



Режим	Режим глобальной конфигурации
Руководство по использованию	Команда позволяет привязать standard IPv6 ACL к аутентификации через Telnet/SSH/Web. "no" перед началом команды отменит привязку ACL
Пример	Привязать standard IPv6 ACL к классу доступа access-class 500. Switch(config)#authentication ipv6 access-class 500 in

2.2.7. Аутентификация с помощью логина (authentication line login)

Команда	authentication line {console vty web} login method1 [method2...] no authentication line {console vty web} login	
Параметр	console	вход в систему через последовательный порт (COM-порт)
	vtty	вход в систему через telnet или ssh
	web	вход в систему через HTTP/HTTPS
	method	перечень методов аутентификации, должен указываться среди ключевых слов local, tacacs и radius local: для аутентификации используется локальная база данных tacacs: используется список удаленного сервера TACACS+ для аутентификации radius: аутентификация с помощью удаленного RADIUS-сервера
Состояние по умолчанию	по	Настройки для авторизации через консоль отсутствуют. По умолчанию для подключения через удаленный терминал и HTTP/HTTPS подключена локальная идентификация
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет сконфигурировать VTY (параметры для инициации сеанса Telnet и SSH), Web и Console, задать приоритет режима аутентификации при регистрации пользователей. Может быть выбрана локальная аутентификация, аутентификация по протоколам RADIUS, TACACS, либо любая комбинация этих методов. Если задана комбинация методов аутентификации, выбор предпочтительного метода выполняется слева направо.	



	Если пользователь уже прошел проверку подлинности, менее предпочтительный метод проверки подлинности будет проигнорирован. Если пользователь получил ответ от соответствующего протокола (о том, что он допущен или отвергнут), то не будет предпринято попытки применения следующего метода (исключение из этого правила: если локальная аутентификация была безуспешна, будет предпринята попытка применить следующий метод аутентификации); если ответ от протокола аутентификации не получен, будет предпринята попытка использовать следующий метод аутентификации. Для того, чтобы можно было использовать метод RADIUS, предварительно должны быть сконфигурированы функции AAA RADIUS-сервера. Для того, чтобы можно было использовать метод TACACS, предварительно должен быть сконфигурирован TACACS-сервер. Команда "authentication line console login" используется только с командой login. Команда "authentication line console login" устанавливает на коммутаторе использование метода регистрации с порта Console. Команда "login" позволяет при регистрации с порта Console использовать пароли, заданные командой "password" для аутентификации. Если задана локальная аутентификация, но локальных пользователей не сконфигурировано, то пользователи могут воспользоваться регистрацией на коммутаторе через порт Console. "no" перед началом команды восстанавливает режим аутентификации, используемый по умолчанию
Пример	Настроить вход в telnet и ssh с удаленной аутентификацией RADIUS. <pre>Switch(config)#authentication line vty login radius</pre>

2.2.8. Установка безопасного IP-адреса для аутентификации (authentication securityip)

Команда	authentication securityip <ip-addr> no authentication securityip <ip-addr>	
Параметр	<ip-addr>	безопасный IP-адрес соответствующего клиента в десятично-точечной записи, который может использоваться для регистрации на коммутаторе
Состояние по умолчанию	по	Безопасный IP-адрес не установлен
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда применяется для установки безопасного IP-адреса для аутентификации через Telnet и HTTP. Пока безопасный IP-адрес не установлен, на IP-адрес клиента, который может быть зарегистрирован на коммутаторе, не накладывается никаких ограничений. После того, как безопасный IP-адрес установлен, только клиенты с безопасными IP-адресами могут регистрироваться на коммутаторе. На коммутаторе может быть сконфигурировано не более 32 безопасных IP-адресов. "no" перед началом команды удаляет установленный безопасный IP-адрес
Пример	Установить 192.168.1.21 в качестве безопасного IP-адреса. Switch(config)#authentication securityip 192.168.1.21

2.2.9. Установка безопасного IPv6-адреса для аутентификации (authentication securityipv6)

Команда	authentication securityipv6 <ipv6-addr> no authentication securityipv6 <ipv6-addr>	
Параметр	<ip-addr>	безопасный IPv6-адрес, который может использоваться для регистрации на коммутаторе
Состояние по умолчанию	Безопасный IPv6-адрес не установлен	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет установить безопасный IPv6-адрес для методов регистрации Telnet и HTTP. Пока безопасный IP-адрес не установлен, на IPv6-адрес клиента, который может быть зарегистрирован на коммутаторе, не накладывается никаких ограничений. После того, как безопасный IPv6-адрес установлен, только клиенты с безопасными IPv6-адресами могут регистрироваться на коммутаторе. На коммутаторе может быть сконфигурировано не более 32 безопасных IPv6-адресов. "no" перед началом команды удаляет установленный безопасный IPv6-адрес	
Пример	Установить безопасный IPv6-адрес 2001:da8:123:1::1. Switch(config)#authentication securityipv6 2001:da8:123:1::1	



2.2.10. Авторизация (authorization)

Команда	authorization line {console vty web} exec method [method...] no authorization line {console vty web} exec	
Параметр	console	вход в систему через последовательный порт (COM-порт)
	vty	вход в систему через telnet или ssh
	web	вход в систему через HTTP/HTTPS
	method	перечень методов авторизации, должен указываться среди ключевых слов local, tacacs и radius local: для аутентификации используется локальная база данных tacacs: используется список удаленного TACACS+ сервера для авторизации radius: аутентификация с помощью удаленного RADIUS-сервера
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет задать перечень методов авторизации пользователя через VTY (параметры для инициации сеанса Telnet и SSH), Web и Console. Может быть выбрана локальная авторизация, авторизация по протоколам RADIUS, TACACS, либо любая комбинация этих методов авторизации. Если задана комбинация методов аутентификации, выбор предпочтительного метода выполняется слева направо. Если пользователь прошел авторизацию по некоторому методу, следующие, менее предпочтительные методы авторизации, игнорируются. Если пользователь получил ответ от соответствующего протокола (о том, что он допущен или отвергнут), то не будет предпринято попытки применения следующего метода; если ответ от протокола авторизации не получен, будет предпринята попытка использовать следующий метод авторизации. Для того, чтобы можно было использовать метод RADIUS, предварительно должны быть сконфигурированы функции AAA RADIUS-сервера. Для того, чтобы можно было использовать метод TACACS, предварительно должен быть сконфигурирован TACACS-сервер.	



	Когда локальные пользователи получают разрешение команды username, но команда авторизации не настроена, пользователи входят в коммутатор по методу RADIUS/TACACS и работают в общем режиме. "no" перед началом команды восстанавливает авторизацию по умолчанию
Пример	Настроить метод авторизации telnet на RADIUS. Switch(config)#authorization line vty exec radius

2.2.11. Команда авторизации через VTY (authorization line vty command)

Команда	authorization line vty command <1-15> {local radius tacacs} (none) no authorization line vty command <1-15>	
Параметр	command <1-15>	Уровень охвата заказов на авторизацию 1~15
	local	авторизация осуществляется локально
	radius	авторизация для удаленных серверов RADIUS
	tacacs	авторизация для удаленных серверов Tacas
	отсутствует	режим авторизации не указан
Состояние по умолчанию	Способ авторизации не задан	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать способ и задать приоритет режима авторизации при регистрации пользователей через VTY (параметры для инициации сеанса Telnet и SSH). Может быть выбрана авторизация локальная авторизация, авторизация по протоколам RADIUS и TACACS, либо комбинация этих методов. Если задана комбинация методов авторизации, приоритет имеет первый метод, остальные идут в порядке убывания. Если пользователь прошел авторизацию по методу высшего приоритета, следующие методы авторизации игнорируются. До тех пор, пока соответствующий метод авторизации выдает ответ о допуске или отказе, попытки применения следующего метода не последует. Попытка применить следующий метод авторизации будет предпринята при отсутствии четкого ответа. Для того, чтобы использовать метод RADIUS, предварительно должны быть сконфигурированы функции AAA RADIUS-сервера. Для того,	



	чтобы использовать метод TACACS, предварительно должен быть сконфигурирован TACACS-сервер. None - это метод экранирования, который может быть только последним. При этом происходит возврат непосредственно к пройденной авторизации и успешная настройка команды. "no" перед началом команды восстанавливает режим по умолчанию
Пример	Задать команду "level 1" метода авторизации для регистрации пользователя в telnet как TACACS. Switch(config)#authorization line vty command 1 tacacs

2.2.12. Удаление команды VTY (clear line vty <0-31>)

Команда	clear line vty <0-31>	
Параметр	<0-31>	назначенная строка
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	После ввода этой команды необходимо подтвердить ее выполнение: "Confirm[Y/N] ", при вводе "Y" или "y", выполняется удаление; при вводе " ? ", удаление не выполняется, выводится уведомление. При вводе других символов, удаление не выполняется	
Пример	Пользователи Admin, вынужденные входить в систему через VTY (с помощью Telnet или SSH), отключены. Switch#clear line vty 0 Confirm[Y/N]: y [OK]	

2.2.13. Удаление секретного ключа (crypto key clear rsa)

Команда	crypto key clear rsa	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	



Руководство по использованию	Эта команда используется для очистки секретного ключа ssh и закрытия службы ssh
Пример	Очистить секретный ключ ssh и закрыть службу ssh. Switch#crypto key clear rsa ssh host key is cleared successfully. ssh is closed successfully

2.2.14. Количество строк на терминале (terminal length)

Команда	terminal length <0-512> terminal no length	
Параметр	<0-512>	Число строк, отображаемых на экране, в пределах от 0 до 512 (0 соответствует безостановочному отображению символов)
Состояние по умолчанию	25 строк	
Режим	Привилегированный режим	
Руководство по использованию	Позволяет задать число строк, отображаемых на терминале, если имеются еще данные для отображения, не уместившиеся на экране, будет выведено сообщение More (Еще). Для вывода на экран последующей информации нажмите любую клавишу Команда "terminal no length" отменяет операцию переключения экрана и восстанавливает отображение всего контента	
Пример	Установить вывод по 20 строк на экране. Switch#terminal length 20	

2.2.15. Telnet

Команда	telnet [vrf <vrf-name>] [<ip-addr> <ipv6-addr> host <hostname>][<port>]	
Параметр	<vrf-name>	имя VRF
	<ip-addr>	IP-адрес удаленного хоста; десятично-точечная запись
	<ipv6-addr>	IPv6-адрес удаленного хоста
	<hostname>	имя удаленного хоста, максимальное количество символов 64



	<port>	номер порта, в диапазоне от 0 до 65535
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Эта команда используется, когда коммутатор работает как Telnet-клиент, для регистрации на других удаленных хостах для их настройки. Когда коммутатор работает как Telnet-клиент, он может устанавливать TCP-соединение только с одним удаленным хостом. Если требуется соединение с другим удаленным хостом, текущее TCP-соединение должно быть сброшено «горячей» командой «CTRL+ \». Для доступа по telnet необходимо предварительно установить соответствие между именем хоста и IP/IPv6-адресом. Требующиеся для этого команды см. в ip host и ipv6 host. Если хост имеет и IPv4-адрес и IPv6-адрес, для доступа по telnet следует использовать IPv6-адрес	
Пример	Установить связь с хостом с IP-адресом 20.1.1.1 путем доступа по Telnet. <pre>Switch#telnet 20.1.1.1 23 Connecting Host 20.1.1.1 Port 23... Service port is 23 Connected to 20.1.1.1 login: 123 password: *** router></pre>	

2.2.16. Включение Telnet-сервера (telnet server enable)

Команда	telnet server enable no telnet server enable	
Параметр	none	отсутствует
Состояние по умолчанию	Telnet-сервер включен	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда может быть выполнена только через порт Console. Этой командой можно разрешить или запретить доступ по Telnet. Администратор может включить или отключить функцию доступа к коммутатору по Telnet. Команда “no telnet-server enable” выключает функцию Telnet-сервера
Пример	Выключить Telnet-сервер для коммутатора. Switch(config)#no telnet server enable

2.2.17. Соединение Telnet-сервера (telnet-server max-connection)

Команда	telnet-server max-connection {<max-connection-number> default}	
Параметр	<max-connection-number>	максимальное число соединений, поддерживаемых Telnet в диапазоне от 5 до 16
	default	восстанавливает настройки, заданные по умолчанию
Состояние по умолчанию	Установлено максимальное число соединений, равное 5	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать максимальное число соединений Telnet, поддерживаемых коммутатором	
Пример	Задать максимальное число соединений Telnet, поддерживаемых коммутатором, равным 10. Switch(config)#telnet-server max-connection 10	

2.2.18. Число попыток повторной аутентификации через SSH-сервер

Команда	ssh-server authentication-retries <authentication-retries> no ssh-server authentication-retries	
Параметр	<authentication-retries>	число попыток аутентификации, диапазон значений от 1 до 10
Состояние по умолчанию	Задано число попыток аутентификации SSH равное 3	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда задает число попыток аутентификации SSH. Команда “no ssh-server authentication-retries” восстанавливает число попыток аутентификации SSH, используемое по умолчанию
Пример	Установить число попыток аутентификации SSH-клиентов равное 5. Switch(config)#ssh-server authentication-retries 5

2.2.19. Включение SSH-сервера (ssh-server enable)

Команда	ssh-server enable no ssh-server enable	
Параметр	none	отсутствует
Состояние по умолчанию	Функция SSH-сервера выключена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда включает функцию SSH-сервера на коммутаторе. Для того чтобы клиент SSH мог зайти в коммутатор, необходимо настроить пользователя SSH и включить функцию SSH на коммутаторе. Команда “no ssh-server enable” выключает функцию SSH-сервера	
Пример	Включить SSH-сервер на коммутаторе. Switch(config)#ssh-server enable < modulus > модуль, который будет использован для вычисления ключа хоста; диапазон значений	

2.2.20. Создание ключа безопасности для хоста (ssh-server host-key create rsa)

Команда	ssh-server host-key create rsa [modulus < modulus >]	
Параметр	< modulus >	модуль, который будет использован для вычисления ключа хоста; диапазон значений от 768 до 2048. Значение по умолчанию: 1024
Состояние по умолчанию	Система использует ключ, который ssh-сервер сгенерировал при первом запуске	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Эта команда используется для создания новых ключей безопасности для хоста. Когда SSH-клиент регистрируется на сервере, новый ключ хоста используется для аутентификации. После того как ключ создан и сохранен при помощи команды "write", система будет постоянно использовать этот ключ для аутентификации. Шифрование и дешифрование ключа может занимать значительное время, а некоторые клиенты не поддерживают ключи, сгенерированные модулем 2048, рекомендуется использовать ключ, сгенерированный модулем 1024 бит, заданный по умолчанию. Для отключения сервиса SSH команда отсутствует
Пример	Создать для хоста новый ключ. Switch(config)#ssh-server host-key create rsa

2.2.21. Соединение SSH-сервера (ssh-server max-connection)

Команда	ssh-server max-connection {<max-connection-number> default}	
Параметр	<max-connection-number>	максимальное число поддерживаемых SSH соединений, в пределах от 5 до 16
	default	восстанавливает настройки, заданные по умолчанию
Состояние по умолчанию	Установлено максимальное число соединений, равное 5	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать максимальное число соединений SSH, поддерживаемых коммутатором	
Пример	Задать максимальное число соединений SSH, поддерживаемых коммутатором, равным 10. Switch(config)#ssh-server max-connection 10	

2.2.22. Тайм-аут SSH-сервера (ssh-server timeout)

Параметр	<timeout>	значение времени таймера в диапазоне от 10 до 600 секунд			
Состояние по умолчанию	Установлено время аутентификации SSH 180 с	максимального	времени	ожидания	



Режим	Режим глобальной конфигурации
Руководство по использованию	Позволяет задать максимальное время ожидания аутентификации SSH. Команда “no ssh-server timeout” восстанавливает время таймера аутентификации SSH, используемое по умолчанию
Пример	Установить время таймера аутентификации SSH 240 секунд. Switch(config)#ssh-server timeout 240

2.2.23. Вывод секретного ключа (show crypto key)

Команда	show crypto key	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Выводит информацию о секретных ключах ssh	
Пример	Показать секретный ключ ssh. Switch#show crypto key	

2.2.24. Вывод SSH-сервера (show ssh-server)

Команда	show ssh-server	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Команда выводит на экран информацию о состоянии SSH-сервера и информацию о зарегистрированных пользователях	



Пример	Вывести на экран информацию о состоянии SSH-сервера и информацию о зарегистрированных пользователях. <pre>Switch#show ssh-server</pre> ssh server is enabled ssh-server timeout 180s ssh-server authentication-retries 3 ssh-server max-connection number 6 ssh-server login user number 2

2.2.25. Вывод данных о пользователе Telnet (show telnet login)

Команда	show telnet login	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Команда выводит на экран информацию о пользователе Telnet, подключенном к коммутатору	
Пример	Показать информацию о клиенте Telnet <pre>Switch#show telnet login</pre> Authenticate login by local Login user: qtech	

2.2.26. Вывод данных о пользователях (show users)

Команда	show users	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Команда выводит информацию о пользователях, вошедших в систему через telnet или ssh. Она включает номер линии, имя пользователя и его IP-адрес	
	Поскольку в настоящее время поддерживается 16 пользователей telnet и 16 пользователей ssh, vty0-15 используются для telnet, а 16-31 - для ssh	



Пример	Показать информацию о пользователях Switch#show users Line User Location vty 16 qtech 192.168.1.1 vty 0 admin 192.168.1.2 vty 17 mab 192.168.1.13 vty 1 test 192.168.1.40

2.2.27. Пользователи (who)

Команда	who	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Все режимы конфигурации	
Руководство по использованию	Показывает пользователей, зашедших через vty	
Пример	Показать пользователей, зашедших через vty. Switch#who Telnet user qtech login from 192.168.1.20	

2.3. Команды для настройки IP-адресов коммутатора

2.3.1. Интерфейс VLAN (interface vlan)

Команда	interface vlan <vlan-id> no interface vlan <vlan-id>	
Параметр	<vlan-id>	числовой идентификатор VLAN ID, присвоенный VLAN, в пределах от 1 до 4094
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда позволяет войти в режим настройки интерфейса VLAN. Перед тем, как настраивать VLAN, необходимо убедиться, что он создан. Для выхода из режима настройки интерфейсов VLAN в Режим глобальной конфигурации конфигурирования используйте команду "exit". "no" в начале команды удаляет существующий интерфейс VLAN
Пример	Войти в режим настройки интерфейса VLAN для VLAN1. <pre>Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#</pre>

2.3.2. IP-адрес (ip address)

Команда	ip address <ip-address> <mask> [secondary] no ip address [<ip-address> <mask>] [secondary]	
Параметр	<ip-address>	IP-адрес в десятично-точечной записи
	<mask>	маска подсети в десятично-точечной записи
	[secondary]	указывает, что введенный IP-адрес является вторичным IP-адресом
Состояние по умолчанию	IP-адрес не задан	
Режим	Режим настройки интерфейса VLAN	
Руководство по использованию	Команда позволяет настроить IP-адрес и маску для коммутатора. Перед тем, как присваивать IP-адрес коммутатору необходимо создать интерфейс VLAN. "no" перед началом команды удаляет выполненную настройку IP-адреса	
Пример	Установить IP-адрес 10.1.128.1/24 для интерфейса VLAN1. <pre>Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip address 10.1.128.1 255.255.255.0 Switch(Config-if-Vlan1)#exit Switch(config)#</pre>	



2.3.3. IPv6-адрес (ipv6 address)

Команда	ipv6 address <ipv6address prefix-length> [eui-64] no ipv6 address <ipv6address prefix-length> [eui-64]	
Параметр	<ipv6address >	префикс IPV6-адреса
	<prefix-length>	длина префикса IPV6-адреса, в пределах от 3 до 128
	[eui-64]	означает, что IPV6-адрес для интерфейса eui64 interface id будет создан автоматически
Состояние по умолчанию	При поставке коммутатора IPv6-адрес не настраивается	
Режим	Режим настройки интерфейса VLAN	
Руководство по использованию	Команда позволяет задать для интерфейса агрегируемый глобальный одноадресный (unicast) адрес, уникальный локальный адрес и локальный адрес канала. Префикс IPV6-адреса не должен быть групповым (multicast) адресом, либо IPV6-адресом другого специального применения. Разным интерфейсам VLAN уровня 3 запрещено совместно использовать один и тот же префикс адреса. Как и для любого глобального unicast-адреса, префикс должен быть в пределах от 2001:: до 3fff::, при этом его длина должна быть не менее 3. Длина префикса локального адреса сайта или канала не должна быть менее 10. "no" перед началом команды удаляет заданный IPv6 адрес	
Пример	Задать IPV6-адрес интерфейса третьего уровня для VLAN1. Задать префикс 2001:3f:ed8::99, длина префикса 64. <pre>Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64 Switch(Config-if-Vlan1)#exit Switch(config)#</pre>	

2.3.4. Включение ip-адреса BootP-клиента (ip bootp-client enable)

Команда	ip bootp-client enable no ip bootp-client enable	
Параметр	none	отсутствует
Состояние по умолчанию	BootP-клиент выключен	



Режим	Режим настройки интерфейса VLAN
Руководство по использованию	Команда конфигурирует коммутатор, как BootP-клиент для получения IP-адреса и адреса шлюза. Существует три метода конфигурирования IP-адреса коммутатора: ручное конфигурирование, по протоколу BootP и по протоколу DHCP. Эти три метода взаимоисключающие, использование одновременно двух методов не допускается. Для получения IP-адреса по BootP в сети должен функционировать DHCP-сервер или BootP-сервер. "no" перед началом команды отключает функцию BootP Client и снимает IP-адрес, полученный по протоколу BootP
Пример	Получить IP-адрес, используя протокол BootP. <pre>Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip bootp-client enable Switch(Config-if-Vlan1)#exit Switch(config)#</pre>

2.3.5. Включение IP-адреса DHCP клиента (ip dhcp-client enable)

Команда	ip dhcp-client enable no ip dhcp-client enable	
Параметр	none	отсутствует
Состояние по умолчанию	Конфигурирование с помощью DHCP-клиента выключено	
Режим	Режим настройки интерфейса VLAN	
Руководство по использованию	Команда используется для настройки коммутатора для работы в качестве DHCP-клиента и получения IP-адресов и адреса шлюза по протоколу DHCP. Для получения IP-адреса по DHCP в сети должен функционировать DHCP-сервер. Настройка IP-адреса вручную, настройка по DHCP и BootP это три взаимоисключающих метода конфигурирования, использование одновременно двух методов не допускается. "no" перед началом команды выключает настройку для работы в качестве DHCP-клиента и снимает IP-адрес, полученный по протоколу DHCP	



Пример	Сконфигурировать IP-адрес по протоколу DHCP. Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip dhcp-client enable Switch(Config-if-Vlan1)#exit Switch(config)#

2.4. Команды для настройки протокола SNMP

2.4.1. Включение RMON (rmon enable)

Команда	rmon enable no rmon enable	
Параметр	none	отсутствует
Состояние по умолчанию	Функции RMON выключены	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда включает протокол удаленного мониторинга сети RMON. "no" перед началом команды выключает RMON	
Пример	Отключить протокол RMON. Switch(config)#no rmon enable	

2.4.2. Вывод объекта oid в частной базе MIB (show private-mib oid)

Команда	show private-mib oid	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим и Режим глобальной конфигурации	
Руководство по использованию	Команда показывает исходный идентификатор объекта oid в частной административной базе данных MIB Позволяет выполнить проверку начального oid частного mib с помощью команды show private-mib oid	



Пример	Показать исходный идентификатор объекта oid в частной административной базе данных MIB Switch#show private-mib oid Private MIB OID: 1.3.6.1.4.1.27514

2.4.3. Вывод SNMP (show snmp)

Команда	show snmp	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим и Режим глобальной конфигурации	
Руководство по использованию	Отображает всю информацию счетчиков SNMP	
Пример	Показать всю информацию счетчиков SNMP. Switch#show snmp 0 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 0 Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0 Set-request PDUs 0 SNMP packets output 0 Too big errors (Max packet size 1500) 0 No such name errors 0 Bad values errors 0 General errors 0 Get-response PDUs 0 SNMP trap PDUs	



2.4.4. Вывод ID системы SNMP (show snmp engineid)

Команда	show snmp engineid	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим и Режим глобальной конфигурации	
Руководство по использованию	Выводит на экран ID вычислительной подсистемы	
Пример	Вывести на экран ID вычислительной подсистемы. Switch#show snmp engineid SNMP engineID: 3138633303f1276c	

2.4.5. Вывод группы SNMP (show snmp group)

Команда	show snmp group	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим и Режим глобальной конфигурации	
Руководство по использованию	Команда выводит на экран информацию о группе	
Пример	Вывести на экран информацию о группе. Switch#show snmp group Group Name: initial Security Level: noAuthnoPriv Read View: one Write View: <no writeview specified> Notify View: one	



2.4.6. Вывод MIB SNMP (show snmp mib)

Команда	show snmp mib	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим и Режим глобальной конфигурации	
Руководство по использованию	Команда выводит на экран все MIB, поддерживаемые коммутатором	
Пример	Вывести на экран все MIB, поддерживаемые коммутатором. Switch#show snmp mib	

2.4.7. Вывод статуса SNMP (show snmp status)

Команда	show snmp status	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим и Режим глобальной конфигурации	
Руководство по использованию	Команда выводит на экран информацию о конфигурировании SNMP	
Пример	Вывести на экран информацию о конфигурировании SNMP. Switch#show snmp status Trap enable RMON enable Community Information: V1/V2c Trap Host Information: V3 Trap Host Information: Security IP Information:	



2.4.8. Вывод данных о пользователе SNMP (show snmp user)

Команда	show snmp user	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим и Режим глобальной конфигурации	
Руководство по использованию	Команда выводит на экран информацию о пользователе	
Пример	Вывести на экран информацию о пользователе. Switch#show snmp user User name: qtech123 Engine ID: 1234567890 Auth Protocol: MD5 Priv Protocol: DES-CBC Row status: active	

2.4.9. Вывод информации SNMP (show snmp view)

Команда	show snmp view	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим и Режим глобальной конфигурации	
Руководство по использованию	Команда выводит на экран информацию для просмотра	
Пример	Вывести сводную информацию. Switch#show snmp view View Name : readview 1. -Included active 1.3. Excluded active	



2.4.10. Сообщество SNMP-сервера (snmp-server community)

Команда	<pre>snmp-server community {ro rw} {0 7} <string> [access {<num-std> <name>}] [ipv6-access {<ipv6-num-std> <ipv6-name>}] [read <read-view-name>] [write <write-view-name>]</pre> <pre>no snmp-server community {ro rw} {0 7} <string> [access {<num-std> <name>}] [ipv6-access {<ipv6-num-std> <ipv6-name>}]</pre>	
Параметр	{ro rw}	указывает права доступа к базе данных MIB, ro задает доступ только по чтению, rw - доступ по чтению/записи
	{0 7}	если параметр key имеет значение 0, указанная строка community будет в открытом виде, если параметр key имеет значение 7, строка community будет зашифрована
	<string>	строка community (сообщества)
	<num-std>	номер класса доступа для standard numeric ACL, в диапазоне от 1 до 99
	<name>	наименование класса доступа для standard ACL, длина строки символов в диапазоне от 1 до 32
	<ipv6-num-std>	номер класса доступа для нумерованного standard IPv6 ACL для данного сообщества в пределах 500-599
	<ipv6-name>	наименование класса доступа для standard IPv6 ACL, длина строки символов составляет от 1 до 32
	<read-view-name>	имя SNMP View для чтения, включает от 1 до 32 символов
	<write-view-name>	имя SNMP View для чтения и записи, включает от 1 до 32 символов
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда конфигурирует для коммутатора строку community. Коммутатором поддерживаются не более 4 строк "community". Реализует контроль доступа для конкретного "community view", связывая имя "community" с конкретным представлением, доступным для чтения, или представлением, доступным для записи. "no" в начале команды удаляет сконфигурированную строку "community"
Пример	Задать для строки "community" значение "private" и разрешить доступ по чтению/записи. <pre>Switch(config)#snmp-server community rw 0 private</pre> Удалить строку "community" с именем "private". <pre>Switch(config)#no snmp-server community 0 private</pre>

2.4.11. Включение SNMP-сервера (snmp-server enable)

Команда	snmp-server enable no snmp-server enable	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Подключает функцию прокси-сервера SNMP на коммутаторе. Прокси-сервер SNMP должен быть включен этой командой до того, как станет возможным конфигурирование коммутатора программным обеспечением управления сетью. Команда "no snmp-server enable" выключает прокси-сервер SNMP	
Пример	Подключить коммутатор как прокси-сервер SNMP. <pre>Switch(config)#snmp-server enable</pre>	

2.4.12. Включение сообщений прерывания SNMP-сервера (snmp-server enable traps)

Команда	snmp-server enable traps no snmp-server enable traps	
Параметр	none	отсутствует



Состояние по умолчанию	Отправка сообщений Trap отключена
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда включает на коммутаторе отправку сообщения Trap (прерывание). Если включена функция сообщений Trap, они будут отправлять при изменении UP/Down порта устройства или системы, устройство будет отправлять сообщения Trap в NMS, которая принимает Trap-сообщения. "no" в начале команды отключает функцию отправки сообщений Trap на коммутаторе
Пример	Включить отправку сообщений Trap. Switch(config)#snmp-server enable traps

2.4.13. ID SNMP-сервера (snmp-server engineid)

Команда	snmp-server engineid <engine-string> no snmp-server engineid		
Параметр	<engine-string>	id	вычислительной подсистемы в шестнадцатеричной форме, длина от 1 до 32 символов
Состояние по умолчанию	ID компании + локальный MAC-адрес		
Режим	Режим глобальной конфигурации		
Руководство по использованию	Команда позволяет задать идентификатор id вычислительной подсистемы. "no" в начале команды восстанавливает engine ID по умолчанию		
Пример	Задать в качестве id вычислительной подсистемы A66688999F Switch(config)#snmp-server engineid A66688999F		



2.4.14. Группа SNMP-сервера (snmp-server group)

Команда	<pre>snmp-server group <group-string> {NoauthNopriv AuthNopriv AuthPriv} [[read <read-string>] [write <write-string>] [notify <notify-string>]] [access {<num-std> <name>}] [ipv6-access {<ipv6-num-std> <ipv6-name>}] no snmp-server group <group-string> {NoauthNopriv AuthNopriv AuthPriv} [access {<num-std> <name>}] [ipv6-access {<ipv6-num-std> <ipv6-name>}]</pre>	
Параметр	<group-string>	имя группы, содержит 1-32 символа
	NoauthNopriv	аутентификация и шифрование будут выключены
	AuthNopriv	аутентификация будет включена, но шифрование применяться не будет
	AuthPriv	будут включены и шифрование, и аутентификация
	<read-string>	имя считываемого вида, длина имени - от 1 до 32 символов
	<write-string>	имя записываемого вида, длина имени - от 1 до 32 символов
	<notify-string>	имя вида, для которого посылается сообщение Trap, длина имени - от 1 до 32 символов
	<num-std>	номер класса доступа для standard numeric ACL, в диапазоне от 1 до 99
	<name>	наименование класса доступа для standard ACL, длина строки символов в диапазоне от 1 до 32
	<ipv6-num-std>	номер класса доступа для standard numeric IPv6 ACL для данного community в диапазоне 500-599
	<ipv6-name>	наименование класса доступа для standard IPv6 ACL, длина строки символов составляет от 1 до 32
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда конфигурирует на коммутаторе новую группу. По умолчанию системой сконфигурирован вид сводной информации с именем v1defaultviewname. Рекомендуется использовать этот вид как имя view. Если считываемый или записываемый виды не сконфигурированы, соответствующая операция не будет выполняться. "no" в начале команды удаляет соответствующую группу	
Пример	Создать группу с именем "CompanyGroup", с использованием аутентификации и шифрования, с доступом по чтению и именем "readview", операция записи недоступна. Switch (config)#snmp-server group CompanyGroup AuthPriv read readview	
	AuthPriv	будут включены и шифрование, и аутентификация
	<read-string>	имя считываемого вида, длина имени - от 1 до 32 символов
	<write-string>	имя записываемого вида, длина имени - от 1 до 32 символов
	<notify-string>	имя вида, для которого посылается сообщение Trap, длина имени - от 1 до 32 символов
	<num-std>	номер класса доступа для standard numeric ACL, в диапазоне от 1 до 99
	<name>	наименование класса доступа для standard ACL, длина строки символов в диапазоне от 1 до 32
	<ipv6-num-std>	номер класса доступа для standard numeric IPv6 ACL для данного community в диапазоне 500-599
	<ipv6-name>	наименование класса доступа для standard IPv6 ACL, длина строки символов составляет от 1 до 32
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда конфигурирует на коммутаторе новую группу. По умолчанию системой сконфигурирован вид сводной информации с именем v1defaultviewname. Рекомендуется использовать этот вид как имя view. Если считываемый или записываемый виды не сконфигурированы, соответствующая операция не будет выполняться. "no" в начале команды удаляет соответствующую группу	



Пример	Создать группу с именем "CompanyGroup", с использованием аутентификации и шифрования, с доступом по чтению и именем "readview", операция записи недоступна. Switch (config)#snmp-server group CompanyGroup AuthPriv read readview

2.4.15. Хост SNMP-сервера (snmp-server host)

Команда	<pre>snmp-server host { <host-ipv4-address> <host-ipv6-address> } {v1 v2c v3 {NoauthNopriv AuthNopriv AuthPriv}} <user-string> no snmp-server host { <host-ipv4-address> <host-ipv6-address> } {v1 v2c v3 {NoauthNopriv AuthNopriv AuthPriv}} <user-string></pre>	
Параметр	<host-ipv4-address>	IP-адрес рабочей станции NMS, которая принимает сообщения Trap
	<host-ipv6-address>	IPv6-адрес рабочей станции NMS, которая принимает сообщения Trap
	v1 v2c v3	номер версии протокола, используемый для сообщений Trap
	NoauthNopriv	аутентификация и шифрование будут выключены
	AuthNopriv	аутентификация будет включена, но шифрование применяться не будет
	AuthPriv	будут включены и шифрование, и аутентификация
	<user-string>	строка "community" для сообщений Trap в версиях протокола v1/v2c. В версии v3 эта строка является именем пользователя
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	



Руководство по использованию	В версиях протокола SNMP v1 и v2c эта команда конфигурирует строку Trap community и IPv4 или IPv6-адрес станции управления SNMP, которая будет принимать сообщения Trap. В версии протокола v3 этой командой конфигурирует IPv4 или IPv6-адрес станции управления SNMP сервера, имя пользователя и уровень безопасности. Строка community для сообщений Trap, сконфигурированная этой командой, используется в качестве строки community, заданной по умолчанию для сообщений RMON. Если для событий RMON строк "community" не сконфигурировано, будет использована строка "community", сконфигурированная этой командой. В остальных случаях для сообщений RMON Trap будет использоваться строка RMON. Эта команда позволяет задать IPv4 или IPv6 адреса станции управления, принимающей сообщения SNMP Trap, однако для версий v1 и v2c всего может быть задано не более 8 IPv4 или IPv6-адресов. "no" в начале команды отменяет адреса IPv4 или IPv6
Пример	Сконфигурировать IP-адрес для получения сообщений Trap. <pre>Switch(config)#snmp-server host 1.1.1.5 v1 usertrap</pre>

2.4.16. Безопасный IP-адрес SNMP-сервера (snmp-server securityip)

Команда	snmp-server securityip {<ipv4-address> <ipv6-address>} no snmp-server securityip {<ipv4-address> <ipv6-address>}	
Параметр	<ipv4-address>	безопасный IPv4-адрес NMS, десятично-точечная запись
	<ipv6-address>	безопасный IPv6-адрес NMS, десятично-точечная запись
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Конфигурирует права доступа с безопасного IPv4- или IPv6-адреса станции NMS административного управления коммутатором. Поскольку команда влияет только на IPv4- или IPv6-адрес станции администрирования NMS и безопасный IPv4- или IPv6-адрес, сконфигурированный этой командой, в результате чего пакеты SNMP, посылаемые станцией могут обрабатываться коммутатором, то эта команда применима только для SNMP. Эта команда позволяет задать IPv4- или IPv6-адрес сетевой станции управления, принимающей сообщения SNMP Trap, однако всего может быть задано не более 20 IP-адресов.	



	"no" в начале команды удаляет сконфигурированный безопасный IPv4- или IPv6-адрес
Пример	Сконфигурировать безопасный IP-адрес станции администрирования NMS. Switch(config)#snmp-server securityip 1.1.1.5

2.4.17. Включение безопасного IP-адреса SNMP-сервера (snmp-server securityip enable)

Команда	snmp-server securityip {enable disable}	
Параметр	enable disable	включить или выключить функцию проверки разрешенного IP-адреса для доступа на SNMP
Состояние по умолчанию	Функция проверки безопасного IP-адреса включена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда включает или выключает функцию проверки безопасного IP-адреса NMS	
Пример	Выключить функцию проверки безопасного IP-адреса. Switch(config)#snmp-server securityip disable	

2.4.18. Источник trap-сообщений SNMP-сервера (snmp-server trap-source)

Команда	snmp-server trap-source {<ipv4-address> <ipv6-address>} no snmp-server trap-source {<ipv4-address> <ipv6-address>}	
Параметр	<ipv4-address>	IPv4-адрес для отправки пакета trap в десятичной системе
	<ipv6-address>	IPv4-адрес для отправки пакета trap в шестнадцатеричном формате
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда устанавливает IP-адреса источника для отправки trap-сообщений. Если настройка отсутствует, выбирается адрес источника в соответствии с адресом интерфейса фактического отправленного пакета trap. При настройке IP-адреса установленный адрес источника будет использоваться в качестве адреса источника пакета trap. "no" в начале команды удаляет настройку
Пример	Выбрать IP-адрес для отправки пакета сообщений trap. Switch(config)#snmp-server trap-source 1.1.1.5

2.4.19. Пользователь SNMP-сервера (snmp-server user)

Команда	<pre>snmp-server user <use-string> <group-string> [{authPriv [auth {md5 sha} <word>]} {authNoPriv [{3des aes des} <word>]} [auth {md5 sha} <word>]} [access {<num-std> <name>}] [ipv6-access {<ipv6-num-std> <ipv6-name>}]} no snmp-server user <user-string> [access {<num-std> <name>}] [ipv6- access {<ipv6-num-std> <ipv6-name>}]}]</pre>	
Параметр	<use-string>	имя пользователя, длина имени от 1 до 32 символов;
	<group-string>	имя группы, в которую добавляется пользователь, длина имени от 1 до 32 символов
	authPriv	использовать DES для шифрования данных
	authNoPriv	не использовать DES для шифрования данных
	auth	выполнить аутентификацию пакета
	md5	применить алгоритм HMAC MD5 для аутентификации
	sha	применить алгоритм HMAC SHA для аутентификации
	3des	аутентификация пакетов с шифрованием 3DES
	aes	аутентификация пакетов с шифрованием AES
	des	аутентификация пакетов с шифрованием DES



	<word>	пароль пользователя, длина пароля от 8 до 32 символов
	<num-std>	номер класса доступа для standard numeric ACL, в диапазоне от 1 до 99
	<name>	наименование класса доступа для standard ACL, длина строки символов в диапазоне от 1 до 32
	<ipv6-num-std>	номер класса доступа для нумерованного standard IPv6 ACL для данного community в пределах 500-599
	<ipv6-name>	со списком разрешенных адресов IPv6 ACL, длина строки символов в диапазоне от 1 до 32
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет добавить пользователя в существующую группу. Если шифрование и аутентификация не сконфигурированы, то по умолчанию они выключены. Если шифрование включено, аутентификация также должна быть выполнена. Если при удалении пользователя указано правильное имя пользователя, но некорректное имя группы, пользователь будет удален. "no" в начале команды удаляет пользователя	
Пример	Добавить пользователя с именем tester в группу с именем UserGroup, при аутентификации должен использоваться алгоритм HMAC md5, пароль hellohello; и удалить пользователя. <pre>Switch (config)#snmp-server user tester UserGroup authNoPriv auth md5 hellohello</pre> <pre>Switch (config)#no snmp-server user tester</pre>	

2.4.20. Информация SNMP-сервера (snmp-server view)

Команда	snmp-server view <view-string> <oid-string> {include exclude} no snmp-server view <view-string> [<oid-string>]	
Параметр	<view-string>	имя вида, содержащая от 1 до 32 символов
	<oid-string>	номер OID или имя соответствующего узла, длина имени 1-255 символов



	include exclude	включить или исключить этот OID
Состояние по умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	С помощью этой команды создаются или обновляются сконфигурированные виды сводной информации. Команда поддерживает не только ввод символьной строки переменной OID в качестве параметра, она также поддерживает ввод, при котором в качестве параметра используется имя узла. "no" в начале команды удаляет соответствующий сконфигурированный вид	
Пример	Создать вид сводной информации с именем "readview", в который включен узел iso и исключен узел iso.3, а затем удалить их. <pre>Switch(config)#snmp-server view readview iso include Switch(config)#snmp-server view readview iso.3 exclude Switch(config)#no snmp-server view readview</pre>	

2.4.21. Включение уведомлений об обновлении порта (switchport updown notification enable)

Команда	switchport updown notification enable no switchport updown notification enable	
Параметр	none	отсутствует
Состояние по умолчанию	Отправка сообщений trap при изменении статуса порта UP/Down	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда позволяет включить/отключить отсылку сообщений trap на порт по событию UP/DOWN. Команда управляет отправкой trap сообщения о наличии или отсутствии состояния UP/DOWN на порту. По умолчанию сообщения trap отсылаются на все порты по событию UP/DOWN после включения snmp trap. "no" в начале команды удаляет настройку	



Пример	Отключить функцию отправки trap-сообщения на порт 1/0/1 по событию UP/DOWN. <pre>Switch(config)#interface eth 1/0/1 Switch(config-if-ethernet1/0/1)#no switchport updown notification enable Switch(config-if-ethernet1/0/1)#show running-config current-mode ! Interface Ethernet1/0/1 no switchport updown notification enable</pre>

2.5. Команды для обновления коммутатора

2.5.1. Копирование (FTP) (copy (FTP))

Команда	copy <source-url> <destination-url> [ascii binary]			
Параметр	<source-url>	местонахождение исходных файлов или каталогов, которые требуется скопировать;		
	<destination-url>	адрес назначения, в которое требуется скопировать исходные файлы или каталоги;		
	ascii	использовать стандарт ASCII		
	binary	при передаче файла использовать двоичную систему (метод передачи по умолчанию)		
Состояние по умолчанию	Не задано			
Режим	Привилегированный режим			
Руководство по использованию	Команда позволяет принимать и передавать файлы через FTP. Когда URL соответствует FTP-адресу, форма команды следующая: ftp: //<username>:<password>@{<ipaddress> <ipv6address> <hostname>}/<filename>, где <username> является именем пользователя FTP, <password> пароль пользователя FTP, <ipaddress> <ipv6address> IPv4- или IPv6-адрес FTP сервера/клиента, <hostname> имя хоста, соответствующее IPv6-адресу; не поддерживается загрузка и выгрузка файлов с хостов, соответствующих IPv4-адресу, <filename> имя файла, выгружаемого или загружаемого по FTP. Специальные ключевые слова для имени файла: <table><tr><th>Ключевое слово</th><th>Объяснение</th></tr></table>		Ключевое слово	Объяснение
Ключевое слово	Объяснение			



	running-config Файлы текущей рабочей конфигурирования startup-config Это означает, что при использовании команды copy running-config startup-config файл конфигурирования будет перезагружен. nos.img Системные файлы bootrom Системные файлы начальной загрузки Эта команда поддерживает подсказки командной строки, т.е. пользователь может вводить команды в следующем виде: copy <filename> ftp: // или copy ftp: // <filename> , и по нажатию Enter, система выдаст следующие подсказки: ftp server ip/ipv6 address [x.x.x.x]/[x: x: : x: x] > ftp username> ftp password> ftp filename> Запрос адреса FTP-сервера, имени пользователя, пароля и имени файла
Пример	Сохранить файлы образа системы во флеш-памяти, используя FTP-сервер с адресом 10.1.1.1, имя пользователя Switch, пароль superuser: Switch#copy nos.img ftp://Switch: superuser@10.1.1.1/nos.img Получить с FTP-сервера с адресом 10.1.1.1 файл nos.img, используя имя пользователя Switch и пароль superuser Switch#copy ftp: //Switch: superuser@10.1.1.1/nos.img nos.img Сохранить файлы текущей конфигурирования Switch#copy running-config startup-config

2.5.2. Копирование (FTP) (copy (TFTP))

Команда	copy <source-url> <destination-url> [ascii binary]	
Параметр	<source-url>	местонахождение исходных файлов или каталогов, которые требуется скопировать;
	<destination-url>	адрес назначения, в которое требуется скопировать исходные файлы или каталоги;
	ascii	использовать стандарт ASCII
	binary	при передаче файла использовать двоичную систему (метод передачи по умолчанию)



Состояние по умолчанию	Не задано								
Режим	Привилегированный режим								
Руководство по использованию	Команда применяется для передачи файлов через TFTP. Когда URL соответствует TFTP -адресу, форма команды следующая: <code>tftp: //{<ipaddress> <ipv6address> <hostname>}/<filename></code>, где <code><ipaddress></code> <code><ipv6address></code> IPv4- или IPv6-адрес TFTP сервера/клиента, <code><hostname></code> имя хоста, соответствующее IPv6-адресу, не поддерживается загрузка и выгрузка файлов с хостов, соответствующих IPv4-адресу, <code><filename></code> имя файла, выгружаемого или загружаемого по TFTP. Специальные ключевые слова для имени файла: <table> <tr> <th>Ключевое слово</th><th>Объяснение</th></tr> <tr> <td><code>running-config</code></td><td>Файлы текущей рабочей конфигурирования. Это означает, что при использовании команды <code>copy running-config startup-config</code> файл конфигурирования будет перезагружен</td></tr> <tr> <td><code>nos.img</code></td><td>Системные файлы</td></tr> <tr> <td><code>bootrom</code></td><td>Системные файлы начальной загрузки</td></tr> </table> <code>startup-config</code> Эта команда поддерживает подсказки командной строки, т.е. пользователь может вводить команды в следующем виде: <code>copy <filename> tftp: //</code> или <code>copy tftp: // <filename></code> и по нажатию Enter, система выдаст следующие подсказки: <code>tftp server ip/ipv6 address[x.x.x.x]/[x: x: x: x]>tftp filename></code> Запрос адреса TFTP-сервера, имени файла	Ключевое слово	Объяснение	<code>running-config</code>	Файлы текущей рабочей конфигурирования. Это означает, что при использовании команды <code>copy running-config startup-config</code> файл конфигурирования будет перезагружен	<code>nos.img</code>	Системные файлы	<code>bootrom</code>	Системные файлы начальной загрузки
Ключевое слово	Объяснение								
<code>running-config</code>	Файлы текущей рабочей конфигурирования. Это означает, что при использовании команды <code>copy running-config startup-config</code> файл конфигурирования будет перезагружен								
<code>nos.img</code>	Системные файлы								
<code>bootrom</code>	Системные файлы начальной загрузки								
Пример	Скопировать образ системы из флеш-памяти на TFTP-сервер с адресом 10.1.1.1. <pre>Switch#copy nos.img tftp: //10.1.1.1/nos.img</pre> Скопировать образ с именем nos.img с TFTP-сервера с адресом 10.1.1.1. <pre>Switch#copy tftp: //10.1.1.1/nos.img nos.img</pre> Сохранить файлы текущей конфигурирования <pre>Switch#copy running-config startup-config</pre>								



2.5.3. Файлы на FTP-сервере (ftp-dir)

Команда	ftp-dir <ftp-server-url>	
Параметр	<ftp-server-url>	адрес FTP-сервера
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Команда позволяет просмотреть список файлов на FTP-сервере. Параметр <ftp-server-url> имеет следующий формат: ftp: //<username>: <password>@{ <ipv4address> <ipv6address> }, где <username> имя пользователя FTP, <password> пароль пользователя, { <ipv4address> <ipv6address> } IPv4- или IPv6-адрес FTP-сервера	
Пример	Просмотреть список файлов на сервере с помощью FTP-клиента, имя пользователя - "Switch", пароль - "superuser". Switch#ftp-dir ftp://Switch:superuser@10.1.1.1	

2.5.4. Включение FTP-сервера (ftp-server enable)

Команда	ftp-server enable no ftp-server enable	
Параметр	none	отсутствует
Состояние по умолчанию	FTP-сервер не запущен	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда запускает FTP-сервер. Когда функция FTP-сервера включена, коммутатор может выполнять функции FTP-клиента. Команда "no ftp-server enable" выключает FTP-сервер и прекращает регистрацию пользователей по FTP	
Пример	Включить FTP-сервер. Switch(config)# ftp-server enable	



2.5.5. Тайм-аут FTP-сервера (ftp-server timeout)

Команда	ftp-server timeout <seconds>	
Параметр	<seconds>	пороговое время простоя (в секундах) для FTP-соединения, диапазон значений - от 5 до 3600
Состояние по умолчанию	По умолчанию системой установлено 600 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Командой задается время ожидания для FTP соединения. Когда время простоя соединения передачи данных по FTP превысит это предельное значение, FTP-соединение будет отключено	
Пример	Задать пороговое время простоя 100 секунд. Switch(config)#ftp-server timeout 100	

2.5.6. IP-адрес FTP (ip ftp)

Команда	ip ftp username <username> password [0 7] <password> no ip ftp username <username>	
Параметр	<username>	имя пользователя для FTP-доступа, длина имени не более 32 символов
	[0 7]	если выбран 0 — пароли не будут шифроваться, если выбрано 7 — будет применяться шифрование паролей
	<password>	пароль для FTP-доступа
Состояние по умолчанию	Используется анонимный доступ по FTP	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать имя пользователя и пароль для доступа по ftp. "no" перед началом команды приведет к одновременному удалению настроенных имени пользователя и пароля	
Пример	Сконфигурировать имя пользователя Switch для FTP-доступа, пароль superuser. Switch(config)#ip ftp username Switch password 0 superuser	



2.5.7. Вывод FTP (show ftp)

Команда	show ftp	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим и глобальной конфигурации	
Руководство по использованию	Выводит на экран параметры конфигурирования FTP-сервера	
Пример	Выводит на экран параметры конфигурирования FTP-сервера Switch#show ftp Timeout : 600	

2.5.8. Вывод TFTP (show tftp)

Команда	show tftp	
Параметр	none	отсутствует
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим и глобальной конфигурации	
Руководство по использованию	Команда выводит на экран параметры конфигурирования TFTP-сервера	
Пример	Вывести на экран параметры конфигурирования TFTP-сервера. Switch#show tftp timeout : 60 Retry Times : 10	

2.5.9. Включение TFTP-сервера (tftp-server enable)

Команда	tftp-server enable no tftp-server enable	
Параметр	none	отсутствует



Состояние по умолчанию	TFTP сервер отключен
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда запускает TFTP-сервер. Команда “no ftp-server enable” выключает TFTP -сервер и прекращает регистрацию пользователей по TFTP
Пример	Запустить TFTP-сервер. Switch(config)#ftp-server enable

2.5.10. Число попыток передачи данных TFTP (tftp-server retransmission-number)

Команда	tftp-server retransmission-number <number>	
Параметр	<number>	максимальное число попыток, от 1 до 20
Состояние по умолчанию	Установлено число попыток равное 5	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет задать предельное число попыток передачи данных по протоколу TFTP	
Пример	Установить предельное число попыток равным 10. Switch(config)#tftp-server retransmission-number 10	

2.5.11. Тайм-аут передачи данных TFTP-сервера (tftp-server transmission-timeout)

Команда	tftp-server transmission-timeout <seconds>	
Параметр	<seconds>	значение времени таймера в секундах, в пределах от 5 до 3600 секунд
Состояние по умолчанию	В системе задано 600 секунд	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда позволяет задать время ожидания для передачи данных по протоколу TFTP
Пример	Установить время таймера равным 60 секундам. Switch(config)#tftp-server transmission-timeout 60

2.6. Команды для работы с файловой системой

2.6.1. Текущее устройство (cd)

Команда	cd <directory>	
Параметр	<directory>	имя подкаталога, ряд последовательных символов, длина которых варьируется от 1 до 80
Состояние по умолчанию	Рабочим каталогом по умолчанию является флеш-память	
Режим	Привилегированный режим	
Руководство по использованию	Команда позволяет менять рабочий каталог устройства хранения данных. После выполнения этой команды текущее устройство хранения перейдет в новый рабочий каталог, который можно посмотреть командой "pwd"	
Пример	Изменить рабочий каталог текущего устройства хранения данных на флеш-память. Switch#cd flash: Switch#pwd flash: /	

2.6.2. Копирование (copy)

Команда	copy <source-file-url > <dest-file-url>	
Параметр	<source-file-url>	адрес источника копируемого файла или каталога
	<dest-file-url>	адрес назначения копируемого файла или каталога
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	



Руководство по использованию	По команде указанный файл на коммутаторе копируется и сохраняется как новый файл. Когда пользователи работают с файлами, хранящимися на резервных мастер-платах и линейных платах в режиме IMG, URL-адреса исходного файла и файла назначения должны иметь вид, описанный в следующих требованиях. Префикс URL-адреса исходного файла должен быть в одной из следующих форм: начинаться с “flash: /” “ftp: //username: pass@server-ip/file-name” “tftp: //server-ip/file-name” Префикс URL-адреса конечного файла должен быть в одной из следующих форм: начинаться с “flash: /” “ftp: //username: pass@server-ip/file-name” “tftp: //server-ip/file-name” если префикс URL-адреса исходного файла ftp: // или tftp: //, URL-адрес файла назначения не должен иметь ни одного из этих двух префиксов. Чтобы использовать эту команду, указанный исходный файл должен существовать, а файл назначения не должен совпадать по имени ни с одним из существующих каталогов или файлов, иначе может появиться предупреждение о том, что операция копирования не удалась или, что вы пытаетесь перезаписать существующий файл. Если исходный и конечный файлы находятся в разных каталогах, то после выполнения этой команды пользователи могут копировать файлы из других каталогов в текущий каталог
Пример	Скопировать файл “flash: /nos.img” и сохранить как “flash/ 6.1.11.0.img”. Switch#copy flash:/nos.img flash:/nos-6.1.11.0.img Copy flash:/nos.img to flash:/nos-6.1.11.0.img? [Y: N] y Copied file flash:/nos.img to flash:/nos-6.1.11.0.img

2.6.3. Удаление (delete)

Команда	delete <file-url>	
Параметр	<file-url>	полный путь к удаляемому файлу
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	



Руководство по использованию	Команда удаляет указанный файл на устройстве хранения
Пример	Удалить файл flash: /nos.img. Switch#delete flash: /nos5.img Delete file flash: /nos5.img? [Y: N]y Deleted file flash: /nos.img

2.6.4. Каталог (dir)

Команда	dir [WORD]	
Параметр	[WORD]	имя отображаемого каталога. Существуют следующие форматы: directory name, slot-xx#directory name, flash: /directory name, cf: /directory name
Состояние по умолчанию	Отсутствие параметра <WORD> означает отображение информации о текущем рабочем каталоге	
Режим	Привилегированный режим	
Руководство по использованию	Команда задает отображение информации о заданном каталоге на устройстве хранения. Эта команда не поддерживает рекурсивное отображение всех подкаталогов	
Пример	Показать информацию каталога "flash: /". Switch#dir flash: / nos.img 2,449,496 1980-01-01 00: 01: 06 ---- startup-config 2,064 1980-01-01 00: 30: 12 ---- Total 7, 932, 928 byte(s) in 4 file(s), free 4, 966, 400 byte(s) Switch#	

2.6.5. Текущая директория (pwd)

Команда	pwd	
Параметр	none	отсутствует
Состояние по умолчанию	По умолчанию используется директория flash	
Режим	Привилегированный режим	



Руководство по использованию	Команда показывает текущую рабочую директорию
Пример	Показать текущую рабочую директорию Switch#pwd flash: /

2.6.6. Переименование (rename)

Команда	rename <source-file-url> <new-filename >	
Параметр	<source-file-url>	исходный файл, в котором допустимо как указание, так и отсутствие указания пути к нему
	<new-filename>	имя файла без указания пути к нему
Состояние по умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	По команде выполняется переименование указанного файла на коммутаторе. При использовании этой команды, если новое имя файла не используется в качестве имени какого-либо существующего каталога или файла, операция может быть выполнена, в противном случае будет выдано сообщение об ошибке	
Пример	Изменить имя файла "nos.img" в текущей рабочей директории на "nos-6.1.11.0.img". Switch# rename nos5.img nos-6.1.11.0.img Rename flash: /nos5.img to flash: /nos-6.1.11.0.img ok !	



3. Руководство по настройке портов

3.1. Команды для настройки Ethernet-порта

3.1.1. Пропускная способность (bandwidth)

Команда	bandwidth control < bandwidth > {transmit receive both} no bandwidth control
Параметр	bandwidth ограничение пропускной способности, которое отображается в кбит/с в диапазоне от 1-1000000K
Значение по умолчанию	Ограничение пропускной способности выключено
Режим	Режим конфигурации порта
Руководство по использованию	Команда bandwidth control <bandwidth>[both receive transmit] применяется для установки скорости полосы пропускания. Команда no bandwidth control восстанавливает конфигурирование по умолчанию
Пример	Установить скорость передачи 40000 кбит/с для портов 0/0/1-8. Switch(config)#interface ethernet 1/0/1-8 Switch(Config-If-Port-Range)#bandwidth control 40000 both

3.1.2. Удаление данных интерфейса счетчиков (clear counters interface)

Команда	clear counters [interface {ethernet < interface-list > vlan < vlan-id > port-channel < port-channel-number > < interface-name > }]								
Параметр	<table> <tr> <td>interface-list</td><td>номер Ethernet-порта</td></tr> <tr> <td>vlan-id</td><td>номер интерфейса VLAN</td></tr> <tr> <td>port-channel-number</td><td>номер магистрального интерфейса</td></tr> <tr> <td>interface-name</td><td>имя интерфейса, например, port-channel 1</td></tr> </table>	interface-list	номер Ethernet-порта	vlan-id	номер интерфейса VLAN	port-channel-number	номер магистрального интерфейса	interface-name	имя интерфейса, например, port-channel 1
interface-list	номер Ethernet-порта								
vlan-id	номер интерфейса VLAN								
port-channel-number	номер магистрального интерфейса								
interface-name	имя интерфейса, например, port-channel 1								
Значение по умолчанию	Информация счетчиков не удаляется								
Режим	Привилегированный режим								



Руководство по использованию	Если порт не указан, будет очищена статистика всех портов
Пример	Очистить статистику Ethernet-порта 0/0/1. Switch#clear counters interface ethernet 1/0/1

3.1.3. Описание (description)

Команда	description < string > no description
Параметр	string строка символов, которая не должна превышать 200 символов
Значение по умолчанию	Имя порта не задано
Режим	Режим конфигурации порта
Руководство по использованию	Эта команда используется для помощи пользователям в управлении коммутатором, например, позволяет присвоить имя порта в соответствии с его назначением, например, имя "financial" портов 1/0/1-2 для финансового отдела, имя "engineering" портов 1/0/9 для инженерного отдела, а имя Server портов 1/0/12 потому, что они подключены к серверу. Таким образом, выявляется статус распределения портов
Пример	Указать описание порта 1/0/1-2 как financial. Switch(config)#interface ethernet 1/0/1-2 Switch(Config-If-Port-Range)#description financial

3.1.4. Управление потоком (flow control)

Команда	flow control no flow control
Параметр	-
Значение по умолчанию	Управление потоком выключено
Режим	Режим конфигурации порта



Руководство по использованию	После того, как функция управления потоком будет включена, порт будет уведомлять передающее устройство о необходимости снизить скорость передачи во избежание потери пакетов, когда принимаемый трафик превышает пропускную способность кэша порта. Порты коммутатора поддерживают управление потоком IEEE802.3X; порты, работающие в режиме полудуплекса, поддерживают управление потоком методом обратного давления (backpressure). Если управление потоком приводит к серьезной блокировке, коммутатор автоматически начнет управлять HOL (будет отбрасывать некоторые пакеты в очередях COS, которые могут привести к блокировке), чтобы предотвратить значительное снижение производительности сети
Пример	Включить функцию управления потоком в портах 0/0/1-8. Switch(config)#interface ethernet 1/0/1-8 Switch(Config-If-Port-Range)#flow control

3.1.5. Режим порта Ethernet (interface ethernet)

Команда	interface ethernet < interface-list >	
Параметр	interface-list	номер порта
Значение по умолчанию	-	
Режим	Режим глобальной конфигурации	
Руководство по использованию	С помощью этой команды можно войти в режим настройки порта и выполнить команду exit для выхода из режима порта Ethernet в режим глобальной конфигурации	
Пример	Войти в режим режим порта Ethernet для портов 1/0/1, 1/0/4-5, 1/0/8. Switch(config)#interface ethernet 1/0/1; 1/0/4-5; 1/0/8 Switch (Config-If-Port-Range)#	

3.1.6. Петля (Loopback)

Команда	loopback no loopback
Параметр	-
Значение по умолчанию	Тестовая петля для Ethernet-порта выключена
Режим	Режим конфигурации порта



Руководство по использованию	Включает функцию петли для проверки правильности работы Ethernet-порта. После того, как петля будет включена, порт установит соединение с самим собой, при этом весь трафик, посылаемый портом, будет приниматься этим же самым портом
Пример	Включить тестовую петлю для Ethernet-портов 0/0/1-8. Switch(config)#interface ethernet 1/0/1-8 Switch (Config-If-Port-Range)#loopback

3.1.7. Интервал сбора статистики скорости порта (Port-rate-statistics interval)

Команда	port-rate-statistics interval < interval-value >	
Параметр	interval-value	интервал сбора статистики передачи данных через порт, в секундах, в диапазоне от 5 до 600 секунд, с шагом 5
Значение по умолчанию	Отображается только статистика скорости порта за 5 секунд и 5 минут	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда задает интервал сбора статистики скорости передачи данных через порт	
Пример	Задать интервал port-rate-statistics равным 20 секундам. Switch(config)#port-rate-statistics interval 20	

3.1.8. Аномалия скорости (rate-violation)

Команда	rate-violation [broadcast multicast unicast all] <200-2000000> no rate-violation	
Параметр	broadcast	широковещательный трафик
	multicast	multicast-трафик
	unicast	unicast- пакеты,
	all	все пакеты
	<200-2000000>	разрешенное количество пакетов в секунду



Значение по умолчанию	Скорость приема пакетов не ограничена
Режим	Режим конфигурации порта
Руководство по использованию	Команда в основном применяется для обнаружения прохождения через порт аномальных потоков данных. Например, если аномально большое число broadcast-сообщений обусловлено петлей, причем ухудшается выполнение других задач коммутатора, порт будет выключен, чтобы гарантировать выполнение других задач коммутатора. Эта команда должна быть связана с командой "rate-violation control"
Пример	Установить для порта 1/0/8-10 (порты GB) скорость передачи данных 10000pps, при превышении указанного количества пакетов настроить отключение порта, время восстановления порта — 1200 секунд, когда скорость приема пакетов превысит 10 000, порт будет отключен, а затем, через 1200 секунд, порт снова заработает. <pre>Switch(config)#interface ethernet 1/0/8-10 Switch(Config-Port-Range)#rate-violation unicast 10000 Switch(Config-Port-Range)#rate-violation control shutdown recovery 1200</pre>

3.1.9. Управление действиями при аномалии скорости (rate-violation control)

Команда	rate-violation control [shutdown recovery <0-86400> block] no rate-violation control	
Параметр	shutdown	после нарушения порт выключается
	recovery	восстановление и включение порта через определённый промежуток времени
	block	порт блокируется. Этот параметр является взаимоисключающим с функциями STP, MRPP, Loopback detection и ULPP. Эта функция не может быть установлена в режим блокировки, если другие модули устанавливают статус STP
	<0-86400>	время автоматического восстановления после выключения
Значение по умолчанию	Для "rate-violation" действия не предусмотрены	
Режим	Режим конфигурации порта	



Руководство по использованию	Команда в основном применяется для управления действиями при достижении ограничения, указанного командой действия при превышении лимита "rate-violation"
Пример	Настроить блокировку порта после установки скорости передачи одноадресного unicast-пакета порта 1/8-10 (порты GB) равной 10000pps. <pre>Switch(Config)#interface ethernet 1/0/8-10 Switch(Config-Port-Range)#rate-violation unicast 10000 Switch(Config-Port-Range)#rate-violation control block</pre>

3.1.10. Вывод интерфейса (show interface)

Команда	<pre>show interface [ethernet < interface-number > port-channel < port-channel-number > vlan < vlan-id > < interface-name > undefined] [detail] show interface ethernet status show interface ethernet counter {packet rate}</pre>	
Параметр	interface-number	номер Ethernet-порта
	port-channel-number	номер агрегированного интерфейса
	vlan-id	номер интерфейса VLAN, в пределах от 1 до 4094
	interface-name	имя интерфейса, например, port-channel1
	detail	показать подробную информацию о порте
Значение по умолчанию	Информация не отображается	
Режим	Привилегированный режим и режим конфигурации	
Руководство по использованию	Команда позволяет просматривать информацию о конфигурации, связанной с интерфейсом	
Пример	Вывести на экран информацию для интерфейса VLAN 1. <pre>Vlan1 is up, line protocol is up, dev index is 11001 Device flag 0x1003(UP BROADCAST MULTICAST) Time since last status change: 0w-0d-1h-14m-57s (4497 seconds) IPv4 address is: 192.168.2.1 255.255.255.0 (Primary) VRF Bind: Not Bind</pre>	



	Hardware is EtherSVI, address is 00-1f-ce-10-b0-1a MTU is 1500 bytes , BW is 0 Kbit Encapsulation ARPA, loopback not set 5 minute input rate 244 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec The last 5 second input rate 0 bits/sec, 0 packets/sec The last 5 second output rate 0 bits/sec, 0 packets/sec Input packets statistics: Input queue 0/600, 0 drops 1012 packets input, 193127 bytes, 0 no buffer 0 input errors, 0 CRC, 0 oversize, 0 undersize 0 jabber, 0 fragments Output packets statistics: 448 packets output, 108316 bytes, 0 underruns 0 output errors, 0 collisions

3.1.11. Остановка (Shutdown)

Команда	Shutdown
Параметр	-
Значение по умолчанию	Ethernet-порт включен
Режим	Режим конфигурации порта
Руководство по использованию	Когда Ethernet-порт выключен кадры с данными не посылаются в порт, если пользователь введет команду "show interface", то состояние порта, выведенное на экран по этой команде, будет "down" (выключен)
Пример	Включить порты 0/0/1-8. Switch(config)#interface ethernet1/0/1-8 Switch(Config-If-Port-Range)#no shutdown

3.1.12. Скорость и режим дуплекса (speed-duplex)

Команда	speed-duplex {force1G [auto full]] force10G-auto force25G-auto force40G-auto force100G-auto} no speed-duplex	
Параметр	force1G	принудительная скорость 1G
	auto	автоматическое согласование скорости



	full	установка полного дуплекса
	force10G-auto	принудительная скорость 10G в автоматическом режиме полного дуплекса
	force25G-auto	принудительная скорость 25G в автоматическом режиме полного дуплекса
	force40G-auto	принудительная скорость 40G в автоматическом режиме полного дуплекса
	force100G-auto	принудительная скорость 100G в автоматическом режиме полного дуплекса
Значение по умолчанию	Используются автоматическое согласование скорости и режим дуплекса	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда позволяет настроить скорость и режим дуплекса портов. При настройке скорости и режима дуплекса скорость и режим дуплекса должны быть совместимы с удаленным пиром, т.е. если на удаленном порту задано автоматическое согласование, на локальном порту должно быть задано то же самое. Если на удаленном порту настройки заданы в принудительном режиме, именно этот режим должен использоваться и на локальном порту	
Пример	Соединить порт 1 коммутатора Switch1 с портом 1 коммутатора Switch2; принудительно установить на них скорость 100G и режим полного дуплекса. <pre>Switch1(config)#interface ethernet1/0/1 Switch1(Config-If-Ethernet1/0/1)#speed-duplex force100G-auto</pre> <pre>Switch2(config)#interface ethernet1/0/1 Switch2(Config-If-Ethernet1/0/1)#speed-duplex force100G-auto</pre>	

3.1.13. Управление трафиком (storm-control)

Команда	storm-control { kbps pps } no storm-control pps	
Параметр	kbps	лимит обработки трафика, в килобитах в секунду
	pps	лимит обработки трафика, в пакетах в секунду



Значение по умолчанию	Лимит обработки трафика в килобитах в секунду
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда задает ограничения входящего трафика в килобитах в секунду или в пакетах в секунду, затем устанавливается предельное значение широковещательного, многоадресного или неизвестного одноадресного трафика в режиме порта
Пример	Настроить разрешение для портов 1-8 на передачу 1000 кбит широковещательных пакетов в секунду. <pre>Switch(config)#storm-control kbps</pre> <pre>Switch(config-if-port-range)#storm-control broadcast 1000</pre>

3.1.14. Управление трафиком (storm-control)

Команда	storm-control {unicast broadcast multicast} < value> no storm-control {unicast broadcast multicast}	
Параметр	unicast	ограничение одноадресного трафика для неизвестного назначения
	broadcast	ограничения широковещательного трафика
	multicast	ограничения многоадресного трафика
	value	Ограничение скорости потока в секунду, диапазон pps от 1 до 1 488 095; диапазон kbps от 1 до 1 000 000
Значение по умолчанию	Лимит не задан. Таким образом, широковещательные, многоадресные и одноадресные сообщения неизвестного назначения пропускаются со скоростью линии	
Режим	Режим конфигурации порта	
Руководство по использованию	Все порты коммутатора принадлежат к одному широковещательному домену, если не задана VLAN. Коммутатор отправляет все три типа трафика на все порты в широковещательном домене, что может привести к широковещательным штормам и, следовательно, значительно снизить производительность коммутатора. Подключение Broadcast Storm Control лучше защищает коммутатор от широковещательных штормов. Если для разрешенного трафика установлено значение 1000 кбит/с, это означает, что трафик со скоростью 1000 кбит/с разрешен, а другой трафик подавляется. Коммутатор поддерживает два типа ограничения скорости, включая	



	kpps, который ограничивается пропускной способностью, и rps, который ограничивается количеством пакетов. Можно выбрать только один из двух методов нельзя установить оба одновременно (в режиме глобальной конфигурации). Подавление широковещания аналогично управлению пропускной способностью. Имеется ограничение по гранулярности чипа. Коммутатор поддерживает гранулярность 16 кбит/с. Если введенное пользователем значение <Kbits> не является целым числом, кратным 16, система автоматически подгонит его к целому числу, кратному 16, и выведет пользователю действительное значение ограничения
Пример	Настроить разрешение для портов 1-8 на передачу 1000 кбит широковещательных пакетов в секунду. Switch(config-if-port-range)#storm-control broadcast 1000

3.1.15. Управление фильтрацией (storm-control bypass)

Команда	storm-control bypass {arp bpdu igmp rma rek } <enable disable >	
Параметр	arp	пакеты протокола arp-запроса
	bpdu	пакеты протокола bpdu
	igmp	пакеты протокола igmp
	rma	групповой адрес — сохраненные пакеты multicast-адресов
	rek	специальные частные пакеты, которые использует realtak
	enable	включить определенный протокол для ограничения фильтрации
	disable	отключить определенный протокол для ограничения фильтрации
Значение по умолчанию	Отключено	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда задает фильтрацию ограничения широковещания для определенных протоколов в глобальном режиме, затем настраивает лимит вещания в режиме порта. В этом случае невозможно ограничить пакеты протоколов, выходящие из порта

3.1.16. Отмена приема пакетов (switchport discard packet)

Команда	switchport discard packet { all untag } no switchport discard packet { all untag }	
Параметр	all	ни один пакет, включая тегированный, нетегированный или deal не пропускаются
	untag	не принимаются нетегированные пакеты
Значение по умолчанию	Ограничения отсутствуют	
Режим	Режим конфигурации порта	
Руководство по использованию	Задавать эту команду рекомендуется только в случае особой необходимости	
Пример	Установить для порта 1/0/8 запрет на прием всех пакетов. Switch(config)#interface ethernet 1/0/8 Switch(config-if-ethernet1/0/8)#switchport discard packet all	

3.1.17. Управление потоком коммутатора (switchport flood-control)

Команда	switchport flood-control { bcast mcast ucast } no switchport flood-control { bcast mcast ucast }	
Параметр	bcast	предотвращает передачу широковещательных пакетов в выбранный порт
	mcast	предотвращает передачу неизвестных многоадресных пакетов в выбранный порт
	ucast	предотвращает передачу неизвестных одноадресных пакетов в выбранный порт
Значение по умолчанию	Коммутатор передает широковещательные, неизвестные многоадресные и неизвестные одноадресные пакеты на другие порты в широковещательном домене	



Режим	Режим настройки портов
Руководство по использованию	Эта команда действительна для портов 100М и 1000М, а также для портов Access, Trunk и Hybrid. Когда команда действует, порт разрешает прохождение одноадресного или многоадресного трафика, после того как порт узнал соответствующий одноадресный mac или многоадресный mac. Эта команда контролирует только запрет на получение широковещательных, многоадресных и неизвестных одноадресных пакетов, отправляемых с других портов на указанный порт, но не контролирует отправку таких пакетов с указанного порта. Например, если для порта 1/0/1 задана команда <code>switchport flood-control bcast</code>, на порт 1/0/1 не могут быть отправлены широковещательные пакеты с других портов, но порт 1/0/1 может принимать и отправлять широковещательные пакеты
Пример	Задать flood-control по признаку bcast и mcast для порта 1/0/1 или порта 1/0/8-10 соответственно. <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport flood-control bcast Switch(config)#interface ethernet 1/0/8-10 Switch(config-if-port-range)#switchport flood-control mcast</pre>

3.1.18. Переадресация потока коммутатора (switchport flood-forwarding)

Команда	switchport flood-forwarding mcast no switchport flood-forwarding mcast	
Параметр	mcast	предотвращает передачу неизвестных многоадресных пакетов в выбранный порт
Значение по умолчанию	Коммутатор передает неизвестные многоадресные пакеты на другой порт в широковещательном домене	
Режим	Режим конфигурации порта	
Руководство по использованию	Эта команда действительна для портов 100М и 1000М, а также для портов Access, Trunk и Hybrid. Команда обычно комбинируется с "ip imgrp snooping", "ip imgrp snooping" не поддерживает неизвестный многоадресный и широковещательный трафик, но может отправлять неизвестный многоадресный трафик после настройки "switchport flood-forwarding mcast"	
Пример	Установить переадресацию широковещательных сообщений на порту коммутатора 1/0/1. <pre>switch#</pre>	



	<pre>switch#confi switch(config)#interface ethernet 1/0/1 switch(config-if-ethernet1/0/1)# switchport flood-forwarding mcast switch(config-if-ethernet1/0/1)#exit switch(config)#</pre>

3.2. Команды для настройки изоляции портов

3.2.1. Изоляция группы портов (isolate-port group)

Команда	<pre>isolate-port group < WORD > no isolate-port group < WORD ></pre>	
Параметр	WORD	имя, идентифицирующее группу, длиной не более 32 символов
Значение по умолчанию	-	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Пользователи могут в соответствии со своими требованиями создавать различные группы изолированных портов. Например, если необходимо изолировать все downlink порты в vlan коммутатора, можно создать группу изолированных портов и добавить в нее все downlink-порты из этого vlan. Коммутатор поддерживает не более 16 групп изолированных портов. Если необходимо изменить настройки или конфигурирование группы изолированных портов, следует сначала удалить существующую группу командой отмены no	
Пример	Создать группу изолированных портов с именем "test". <pre>Switch>enable Switch#config Switch(config)#isolate-port group test</pre>	

3.2.2. Интерфейс изоляции порта группы (isolate-port group switchport interface)

Команда	<pre>isolate-port group < WORD > switchport interface [ethernet] < IFNAME > no isolate-port group < WORD > switchport interface [ethernet] < IFNAME ></pre>	
Параметр	WORD	имя, идентифицирующее группу, длиной не более 32 символов



	IFNAME	имя интерфейса
Значение по умолчанию	-	
Режим	В режиме глобальной конфигурации или режиме конфигурации Vlan	
Руководство по использованию	В соответствии со своими требованиями, пользователи могут добавлять Ethernet-порты в группы изолированных портов, изолировать их друг от друга (режим глобальной конфигурации) во всех vlan, а также изолировать их друг от друга (режим vlan) в некоторых vlan или удалить их из группы изолированных портов. Если порт Ethernet является членом более чем одной группы изоляции, он будет изолирован от каждого порта всех групп, в которые он входит	
Пример	Добавить Ethernet-порты 0/0/1-2 и 0/0/5 в группу изолированных портов с именем "test", добавить Ethernet-порт 1/0/3-4 в группу изолированных портов с именем "1" в vlan10. <pre>Switch(config)#isolate-port group test switchport interface ethernet 1/0/1-2; 1/0/5</pre> <pre>Switch(config-vlan10)#isolate-port group 1 switchport interface ethernet 1/0/3-4</pre>	

3.2.3. Вывод данных об изоляции порта группы (show isolate-port group)

Команда	show isolate-port group [< WORD >]	
Параметр	WORD	имя, идентифицирующее группу, длиной не более 32 символов
Значение по умолчанию	Вывод на экран информации для всех групп изолированных портов	
Режим	Привилегированный режим и глобальной конфигурации	
Руководство по использованию	С помощью этой команды пользователи могут просматривать информацию о настройке изоляции портов	
Пример	Вывести на экран настройки изоляции портов для группы с именем "test". <pre>Switch(config)#show isolate-port group test</pre> <pre>Isolate-port group test</pre> <pre>The isolate-port Ethernet1/0/5</pre> <pre>The isolate-port Ethernet1/0/2</pre>	



3.3. Команды обнаружения петель в портах

3.3.1. Управление обнаружением петель (loopback-detection control)

Команда	loopback-detection control {shutdown block } no loopback-detection control	
Параметр	shutdown	задает в качестве метода управления выключение, это означает, что при обнаружении петли порт будет выключен
	block	задает в качестве метода управления блокирование; это означает, что при обнаружении петли через порт будет разрешена передача только сообщений bpdu и loopback detection
Значение по умолчанию	Функция обнаружения петли выключена	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда позволяет включить функцию управления обнаружением петель на портах, которая отключается по NO в начале команды	
Пример	Включить функцию контроля обнаружения петель в режиме порта1/2. Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#loopback-detection control shutdown Switch(Config-If-Ethernet1/0/2)#no loopback-detection control	

3.3.2. Тайм-аут восстановления после обнаружения петли (loopback-detection control-recovery timeout)

Команда	loopback-detection control-recovery timeout <0-3600>	
Параметр	0-3600	секунд: время восстановления после контролируемого состояния, 0 — восстановление выполняться не будет
Значение по умолчанию	Восстановление автоматически не выполняется	
Режим	Режим глобальной конфигурации	
Руководство по использованию	При данной команде, когда в порту обнаружена петля и он работает в контролируемом режиме, порт находится в этом режиме постоянно и восстановления не происходит. Порт не будет посылать пакеты для обнаружения в режиме shutdown, однако он будет посылать пакеты обнаружения петли, независимо от того, находится ли петля в режиме	



	блокировки или обучения. Если задано время восстановления, то нормальное состояние портов будет восстановлено по истечении соответствующего таймера. Время восстановления является полезным параметром, позволяющим выключить режим shutdown, поскольку порт может продолжать обнаруживать петлю в других режимах, так что эту команду лучше не использовать
Пример	Включить автоматическое восстановление режима управления обнаружением петли по истечении 30 секунд. Switch(config)#loopback-detection control-recovery timeout 30

3.3.3. Интервал обнаружения петель (loopback-detection interval-time)

Команда	loopback-detection interval-time < loopback > < no-loopback > no loopback-detection interval-time	
Параметр	loopback	интервал обнаружения при обнаружении петли, в пределах от 5 до 300 секунд
	no-loopback	интервал обнаружения, если петли нет, в пределах от 1 до 30 секунд
Значение по умолчанию	5 секунд, если петля существует, в противном случае – 3 секунды	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Если петля не обнаружена, возможно, интервал обнаружения задан относительно небольшим и поскольку он слишком мал, петля не может быть обнаружена, хотя на самом деле существует. В дальнейшем это скажется на работоспособности сети. Поэтому рекомендуется выбирать достаточно большой интервал времени обнаружения петли при наличии петли	
Пример	Задать интервал обнаружения петли 35 с, 15 с. Switch(config)#loopback-detection interval-time 35 15	

3.3.4. loopback-detection specified-vlan

Команда	loopback-detection specified-vlan < vlan-list > no loopback-detection specified-vlan [< vlan-list >]	
Параметр	vlan-list	идентификатор VLAN



Значение по умолчанию	Функция обнаружения петель в портах выключена
Режим	Режим конфигурации порта
Руководство по использованию	Для магистрального (trunk) порта для многих vlan, обнаружение петель может быть реализовано по принципу порт+vlan. Это означает, что объектами обнаружения могут быть указанные vlan в порту. Если порт является портом доступа (ACCESS), в порту будет проверяться только один vlan, несмотря на то, что может быть задано множество vlan. Эта функция не поддерживается для Port-channel
Пример	Включить функцию обнаружения петель в режиме порта 1/0/2 <pre>Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#switchport mode trunk Switch(Config-If-Ethernet1/0/2)#switchport trunk allowed vlan all Switch(Config-If-Ethernet1/0/2)#loopback-detection specified-vlan 1; 3; 5-20 Switch(Config-If-Ethernet1/0/2)#no loopback-detection specified-vlan 1; 3; 5-20</pre>

3.3.5. Вывод данных об обнаружении петель (show loopback-detection)

Команда	show loopback-detection [interface < interface-list >]	
Параметр	interface-list	список отображаемых портов, например, ethernet 1/0/1
Значение по умолчанию	-	
Режим	Привилегированный режим и режим конфигурации	
Руководство по использованию	Позволяет вывести на экран состояние и результаты обнаружения петель в портах	
Пример	Показать состояние обнаружения петли в порту 4. <pre>Switch(config)#show loopback-detection interface Ethernet 1/0/4 loopback detection config and state information in the switch! PortName Loopback Detection Control Mode Is Controlled Ethernet1/4 Enable Shutdown No</pre>	



3.4. Команды для настройки функции ULDP

3.4.1. Агрессивный режим ULDP (uldp aggressive-mode)

Команда	uldp aggressive-mode no uldap aggressive-mode
Параметр	-
Значение по умолчанию	Режим глобальной конфигурации и режим конфигурации порта
Режим	Нормальный режим работы
Руководство по использованию	Режим работы функции ULDP можно задать только в том случае, если он включен в глобальном режиме конфигурации. Когда в глобальном режиме конфигурации включен агрессивный режим ULDP, все существующие оптические порты будут работать в агрессивном режиме. Для того, чтобы агрессивный режим ULDP был установлен в медных и оптических портах, он должен быть включен в режиме настройки портов
Пример	Включить агрессивный режим ULDP в глобальном режиме конфигурации. Switch(config)#uldp aggressive-mode

3.4.2. Включение ULDP (uldp enable)

Команда	uldp {enable disable}
Параметр	-
Значение по умолчанию	Функция ULDP выключена
Режим	Режим глобальной конфигурации и режим конфигурации порта
Руководство по использованию	Функцию ULDP можно настроить для портов только в том случае, если она до этого включена в режиме глобальной конфигурации. Если функция ULDP включена в режиме глобальной конфигурации, она будет действительна для всех оптических портов. Для медных и оптических портов, после того как функция ULDP включена в режиме глобальной конфигурации, эту команду следует ввести и в режиме настройки интерфейсов
Пример	Включить функцию ULDP в режиме глобальной конфигурации. Switch(config)#uldp enable



3.4.3. Интервал приветственных сообщений ULDP (uldp hello-interval)

Команда	uldp hello-interval < integer > no uldap hello-interval	
Параметр	integer	Интервал отправки сообщений hello, в пределах от 5 до 100 секунд, по умолчанию 10 секунд
Значение по умолчанию	10 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Интервал отправки сообщений hello возможно задать только в том случае, когда функция ULDP включена в режиме глобальной конфигурации, значение интервала должно быть в пределах от 5 до 100 секунд	
Пример	Задать интервал отправки сообщений hello равным 12 секундам. Switch(config)#uldp hello-interval 12	

3.4.4. Ручная остановка ULDP (uldp manual-shutdown)

Команда	uldp manual-shutdown no uldap manual-shutdown	
Параметр	-	
Значение по умолчанию	Автоматический режим	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда может задаваться, если функция ULDP уже включена в глобальном режиме конфигурации	
Пример	Задать режим отключения вручную в режиме глобальной конфигурации. Switch(config)#uldp manual-shutdown	



3.4.5. Время восстановления ULDP (uldp recovery-time)

Команда	uldp recovery-time < integer > no uldap recovery-time	
Параметр	integer	значение таймера восстановления ULDP. Должно находиться в пределах от 30 до 86400 секунд
Значение по умолчанию	По умолчанию задано 0, т.е. восстановление отключено	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Если интерфейс выключен функцией ULDP, то по истечении таймера интерфейс будет автоматически включен. Если таймер восстановления 0 секунд, интерфейс включен не будет	
Пример	Установить таймер восстановления 600 секунд. Switch(config)#uldp recovery-time 600	

3.4.6. Сброс ULDP (uldp reset)

Команда	uldp reset	
Параметр	-	
Значение по умолчанию	-	
Режим	Режим глобальной конфигурации и режим конфигурации порта	
Руководство по использованию	Эта команда может действовать только в том случае, если указанный интерфейс отключен функцией ULDP	
Пример	Сбросить состояние ULDP для всех отключенных портов. Switch(config)#uldp reset	

3.4.7. Вывод данных ULDP (show uldap)

Команда	show uldap [interface ethernet < interface-name >]	
Параметр	interface-name	имя интерфейса
Значение по умолчанию	-	



Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Если команда введена без параметров, на экран будут выведены настройки ULDP для режима глобальной конфигурации. Если указано имя интерфейса, то наряду с настройками ULDP для режима глобальной конфигурации, будет отображена информация об указанном интерфейсе и интерфейсах, являющихся для него соседними
Пример	Вывести на экран настройки ULDP для режима глобальной конфигурации. Switch(config)#show uldp

```

uldp enable
uldp hello interval is          10
uldp shut down mode is         AUTO
uldp global work mode is       NORMAL
the total number of the port is 4

PortName
NeighborNum    PhyLink    LineProto    WorkMode    PortState
Ethernet1/0/250    UP        DOWN        NORMAL    INACTIVE
Ethernet1/0/260    UP        DOWN        NORMAL    INACTIVE
Ethernet1/0/260    UP        DOWN        NORMAL    INACTIVE
Ethernet1/0/280    UP        DOWN        NORMAL    INACTIVE

```

3.5. Команды для функции LLDP

3.5.1. Очистка удаленных таблиц LLDP (clear lldp remote-table)

Команда	clear lldp remote-table
Параметр	-
Значение по умолчанию	Записи не удаляются
Режим	Режим конфигурации порта
Руководство по использованию	Команда позволяет очистить таблицу сделанных удаленно записей в текущем порту
Пример	Очистить таблицу удаленных записей в текущем порту Switch(Config-If-Ethernet 1/0/1)# clear lldp remote-table



3.5.2. Включение LLDP (lldp enable)

Команда	lldp {enable disable}
Параметр	-
Значение по умолчанию	Функция LLDP отключена
Режим	Режим глобальной конфигурации
Руководство по использованию	Если функция LLDP включена в режиме глобальной конфигурации, она будет включена и на каждом порту
Пример	Включить функцию LLDP коммутатора. Switch(config)#lldp enable

3.5.3. Включение порта LLDP (lldp enable (port))

Команда	lldp {enable disable}
Параметр	-
Значение по умолчанию	Открыт
Режим	Режим конфигурации порта
Руководство по использованию	Когда функция LLDP включена в режиме глобальной конфигурации, она включена и на каждом порту. Команда используется для выключения функции LLDP в порту, если она не является в нем необходимой
Пример	Выключить функцию LLDP в порту ethernet 0/0/5 коммутатора. Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)#lldp disable

3.5.4. TLV адреса управления LLDP (lldp management-address tlv)

Команда	lldp management-address tlv [A.B.C.D] no lldp management-address tlv	
Параметр	A.B.C.D	опциональный параметр, это адрес управления, который пользователь назначает для порта, должен быть одноадресным IPv4-адресом



Значение по умолчанию	Отключено
Режим	Режим конфигурации порта
Руководство по использованию	Пользователи могут выбрать IPv4-адрес управления в соответствии с конфигурацией. Если пользователь указывает адрес управления при включении функции, этот адрес будет использоваться для отправки TLV адреса управления; если пользователь не назначил адрес управления, TLV адреса управления будет отправлен путем выбора IPv4-адреса в качестве адреса управления из VLAN уровня 3. Если адрес не назначен, то при отсутствии адреса управления информация TLV адреса управления не будет отправляться
Пример	Включить функцию TLV адреса управления для ethernet 1/0/1 и назначить адрес. Switch1(Config-If-Ethernet1/0/1)# lldp management-address tlv 192.168.24.32

3.5.5. Режим LLDP (lldp mode)

Команда	lldp mode <send receive both disable >	
Параметр	send	LLDP будет только отправлять сообщения
	receive	LLDP будет только принимать сообщения
	both	LLDP будет только принимать и отправлять сообщения
	disable	LLDP не будет ни отправлять, ни принимать сообщения
Значение по умолчанию	Рабочее состояние порта "both"	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда позволяет задать режим работы агента lldp в порту	
Пример	Задать в порту ethernet 0/0/5 коммутатора состояние "receive" (получение сообщений) Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)#lldp mode receive	



3.5.6. Множитель времени жизни сообщений LLDP (lldp msgTxHold)

Команда	lldp msgTxHold < value > no lldp msgTxHold	
Параметр	value	множитель времени жизни, в пределах от 2 до 10
Значение по умолчанию	Значение множителя задано равным 4	
Режим	Режим глобальной конфигурации	
Руководство по использованию	После того, как задан множитель, время жизни сообщений определяется, как произведение множителя на интервал отправки сообщений, максимальное значение 65535 секунд	
Пример	Задать множитель для времени жизни сообщений равным 6. Switch(config)#lldp msgTxHold 6	

3.5.7. Максимальное число записей LLDP (lldp neighbors max-num)

Команда	lldp neighbors max-num < value > no lldp neighbors max-num	
Параметр	value	предельное число записей, от 5 до 500
Значение по умолчанию	максимальное число записей в удаленной MIB равно 100	
Режим	Режим конфигурации порта	
Руководство по использованию	Позволяет задать максимальное число записей, сохраняемых в удаленной MIB	
Пример	Задать для удаленной MIB в порту ethernet 1/0/5 коммутатора предельное число записей 200. Switch(config)#interface ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)# lldp neighbors max-num 200	

3.5.8. Интервал уведомлений LLDP (lldp notification interval)

Команда	lldp notification interval < seconds > no lldp notification interval	
Параметр	seconds	интервал уведомления, в пределах от 5 до 3600 секунд



Значение по умолчанию	Задан интервал в 5 секунд
Режим	Режим глобальной конфигурации
Руководство по использованию	После того, как установлен интервал уведомления, всякий раз, когда обнаружено изменение удаленной таблицы, по истечении интервала уведомления будет посылаться сообщение "trap"
Пример	Установить интервал отправки сообщений Trap равным 20 секундам. Switch(config)#lldp notification interval 20

3.5.9. Слишком много уведомлений LLPD (lldp tooManyNeighbors)

Команда	lldp tooManyNeighbors {discard delete}	
Параметр	discard	Отбрасывает текущее сообщение
	delete	Удаляет сообщение с наименьшим TTL в удаленной таблице
Значение по умолчанию	Отбрасывает текущее сообщение	
Режим	Режим конфигурации порта	
Руководство по использованию	Когда удаленная MIB заполнена полностью, выбор опции discard приводит к отбрасыванию принятого сообщения. Если выбрана опция delete, из удаленной таблицы будет удалено сообщение с наименьшим TTL	
Пример	Задать для порта ethernet 1/0/5 режим удаления. Switch(config)#interface ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)#lldp tooManyNeighbors delete	

3.5.10. Задержка передачи LLDP (lldp transmit delay)

Команда	lldp transmit delay < seconds > no lldp transmit delay	
Параметр	seconds	интервал времени, в пределах от 1 до 8192 с
Значение по умолчанию	задан интервал в 2 секунды	



Режим	Режим глобальной конфигурации
Руководство по использованию	При постоянной отправке сообщений задержка отправки позволяет защитить удаленный хост от большого числа повторных обновлений информации, обусловленных отправкой большого количества сообщений
Пример	Установить задержку отправки сообщений в 3 секунды. Switch(config)#lldp transmit delay 3

3.5.11. Опциональный TLV передачи LLDP (lldp transmit optional tlv)

Команда	lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap] no lldp transmit optional tlv	
Параметр	portDesc	описание порта
	sysName	имя системы
	sysDesc	описание системы
	sysCap	функции системы
Значение по умолчанию	Сообщения не содержат опции TLV	
Режим	Режим конфигурации порта	
Руководство по использованию	При настройке optional TLV каждый TLV может появляться в сообщении только один раз, portDesc optional TLV это имя локального порта; sysName optional TLV это имя локальной системы; sysDesc optional TLV это описание локальной системы; sysCap optional TLV это функции локальной системы	
Пример	Задать в порту ethernet 0/0/5 коммутатора отправку информации portDesc и sysCap TLV. Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)# lldp transmit optional tlv portDesc sysCap	

3.5.12. Сообщения прерывания LLDP (lldp trap)

Команда	lldp trap <enable disable>
Параметр	-



Значение по умолчанию	Отправка сообщений Trap выключена
Режим	Режим конфигурации порта
Руководство по использованию	Команда позволяет включить в порту отправку сообщений Trap
Пример	Включить отправку сообщений Trap на порту ethernet 1/0/5 коммутатора. <pre>Switch(config)#in ethernet1/0/5 Switch(Config-If-Ethernet1/0/5)#lldp trap enable</pre>

3.5.13. Интервал отправки LLDP (lldp tx-interval)

Команда	lldp tx-interval < integer > no lldp tx-interval	
Параметр	integer	интервал отправки сообщений обновления, варьируется от 5 до 32 768 секунд
Значение по умолчанию	30 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Когда задан интервал отправки сообщений LLDP, они могут быть приняты только по истечении этого интервала. Интервал должен быть меньше или равен половине времени старения, так как слишком большой интервал приведет к тому, что состояние старения и восстановления будет происходить слишком часто; а слишком короткий интервал увеличит сетевой трафик и снизит пропускную способность порта. Значение времени старения сообщений - это произведение множителя и интервала между отправкой сообщений. Максимальное время старения составляет 65 535 секунд. Когда используется интервал отправки (tx-interval), заданный по умолчанию и соответствующими командами задана задержка, интервал отправки будет в 4 раза больше задержки, а не 40 секунд, которые заданы по умолчанию	
Пример	Установить интервал отправки сообщений 40 с <pre>Switch(config)#lldp tx-interval 40</pre>	



3.5.14. Вывод данных отладки LLDP (show debugging lldp)

Команда	show debugging lldp
Параметр	-
Значение по умолчанию	-
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Ввод команды "show debugging lldp" позволяет пользователям проверить информацию о всех портах, на которых включена отладка LLDP
Пример	Вывести информацию о всех портах, на которых включена отладка LLDP. <pre>Switch(config)#show debugging lldp ====BEGINNING OF LLDP DEBUG SETTINGS==== debug lldp packets interface Ethernet1/0/1 =====END OF DEBUG SETTINGS=====</pre>

3.5.15. Вывод данных LLDP (show lldp)

Команда	show lldp
Параметр	-
Значение по умолчанию	Не отображать информацию о конфигурировании глобального LLDP
Режим	Привилегированный режим, Режим глобальной конфигурации
Руководство по использованию	Введя команду "show lldp", пользователи могут проанализировать всю информацию LLDP режима глобальной конфигурации
Пример	Вывести на экран всю информацию LLDP режима глобальной конфигурации, доступную на коммутаторе. <pre>Switch(config)#show lldp -----LLDP GLOBAL INFORMATION----- LLDP has been enabled globally. LLDP enabled port : Ethernet1/0/1 Ethernet1/0/7 LLDP interval : 30 LLDP txTTL : 120</pre>



	LLDP NotificationInterval : 5 LLDP txDelay : 2 LLDP-MED FastStart Repeat Count : 4 END

3.5.16. Вывод Ethernet-интерфейса LLDP (show lldp interface ethernet)

Команда	show lldp interface ethernet < IFNAME >	
Параметр	IFNAME	имя интерфейса
Значение по умолчанию	Настройки LLDP в порту на экран не выводятся	
Режим	Привилегированный режим, Режим глобальной конфигурации	
Руководство по использованию	Команда "show lldp interface ethernet XXX" позволяет пользователям проверить настройки LLDP в указанном порту	
Пример	Вывести на экран информацию о настройках LLDP в порту после включения на коммутаторе функции LLDP в режиме глобальной конфигурации. <pre>Switch (config-if-ethernet1/0/1)#show lldp int e 1/0/1 Port name : Ethernet1/0/1 LLDP Agent Adminstatus : Both LLDP Operation TLV : default LLDP Management Address TLV status : unenable LLDP Trap Status : disable LLDP maxRemote : 100 LLDP Overflow handle : discard LLDP interface remote status : Free lldp dot3 TLV: MED Optional TLV : default MED Trap Status: Disable MED TLV Transmit Status: Disable MED Fast Transmit Status: Disable *****</pre>	

3.5.17. Вывод данных Ethernet-интерфейса соседних устройств LLDP (show lldp neighbors interface ethernet)

Команда	show lldp neighbors interface ethernet < IFNAME >	
Параметр	IFNAME	имя интерфейса



Значение по умолчанию	Информация LLDP о соседних устройствах порта на экран не выводится
Режим	Привилегированный режим, Режим глобальной конфигурации
Руководство по использованию	Команда "show lldp interface ethernet XXX" позволяет пользователям проверить настройки LLDP в указанном порту
Пример	Вывести на экран информацию LLDP после включения на коммутаторе функции LLDP в режиме глобальной конфигурации. <pre>Switch (config-if-ethernet1/0/1)#show lld nei int e 1/0/1</pre> Port name : Ethernet1/0/1 Port Remote Counter : 1 TimeMark : 92 ChassisIdSubtype : 4 ChassisId : 00-e0-4c-00-00-00 PortIdSubtype : Local PortId : gi1 Lldp Port Pvid TLV : Lldp port Pvid 1

3.5.18. Вывод данных трафика LLDP (show lldp traffic)

Команда	show lldp traffic																												
Параметр	-																												
Значение по умолчанию	Статистика пакетов данных LLDP на экран не выводится																												
Режим	Привилегированный режим, Режим глобальной конфигурации																												
Руководство по использованию	Команда "show lldp traffic" позволяет пользователям проверить статистику пакетов данных LLDP																												
Пример	Вывести на экран статистику пакетов данных LLDP после включения на коммутаторе функции LLDP в режиме глобальной конфигурации. <pre>Switch(config)#show lldp traffic</pre> <table><thead><tr><th>PortName</th><th>Ageouts</th><th>FramesDiscarded</th><th>FramesInErrors</th></tr><tr><th>FramesIn</th><th>FramesOut</th><th>TLVsDiscarded</th><th></th></tr><tr><th>TLVsUnrecognized</th><th></th><th></th><th></th></tr></thead><tbody><tr><td>Ethernet1/0/1</td><td>0</td><td>0</td><td>43</td></tr><tr><td>42</td><td>0</td><td>0</td><td></td></tr><tr><td>Ethernet1/0/7</td><td>0</td><td>0</td><td>0</td></tr><tr><td>42</td><td>0</td><td>0</td><td></td></tr></tbody></table>	PortName	Ageouts	FramesDiscarded	FramesInErrors	FramesIn	FramesOut	TLVsDiscarded		TLVsUnrecognized				Ethernet1/0/1	0	0	43	42	0	0		Ethernet1/0/7	0	0	0	42	0	0	
PortName	Ageouts	FramesDiscarded	FramesInErrors																										
FramesIn	FramesOut	TLVsDiscarded																											
TLVsUnrecognized																													
Ethernet1/0/1	0	0	43																										
42	0	0																											
Ethernet1/0/7	0	0	0																										
42	0	0																											



3.6. Команды для настройки канала порта (Port Channel)

3.6.1. Интерфейс Port Channel (interface port-channel)

Команда	interface port-channel < port-channel-number >	
Параметр	port-channel-number	номер Port Channel
Значение по умолчанию	-	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда подключает режим настройки интерфейса port-channel	
Пример	Войти в режим настройки интерфейса port-channel 1. Switch(config)#interface port-channel 1 Switch(Config-If-Port-Channel1)#	

3.6.2. Приоритет порта протокола LACP (lacp port-priority)

Команда	lacp port-priority < port-priority > no lacp port-priority	
Параметр	port-priority	приоритет порта протокола LACP, в диапазоне от 0 до 65 535
Значение по умолчанию	Системой задано значение 32768	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда меняет приоритет порта протокола LACP, "no" перед началом команды восстанавливает значение по умолчанию	
Пример	Задать приоритет порта протокола LACP. Switch(Config-If-Ethernet1/0/1)# lacp port-priority 30000	

3.6.3. Приоритет системы протокола LACP (lacp system-priority)

Команда	lacp system-priority < system-priority > no lacp system-priority	
Параметр	system-priority	приоритет системы протокола LACP, в диапазоне от 0 до 65 535



Значение по умолчанию	Системой задано значение 32 768
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда меняет приоритет системы протокола LACP, "no" в начале команды восстанавливает значение по умолчанию
Пример	Задать приоритет системы протокола LACP. Switch(config)#lacp system-priority 30000

3.6.4. Тайм-аут LACP (lacp timeout)

Команда	lacp timeout {short long} no lacp timeout	
Параметр	-	
Значение по умолчанию	Long (длительный таймаут)	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда устанавливает таймаут для протокола LACP	
Пример	Установить режим таймаута "short " для протокола LACP. Switch(Config-If-Ethernet1/0/1)#lacp timeout short	

3.6.5. Балансировка нагрузки (load-balance)

Команда	load-balance {src-mac dst-mac dst-src-mac src-ip dst-ip dst-src-ip ingress-port dst-src-mac-ip} no load-balance	
Параметр	src-mac	балансировка нагрузки на основе MAC-адресов источника
	dst-mac	балансировка нагрузки на основе MAC-адресов назначения
	dst-src-mac	балансировка нагрузки на основе MAC-адресов источника и назначения



	src-ip	балансировка нагрузки на основе IP-адресов источника
	dst-ip	балансировка нагрузки на основе IP-адресов назначения
	dst-src-ip	балансировка нагрузки на основе IP-адресов источника и назначения
	ingress-port	выполняет балансировку нагрузки в соответствии с MAC-адресом назначения и источника, а также IP источника
	dst-src-mac-ip	выполняет балансировку нагрузки в соответствии с портом приема потока
Значение по умолчанию	Балансировка нагрузки в соответствии с MAC-адресом источника	
Режим	Режима глобальной конфигурации	
Руководство по использованию	Используя port-channel для баланса нагрузки, пользователь может настроить режим баланса нагрузки в соответствии с требованиями. Если конкретный режим баланса нагрузки в командной строке отличается от текущего режима баланса нагрузки группы портов, то меняется баланс нагрузки группы портов в соответствии с конкретным балансом нагрузки командной строки; в противном случае придет сообщение о том, что текущий режим уже настроен	
Пример	Установить режим баланса нагрузки группы портов (port-group). Switch(config)#interface port-channel 1 Switch(Config-If-Port-Channel1)#load-balance src-mac	

3.6.6. Группа портов (port-group)

Команда	port-group < port-group-number > no port-group < port-group-number >	
Параметр	port-group-number	номер группы port channel, в диапазоне 1–127
Значение по умолчанию	Группа портов не задана	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда позволяет создать максимум 127 групп портов
Пример	Создать группу портов. Switch(config)# port-group 1 Удалить группу портов. Switch(config)#no port-group 1

3.6.7. Режим группы портов (port-group mode)

Команда	port-group < port-group-number > mode {active passive on} no port-group	
Параметр	port-group-number	номер группы port channel, в пределах от 1 до 15;
	active	включает протокол LACP на порту, устанавливает на нем активный режим (Active mode);
	passive	включает протокол LACP на порту, устанавливает на нем пассивный режим (Passive mode);
	on	принудительно вводит порт в состав port channel, протокол LACP при этом не включается
Значение по умолчанию	Порты коммутатора не принадлежат port-channel. Протокол LACP не включен	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда позволяет добавить физический порт в port channel. "No" перед началом команды удаляет указанный порт из port channel	
Пример	В режиме настройки порта Ethernet1/0/1 добавить текущий порт "port-group 1" в режиме "active". Switch(Config-If-Ethernet1/0/1)#port-group 1 mode active	

3.6.8. Вывод данных группы портов (show port-group)

Команда	show port-group [< port-group-number >] {brief detail }	
Параметр	port-group-number	номер группы port channel, которую необходимо показать, от 1 до 128
Значение по умолчанию	-	



Режим	Все режимы конфигурации
Руководство по использованию	Если пользователь не задает "port-group-number", то отображается информация обо всех существующих port-group; если port channel, отвечающего параметру "port-group-number", не существует, будет выведено сообщение об ошибке, в ином случае отобразится информация о текущем port-channel для указанного номера группы
Пример	Вывести на экран сводную информацию для группы портов 1. Switch#show port-group brief ID: номер группы портов; Mode: режим группы портов, например, active или passive; Ports: различные типы номеров портов в группе портов, первый - номер выбранных портов, второй - номер резервных портов, третий - номер не выбранных портов. <pre>ID Mode Partner ID Ports Load-balance 1 active 0x0000,00-00-00-00-00-00 0,0,1 src-mac</pre>

3.7. Настройка MTU

3.7.1. MTU (Mtu)

Команда	mtu [< mtu-value >] no mtu	
Параметр	mtu-value	значение MTU кадров, которые могут быть получены, в байтах, в диапазоне <1500-12270>. Соответствующий размер кадра составляет <1518/1522-12288/12292>. Без настройки этого параметра допустимый максимальный размер кадра составляет 12288/12292
Значение по умолчанию	Функция MTU по умолчанию не включена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Необходимо установить MTU на обеих сторонах коммутатора, иначе кадры с MTU будут отбрасываться	
Пример	Включить функцию MTU в коммутаторе. Switch(config)#mtu	



3.8. Команды для EFM OAM

3.8.1. Удаление данных Ethernet OAM (clear ethernet-oam)

Команда	clear ethernet-oam [interface {ethernet } < IFNAME >]	
Параметр	IFNAME	имя порта, в котором нужно удалить статистику OAM
Значение по умолчанию	Отсутствует	
Режим	Привилегированный режим	
Руководство по использованию	Отсутствует	
Пример	Очистить статистическую информацию пакетов OAM и событиях соединения на всех портах. Switch(config)#clear ethernet-oam	

3.8.2. Ethernet OAM (ethernet-oam)

Команда	ethernet-oam no ethernet-oam	
Параметр	-	
Значение по умолчанию	Отключено	
Режим	Настройка портов	
Руководство по использованию	Отсутствует	
Пример	Включить ethernet-oam в Ethernet 1/0/4 Switch(config)#interface ethernet 1/0/4 Switch(Config-If-Ethernet1/0/4)#ethernet-oam	



3.8.3. Верхний порог события ошибочного кадра для Ethernet OAM (ethernet-oam errored-frame threshold high)

Команда	ethernet-oam errored-frame threshold high {< high-frames > none} no ethernet-oam errored-frame threshold high	
Параметр	high-frames	верхний порог обнаружения события ошибочного кадра, в диапазоне от 2 до 4 294 967 295
	none	отменяет настройку верхнего порогового значения
Значение по умолчанию	Отсутствует	
Режим	Настройка портов	
Руководство по использованию	В течение определенного периода обнаружения, если количество ошибочных кадров больше или равно верхнему порогу, вызывается критическое событие в канале связи, и устройство уведомляет об этом пир, отправляя Information OAMPDU, в котором значение флага Link Fault в поле Flags равно 1. Верхний порог не может быть меньше нижнего порога	
Пример	Установить верхний порог события ошибочного кадра для Ethernet 1/0/4 на 3000. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame threshold high 3000	

3.8.4. Нижний порог события ошибочного кадра для Ethernet OAM (ethernet-oam errored-frame threshold low)

Команда	ethernet-oam errored-frame threshold low < low-frames > no ethernet-oam errored-frame threshold low	
Параметр	low-frames	нижний порог обнаружения события ошибочного кадра, в диапазоне от 1 до 4 294 967 295
Значение по умолчанию	1	
Режим	Настройка портов	



Руководство по использованию	Если, в течение заданного периода обнаружения, количество событий ошибочных кадров больше или равно нижнему порогу, вызывается событие "errored frame", и устройство уведомляет об этом пир, посылая уведомление о событии OAMPDU. Обратите внимание, что нижний порог не может быть больше верхнего
Пример	Настроить нижний порог события ошибочного кадра на Ethernet 1/0/4 на 100. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame threshold low 100

3.8.5. Диапазон обнаружения ошибочных кадров Ethernet OAM (ethernet-oam errored-frame window)

Команда	ethernet-oam errored-frame window < seconds > no ethernet-oam errored-frame window	
Параметр	seconds	время подсчета указанного номера кадра, в диапазоне от 5 до 300, измеряется в 200 мс
Значение по умолчанию	5	
Режим	Настройка портов	
Руководство по использованию	Команда позволяет обнаруживать ошибочные кадры порта по истечении определенного периода обнаружения. Если количество ошибочных кадров больше или равно пороговому значению, вызывается соответствующее событие, о котором устройство уведомляет пир через OAMPDU	
Пример	Настроить период обнаружения события ошибочного кадра на порту 1/0/4 на 20 секунд. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame window 100	

3.8.6. Верхний порог обнаружения события ошибочного кадра для Ethernet OAM (ethernet-oam errored-frame-seconds threshold high)

Команда	ethernet-oam errored-frame-seconds threshold high {< high-seconds > none} no ethernet-oam errored-frame-seconds threshold high	
Параметр	high-seconds	верхний порог обнаружения события ошибочного кадра, в диапазоне от 2 до 18 446 744 073 709 551 615



	none	отменяет настройку верхнего порогового значения
Значение по умолчанию	Отсутствует	
Режим	Настройка портов	
Руководство по использованию	Если количество ошибочных кадров больше или равно верхнему порогу в течение заданного периода обнаружения, вызывается серьезное событие в канале связи, и устройство посылает информационный OAMPDU, где поле Flags имеет значение флага Link Fault 1. Верхнее пороговое значение не может быть меньше нижнего порогового значения	
Пример	Настроить верхний порог события ошибочных кадров на порту 1/0/4 на 3000. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds threshold high 3000	

3.8.7. Нижний порог обнаружения события ошибочного кадра для Ethernet OAM (ethernet-oam errored-frame-seconds threshold Low)

Команда	ethernet-oam errored-frame-seconds threshold low < low-seconds > no ethernet-oam errored-frame-seconds threshold low	
Параметр	low-seconds	нижний порог событий секунд ошибочных кадров, в диапазоне от 1 до 65 535 секунд
Значение по умолчанию	1	
Режим	Настройка портов	
Руководство по использованию	Если, в течение заданного периода обнаружения, длительность события ошибочных кадров больше или равно нижнему порогу в течение заданного периода обнаружения, вызывается событие "errored frame period", и устройство уведомляет об этом пир, посылая уведомление о событии OAMPDU. Обратите внимание, что нижний порог не должен быть больше верхнего	
Пример	Настройте нижний порог события периода ошибочных кадров на порту 1/0/4 на 100. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds threshold low 100	



3.8.8. Окно времени ошибочных кадров Ethernet OAM (ethernet-oam errored-frame-seconds window)

Команда	ethernet-oam errored-frame-seconds window < seconds > no ethernet-oam errored-frame-seconds window	
Параметр	seconds	время подсчета для указанного номера кадра, диапазон от 50 до 450, единица измерения — 200 мс
Значение по умолчанию	300	
Режим	Настройка портов	
Руководство по использованию	Обнаружение времени ошибочных кадров порта по истечении определенного периода обнаружения. Если количество секунд ошибочных кадров больше или равно пороговому значению, вызывается соответствующее событие, о котором устройство уведомляет пир через OAMPDU	
Пример	Настроить период обнаружения событий ошибочных кадров на порту 1/0/4 на 120 секунд. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds window 600	

3.8.9. Верхнее пороговое значение обнаружения события ошибочного символа Ethernet OAM (ethernet-oam errored-symbol-period threshold High)

Команда	ethernet-oam errored-symbol-period threshold high {< high-symbols > none} no ethernet-oam errored-symbol-period threshold high	
Параметр	high-symbols	верхнее пороговое значение обнаружения события ошибочного символа, в диапазоне от 2 до 18 446 744 073 709 551 615 символов
	none	отменяет настройку верхнего порогового значения
Значение по умолчанию	отсутствует	
Режим	Настройка портов	



Руководство по использованию	В течение определенного периода обнаружения, если количество ошибочных символов больше или равно верхнему порогу порогу, вызывается критическое событие в канале связи, и устройство уведомляет об этом пир, отправляя Information OAMPDU, в котором значение флага Link Fault в поле Flags равно 1. Верхнее пороговое значение не может быть меньше нижнего
Пример	Задать верхний порог для события "errored symbol" на порту 1/0/4 с параметром "none". Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period threshold high none

3.8.10. Нижнее пороговое значение обнаружения события ошибочного символа Ethernet OAM (ethernet-oam errored-symbol-period threshold Low)

Команда	ethernet-oam errored-symbol-period threshold low < low-symbols > no ethernet-oam errored-symbol-period threshold low	
Параметр	low-symbols	нижнее пороговое значение обнаружения события ошибочного символа, в диапазоне от 1 до 18 446 744 073 709 551 615 символов
Значение по умолчанию	1	
Режим	Настройка портов	
Руководство по использованию	Если, в течение заданного периода обнаружения, количество ошибочных символов больше или равно нижнему порогу, вызывается событие "errored symbol", и устройство уведомляет об этом пир, отправляя уведомление о событии OAMPDU. Обратите внимание, что нижний порог не должен быть больше верхнего	
Пример	Задать нижний порог события "errored symbol" (ошибочный символ) на порту 1/0/4 равным 5. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period threshold low 5	



3.8.11. Период обнаружения ошибочного символа Ethernet OAM (ethernet-oam errored-symbol-period window)

Команда	ethernet-oam errored-symbol-period window < seconds > no ethernet-oam errored-symbol-period window	
Параметр	seconds	время подсчета указанного номера кадра, диапазон от 5 до 300, единица измерения — 200 мс
Значение по умолчанию	5	
Режим	Настройка портов	
Руководство по использованию	Команда задает обнаружение ошибочных символов порта по истечении определенного периода обнаружения. Если количество ошибочных символов больше или равно пороговому значению, вызывается соответствующее событие, и устройство уведомляет об этом пир через OAMPDU	
Пример	Установить период обнаружения события ошибочного символа на порту 1/0/4 равным 2 с. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period window 10	

3.8.12. Мониторинг соединения Ethernet OAM (ethernet-oam link-monitor)

Команда	ethernet-oam link-monitor no ethernet-oam link-monitor	
Параметр	-	
Значение по умолчанию	Включено	
Режим	Настройка портов	
Руководство по использованию	Команда подключает функцию OAM для мониторинга локальных ошибок в каналах. Как правило, мониторинг соединения включается при включении функции OAM порта. Если функция отслеживания локальных ошибок соединения OAM выключена, информация о событии OAMPDU от равноправного сервера по-прежнему нормально принимается и обрабатывается	
Пример	Включить мониторинг соединения порта 1/0/4. Switch(Config-If-Ethernet1/0/4)#ethernet-oam link-monitor	



3.8.13. Режим Ethernet OAM (ethernet-oam mode)

Команда	ethernet-oam mode {active passive} no ethernet-oam mode	
Параметр	Active	активный режим (установка соединения)
	passive	пассивный режим (ожидание запроса на соединение)
Значение по умолчанию	активный режим (установка соединения)	
Режим	Настройка портов	
Руководство по использованию	Один из подключенных OAM модулей должен находится в активном режиме. После включения OAM изменить режим работы OAM нельзя, поэтому, если необходимо изменить режим работы необходимо отключить функцию OAM	
Пример	Установить режим работы функции OAM на ethernet 1/0/4 в режим "passive". Switch(Config-If-Ethernet1/0/4)#ethernet-oam mode passive	

3.8.14. Интервал Ethernet OAM (ethernet-oam period)

Команда	ethernet-oam period < seconds > no ethernet-oam mode	
Параметр	seconds	Период отправки, от 1 до 2 секунд
Значение по умолчанию	1 секунда	
Режим	Настройка портов	
Руководство по использованию	С помощью этой команды настраивается интервал передачи сообщений OAMPDU, которые поддерживают штатное соединение OAM	
Пример	Задать интервал передачи сообщений OAMPDU для ethernet 1/0/4 равным 2 секундам. Switch(Config-If-Ethernet1/0/4)# ethernet-oam period 2	



3.8.15. Удаленная индикация сбоев Ethernet OAM (ethernet-oam remote-failure)

Команда	ethernet-oam remote-failure no ethernet-oam remote-failure
Параметр	-
Значение по умолчанию	Включено
Режим	Настройка портов
Руководство по использованию	Если включена функция удаленной индикации сбоев, то при возникновении критического события или сбоя канала на локальном уровне, он оповестит об этом пир, отправив Information OAMPDU, зарегистрирует информацию о сбое и отправит предупреждение SNMP trap. Когда удаленная индикация отказа отключена, несмотря на то, что локальное критическое событие или событие неисправности канала не отслеживается, информация об индикации отказа от пира по-прежнему нормально принимается и обрабатывается
Пример	Подключить удаленную индикацию сбоев ethernet 1/0/4. Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-failure

3.8.16. Удаленная петля Ethernet OAM (ethernet-oam remote-loopback)

Команда	ethernet-oam remote-loopback no ethernet-oam remote-loopback
Параметр	-
Значение по умолчанию	Отключено
Режим	Настройка порта
Руководство по использованию	В автоматическом режиме только OAM может посылать запросы на удаленную петлю, OAM, работающие в пассивном режиме, не могут посылать удаленные петли, когда удаленный OAM работает в режиме петли, все пакеты, кроме пакетов OAM PDU, следуют по одному маршруту обратно к локальному порту (Примечание: в режиме удаленного тестирования OAM нормальная работа канала не возможна), администратор может проверить задержку соединения, колебания и пропускную способность петли. Он может выполнить конфигурирование обратной петли после создания OAM-связи, если OAM-связь будет разорвана во время обратной петли, обратная петля



	будет автоматически отменена. Вместе с "ethernet-oam remote-loopback" поддерживается команда "mutex"
Пример	Включить удаленный OAM порта 1/0/4 в режим удаленной петли. <pre>Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-loopback</pre> Normal forwarding will be suspended during the remote-loopback, are you sure to start remote-loopback? [Y/N]

3.8.17. Поддержка обратной петли Ethernet OAM (ethernet-oam remote-loopback supported)

Команда	ethernet-oam remote-loopback supported no ethernet-oam remote-loopback supported	
Параметр	-	
Значение по умолчанию	Отключено	
Режим	Режим конфигурации порта	
Руководство по использованию	Только порты с включенной поддержкой обратной петли могут получать запросы обратной петли OAM и находиться в режиме обратной петли. Поэтому при включении удаленной петли и петли в OAM убедитесь, что удаленный настроен на поддержку петли. Для взаимного исключения используйте команду "ethernet-oam remote-loopback"	
Пример	Включить функцию поддержки обратной петли OAM для ethernet 1/0/4 Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-loopback supported	

3.8.18. Тайм-аут Ethernet OAM (ethernet-oam timeout)

Команда	ethernet-oam timeout < seconds > no ethernet-oam timeout	
Параметр	seconds	тайм-аут в диапазоне от 5 до 10 секунд
Значение по умолчанию	5 секунд	
Режим	Настройка портов	



Руководство по использованию	По данной команде OAM-соединение будет разорвано, если по истечении указанного периода не будет получено ни одного OAMPDU
Пример	Установить таймаут OAM-соединения для ethernet 1/0/4 равным 6 секундам. Switch(Config-If-Ethernet1/0/4)#ethernet-oam timeout 6

3.8.19. Вывод данных Ethernet OAM (show ethernet-oam)

Команда	show ethernet-oam [{local remote} interface {ethernet } < IFNAME >]	
Параметр	IFNAME	порт, на котором будет отображаться информация о соединении OAM
Значение по умолчанию	Не применимо	
Режим	Привилегированный режим	
Руководство по использованию	Не применимо	
Пример	Показать сводную информацию о соединении Ethernet OAM. Switch#show ethernet-oam Switch#show ethernet-oam Коды функционала: L - монитор соединения, R - удаленная петля U - однонаправленный, V - извлечение переменных Interface Local-Mode Local-Capability Remote-MAC-Addr Remote-Mode Remote-Capability 1/0/1 active L	

3.8.20. Вывод данных о событиях Ethernet OAM (show ethernet-oam events)

Команда	show ethernet-oam events {local remote} [interface {ethernet } < IFNAME >]	
Параметр	IFNAME	порт, на котором должна отображаться статистическая информация о событиях в канале OAM



Значение по умолчанию	Не применимо
Режим	Привилегированный режим
Руководство по использованию	Не применимо
Пример	Отобразить статистическую информацию о событиях на канале Ethernet 1/0/1. Switch#show ethernet-oam events local interface 1/0/1 ethernet1/0/1 link-events : OAM_local_errored-symbol-period-events: ----- event time stamp : 3539 errored symbol window(200ms) : 5 errored symbol low threshold : 1 errored symbol high threshold : none errored symbol : 1200120 errored running total : 2302512542 event running total : 232 OAM_local_errored-frame-period-events: ----- event time stamp : 3539 errored frame window(200ms) : 50 errored frame low threshold : 1 errored frame high threshold : none errored frame : 1200120 errored running total : 2302512542 event running total : 52 OAM_local_errored-frame-events: ----- event time stamp : 3539 errored frame window(200ms) : 5 errored frame low threshold : 1 errored frame high threshold : none errored frame : 1200120 errored running total : 2302512542 event running total : 75 OAM_local_errored-frame-seconds-summary-events: ----- event time stamp : 3520 errored frame seconds summary window(200ms) : 300 errored frame low threshold : 1 errored frame high threshold : none errored frame : 1200120 errored running total : 2302512542 event running total : 232 OAM_local_link-fault : 0 OAM_local_dying gasp : 0 OAM_local_critical event : 0



3.8.21. Вывод данных конфигурирования событий соединения Ethernet OAM (show ethernet-oam link-events-configuration)

Команда	show ethernet-oam link-events-configuration [interface {ethernet } < IFNAME >]	
Параметр	IFNAME	порт, на котором должна отображаться статистическая информация о событиях в канале OAM
Значение по умолчанию	Не применимо	
Режим	Привилегированный режим	
Руководство по использованию	Не применимо	
Пример	Показать конфигурирование событий соединения на ethernet 1/0/1. <pre>Switch#show ethernet-oam link-events-configuration interface ethernet 1/0/1 Ethernet1/0/1 link-monitor configuration : event high-threshold low-threshold window(200ms) ----- Err-symbol-Period none 1 2 Err-frame-Period none 1 10 Err-frame none 2 5 Err-frame-second-summary none 2 600</pre>	

3.8.22. Вывод состояния петли Ethernet OAM (show ethernet-oam loopback status)

Команда	show ethernet-oam loopback status [interface {ethernet } < IFNAME >]	
Параметр	IFNAME	означает отображение информации о состоянии порта OAM loopback
Значение по умолчанию	-	
Режим	Привилегированный режим	
Руководство по использованию	Команда выводит на экран состояние петли OAM всех или обозначенных портов коммутатора	



Пример	Вывести на экран состояние петли OAM всех портов. Switch(config)#show ethernet-oam loopback status OAM Loopback Status: Ethernet1/0/1: disable Ethernet1/0/2: disable Ethernet1/0/3: disable

3.9. Конфигурирование Port Security

3.9.1. Удаление защищенных адресов порта (clear port-security)

Команда	clear port-security {all configured dynamic sticky} [[address < mac-addr> interface < interface-id>] [vlan < vlan-id>]]	
Параметр	All	все защищенные MAC-адреса на интерфейсах
	configured	все добавленные вручную защищенные MAC-адреса
	dynamic	динамические изученные защищенные MAC-адреса
	Sticky	MAC-адреса, добавленные функцией sticky
	mac-addr	указанный защищенный MAC-адрес
	interface-id	записи защищенных MAC-адресов указанного интерфейса
	vlan-id	указанный VLAN
Значение по умолчанию	-	
Режим	Привилегированный режим	
Руководство по использованию	Команда очищает защищенные MAC-адреса на интерфейсе	
Пример	Очистить все защищенные MAC-адреса на интерфейсе Switch#clear port-security all	



3.9.2. Вывод данных защиты порта (show port-security)

Команда	show port-security [interface < interface-id >] [address vlan]	
Параметр	interface-id	показать конфигурирование защиты порта на интерфейсе
	address	показать безопасный адрес интерфейса
	vlan	показать максимальное количество каждой VLAN, сконфигурированной на магистральном/гибридном интерфейсе
Значение по умолчанию	-	
Режим	Любой режим	
Руководство по использованию	Команда показывает конфигурирование защиты порта	
Пример	Показать все защищенные MAC-адреса на интерфейсах. Switch# show port-security address interface ethernet 1/0/1	

3.9.3. Настройка защиты порта (switchport port-security)

Команда	switchport port-security no switchport port-security	
Параметр	-	
Значение по умолчанию	Отключено	
Режим	Настройка портов	
Руководство по использованию	Настраивает механизм обеспечения защиты порта для интерфейса. "no" перед началом команды отключает эту функцию	
Пример	Включить механизм "port-security" на интерфейсе. Switch(config-if- ethernet1/0/1)#switchport port-security	



3.9.4. Настройка MAC-адреса защиты порта (switchport port-security mac-address)

Команда	switchport port-security mac-address < mac-address > [vlan < vlan-id >] no switchport port-security mac-address < mac-address > [vlan < vlan-id >]	
Параметр	mac-address	задать указанный MAC-адрес в качестве статического
	vlan-id	указанный VLAN MAC-адреса действует только на магистральных и гибридных интерфейсах
Значение по умолчанию	Привязанные MAC-адреса отсутствуют	
Режим	Настройка портов	
Руководство по использованию	При настройке статических защищенных MAC-адресов необходимо следить, чтобы текущее количество MAC-адресов не превышало максимальный лимит, разрешенный интерфейсом. Если максимальное число MAC-адресов превышено, это приведет к нарушению	
Пример	Настройка защищенного MAC-адреса на интерфейсе Switch (config-if- ethernet1/0/1)# switchport port-security mac-address 00-00-00-00-01	

3.9.5. Предельное число защищенных MAC-адресов защиты порта (switchport port-security maximum)

Команда	switchport port-security maximum < value > [vlan < vlan-list >] no switchport port-security maximum < value > [vlan < vlan-list >]	
Параметр	Value	задает предельное число защищенных статических MAC-адресов, разрешенных для интерфейса, от 1 до 128. Определяется максимальным числом MAC на устройстве
	vlan-list	задает максимальное значение для указанной VLAN, действует только на магистральных и гибридных интерфейсах
Значение по умолчанию	После включения функции "port-security", если нет других настроек, максимальное количество защищенных MAC-адресов на интерфейсе равно 1. Количество интерфейсов в VLAN по умолчанию не ограничено	
Режим	Настройка портов	



Руководство по использованию	Обратите внимание на количество соединений между интерфейсами и VLAN, а также установите максимальное количество интерфейсов, настроенных стандартным образом
Пример	Настроить максимальное количество защищенных MAC-адресов на интерфейсе. Switch(config-if- ethernet1/0/1)# switchport port-security maximum 100

3.9.6. Нарушение защиты порта (switchport port-security violation)

Команда	switchport port-security violation {protect recovery restrict shutdown} no switchport port-security violation	
Параметр	protect	режим защиты, запрещает изучение нового MAC-адреса, отбрасывает пакеты и не отправляет предупреждения
	recovery	после срабатывания действия нарушения, функция изучения MAC-адресов может быть восстановлена
	restrict	режим запрета, запускает действия, не позволяющие узнать новый MAC-адрес, отбрасывает пакеты, отправляет snmp trap и записывает настройки в системный журнал (syslog)
	shutdown	отключение, режим задан по умолчанию. В этом случае интерфейс сразу отключается, отправляет snmp trap и записывает настройки в системный журнал (syslog)
Значение по умолчанию	shutdown	
Режим	Настройка портов	
Руководство по использованию	Когда превышено максимальное число настроенных MAC-адресов, MAC-адрес доступа к интерфейсу не принадлежит этому интерфейсу в таблице MAC-адресов или MAC-адрес настроен на несколько интерфейсов в одном VLAN, они оба будут нарушать безопасность MAC-адресов	
Пример	Задать параметр "protect" для режима нарушения безопасности. Switch(config-if-ethernet1/0/1)#switchport port-security violation protect	



3.10. Настройка DDM

3.10.1. Удаление нарушения порогового значения трансивера (clear transceiver threshold-violation)

Команда	clear transceiver threshold-violation [interface ethernet <interface-list>]	
Параметр	interface-list	список интерфейсов, в котором необходимо удалить информацию нарушения порогового значения
Значение по умолчанию	-	
Режим	Привилегированный режим	
Руководство по использованию	Команда удаляет нарушения порогового значения, обнаруженные трансивером	
Пример	Удалить значение нарушений порогового значения мониторинга трансивера на портах 21, 25, 26, 28. Switch#clear transceiver threshold-violation interface ethernet 1/0/21; 25-26; 28	

3.10.2. Вывод данных трансивера (show transceiver)

Команда	show transceiver [interface ethernet <interface-list>] [detail]	
Параметр	interface-list	список интерфейсов, которые необходимо отобразить для мониторинга трансивера
	detail	показывает подробный мониторинг на трансивере
Значение по умолчанию	-	
Режим	Режим пользователя, Привилегированный режим, Режим глобальной конфигурации	
Руководство по использованию	По команде отображается подробная информация мониторинга трансивера	



Пример	Показать краткую информацию о DDM для всех портов. Switch#show transceiver					
	Interface	Temp (°C)	Voltage (V)	Bias (mA)	RX Power (dBm)	TX Power (dBm)
	1/0/25	33	3.31	6.11	-30.54 (A-)	-6.01
	1/0/26	33	5.00 (W+)	6.11	-20.54 (W-)	-6.02

3.10.3. Вывод мониторинга трансивера (show transceiver threshold-violation)

Команда	show transceiver threshold-violation [interface ethernet <interface-list>]	
Параметр	interface-list	список интерфейсов, для которых необходимо вывести мониторинг трансивера
Значение по умолчанию	-	
Режим	Привилегированный режим и глобальной конфигурации	
Руководство по использованию	Команда показывает информацию мониторинга трансивера	

Ethernet 1/0/25 transceiver threshold-violation

information: Transceiver monitor is enabled.

Monitor interval is set to 30 minutes. The current time is Jan 02 12: 30: 50 2010.

The last threshold-violation time is Jan 01 1: 30: 50 2010.

Brief alarm information:

RX loss of signal

RX power low

Detail diagnostic and threshold information:

Diagnostic Threshold

	Realtime Value	High Alarm	Low Alarm	High Warn	Low Warn
Temperature (°C)	33	70	0	70	0
Voltage (V)	7.31	10.00	0.00	5.00	0.00
Bias current (mA)	3.11	10.30	0.00	5.00	0.00



RX Power (dBm)	-30.54(A-)	9.00	-25.00(-34)	9.00	-25.00
TX Power (dBm)	-1.01	9.00	12.05	9.00	-10.00

Ethernet 1/0/26 transceiver threshold-violation
information: Transceiver monitor is disabled.

Monitor interval is set to 30 minutes.

The last threshold-violation doesn't exist.

3.10.4. Мониторинг трансивера (transceiver-monitoring)

Команда	transceiver-monitoring {enable disable}
Параметр	-
Значение по умолчанию	Отключено
Режим	Настройка портов
Руководство по использованию	Команда позволяет включать/выключать функцию мониторинга трансивера
Пример	Включить функцию мониторинга трансивера для ethernet1/0/1. Switch(config-if-ethernet1/0/1)#transceiver-monitoring enable

3.10.5. Интервал мониторинга трансивера (transceiver-monitoring interval)

Команда	transceiver-monitoring interval <minutes> no transceiver-monitoring interval	
Параметр	minutes	интервал мониторинга, который необходимо задать
Значение по умолчанию	15 минут	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда задает интервал мониторинга трансивера. "No" в начале команды возвращает интервал по умолчанию в 15 минут	
Пример	Задать интервал мониторинга трансивера в 1 минуту. Switch(config)#transceiver-monitoring interval 1	



3.10.6. Порог трансивера (transceiver threshold)

Команда	transceiver threshold {default {temperature voltage bias rx-power tx-power} {high-alarm low-alarm high-warn low-warn} {<value> default}}	
Параметр	default	восстанавливает порог по умолчанию, установленный производителем. Если индикатор мониторинга не указан, восстанавливаются все пороги, если индикатор мониторинга указан, восстанавливается только соответствующий порог
	temperature	индикатор мониторинга — температура
	voltage	индикатор мониторинга — напряжение
	bias	индикатор мониторинга — смещение тока
	rx-power	индикатор мониторинга — мощность получения
	tx-power	индикатор мониторинга — мощность отправки
	high-alarm	аварийное сообщение по максимальному значению, а именно, аварийное сообщение с A+ при превышении порогового значения
	low-alarm	аварийное сообщение по минимальному значению, а именно, аварийное сообщение с Aif превышения порогового значения
	high-warn	предупреждение индикатор мониторинга по максимальному значению, а именно, предупреждение W+ при превышении порогового значения
	low-warn	предупреждение индикатор мониторинга по минимальному значению, а именно, предупреждение W- при превышении порогового значения
Значение по умолчанию	Пороговое значение задано производителем	
Режим	Настройка портов	
Руководство по использованию	Для каждого индикатора мониторинга представлены следующие диапазоны пороговых параметров: Температура: -128,00–128,00 °C	



	Напряжение: 0,00~7,00 В Ток смещения: 0,00~140,00 мА х-мощность: -50,00~9,00 дБм tx-мощность: -50,00~9,00 дБм Максимальная длина параметра порога, задаваемого пользователем, составляет 20 бит. После того, как пользователь установит порог параметра, порог, установленный производителем, будет показываться в круглых скобках при отображении значения, а сигнал тревоги будет генерироваться в соответствии с настройками пользователя
Пример	Настроить пороговое значение tx-мощности оптоволоконного модуля, порог для предупреждения по минимальному значению -12 на ethernet1/0/1. Switch(config-if-ethernet1/0/1)#transceiver threshold tx-power low-warn -12

3.11. Настройка LLDP-MED

3.11.1. Физический адрес (civic location)

Команда	civic location {dhcp server switch endpointDev} < country-code > no civic location	
Параметр	dhcp server	задает тип устройства как DHCP-сервер
	Switch	задает тип устройства как коммутатор
	endpointDev	задает тип устройства как LLDP-MED Endpoint
	country-code	задает код страны, состоящий из 2 букв, например, DE или US, он должен соответствовать коду страны по стандарту ISO 3166
Значение по умолчанию	Форматом Civic Address LCI не задано местоположение	
Режим	Настройка портов	
Руководство по использованию	Команда позволяет задать тип устройства и код страны местоположения в формате Civic Address LCI и войти в режим адреса Civic Address LCI для более детальной настройки местоположения	



Пример	Настроить тип устройства как коммутатор и код страны как Россия для местоположения с форматом Civic Address LCI в Ethernet 19. <pre>Switch(Config-If-Ethernet1/0/19)# civic location switch RU Switch(Med-Civic)#</pre>

3.11.2. Данные физического местоположения {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo}

Команда	<pre>{description-language province-state city county street locationNum location floor room postal otherInfo} <address> no {description-language province-state city county street locationNum location floor room postal otherInfo}</pre>	
Параметр	description-language	Язык описания местоположения, например, «русский»
	province-state	Регион, область, штат, кантон, провинция, префектура и т.д., например, «Калининградская»
	city	Город, например, «Москва»
	county	Округ, приход, например, «ДВО»
	street	Улица, например, «Рябиновая»
	locationNum	Номер дома, например, «9»
	location	Наименование и имя владельца объекта, например, «Компания Кьютек»
	floor	Номер этажа, например, «13»
	room	Номер помещения, например, «1308»
	postal	Почтовый индекс, например, «12347-1234»
	otherInfo	Дополнительные данные по местоположению, например, «южное крыло»
	address	Подробный адрес, не должен превышать 250 символов



Значение по умолчанию	Подробная информация о местоположении в режиме Civic Address LCI не настроена на порте
Режим	Режим адреса Civic Address LCI
Руководство по использованию	С помощью этой команды можно указать подробную информацию о местоположении в режиме Civic Address LCI на порту, можно указать максимум 10 типов адресов
Пример	Настроить подробную информацию о местоположении в режиме Civic Address LCI. Switch(Med-Civic)# city Moscow Switch(Med-Civic)# street Ryabinovaya

3.11.3. Местоположение ECS (ecs location)

Команда	ecs location < tel-number > no ecs location	
Параметр	tel-number	символы местоположения в формате ECS ELIN, например, номер телефона экстренной помощи, длина строки символов от 10 до 25
Значение по умолчанию	В формате ECS ELIN расположение не задано	
Режим	Настройка портов	
Руководство по использованию	Диапазон длины строки символов местоположения от 10 до 25 в формате ECS ELIN	
Пример	Задать местоположение в формате ECS ELIN на порту 19. Switch(Config-If-Ethernet1/0/19)# ecs location 74954778118	

3.11.4. Быстрая отправка пакетов LLDP (lldp med fast count)

Команда	lldp med fast count < value > no lldp med fast count	
Параметр	Value	значение для быстрой отправки пакетов, диапазон от 1 до 10, единица измерения - запись
Значение по умолчанию	4	



Режим	Режим глобальной конфигурации
Руководство по использованию	С помощью этой команды задается число для быстрой отправки пакетов
Пример	Установить число быстрых пакетов на 5 Switch(config)#lldp med fast count 5

3.11.5. Отправка сообщений прерывания LLDP (lldp med trap)

Команда	lldp med trap {enable disable}
Параметр	-
Значение по умолчанию	Отключено
Режим	Настройка портов
Руководство по использованию	Команда включает или отключает отправку trap сообщений LLDP-MED порта
Пример	Включить отправку trap сообщений LLDPMED на порту 19. Switch(Config-If-Ethernet1/0/19)# lldp med trap enable

3.11.6. Отправка всеми коммутаторами через LLDP-MED TLV (lldp transmit med tlv all)

Команда	lldp transmit med tlv all no lldp transmit med tlv all
Параметр	-
Значение по умолчанию	Порт не включает функцию отправки LLDP-MED TLV
Режим	Настройка портов
Руководство по использованию	После настройки этой команды, если порт может отправлять LLDP-MED TLV, отправленные LLDP-пакеты с LLDP-MED TLV будут поддерживаться всеми коммутаторами. Однако LLDP пакеты отправляются портом без LLDP-MED TLV после того, как коммутатор настроил соответствующую команду по



Пример	Порт 19 включает функцию отправки LLDP-MED TLV. Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv all

3.11.7. Пропускная способность LLDP-MED TLV (lldp transmit med tlv capability)

Команда	lldp transmit med tlv capability no lldp transmit med tlv capability
Параметр	-
Значение по умолчанию	Функция отправки LLDP-MED Capability TLV отключена
Режим	Настройка портов
Руководство по использованию	После настройки этой команды, если порт способен отправлять LLDP-MED TLV, отправленные LLDP-пакеты будут содержать LLDP-MED Capability TLV. Однако LLDP-пакеты будут отправляться портом без LLDP-MED Capability TLV после настройки команды "no". Примечание: LLDP-MED Capability TLV является важной функцией для LLDP-MED TLV, если не настроить порт на отправку LLDP-MED Capability TLV в первую очередь, другие LLDP-MED TLV не будут отправлены
Пример	Подключить для порта 19 функцию отправки LLDP-MED Capability TLV. Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv capability

3.11.8. Настройка порта для отправки LLDP-MED Extended Power-Via-MDI TLV (lldp transmit med tlv extendPoe)

Команда	lldp transmit med tlv extendPoe no lldp transmit med tlv extendPoe
Параметр	-
Значение по умолчанию	Функция отправки LLDP-MED Extended Power-Via-MDI TLV отключена
Режим	Настройка портов
Руководство по использованию	Команда выполняет настройку указанного порта для отправки LLDP-MED Extended Power-Via-MDI TLV. No в начале команды отключает функцию



Пример	Включить для порта 19 функцию отправки LLDP-MED Extended Power-Via-MDI TLV. Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv extendPoe

3.11.9. Идентификация местоположения LLDP-MED TLV (lldp transmit med tlv location)

Команда	lldp transmit med tlv location no lldp transmit med tlv location
Параметр	-
Значение по умолчанию	Отключено
Режим	Режим конфигурации порта
Руководство по использованию	Команда позволяет настроить для указанного порта отправку LLDP-MED Location Identification (идентификация местоположения). TLV. После настройки этой команды, если порт имеет возможность отправки LLDP-MED TLV, LLDP-пакеты, отправляемые с порта, будут включать LLDP-MED Location Identification TLV. В противном случае LLDP-пакеты, отправляемые с порта, не будут включать LLDP-MED Location Identification TLV по этой же команде с "no" перед началом команды, даже если порт имеет возможность отправлять LLDP-MED TLV. Примечание: Перед настройкой этой функции необходимо настроить возможность отправки LLDP-MED Capability TLV. Если устройство не поддерживает POE или функция POE порта отключена командой, этот TLV не будет отправлен
Пример	Включить на порту 19 функцию отправки LLDP-MED Location Identification TLV. Switch(Config-If-Ethernet1/0/19)#lldp transmit med tlv location

3.11.10. Управление реестром отправки LLDP-MED TLV (lldp transmit med tlv inventory)

Команда	lldp transmit med tlv inventory no lldp transmit med tlv inventory
Параметр	-
Значение по умолчанию	Функция отключена



Режим	Настройка портов
Руководство по использованию	После настройки этой команды, если порт имеет возможность v, LLDP-пакеты с LLDP-MED Inventory Management TLV отправляются портом. Однако, LLDP -пакеты без LLDP-MED Inventory Management TLVs будут отправляться портом после того, как коммутатор задаст соответствующую команду "no". Примечание: LLDP-MED Capability TLV, отправляемый портом, должен быть настроен перед отправкой LLDP-MED Inventory Management TLV, иначе конфигурирование не будет успешным
Пример	Включить для порта 19 функцию отправки LLDP-MED Inventory Management TLV. Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv inventory

3.11.11. Сетевая политика передачи LLDP-MED TLV (lldp transmit med tlv networkPolicy)

Команда	lldp transmit med tlv networkPolicy no lldp transmit med tlv networkPolicy
Параметр	-
Значение по умолчанию	Функция отключена для отправки LLDP-MED Network Policy TLV
Режим	Настройка портов
Руководство по использованию	После настройки этой команды, если порт имеет возможность отправлять LLDP-MED TLV, LLDP-пакеты с LLDP-MED Network Policy TLV отправляются портом. Однако, LLDP пакеты без LLDP-MED Network Policy TLV будут отправляться портом после того, как коммутатор задаст соответствующую команду "no". Примечание: LLDP-MED Capability TLV отправляемый портом, должен быть настроен перед отправкой LLDP-MED Network Policy TLV, иначе конфигурирование не будет успешной
Пример	Включить на порту 19 функцию отправки LLDP-MED Network Policy TLV. Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv networkPolicy



3.11.12. Сетевая политика (network policy)

Команда	network policy {voice voice-signaling guest-voice guest-voice-signaling softphone-voice video-conferencing streaming- video video-signaling} [status {enable disable}] [tag {tagged untagged}] [vid { < vlan-id > dot1p}] [cos < cos-value>] [dscp < dscp-value >] no network policy {voice voice-signaling guest-voice guest-voice-signaling softphone-voice video-conferencing streaming- video video-signaling}	
Параметр	status	подтверждение применения сетевой политики
	enable	сетевая политика указанного типа определена, значение по умолчанию для сетевой политики - enable
	disable	сетевая политика указанного типа была определена, значение по умолчанию для сетевой политики disable
	tag	задает для указанного приложения использование метода VLAN с тегами или без тегов
	tagged	настраивает трафик указанного приложения на использование метода тегированных vlan, при этом поля (такие как идентификатор VLAN, приоритет Layer2 и значение DSCP) становятся действительными
	untagged	настраивает трафик без тегов для указанного приложения, поля (такие как VLAN ID, приоритет Layer2) игнорируются, действует только поле значения DSCP. Untagged - это значение по умолчанию для метода VLAN
	vid	настройка идентификатора VLAN, к которому принадлежит указанное приложение
	vlan-id	настройка идентификатора VLAN ID, диапазон от 1 до 4094
	dot1p	настройка заданного приложения на тегирование трафика с помощью приоритета 802.1p, при этом для загрузки трафика применяется vlan 0
	cos	настройка приоритета кадра Ethernet для VLAN



	cos-value	настройка значения приоритета кадра Ethernet для VLAN, диапазон от 0 до 7, значение по умолчанию - 5
	Dscp	настройка DSCP VLAN
	dscp-value	значение DSCP, введенное пользователем, диапазон от 0 до 63, значение по умолчанию 46
Значение по умолчанию	Для порта не настроена сетевая политика	
Режим	Настройка портов	
Руководство по использованию	Пользователи могут настроить несколько сетевых политик для порта, но их типы приложений не могут дублироваться, а одна сетевая политика должна соответствовать сетевой политике TLV LLDP-MED. Если пользователь настроит несколько политик для порта, он будет отправлять несколько LLDP-MED network policy TLV в пакет LLDP. Если пользователь не задает никаких сетевых политик, ни одна LLDP-MED network policy TLV не отправляется в LLDP пакет	
Пример	Настроить сетевую политику с типом приложения «voice» на порту 19. Switch(Config-If-Ethernet1/0/19)# network policy voice tag tagged vid 2 cos 6 dscp 23	

3.11.13. Вывод данных LLDP (show lldp)

Команда	show lldp
Параметр	-
Значение по умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	Команда позволяет вывести на экран информацию LLDP и LLDP-MED режима глобальной конфигурации
Пример	Вывести на экран всю информацию LLDP и LLDP-MED режима глобальной конфигурации Switch#show lldp -----LLDP GLOBAL INFORMATION----- LLDP has been enabled globally. LLDP enabled port : Ethernet1/0/19



	LLDP interval : 5 LLDP txTTL : 20 LLDP NotificationInterval : 5 LLDP txDelay : 1 LLDP-ME LLDP-MED FastStart Repeat Count : 4 END

3.11.14. Вывод данных LLDP [Ethernet-интерфейс <IFNAME>] (show lldp [interface ethernet <IFNAME>])

Команда	show lldp [interface ethernet <IFNAME>]	
Параметр	IFNAME	имя порта
Значение по умолчанию	-	
Режим	Привилегированный режим	
Руководство по использованию	Команда позволяет вывести на экран информацию о настройках LLDP и LLDP-MED в порту	
Пример	Показать конфигурирование LLDP и LLDP-MED для порта 19. Switch#show lldp interface ethernet 1/0/19 Port name : Ethernet1/0/19 LLDP Agent Adminstatus : Both LLDP Operation TLV : default LLDP Trap Status : disable LLDP maxRemote : 100 LLDP Overflow handle : discard LLDP interface remote status : Free MED Optional TLV : capabilities networkPolicy location power inventory MED Trap Status: Enable MED TLV Transmit Status: Disable MED Fast Transmit Status: Disable	

3.11.15. Вывод данных соседних устройств LLDP (show lldp neighbors)

Команда	show lldp neighbors [interface ethernet < IFNAME >]	
Параметр	IFNAME	номер порта; например, 1/0/1
Значение по умолчанию	-	
Режим	Привилегированный режим	



Руководство по использованию	С помощью этой команды проверяется информация LLDP и LLDP-MED соседних устройств после того, как порт получил LLDP-пакеты, отправленные соседними устройствами
Пример	Показать информацию о соседних устройствах порта 1. <pre>Switch #show lldp neighbors interface ethernet 1/0/1</pre> Port name : Ethernet1/0/1 Port Remote Counter : 1 TimeMark : 20 ChassisIdSubtype : 4 ChassisId : 00-03-0f-00-00-02 PortIdSubtype : Local PortId : 3 PortDesc : Ethernet1/0/1 SysName : switch SysDesc : switch QTECH, Compiled Feb 12 17: 39: 53 2024 SoftWare Version 8.2.3.200 BootRom Version 2011.12.4 HardWare Version Device serial number Copyright (C) 2001-2024 by QTECH. All rights reserved

3.11.16. Вывод данных трафика LLDP (show lldp traffic)

Команда	show lldp traffic
Параметр	-
Значение по умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	После того как порт получил LLDP-пакеты от соседнего устройства, эту команду можно использовать для просмотра статистики отправленных и полученных пакетов LLDP и LLDP-MED



Пример	Просмотр статистики отправленных и полученных пакетов после включения функции LLDP. Switch(config)#show lldp traffic						
	PortName Ageouts	Frames Discarded	FramesIn Errors	Frames In	Frame sOut	TLVsDiscarded	TLVsUnrecognized
	Ethernet1/0/1	0	0	0	0	7	0

3.12. Настройка BPDU-Tunnel

3.12.1. Протокол BPDU-Tunnel (bpdu-tunnel-protocol)

Команда	bpdu-tunnel-protocol{stp gvrp dot1x user-defined-protocol <name>} no bpdu-tunnel-protocol {stp gvrp dot1x user-defined-protocol <name>}	
Параметр	stp	включить bpdu-tunnel-protocol функции stp в порту
	gvrp	включить bpdu-tunnel-protocol функции avrp в порту
	dot1x	включить bpdu-tunnel-protocol функции dot1x в порту
	name	включить bpdu-tunnel-protocol функции neme в порту, имя протокола составляет от 1 до 32 байт, состоящих из символа, данных и подчеркивания, причем первый и последний символ не может быть с подчеркиванием
Значение по умолчанию	-	
Режим	Режим конфигурации порта	
Руководство по использованию	После завершения настройки bpdu-tunnel-protocol MAC-адреса назначения какого-либо протокола, пользователи могут включить функцию bpdu-tunnel-protocol протокола в порту. Функции Stp, gvrp или dot1x является взаимоисключающей с функцией bpdu-tunnel-protocol порта, т. е. если порт настроен с функцией stp, gvrp или dot1x, функция bpdu-tunnel-protocol настроенного протокола отключается; если на порту настроена функция bpdu-tunnel-protocol функции stp, gvrp или dot1x настроить в порту нельзя	
Пример	Настроить "bpdu-tunnel-protocol" для включения протокола stp в порту 1/0/1. Switch(Config-If-Ethernet1/0/1)# bpdu-tunnel-protocol stp	



3.12.2. Группа MAC-адресов протокола BPDU-Tunnel (bpdu-tunnel-protocol group-mac)

Команда	bpdu-tunnel-protocol {stp gvrp dot1x} {group-mac <mac> default-group-mac} no bpdu-tunnel-protocol {stp gvrp dot1x}	
Параметр	Stp	настроить MAC-адрес bpdu-tunnel-protocol протокола stp;
	Gvrp	настроить MAC-адрес bpdu-tunnel-protocol протокола gvrp;
	dot1x	настроить MAC-адрес bpdu-tunnel-protocol протокола dot1x;
	Mac	MAC-адрес bpdu-tunnel-protocol должен быть адресом multicast и не может быть сохраненным адресом protocol, а именно адресом между 01-80-c2-00-00-00 и 01-80-c2-00-00-30;
	default-group-mac	MAC-адрес по умолчанию 01-00-0c-cd-00-02
Значение по умолчанию	-	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда должна быть задана перед настройкой bpdu-tunnel-protocol в порту	
Пример	Настроить адрес 01-01-00-0c -00-02 bpdu-tunnel-protocol протокола stp. Switch(Config)# bpdu-tunnel-protocol stp group-mac 01-01-00-0c -00-02	



3.12.3. Протокол MAC-адресов BPDU-Tunnel (bpdu-tunnel-protocol protocol-mac)

Команда	bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> {group-mac <mac> default-group-mac} no bpdu-tunnel-protocol user-defined-protocol <name>	
Параметр	name	это имя протокола, включает от 1 до 32 символов, и состоит из символов, данных и подчеркивания, первый и последний символ не могут быть подчеркиванием
	group-mac <mac>	это mac-адрес bpdu-tunnel-protocol, он должен быть multicast, и это не адрес сохранения протокола, а именно адрес между 01-80-c2-00-00-00 и 01-80-c2-00-00-30
	protocol-mac <mac>	mac-адрес протокола
	default-group-mac	mac-адрес по умолчанию 01-00-0c-cd-00-02
Значение по умолчанию	-	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда должна быть задана до применения bpdu-tunnel-protocol в порту	
Пример	Настроить 01-01-00-0c-00-03 в качестве bpdu-tunnel-protocol протокола mrpp. Switch(Config)# bpdu-tunnel-protocol user-defined-protocol mrpp protocol-mac 00-03-0f-00-00-02 group-mac 01-01-00-0c -00-03	

3.12.4. Ethernet протокола BPDU-Tunnel (bpdu-tunnel-protocol ethernetii)

Команда	bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> escape-type ethernetii protocol-type <type> {group-mac <mac> default-group-mac} no bpdu-tunnel-protocol user-defined-protocol <name>	
Параметр	name	это имя протокола, включает от 1 до 32 символов, и состоит из символов, данных и подчеркивания, первый и последний символ не могут быть подчеркиванием



	protocol-mac <mac>	mac-адрес протокола
	Type	значение протокола, в формате xx-xx
	group-mac <mac>	это mac-адрес bpdu-tunnel-protocol, он должен быть multicast, и это не адрес сохранения протокола, а именно адрес между 01-80-c2-00-00-00 и 01-80-c2-00-00-30;
	default-group-mac	MAC-адрес по умолчанию 01-00-0c-cd-00-02
Значение по умолчанию	-	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда должна быть задана до применения bpdu-tunnel-protocol в порту	
Пример	Настройте 01-01-00-0c-00-04 в качестве "bpdu-tunnel-protocol" протокола lldp. <pre>Switch(Config)# bpdu-tunnel-protocol user-defined-protocol lldp protocol-mac 01-80-c2-00-00-0e encaps-type ethernetii protocol-type 88-cc group-mac 01-01-00-0c -00-04</pre>	

3.12.5. Привязка протокола BPDU-Tunnel (bpdu-tunnel-protocol snap)

Команда	<pre>bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> encaps-type snap {oui <oui> } protocol-type <type> {group-mac <mac> default-group-mac} no bpdu-tunnel-protocol user-defined-protocol <name></pre>	
Параметр	Name	это имя протокола, включает от 1 до 32 символов, и состоит из символов, данных и подчеркивания, первый и последний символ не могут быть подчеркиванием
	protocol-mac <mac>	mac-адрес протокола
	Oui	значение oui в формате xx-xx-xx
	Type	значение протокола, в формате xx-xx



	group-mac <mac>	это mac-адрес для bpdu-tunnel-protocol, он должен быть multicast, и это не адрес сохранения протокола, а именно адрес между 01-80-c2-00-00-0 и 01-80-c2-00-00-30
	default-group-mac	адрес по умолчанию 01-00-0c-cd-00-02
Значение по умолчанию	-	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда должна быть задана до применения bpdu-tunnel-protocol в порту	
Пример	Настроить 01-01-00-0c-00-05 как bpdu-tunnel-protocol протокола Apple Talk. Switch(Config)# bpdu-tunnel-protocol user-defined-protocol lldp protocol-mac 00-03-c2-00-00-05 escape-type snap oui 08-00-07 protocol-type 80-9b group-mac 01-01-00-0c -00-05	

3.12.6. Протокол LLC BPDU-Tunnel (bpdu-tunnel-protocol llc)

Команда	bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> escape-type llc dsap <dsap> ssap <ssap> {group-mac <mac> default-group-mac} no bpdu-tunnel-protocol user-defined-protocol <name>	
Параметр	name	это имя протокола, включает от 1 до 32 символов, и состоит из символов, данных и подчеркивания, первый и последний символ не могут быть подчеркиванием
	protocol-mac <mac>	MAC-адрес протокола
	dsap	значение dsap протокола, которое варьируется от 0 до 255
	ssap	значение ssap протокола, которое варьируется от 0 до 255
	group-mac <mac>	MAC-адрес bpdu-tunnel-protocol, должен быть multicast, а не адресом сохранения протокола, а именно адрес между 01-80-c2-00-00-00 и 01-80-c2-00-00-30



	default-group-mac	MAC-адрес по умолчанию 01-00-0c-cd-00-02
Значение по умолчанию	-	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда должна быть задана до применения bpdu-tunnel-protocol в порту	
Пример	Настроить 01-01-00-0c-00-06 как bpdu-tunnel-protocol протокола NetBIOS. <pre>Switch(Config)# bpdu-tunnel-protocol user-defined-protocol lldp protocol-mac 00-03-c2-00-00-06 escape-type llc dsap 240 ssap 224 group-mac 01-01-00-0c-00-06</pre>	

3.13. Настройка функции энергосбережения EEE

3.13.1. Включение EEE (eee enable)

Команда	eee enable no eee enable
Параметр	-
Значение по умолчанию	-
Режим	Режим конфигурации порта
Руководство по использованию	Команда настраивает функцию энергосбережения EEE для указанного порта. По умолчанию функция энергосбережения EEE на порту отсутствует. После настройки порта на включение функции энергосбережения EEE порт перейдет в состояние энергосбережения, если прекратить отправку пакетов на порт, порт будет отключен. При отправке пакетов на порт, режим будет изменен с режима энергосбережения на нормальный режим
Пример	Включить функцию энергосбережения EEE: <pre>Switch(config-if-ethernet1/0/1)#eee enable</pre>



3.14. Команды отключения светодиода (LED) портов

3.14.1. Интервал отключения LED (port-led shutoff time-range)

Команда	port-led shutoff time-range < time-range-name > no port-led shutoff	
Параметр	time-range-name	это имя временного диапазона, заданное пользователем, оно состоит из 1-64 символов, включая буквы, цифры, подчеркивания. Первый и последний символы не могут быть подчеркиваниями
Значение по умолчанию	-	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Функция отключения светодиода (LED) порта может выключить все светодиоды в соответствии с заданным временем независимо от наличия соединения на физическом уровне. Это позволяет экономить электроэнергию. Если диапазон времени не задан, по умолчанию используется все время; когда диапазон превышен, светодиод порта может быть включен в соответствии со статусом link-act	
Пример	Настроить отключение всех светодиодов в t1. switch(config)#: port-led shutoff time-range t1	



4. MAC-АДРЕСА

4.1. Таблица MAC-адресов

4.1.1. Удаление таблицы коллизий MAC-адресов (clear collision-mac-address-table)

Синтаксис	clear collision-mac-address-table
Параметр	отсутствует
Состояние по умолчанию	отсутствует
Режим	Привилегированный режим
Применение	Если включить функцию хеш-коллизии MAC-таблицы, которая выдала ffp (mac-address-table avoid-collision), то MAC-адрес нельзя будет очистить
Пример	Очистите таблицу хеш-коллизий MAC-адресов. Switch#clear collision-mac-address-table

4.1.2. Удаление записей динамических адресов в таблице MAC-адресов (clear mac-address-table dynamic)

Синтаксис	clear mac-address-table dynamic [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet portchannel] <interface-name>]	
Параметр	<mac-addr>	MAC-адрес, который нужно удалить
	<vlan-id>	идентификатор Vlan
	<interface-name>	имя порта для пересылки MAC-пакетов
Состояние по умолчанию	Отсутствует	
Режим	Привилегированный режим	



Применение	Команда позволяет удалить все записи динамических адресов, которые существуют в таблице MAC-адресов, за исключением записей приложений и системных записей. Записи MAC-адресов можно классифицировать по различным источникам, типы которых приведены ниже: DYNAMIC, STATIC, APPLICATION, SYSTEM. DYNAMIC это динамические записи MAC-адресов, полученные коммутатором, они могут быть состарены коммутатором автоматически
Пример	Удалить все динамические MAC-адресов Switch#clear mac-address-table dynamic

4.1.3. Включение/выключение обучения MAC-адресов (mac-address-learning enable | disable)

Синтаксис	mac-address-learning (enable disable) (vlan <vlan-id> interface ethernet <interface-name>)	
Параметр	enable	включение обучения MAC-адресов через порт
	disable	выключение обучения MAC-адресов через порт
	<vlan-id>	идентификатор VLAN, диапазон: 1-4094
	<interface-name>	имя порта
Состояние по умолчанию	Все порты автоматически обучаются MAC-адресам	
Режим	Режим глобальной конфигурации	
Применение		
Пример	Отключить функцию обучения MAC-адресам порта 8 Switch#config Switch(config)#mac-address-learning disable interface ethernet 1/0/8	

4.1.4. Время старения таблицы MAC-адресов (mac-address-table aging-time)

Синтаксис	mac-address-table aging-time <0 aging-time> no mac-address-table aging-time	
Параметр	0	0 отключить время жизни



	aging-time	время жизни в секундах, диапазон от 10 до 1 000 000
Состояние по умолчанию	Время жизни MAC-адресов по умолчанию 300 секунд	
Режим	Режим глобальной конфигурации	
Применение	Если ни один адрес назначения пакетов не совпадает с адресом, указанным во времени жизни, запись адреса будет состарена. Пользователю лучше установить время старения в зависимости от состояния сети, обычно используется значение по умолчанию	
Пример	Установить время жизни в 600 секунд. Switch#config Switch(config)#mac-address-table aging-time 600	

4.1.5. Статические записи / «черные дыры» таблицы MAC-адресов (mac-address-table static | blackhole)

Синтаксис	mac-address-table {static blackhole} address <mac-addr> vlan <vlan-id> [interface ethernet <interface-name>] [source destination both] no mac-address-table {static blackhole dynamic} [address <mac-addr>] [vlan <vlan-id>] [interface ethernet <interface-name>]	
Параметр	Static	статические записи
	blackhole	фильтр записей, который предназначен для отбрасывания кадров с определенного MAC-адреса, параметр может фильтровать адрес источника, адрес назначения или оба адреса. При выборе фильтра записей адрес blackhole (черной дыры) не может быть основан на порту, и не может быть настроен на интерфейс
	Dynamic	динамические адреса
	<mac-addr>	добавляемый или удаляемый MAC-адрес
	<vlan-id>	номер VLAN
	<interface-name>	имя порта, передающего пакет с MAC-адресом
	Source	фильтрация по адресу источника



	destination	фильтрация по адресу назначения
	both	фильтрация по обоим адресам По умолчанию фильтрация установлена по адресу назначения и отправления
Состояние по умолчанию	Если настроен и включен интерфейс VLAN, система сгенерирует система создаст запись статического сопоставления адресов, в которой присущий MAC-адрес соответствует номеру VLAN	
Режим	Режим глобальной конфигурации	
Применение	В некоторых особых случаях, например, когда коммутатор не может осуществлять динамическое обучение MAC-адресам, пользователи могут использовать эту команду для установки вручную соответствия между MAC-адресом, портом и VLAN. Команда "no mac-address-table all" используется для удаления всех динамических, статических и фильтруемых MAC-адресов из списка MAC-адресов коммутатора, за исключением соответствий таблицы, заданных в системе. Записи MAC-адресов можно классифицировать по различным источникам, типы которых приведены ниже: DYNAMIC, STATIC, APPLICATION, SYSTEM. DYNAMIC это динамические записи MAC-адресов, полученные коммутатором, они могут быть состарены коммутатором автоматически. STATIC статические записи MAC-адресов (включая записи blackhole), добавленные пользователем. APPLICATION статические записи MAC-адресов, добавленные протоколом приложения (например, dot1x, порт безопасности...). SYSTEM добавленные записи статических MAC-адресов в соответствии с интерфейсом VLAN. При добавлении записей STATIC, они могут перекрыть конфликтующие записи DYNAMIC, за исключением записей APPLICATION и SYSTEM. После настройки статического многоадресного MAC этой командой, многоадресный MAC трафик будет перенаправляться на указанный порт указанной VLAN	
Пример	Порт 1/0/1 принадлежит VLAN200 и устанавливает сопоставление адресов с MAC-адресом 00-03-0f-f0-00-18. <pre>Switch#config Switch(config)#mac-address-table static address 00-03-0f-f0-00-18 vlan 200 interface ethernet 1/0/1</pre>	



4.1.6. Статический многоадресный MAC таблицы I2-адресов (I2-address-table static-multicast address)

Синтаксис	I2-address-table static-multicast address {< ip-addr> <mac-addr> } vlan < vlan-id > interface [ethernet < interface-name>] port-channel <port-channel-id> no I2-address-table static-multicast (address {< ip-addr> <mac-addr> } vlan < vlan-id >) [interface (ethernet < interface-name>) port-channel <port-channel-id>)]	
Параметр	< ip-addr>	добавляемый или удаляемый IP адрес
	<mac-addr>	добавляемый или удаляемый MAC-адрес
	< interface-name>	порт, передающий пакеты данных MAC
	<port-channel-id>	имя агрегированного порта передачи пакетов данных MAC
	< vlan-id >	номер VLAN
Состояние по умолчанию	Если настроен и включен интерфейс VLAN, система сгенерирует запись статического сопоставления адресов, в которой присущий MAC-адрес соответствует номеру VLAN	
Режим	Режим глобальной конфигурации	
Применение	В некоторых особых случаях, например, когда коммутатор не может осуществлять динамическое обучение MAC-адресам, пользователи могут использовать эту команду для установки вручную соответствия между MAC-адресом, портом и VLAN. После настройки статического многоадресного MAC этой командой, многоадресный MAC трафик будет перенаправляться на указанный порт указанной VLAN	
Пример	Настроить статический многоадресный ip 232.0.0.1, исходящим является ethernet 1/0/1. Switch#config Switch(config)# I2-address-table static-multicast address 232.0.0.1 vlan 200 interface ethernet 1/0/1	



4.1.7. Вывод коллизий таблицы MAC-адресов (show collision-mac-address-table)

Синтаксис	show collision-mac-address-table
Параметр	Отсутствует
Состояние по умолчанию	Отсутствует
Режим	Режим глобальной конфигурации
Применение	При включении функции хеш-коллизий, таблица MAC-адресов, которая выдает ffp (mac-address-table avoid-collision), то коллизий mac, которые выданы ffp, используют * для подписи
Пример	Показать таблицу хеш-коллизий mac. <pre>Switch#config Switch(config)#show collision-mac-address-table</pre> The max number can be recorded is 200 The max number of collision is 0 The current number recorded is 0 MAC Address VLAN Collision-count

4.1.8. Вывод таблицы MAC-адресов (show mac-address-table)

Синтаксис	show mac-address-table [static blackhole aging-time <aging-time> count] [address <mac-addr>] [vlan <vlan-id>] [count] [interface <interface-name>]	
Параметр	static	статические записи
	blackhole	фильтруемые адреса
	<aging-time>	время жизни адресов
	count	счетчик адресов
	<mac-addr>	MAC-адреса
	<vlan-id>	номер VLAN
	<interface-name>	имя интерфейса



Состояние по умолчанию	Таблица MAC-адресов не выведена на экран
Режим	Привилегированный режим и режим конфигурации
Применение	С помощью этой команды можно выводить на экран информацию о MAC-адресах, используя разные критерии сортировки. Пользователи также могут использовать команду <code>show mac-address-table</code> для отображения всех записей MAC-адресов.
Пример	Вывести на экран все MAC-адреса. <code>Switch#show mac-address-table blackhole</code>

4.1.9. Вывод записей многоадресной таблицы I2-адресов (show I2-address-table multicast)

Синтаксис	<code>show I2-address-table multicast ([count] [vlan <vlan-id>])</code>	
Параметр	<vlan-id>	номер VLAN записи, диапазон: 1-4094
Состояние по умолчанию	Таблица MAC-адресов не выведена на экран	
Режим	Привилегированный режим и режим конфигурации	
Применение	Эта команда может выводить на экран различные классы записей многоадресной рассылки.	
Пример	Вывести на экран все записи адресов многоадресной рассылки vlan1. <code>Switch#show I2-address-table multicast vlan 1</code> Vlan Address Insert Type Creator Ports	

4.1.10. Удаление статистики MAC-уведомлений (clear mac-notification statistics)

Синтаксис	<code>clear mac-notification statistics</code>
Параметр	Отсутствует
Состояние по умолчанию	Отсутствует
Режим	Привилегированный режим



Применение	Для просмотра результата выполнения данной команды применяется команда "show"
Пример	Switch#clear mac-notification statistics Switch#

4.1.11. Уведомления таблицы MAC-адресов (mac-address-table notification)

Синтаксис	mac-address-table notification no mac-address-table notification
Параметр	отсутствует
Состояние по умолчанию	Отключено
Режим	Режим глобальной конфигурации
Применение	Эта команда работает с переключателем trap на snmp. Если уведомление о MAC-адресе отключено, другие настройки могут быть отображены, но функция будет не действительна
Пример	Включите уведомление о MAC-адресе. Switch#config Switch(config)#mac-address-table notification Switch(config)#

4.1.12. Размер истории уведомлений таблицы MAC-адресов (mac-address-table notification history-size)

Синтаксис	mac-address-table notification history-size <0-500> no mac-address-table notification history-size	
Параметр	history-size	длина данных для отправки уведомления, диапазон от 1 до 500
Состояние по умолчанию	10	
Режим	Режим глобальной конфигурации	



Применение	Эта команда может быть задана последовательно, даже если глобальный режим коммутатора отключен
Пример	Изменить максимальный размер истории на 256. Switch#config Switch(config)#mac-address-table notification history-size 256

4.1.13. Диапазон уведомлений таблицы MAC-адресов (mac-address-table notification interval)

Синтаксис	mac-address-table notification interval <1-30> no mac-address-table notification interval	
Параметр	Interval	интервал для отправки уведомления, в секундах, диапазон от 0 до 30
Состояние по умолчанию	30 секунд	
Режим	Режим глобальной конфигурации	
Применение	Эта команда может быть задана последовательно, даже если глобальный режим коммутатора отключен	
Пример	Задать интервал в 30 с для отправки уведомления о MAC-адресе. Switch#config Switch(config)#mac-address-table notification interval 30	

4.1.14. Уведомления MAC (mac-notification)

Синтаксис	mac-notification {added all removed} no mac-notification	
Параметр	Added	добавленный MAC-адрес
	All	добавленные и удаленные MAC-адреса
	Removed	удаленный MAC-адрес
Состояние по умолчанию	Без уведомления о MAC-адресе	
Режим	Настройка портов	



Применение	Эта команда может быть задана последовательно, даже если глобальный режим коммутатора отключен
Пример	Отправить уведомление trap после добавления MAC-адреса в Ethernet 1/0/1. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# mac-notification added

4.1.15. Вывод сводной информации MAC-уведомлений (show mac-notification summary)

Синтаксис	show mac-notification summary
Параметр	отсутствует
Состояние по умолчанию	Не выводить сводную информацию
Режим	Привилегированный режим
Применение	С помощью этой команды проверяется конфигурирование MAC-адреса и состояние отправки уведомлений trap
Пример	Switch#show mac-notification summary MAC address notification: enabled MAC address snmp traps: disabled MAC address notification interval = 5 MAC address notification history log size = 10 MAC address added = 0 MAC address removed = 0 MAC address moved = 0 MAC address snmp traps generated = 0

4.1.16. Включение уведомлений прерывания MAC-адреса сервера SNMP (snmp-server enable traps mac-notification)

Синтаксис	snmp-server enable traps mac-notification no snmp-server enable traps mac-notification
Параметр	отсутствует
Состояние по умолчанию	Уведомления trap отключены



Режим	Режим глобальной конфигурации
Применение	Эта команда используется с переключателем уведомлений MAC. Если коммутатор отключен, можно отобразить другую конфигурирование, но функция будет недействительной
Пример	Включить trap-уведомление MAC-адреса Switch(config)#snmp-server enable traps mac-notification



5. VLAN

5.1. Команды для настройки сети VLAN

5.1.1. Сеть VLAN (vlan)

Синтаксис	vlan WORD no vlan											
Параметр	WORD	WORD — идентификатор VLAN, который нужно создать/удалить, допустимый диапазон от 1 до 4094, объединяется при помощи ';' и '-'										
Состояние по умолчанию	По умолчанию установлена только VLAN1											
Режим	Режим глобальной конфигурации											
Применение	VLAN1 является VLAN по умолчанию и не может быть настроена или удалена пользователем. Максимальный номер VLAN составляет 4094. Следует отметить, что динамические VLAN, изученные GVRP, не могут быть удалены с помощью этой команды											
Пример	Создать VLAN100 и войти в режим конфигурации VLAN 100. Отобразить статус текущей VLAN; Switch#config Switch(config)#vlan 100 Switch#show vlan <table><thead><tr><th>VLAN Name</th><th>Type</th><th>Media</th><th>Ports</th></tr></thead><tbody><tr><td>1 default</td><td>Static</td><td>ENET</td><td>Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19</td></tr></tbody></table>				VLAN Name	Type	Media	Ports	1 default	Static	ENET	Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19
VLAN Name	Type	Media	Ports									
1 default	Static	ENET	Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19									



				Ethernet1/0/20 Ethernet1/0/21 Ethernet1/0/22 Ethernet1/0/23 Ethernet1/0/24 Ethernet1/0/25 Ethernet1/0/26 Ethernet1/0/27 Ethernet1/0/28
	100	VLAN0100	Static	ENET
	Switch#			

5.1.2. Имя VLAN (name (vlan))

Синтаксис	name NAME no name											
Параметр	NAME	указанная строка имени										
Состояние по умолчанию	Имя VLAN по умолчанию — vlanXXX, где xxx — VID											
Режим	Режим конфигурации VLAN											
Применение	Коммутатор может задавать имена для различных виртуальных локальных сетей VLAN, что облегчает пользователям идентификацию и управление виртуальными локальными сетями											
Пример	Задать имя VLAN100 как 100 Switch#config Switch(config)# vlan 100 Switch(config-vlan100)#name 100 Switch# show vlan <table><thead><tr><th>VLAN Name</th><th>Type</th><th>Media</th><th>Ports</th></tr></thead><tbody><tr><td>1 default</td><td>Static</td><td>ENET</td><td>Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12</td></tr></tbody></table>				VLAN Name	Type	Media	Ports	1 default	Static	ENET	Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12
VLAN Name	Type	Media	Ports									
1 default	Static	ENET	Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12									



				Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19 Ethernet1/0/20 Ethernet1/0/21 Ethernet1/0/22 Ethernet1/0/23 Ethernet1/0/24 Ethernet1/0/25 Ethernet1/0/26 Ethernet1/0/27 Ethernet1/0/28
	100 100	Static	ENET	
	Switch#			

5.1.3. Настройка интерфейса (switchport interface)

Синтаксис	switchport interface [ethernet portchannel] [<interface-name interface-list> no switchport interface [ethernet portchannel] [<interface-name interface-list>]	
Параметр	ethernet	добавляемый порт Ethernet
	portchannel	порт агрегации каналов, который необходимо добавить
	interface-name	имя порта, например, e1/0/1. ethernet или portchannel не должны использоваться
	interface-list	список портов для добавления или удаления, поддерживаются символы «;» и «-», например, ethernet1/0/1; 3; 4-7; 8
Состояние по умолчанию	Вновь созданная VLAN по умолчанию не содержит ни одного порта	
Режим	VLAN	
Применение	Порты доступа являются обычными портами и могут присоединяться к VLAN, но порт может присоединяться только к одной VLAN за один раз	



Пример

Назначить Ethernet порт 1, 3, 4-7 VLAN100.

```
Switch#config
```

```
Switch(config)#vlan 100
```

```
Switch(config-vlan100)#switchport interface ethernet 1/0/1;3;4-7
```

Set the port Ethernet1/0/1 access vlan 100 successfully

Set the port Ethernet1/0/3 access vlan 100 successfully

Set the port Ethernet1/0/4 access vlan 100 successfully

Set the port Ethernet1/0/5 access vlan 100 successfully

Set the port Ethernet1/0/6 access vlan 100 successfully

Set the port Ethernet1/0/7 access vlan 100 successfully

```
Switch#show vlan
```

VLAN Name	Type	Media	Ports
1 default	Static	ENET	Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19 Ethernet1/0/20 Ethernet1/0/21 Ethernet1/0/22 Ethernet1/0/23 Ethernet1/0/24 Ethernet1/0/25 Ethernet1/0/26 Ethernet1/0/27 Ethernet1/0/28
100 VLAN0100 Switch#	Static	ENET	



5.1.4. Настройка запрещенной сети VLAN (switchport forbidden vlan)

Синтаксис	switchport forbidden vlan (WORD all add WORD except WORD remove WORD)	
Параметр	WORD	добавляет список vlanList в качестве запрещенной сети vlan и отменяет предыдущее конфигурирование
	all	установить все VLAN как запрещенные vlan
	add WORD	добавить vlanList в текущий список запрещенных vlanList
	except WORD	установить все VLAN как запрещенные vlan, кроме vlanList
	Remove WORD	удалить vlan, указанный vlanList, из текущего списка запрещенных vlanList
Состояние по умолчанию	Список vlanList пуст	
Режим	Настройка портов	
Применение	Помечает (тегирует) соответствующую позицию для запрещенного vlanList и снимает флаг разрешенного vlanList в порту. Порты, статически присоединенные к этим VLAN, покидают эти VLAN и отправляют сообщение модулю GVRP о переводе соответствующего регистратора порта в запрещенный режим. Команда show running-config выводит на экран текущие настройки	
Пример	Порт покидает соответствующую VLAN и соответствующую зарегистрированную машину GVRP, чтобы перейти в запрещенный режим. <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode hybrid Switch(config-if-ethernet1/0/1)#switchport forbidden vlan all Set the port Ethernet1/0/1 mode Hybrid successfully Switch#show running-config ! no service password-encryption ! hostname Switch sysLocation Default sysContact Default !</pre>	



```
username admin privilege 15 password 0 admin
!
authentication line console login local
!
!
!
!
!
snmp-server enable
!
!
!
!
!
!
!
!
!
!
!
vlan 1; 100
!
Interface Ethernet1/0/1 switchport mode hybrid
switchport forbidden vlan 1-4094
!
Interface Ethernet1/0/2
!
Interface Ethernet1/0/3
switchport mode trunk
switchport trunk native vlan 100
!
Interface Ethernet1/0/4
!
Interface Ethernet1/0/5
!
Interface Ethernet1/0/6
!
Interface Ethernet1/0/7
!
Interface Ethernet1/0/8
```



	!
	Interface Ethernet1/0/9 Switch#

5.1.5. Режим переключения (switchport mode)

Синтаксис	switchport mode (access hybrid trunk tunnel)	
Параметр	access	порт доступа (Access)
	hybrid	гибридный порт (Hybrid)
	trunk	магистральный порт (trunk)
	tunnel	туннельный порт (tunnel)
Состояние по умолчанию	По умолчанию порт работает в режиме доступа	
Режим	Режим конфигурации порта	
Применение	Порты в режиме trunk называются магистральными. Магистральные порты могут пропускать трафик нескольких VLAN. VLAN в разных коммутаторах могут быть объединены с помощью магистральных портов. Порты в режиме access называются портами доступа. Порт доступа может быть назначен на одну и только одну VLAN одновременно. Гибридные порты могут пропускать трафик нескольких VLAN, принимать и отправлять пакеты нескольких VLAN, используются для подключения коммутатора или компьютера пользователя. Когда гибридный порт получает данные, операция происходит так же, как и при получении данных магистральным портом, но, когда он передает данные, операция отличается. Поскольку гибридные порты могут разрешить отправку пакетов нескольких VLAN без тегов, то магистральные порты могут разрешить отправку пакетов только VLAN по умолчанию без тегов. Атрибут порта нельзя напрямую переключить между Hybrid и Trunk, его нужно сначала настроить как access, а затем как Hybrid или Trunk. Удаление атрибута Trunk или Hybrid возвращает атрибут порта к атрибуту по умолчанию (access) и приписывает его к vlan1. Команда show switchport in terface выводит на экран настройки	
Пример	Установить для порта 1 режим hybrid. <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# switchport mode hybrid Set the port Ethernet1/0/1 mode Hybrid successfully Switch(config-if-ethernet1/0/1)#show switchport interface ethernet 1/0/1</pre>	



	Ethernet1/0/1 Type : Universal Mode : Hybrid Port VID : 1 Switch(config-if-ethernet1/0/1)#

5.1.6. Нативная сеть VLAN гибридного порта (switchport hybrid native vlan)

Синтаксис	switchport hybrid native vlan <vlan-id> no switchport hybrid native vlan	
Параметр	<vlan-id>	Идентификатор VLAN (например, 100), PVID гибридного порта
Состояние по умолчанию	По умолчанию PVID гибридного порта равен 1	
Режим	Режим конфигурации порта	
Применение	Нетегированному кадру, пришедшему на гибридный порт, будет назначен тег "native PVID", заданный данной командой, и он направляется на "native PVID". Команда show switchport interface выводит на экран настройки	
Пример	Задать для "native vlan" значение 100 для гибридного порта. Switch#config Switch(config) # interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)#switchport mode hybrid Switch(config-if-ethernet1/0/2)#switchport hybrid native vlan 100 Switch# show switchport interface ethernet 1/0/2 Ethernet1/0/2 Type : Universal Mode : Hybrid Port VID : 100 Switch#	

5.1.7. Разрешенная сеть VLAN гибридного порта (switchport hybrid allowed vlan)

Синтаксис	switchport hybrid allowed vlan (WORD all add WORD except WORD remove WORD) (tag untag) no switchport hybrid allowed vlan	
Параметр	WORD	задает в списке vlan List разрешенный vlan предыдущие настройки будут перезаписаны;



	all	разрешены все vlan
	add WORD	добавить номера vlan к списку разрешенных
	except WORD	разрешены все vlan, кроме указанных
	Remove WORD	удалить указанные vlan из списка разрешенных сетей vlanList;
	tag	передавать указанные vlan с сохранением тега
	untag	передавать указанные vlan со снятием тега
Состояние по умолчанию	Любой трафик VLAN запрещен	
Режим	Режим конфигурации порта	
Применение	Эта команда может быть использована для указания vlan, трафик которых разрешен для передачи через гибридный порт, трафик остальных vlan запрещен. Разница между параметрами tag и untag заключается в настройке разрешенных VLAN: если задать для VLAN режим untag, кадры, передаваемые через гибридный порт, не будут содержать тегов VLAN; если задать для VLAN режим tag, в кадрах, передаваемых через гибридный, будут указаны соответствующие теги VLAN. Гибридные порты не могут одновременно разрешать одни и те же VLAN в режиме тегов и без тегов. При изменении параметров VLAN с передачи с установкой тега на снятие и наоборот, последняя конфигурирование перезаписывает предыдущую. Команда show switchport interface выводит на экран настройки	
Пример	Установить для разрешенной vlan гибридного порта значение 1,100 с режимом тегов <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode hybrid Set the port Ethernet1/0/1 mode Hybrid successfully Switch(config-if-ethernet1/0/1)#switchport hybrid allowed vlan 1; 100 tag set the Hybrid port Ethernet1/0/1 tag allowed vlan successfully Switch#show switchport interface ethernet 1/0/1</pre> Ethernet1/0/1 Type : Universal Mode : Hybrid Port VID : 1 Hybrid tag allowed Vlan: 1; 100 Switch#	



5.1.8. Настройка сети доступа VLAN (switchport access vlan)

Синтаксис	switchport access vlan <valn-id> no switchport access vlan	
Параметр	< valn-id >	Идентификатор VLAN (например, 100), допустимый диапазон от 1 до 4094
Состояние по умолчанию	По умолчанию все порты принадлежат к VLAN1	
Режим	Режим конфигурации порта	
Применение	В указанную сеть VLAN можно добавить только порт доступа коммутатора, одной командой к VLAN может быть добавлен только один порт доступа. Команда “ no switchport access vlan ” удаляет соответствующий порт из указанного VLAN, после этого порт будет принадлежать VLAN1. Команда show switchport interface выводит на экран настройки	
Пример	Добавить указанный порт доступа в VLAN100. <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode access Set the port Ethernet1/0/1 mode Access successfully Switch(config-if-ethernet1/0/1)# switchport access vlan 100 Set the port Ethernet1/0/1 access vlan 100 successfully</pre> Switch#show switchport interface ethernet 1/0/1 <pre>Ethernet1/0/1 Type : Universal Mode : Access Port VID : 100 Switch#</pre>	

5.1.9. Настройка магистрального порта разрешенной сети VLAN (switchport trunk allowed vlan)

Синтаксис	switchport trunk allowed vlan (WORD all add WORD except WORD remove WORD) (tag untag) no switchport trunk allowed vlan	
Параметр	WORD	указанные VID, диапазон от 1 до 4094;
	all	все VID
	add WORD	добавить указанные VID в список разрешенных;



	except WORD	все VID добавляются к разрешенным vlan, за исключением указанных VID;
	Remove WORD	удалить указанные vlan из списка разрешенных
Состояние по умолчанию	Все пакеты всех VLAN могут проходить через магистральный порт	
Режим	Режим конфигурации порта	
Применение	Эта команда позволяет задать, пакеты каких VLAN смогут проходить через магистральный порт. Пакеты тех VLAN, которые не указаны в команде, будут отбрасываться. Команда show switchport interface выводит на экран настройки	
Пример	Разрешить для VLAN 1, 3-5 трафик на магистральном порту. <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# switchport trunk allowed vlan 1; 3-5 set the trunk port Ethernet1/0/1 allowed vlan successfully.</pre> Switch#show switchport interface ethernet 1/0/1 Ethernet1/0/1 Type : Universal Mode : Trunk Port VID : 1 Trunk allowed Vlan: 1; 3-5 Switch#	

5.1.10. Настройка магистрального порта нативной сети VLAN (switchport trunk native vlan)

Синтаксис	<pre>switchport trunk native vlan < vlan-id > no switchport trunk allowed vlan</pre>	
Параметр	<vlan-id>	идентификатор PVID для магистрального порта
Состояние по умолчанию	Магистральному порту присвоен PVID 1	
Режим	Режим конфигурации порта	
Применение	Идентификаторы PVID определены в стандарте 802.1Q. PVID в магистральном порту используется для тегирования нетегированных кадров. Когда кадр без тега поступает в магистральный порт, порт	



	позначит его собственным PVID, установленным с помощью этой команды для пересылки в VLAN. Команда show switchport in terface выводит на экран настройки
Пример	Установить значение native VLAN 100 для магистрального порта. <pre>Switch#config Switch(config)#interface ethernet 1/0/3 Switch(config-if-ethernet1/0/3)# switchport trunk native vlan 100 Set the port Ethernet1/0/3 native vlan 100 successfully</pre> <pre>Switch#show switchport interface ethernet 1/0/3 Ethernet1/0/3 Type : Universal Mode : Trunk Port VID : 100 Trunk allowed Vlan: 1-4094 Switch#</pre>

5.1.11. Очистка списка разрешений (switchport mode trunk allow-null)

Синтаксис	switchport mode trunk allow-null
Параметр	отсутствует
Состояние по умолчанию	Режим доступа (access)
Режим	Настройка портов
Применение	Команда позволяет настроить порт как магистральный, разрешает ему выходить из всех VLAN и очищает список разрешений. Команда show switchport interface выводит на экран настройки
Пример	<pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# switchport mode trunk allow-null Set the port Ethernet1/0/1 mode Trunk successfully</pre> <pre>Switch#show switchport interface ethernet 1/0/1 Ethernet1/0/1 Type : Universal Mode : Trunk Port VID : 1 switchport mode trunk allow-null</pre>



	Switch#

5.1.12. Включение отбрасывания VLAN (vlan ingress enable)

Синтаксис	vlan ingress enable no vlan ingress enable
Параметр	отсутствует
Состояние по умолчанию	Правила для входящих пакетов VLAN включены
Режим	Режим конфигурации порта
Применение	Когда в порту включены правила для входящих пакетов VLAN, при получении данных система проверяет состояние порта-источника, а затем передает данные в порт назначения только в том случае, если этот порт является членом VLAN, или отбрасывает данные. Команда show running-config выводит на экран настройки
Пример	Выключить в порту правила для входящих пакетов VLAN. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# no vlan ingress enable Switch# show running-config ! no service password-encryption ! hostname Switch sysLocation Default sysContact Default ! username admin privilege 15 password 0 admin ! authentication line console login local ! ! ! ! snmp-server enable ! !



	<pre> ! ! ! ! ! ! ! vlan 1 ! Interface Ethernet1/0/1 no vlan ingress enable ! Interface Ethernet1/0/2 Switch# </pre>

5.1.13. Включение преобразования тегов VLAN (vlan-translation enable)

Синтаксис	<pre> vlan-translation enable no vlan-translation enable </pre>
Параметр	отсутствует
Состояние по умолчанию	По умолчанию функция преобразования тегов VLAN translation на порту не включена
Режим	Режим конфигурации порта
Применение	Функции vlan-translation и dot1q-tunnel являются взаимоисключающими, поэтому рекомендуется включить vlan-translation на магистральном порту и вручную отключить фильтрацию портов. Команда show vlan-translation выводит на экран настройки
Пример	Включить функцию VLAN translation на порту 1. <pre> Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# vlan-translation enable Switch# show vlan-translation Interface Ethernet1/0/1: vlan-translation is enable, miss drop is not set Switch# </pre>



5.1.14. Трансляция VLAN (vlan-translation)

Синтаксис	vlan-translation <old-valn-id> to <new-vlan-id> {in out} no vlan-translation <old-valn-id> {in out}	
Параметр	old-valn-id	исходный идентификатор VLAN
	new-vlan-id	преобразованный ID VLAN
	in	преобразование входящих данных
	out	преобразование исходящих данных
Состояние по умолчанию	Трансляция VLAN на порту отключена	
Режим	Режим конфигурации порта	
Применение	Эта команда используется для настройки отношения трансляции функции трансляции VLAN. Пакеты данных будут проверяться на соответствие заданным в команде правилам трансляции, при соответствии правилам их VLAN ID будет заменяться указанным в команде, если нет, пакеты будут пересланы исходной VLAN. Эту команду нельзя использовать одновременно с командой "dot1q-tunnel enable". Команда show vlan-translation отображает настройки трансляции	
Пример	Переместить данные VLAN100, введенные с порта1, в VLAN2 после трансляции на входе. <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# vlan-translation enable Switch(config-if-ethernet1/0/1)#vlan-translation 100 to 2 in Switch# show vlan-translation Interface Ethernet1/0/1: vlan-translation is enable, miss drop is not set vlan-translation 100 to 2 in Switch#</pre>	



5.1.15. Отбрасывание пакетов при трансляции VLAN (vlan-translation miss drop)

Синтаксис	vlan-translation miss drop {in out both} no vlan-translation miss drop {in out both}	
Параметр	in	отбрасывание для входящих пакетов
	out	отбрасывание для исходящих пакетов
	both	отбрасывание исходящих и входящих пакетов
Состояние по умолчанию	При несоответствии пакетов заданным правилам трансляции, их отбрасывание не производится	
Режим	Режим конфигурации порта	
Применение	Когда установлена трансляция из исходного VLAN в текущий VLAN, пакеты, не соответствующие правилам трансляции, по умолчанию отбрасываться не будут. Их отбрасывание можно задать, введя данную команду. Команда show vlan-translation выводит на экран настройки	
Пример	Задать отбрасывание входящих пакетов на порт 1, не соответствующих правилам трансляции. <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# vlan-translation enable Switch(config-if-ethernet1/0/1)#vlan-translation miss drop in</pre> Switch# show vlan-translation Interface Ethernet1/0/1: vlan-translation is enable, miss drop is set in Switch#	

5.1.16. Включение туннеля Dot1q (dot1q-tunnel enable)

Синтаксис	dot1q-tunnel enable no dot1q-tunnel enable
Параметр	отсутствует



Состояние по умолчанию	Функция туннеля Dot1q на порту не включена
Режим	Режим конфигурации порта
Применение	После включения команды "dot1q-tunnel" на порту пакеты данных без тега VLAN (метки) будут упаковываться с тегом при прохождении через порт; тегированные пакеты будут упаковываться с внешним тегом. Атрибут TPID в теге это глобальная настройка TPID, которая по умолчанию равна 0x8100, а VLAN ID - это идентификатор VLAN, к которой принадлежит порт. Пакеты данных с двойным тегом пересылаются в соответствии с MAC-адресом и внешним тегом до тех пор, пока внешний тег не будет удален при передаче за пределы порта доступа. Поскольку длина пакета данных может быть превышена при упаковке внешним тегом, рекомендуется использовать эту команду с функцией Jumbo. Обычно эта команда используется на портах доступа. Эта команда не может быть применена, если включена vlan-трансляция. Команда show dot1q-tunnel выводит на экран настройки
Пример	Добавить порт 1 в VLAN3, включить функцию туннеля dot1q. <pre>Switch#config Switch(config)#vlan 3 Switch(config-vlan3)#switchport interface ethernet 1/0/1 Switch(config-vlan3)#exit Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# dot1q-tunnel enable</pre> Switch# show dot1q-tunnel <pre>Interface Ethernet1/0/1: dot1q-tunnel is enable Switch#</pre>

5.1.17. Включение расширения Selective QinQ (dot1q-tunnel selective enable)

Синтаксис	dot1q-tunnel selective enable no dot1q-tunnel selective enable
Параметр	отсутствует
Состояние по умолчанию	Расширение selective QinQ не включено



Режим	Настройка портов
Применение	Команда "Enable selective QinQ" должна применяться с гибридным режимом, и ее не следует использовать одновременно с командой "dot1q-tunnel enable". Команда show running-config выводит на экран настройки
Пример	Подключить функцию dot1q-tunnel selective enable на порте 1. <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# dot1q-tunnel selective enable Switch# show running-config ! no service password-encryption ! hostname Switch sysLocation Default sysContact Default ! username admin privilege 15 password 0 admin ! authentication line console login local ! ! ! ! snmp-server enable ! ! ! ! ! ! ! ! ! ! vlan 1; 3 ! Interface Ethernet1/0/1 dot1q-tunnel selective enable !</pre>



	<pre> Interface Ethernet1/0/2 ! Interface Ethernet1/0/3 ! Switch# </pre>

5.1.18. Отношение Selective QinQ и VLAN (dot1q-tunnel selective s-vlan)

Синтаксис	<pre> dot1q-tunnel selective s-vlan <s-vlan> c-vlan <c-vid-list> no dot1q-tunnel selective s-vlan <s-vlan> c-vlan <c-vid-list> </pre>	
Параметр	<s-vlan>	идентификатор VLAN сети провайдера (внешний тег)
	<c-vid-list>	диапазон идентификаторов VLAN пользователя
Состояние по умолчанию	Отношения сопоставления отсутствуют	
Режим	Настройка портов	
Применение	Эта команда используется для настройки отношения сопоставления для Selective QinQ. Если пакеты соответствуют отношению сопоставления, они будут помечены тегом SP vlan в качестве внешнего тега VLAN. Команда show running-config выводит на экран настройки	
Пример	Пометить пакеты с VLAN 3 по VLAN 5 тегом VLAN 1 в качестве внешнего тега VLAN на Ethernet1/0/1. <pre> Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# dot1q-tunnel selective s-vlan 1 c-vlan 3-5 Switch(config-if-Ethernet1/0/1)# dot1q-tunnel selective enable Switch# show running-config ! no service password-encryption ! hostname Switch sysLocation Default sysContact Default ! username admin privilege 15 password 0 admin ! authentication line console login local </pre>	



```

!
!
!
!
snmp-server enable
!
!
!
!
!
!
!
!
!
!
vlan 1; 3
!
Interface Ethernet1/0/1
dot1q-tunnel selective s-vlan 1 c-vlan 3-5 dot1q-tunnel selective enable
!
Interface Ethernet1/0/2
!
Interface Ethernet1/0/3
!
Interface Ethernet1/0/4
!
Interface Ethernet1/0/5
!
Interface Ethernet1/0/6
Switch#

```

5.1.19. Таймер слияния GARP (garp timer join)

Синтаксис	garp timer join <200-500>	
Параметр	<200-500>	миллисекунда
Состояние по умолчанию	200 миллисекунд	



Режим	Режим глобальной конфигурации
Применение	Убедитесь, что значения находятся в пределах диапазона. Если да, измените значение таймера GARP на указанное, иначе возврат настроек будет неверным. Команда show garp timer выводит на экран настройки
Пример	Установить таймер слияния GARP равным 210 мс. <pre>Switch#config Switch(config)# garp timer join 210 Switch#show garp timer GARP join timer value is : 210 (ms) GARP leave timer value is : 600 (ms) GARP leaveall timer value is : 10000 (ms) Switch#</pre>

5.1.20. Таймер удаления GARP (garp timer leave)

Синтаксис	garp timer leave <500-1200>	
Параметр	<500-1200>	миллисекунда
Состояние по умолчанию	600 миллисекунд	
Режим	Режим глобальной конфигурации	
Применение	Убедитесь, что значения находятся в пределах диапазона. Если да, измените значение таймера GARP на указанное, иначе возврат настроек будет неверным. Команда show garp timer выводит на экран настройки	
Пример	Установить таймер удаления GARP на 700 мс. <pre>Switch#config Switch(config)#garp time leave 700 Switch#show garp timer GARP join timer value is : 210 (ms) GARP leave timer value is : 700 (ms) GARP leaveall timer value is : 10000 (ms) Switch#</pre>	



5.1.21. Таймер удаления всех (leaveAll) GARP (garp timer leaveall)

Синтаксис	garp timer leaveall <5000-60000>	
Параметр	<500-60000>	миллисекунда
Состояние по умолчанию	10000 миллисекунд	
Режим	Режим глобальной конфигурации	
Применение	Убедитесь, что значения находятся в пределах диапазона. Если да, измените значение параметра таймера leaveAll GARP на указанное, иначе появится ошибка настройки. Команда show garp timer выводит на экран настройки	
Пример	Задать значение garp leaveAll равным 20000 мс. <pre>Switch#config Switch(config)#garp time leaveall 20000</pre> Switch(config)#show garp timer GARP join timer value is : 210 (ms) GARP leave timer value is : 700 (ms) GARP leaveall timer value is : 20000 (ms) <pre>Switch#</pre>	

5.1.22. Удаление таймеров GARP (no garp timer)

Синтаксис	no garp timer (join leave leaveall)	
Параметр	join	таймер слияния
	leave	таймер удержания
	leaveall	таймер выхода для всех
Состояние по умолчанию	200 600 10000 миллисекунд для таймера join leave leaveall соответственно	
Режим	Режим глобальной конфигурации	
Применение	Убедитесь, что значения по умолчанию находятся в пределах диапазона. Если да, измените значение таймера GARP join leave leaveAll на указанное, иначе появится ошибка настройки. Команда show garp timer join выводит на экран настройки	



Пример	Восстановить значение по умолчанию для таймера GARP timer join. Switch#config Switch(config)# no garp timer join Switch(config)# show garp timer join GARP join timer value is : 200 (ms) Switch#

5.1.23. Режим глобальной конфигурации GVRP (gvrp(Global))

Синтаксис	gvrp no gvrp
Параметр	отсутствует
Состояние по умолчанию	Функция GVRP выключена
Режим	Режим глобальной конфигурации
Применение	Только включение функции GVRP в режиме глобальной конфигурации обеспечит правильную работу модуля GVRP. Команда show running-config выводит на экран настройки
Пример	Включить функцию GVRP в режиме глобальной конфигурации. Switch#config Switch(config)#gvrp Switch(config)#show running-config ! no service password-encryption ! hostname Switch sysLocation Default sysContact Default ! username admin privilege 15 password 0 admin ! authentication line console login local ! ! ! !



	<pre>snmp-server enable ! ! ! ! ! ! ! ! ! vlan 1 ! gvrp ! Interface Ethernet1/0/1 Switch#</pre>

5.1.24. GVRP порта (gvrp(Port))

Синтаксис	<pre>gvrp no gvrp</pre>
Параметр	отсутствует
Состояние по умолчанию	Отключено
Режим	Настройка портов
Применение	Функция GVRP может быть включена только на магистральных и гибридных портах, если включить функцию на порту доступа будет выдана ошибка. Когда GVRP включен для порта, этот порт присоединяется к GVRP (т.е. добавляется оборудование, соответствующее GVRP порта). Команда show gvrp port-member выводит на экран настройки
Пример	Включить функцию GVRP в порту. <pre>Switch#config Switch(config)# interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode hybrid Set the port Ethernet1/0/1 mode Hybrid successfully Switch(config-if-ethernet1/0/1)#gvrp</pre>



	<pre>Switch#show gvrp port-member</pre> Ports which were enabled gvrp included: Ethernet1/0/1 <pre>Switch#</pre>

5.1.25. Частная сеть VLAN (private-vlan)

Синтаксис	<pre>private-vlan {primary isolated community}</pre> <pre>no private-vlan</pre>	
Параметр	primary	устанавливает текущую сеть VLAN как первичную (Primary)
	isolated	устанавливает текущую сеть VLAN как изолированную (Isolated)
	community	устанавливает текущую сеть VLAN как общую (Community)
Состояние по умолчанию	Настройки private vlan не включены	
Режим	Режим конфигурации VLAN	
Применение	Имеется три режима частной VLAN: Primary VLAN, Isolated VLAN и Community VLAN. Порты в первичной VLAN являются портами трех частных VLAN. Порты Primary VLAN, isolated VLAN и community VLAN могут взаимодействовать с портами isolated VLAN и community VLAN, связанными с Primary VLAN. Порты в Isolated VLAN изолированы друг от друга и могут связываться только с портами primary VLAN, которой они принадлежат. Порты community VLAN могут связываться друг с другом и с портами primary VLAN, которой они принадлежат. Связь между портами community VLAN и портами isolated VLAN отсутствует. Только VLAN, содержащие пустые Ethernet-порты могут быть настроены как частные VLAN, и только частные VLAN с соответствующими частными связями могут устанавливать порты своих членов как Ethernet-порты доступа. Когда обычная сеть VLAN устанавливается как частная, закрепления Ethernet-портов для нее стираются. Следует отметить, что сообщения private VLAN не передаются по протоколу GVRP. Команда <code>show vlan private-vlan</code> выводит на экран настройки	
Пример	Задать VLAN100, 200, 300 как частные, а именно как primary, Isolated, Community соответственно.	



```
Switch#config Switch(config)#vlan 100; 200; 300
Switch(config)#vlan 100
Switch(config-vlan100)#private-vlan primary
Примечание: Это удалит все порты доступа из vlan 100
Switch(config-vlan100)#vlan 200
Switch(config-vlan200)#private-vlan isolated
Примечание: Это удалит все порты доступа из vlan 200
Switch(config-vlan200)#vlan 300
Switch(config-vlan300)#private-vlan community
Примечание: Это удалит все порты доступа из vlan 300
Switch# show vlan private-vlan
```

VLAN Name	Type	Asso VLAN Ports
100	VLAN0100	Primary
200	VLAN0200	Isolate
300	VLAN0300	Community

```
Switch#
```

5.1.26. Ассоциация частной VLAN (private-vlan association)

Синтаксис	<pre>private-vlan association <secondary-vlan-list> no private-vlan association</pre>	
Параметр	<secondary-vlan-list>	список вторичных VLAN, ассоциированных с первичной VLAN. Вторичные VLAN могут быть двух видов: изолированные (isolated) и общие (community). Пользователь может указать несколько вторичных VLAN при помощи символа-разделителя ';'.
Состояние по умолчанию	Связи не настроены	
Режим	Режим конфигурации VLAN	
Применение	Эта команда используется только для private VLAN. Порты вторичных VLAN, ассоциированных с первичным VLAN могут связываться с портами первичного VLAN. Перед настройкой ассоциации private VLAN, private VLAN всех трех типов не должны иметь портов-членов; private VLAN с ассоциацией не могут быть удалены. Когда пользователь удаляет ассоциацию Private VLAN, все порты-участники Private VLAN с удаленной ассоциацией удаляются из Private VLAN. Команда show vlan private-vlan выводит на экран настройки	



Пример	Ассоциировать isolated VLAN200 и community VLAN300 с primary VLAN100. <pre>Switch#config Switch(config)# vlan 100 Switch(config-vlan100)#private-vlan association 200; 300 Set vlan 100 associated vlan successfully Switch(config-vlan100)#show vlan private-vlan</pre> <table><thead><tr><th>VLAN Name</th><th>Type</th><th>Asso VLAN</th><th>Ports</th></tr></thead><tbody><tr><td>-</td><td>-</td><td></td><td></td></tr><tr><td>100</td><td>VLAN0100</td><td>Primary</td><td>200 300</td></tr><tr><td>200</td><td>VLAN0200</td><td>Isolate</td><td>100</td></tr><tr><td>300</td><td>VLAN0300</td><td>Community</td><td>100</td></tr></tbody></table> <pre>Switch#</pre>	VLAN Name	Type	Asso VLAN	Ports	-	-			100	VLAN0100	Primary	200 300	200	VLAN0200	Isolate	100	300	VLAN0300	Community	100
VLAN Name	Type	Asso VLAN	Ports																		
-	-																				
100	VLAN0100	Primary	200 300																		
200	VLAN0200	Isolate	100																		
300	VLAN0300	Community	100																		

5.1.27. Вывод данных туннеля Dot1q (show dot1q-tunnel)

Синтаксис	Show dot1q-tunnel
Параметр	отсутствует
Состояние по умолчанию	Не задано
Режим	Привилегированный режим и режим конфигурации
Применение	Когда туннель Dot1q установлен, эта команда выводит на экран информацию о состоянии всех портов
Пример	Вывести на экран текущее состояние туннеля Dot1q. <pre>Switch#show dot1q-tunnel</pre> Interface Ethernet1/0/1: dot1q-tunnel is enable <pre>Switch#</pre>

5.1.28. Вывод значений таймеров GARP (show garp timer)

Синтаксис	Show garp timer [join leave leaveall]	
Параметр	join	таймер слияния
	leave	таймер удержания



	leaveall	таймер выхода для всех
Состояние по умолчанию	200 600 10000 миллисекунд для таймера join leave leaveall соответственно	
Режим	Привилегированный режим	
Применение	Показывает соответствующее значение таймера, указанного в команде	
Пример	Показать текущее значение всех таймеров GARP. Switch# show garp timer GARP join timer value is : 200 (ms) GARP leave timer value is : 600 (ms) GARP leaveall timer value is : 10000 (ms) Switch#	

5.1.29. Вывод данных машин GVRP (show gvrp fsm information)

Синтаксис	show gvrp fsm information interface (ethernet port-channel IFNAME)	
Параметр	ethernet	физический порт
	port-channel	агрегированный порт
	IFNAME	имя порта
Состояние по умолчанию	MT для зарегистрированных машин, VO для машин в состоянии запроса	
Режим	Привилегированный режим	
Применение	Отображает текущее состояние всех зарегистрированных машин и машин с запросом состояния	
Пример	Показать состояние всех машин Switch# show gvrp fsm information interface ethernet 1/0/1 VA: Очень беспокойный активный участник, AA: Беспокойный активный участник, QA: Спокойный активный участник VP: Очень беспокойный пассивный участник, AP: Беспокойный пассивный участник,	



	QP: Спокойный пассивный участник VO: Очень беспокойный наблюдатель, AO: Беспокойный наблюдатель, QO: Спокойный наблюдатель LA: Уходящий активный участник, LO: Выходящий наблюдатель IN: Входящий LV: Выходящий MT: Пустой INR: Регистрация входа зафиксирована, LVR: Регистрация выхода зафиксирована, MTR: Пустой, регистрация зафиксирована INF: Вход, регистрация запрещена LVF: Выход, регистрация запрещена MTF: Пусто, регистрация запрещена Ethernet1/0/1 gvrp fsm information: Index VLANID Applicant Registrar - 1 1 Qa MT Switch#

5.1.30. Вывод данных машин в статусе leaveAll (show gvrp leaveAll fsm information)

Синтаксис	show gvrp leaveAll fsm information interface (ethernet port-channel IFNAME)	
Параметр	ethernet	физический порт
	port-channel	агрегированный порт
	IFNAME	имя порта
Состояние по умолчанию	Passive (Пассивный)	
Режим	Привилегированный режим	
Применение	Позволяет проверить состояние машин в статусе leaveAll	



Пример	Показать состояние машин в статусе leaveAll на порте. <pre>Switch# show gvrp fsm information interface ethernet 1/0/1</pre> Interface LeaveAll fsm Ethernet1/0/1 Passive Switch#

5.1.31. Данные таймера удержания GVRP (show gvrp leavetimer running information)

Синтаксис	show gvrp leavetimer running information [vlan <1-4094>][interface (ethernet port-channel IFNAME)]	
Параметр	<1-4094>	метка Vlan
	ethernet	физический порт
	port-channel	агрегированный порт
	IFNAME	имя порта
Состояние по умолчанию	Таймер отключен	
Режим	Привилегированный режим	
Применение	Позволяет просмотреть состояние и время действия каждого таймера удержания	
Пример	Показать состояние и время действия каждого таймера удержания на порту. <pre>Switch# show gvrp leavetimer running information interface ethernet 1/0/1</pre> VLANID running state expired time ----- ----- Switch#	

5.1.32. Просмотр портов с включенным GVRP (show gvrp port-member)

Синтаксис	show gvrp [active] port-member	
Параметр	active	порт в активном состоянии



Состояние по умолчанию	GVRP на порту отключен
Режим	Привилегированный режим
Применение	Команда применяется для просмотра всех портов (включенных GVRP), сохраненных в GVRP
Пример	Показать все порты с включенным GVRP. <pre>Switch#show gvrp port-member</pre> Ports which were enabled gvrp included: Ethernet1/0/1 <pre>Switch#</pre>

5.1.33. Вывод данных регистрации VLAN (show gvrp port registerd vlan)

Синтаксис	show gvrp port [dynamic static] registerd vlan interface (Ethernet port-channel IFNAME)	
Параметр	dynamic	динамическая регистрация
	static	статическая регистрация
	Ethernet	физический порт
	port-channel	агрегированный порт
	port IFNAME	имя порта
Состояние по умолчанию	На порту нет динамических или статических зарегистрированных виртуальных локальных сетей	
Режим	Привилегированный режим	
Применение	Команда отображает VLAN, соответствующие машинам, зарегистрированные с помощью динамической или статической регистрации	
Пример	Показать все динамические или статические регистрации VLAN на текущем порту. <pre>Switch#show gvrp port registerd vlan interface ethernet 1/0/1</pre> Current port dynamic registerd vlan included: Current port static registerd vlan included: <pre>Switch#</pre>	



5.1.34. Данные установленных таймеров GVRP (show gvrp timer running information)

Синтаксис	show gvrp timer (join leaveall) running information interface (ethernet port-channel IFNAME)	
Параметр	join	таймер слияния
	leaveall	таймер выхода для всех
	Ethernet	физический порт
	port-channel	агрегированный порт
	port IFNAME	имя порта
Состояние по умолчанию	Таймер joint отключен, а таймер leaveAll включен	
Режим	Привилегированный режим	
Применение	Проверка состояния таймера join leaveAll на порту	
Пример	Показать состояние и время истечения срока действия каждого таймера. <pre>Switch#show gvrp timer join running information interface ethernet 1/0/1 Current port's jointimer running state is: UP Current port's jointimer expired time is: 0.2 s Switch#</pre>	

5.1.35. Вывод данных портов с зарегистрированной VLAN (show gvrp vlan registered port)

Синтаксис	show gvrp vlan <1-4094> registered port	
Параметр	<1-4094>	метка Vlan
Состояние по умолчанию	Не зарегистрировано ни одного порта с указанной VLAN	
Режим	Режим admin	
Применение	отсутствует	



Пример	Показать все порты с текущей зарегистрированной VLAN. <pre>Switch#show gvrp vlan 100 registerd port Ethernet1/0/3 (T) Ethernet1/0/4 (T) Ethernet1/0/5 (T) Ethernet1/0/6 (T) Ethernet1/0/7 (T) Ethernet1/0/8 (T) Ethernet1/0/9 (T) Ethernet1/0/10 (T) Switch#</pre>

5.1.36. Вывод данных VLAN (show vlan)

Синтаксис	show vlan [brief summary] [id <vlan-id>] [name <vlan-name>] [internal usage [id <vlan-id> name <vlan-name>]]	
Параметр	brief	вывод краткой информации
	summary	вывод статистики VLAN
	<vlan-id>	идентификатор VLAN того VLAN, для которого на экран выводится информация, в пределах от 1 до 4094
	<vlan-name>	имя VLAN, информация о котором выводится на экран, строка длиной от 1 до 11 символов
Состояние по умолчанию	отсутствует	
Режим	Привилегированный режим, режим конфигурации	
Применение	Если параметры < vlan-id> или <vlan-name> не заданы, на экран выводится информация о всех VLAN коммутатора	
	<pre>Switch#show vlan summary The max. Vlan entries: 4094 Existing Vlan: Universal Vlan: 1 Private Vlan: 100 200 300 Total Existing Vlan: 4</pre>	



Switch#		
Информация, отображаемая на дисплее	Пояснение	
VLAN	идентификатор VLAN	
Name	имя VLAN	
Type	Тип VLAN, статическая настройка либо полученная при динамическом обучении.	
Media	Тип интерфейса VLAN: Ethernet	
Ports	Порт доступа в VLAN	

5.1.37. Вывод данных VLAN-трансляции (show vlan-translation)

Синтаксис	show vlan-translation	
Параметр	Отсутствует	
Состояние по умолчанию	отсутствует	
Режим	Привилегированный режим и режим конфигурации	
Применение	Команда выводит на экран информацию обо всех портах, находящихся в состоянии VLAN-трансляции	
Пример	Вывести на экран информацию о состоянии текущей VLAN-трансляции. Switch#show vlan-translation Interface Ethernet1/0/1: vlan-translation is enable, miss drop is not set	

5.1.38. Трансляция VLAN Multi-to-One (vlan-translation n-to-1)

Синтаксис	vlan-translation n-to-1 <WORD> to <new-vlan-id> no vlan-translation n-to-1 <WORD>	
Параметр	<WORD>	идентификатор исходной VLAN, его диапазон от 1 до 4094, соединяются символами ';' и '-'. Если две VLAN с разными диапазонами преобразуются в



		разные VLAN ID в одном порту, два диапазона VLAN не должны пересекаться
	<new-vlan-id>	преобразованный идентификатор VLAN, диапазон от 1 до 4094
Состояние по умолчанию	Отключено	
Режим	Настройка портов	
Применение	Трансляция Multi-to-One VLAN используется на границе сети для сопоставления нескольких VLAN с одним VLAN магистральной сети. Когда трафик данных возвращается из магистральной сети на границу сети, он восстанавливает VLAN границы сети для осуществления трансляции Multi-to-One VLAN и экономии ресурсов VLAN магистральной сети. Примечание: При использовании этой функции устройство должно сначала установить оригинальную и транслированную VLAN, а также включить порт нисходящего канала этой функции и порт восходящего канала для подключения к магистральной сети, которые должны быть соединены в оригинальной и транслированной VLAN с тегированным режимом. Эта функция не должна использоваться одновременно с dot1q-tunnel и трансляцией VLAN. Примечание: Трансляция VLAN из одной сети в другую должна включаться после обучения MAC. Команда show vlan-translation n-to-1 выводит на экран настройки	
Пример	На Ethernet 1/0/1 транслировать трафик данных из VLAN с диапазоном от 1 до 5 в VLAN 100, а трафик данных (принадлежащий VLAN с диапазоном от 1 до 5) из VLAN100 транслировать в соответствующий VLAN ID, подключить порт восходящей линии магистральной сети как Ethernet 1/0/5. <pre>Switch#config Switch(config)#vlan 1; 5; 100 Switch(config)#vlan 2-4 Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode trunk Set the port Ethernet1/0/1 mode Trunk successfully Switch(config-if-ethernet1/0/1)#vlan-translation n-to-1 1-5 to 100 Switch(config-if-ethernet1/0/1)#interface ethernet 1/0/5 Switch(config-if-ethernet1/0/5)#switchport mode trunk Set the port Ethernet1/0/5 mode Trunk successfully Switch#show vlan-translation n-to-1 Ethernet1/0/1: vlan-translation n-to-1 enable</pre>	



	vlan-translation n-to-1 1-5 to 100

5.1.39. Вывод данных о трансляции Multi-to-One VLAN (show vlan-translation n-to-1)

Синтаксис	show vlan-translation n-to-1 <interface-name>	
Параметр	<interface-name>	Указывает имя порта, которое будет отображаться. Если параметр отсутствует, функция отображает все настройки порта
Состояние по умолчанию	Информация о трансляции Multi-to-One VLAN отсутствует	
Режим	Привилегированный режим	
Применение	Если в команде указан параметр VLAN, отображаются преобразования n-to-1 для указанной VLAN; если VLAN не указана, отображается вся информация n-to-1	
Пример	Показать все конфигурации портов трансляции VLAN с функцией Multi-to-One. <pre>Switch#show vlan-translation n-to-1</pre> Ethernet1/0/1: <pre>vlan-translation n-to-1 enable vlan-translation n-to-1 1-5 to 100</pre>	

5.1.40. Предпочтение динамической VLAN на основе MAC-адресов (dynamic-vlan mac-vlan prefer)

Синтаксис	dynamic-vlan mac-vlan prefer	
Параметр	Отсутствует	
Состояние по умолчанию	По умолчанию предпочтение отдается VLAN на основе MAC-адресов	
Режим	Режим глобальной конфигурации	
Применение	Команда устанавливает приоритет динамических VLAN на коммутаторе. По умолчанию отдается последовательности VLAN на основе MAC-адресов, VLAN на основе IP-подсетей и VLAN на основе протоколов, т. е. приоритет действует при наличии нескольких динамических VLAN. Данная команда применяется в случае, когда	



	VLAN на основе IP-подсети установлена как предпочтительная, а пользователь хочет вернуть приоритет VLAN на основе MAC-адресов. Команда show dynamic-vlan prefer отображает настройки
Пример	Установить VLAN на основе MAC-адресов в качестве приоритетной. <pre>Switch#config Switch(config)#dynamic-vlan mac-vlan prefer Switch#show dynamic-vlan prefer Mac Vlan/Voice Vlan IP Subnet Vlan Protocol Vlan</pre>

5.1.41. Приоритетность подсети VLAN (dynamic-vlan subnet-vlan prefer)

Синтаксис	dynamic-vlan subnet-vlan prefer
Параметр	Отсутствует
Состояние по умолчанию	По умолчанию предпочтение отдается VLAN на основе MAC-адресов
Режим	Режим глобальной конфигурации
Применение	Команда устанавливает приоритет динамических VLAN на коммутаторе. По умолчанию приоритетными являются VLAN на основе MAC-адресов, VLAN на основе IP-подсетей и VLAN на основе протоколов, т. е. приоритет очереди при наличии нескольких динамических VLAN. Эта команда устанавливает приоритет для использования VLAN на основе IP-подсетей. Команда show dynamic-vlan prefer отображает настройки
Пример	Установить VLAN на основе IP-подсети в качестве приоритетной. <pre>Switch#config Switch(config)#dynamic-vlan subnet-vlan prefer Switch(config)#show dynamic-vlan prefer Mac Vlan/Voice Vlan IP Subnet Vlan Protocol Vlan</pre>



5.1.42. Сеть MAC VLAN (mac-vlan vlan)

Синтаксис	mac-vlan vlan <vlan-id> no mac-vlan vlan <vlan-id>										
Параметр	<vlan-id>	<vlan-id> номер указанной сети VLAN									
Состояние по умолчанию	По умолчанию MAC VLAN не настроена										
Режим	Режим глобальной конфигурации										
Применение	Команда устанавливает указанную VLAN в качестве MAC VLAN. Команда show mac-vlan выводит на экран настройки										
Пример	Задать VLAN100 в качестве MAC VLAN. Switch#config Switch(config)#mac-vlan vlan 100										
	Switch#show vlan <table><tr><td>VLAN Name</td><td>Type</td><td>Media</td><td>Ports</td></tr><tr><td>1 default</td><td>Static</td><td>ENET</td><td>Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19 Ethernet1/0/20 Ethernet1/0/21 Ethernet1/0/22 Ethernet1/0/23 Ethernet1/0/24 Ethernet1/0/25 Ethernet1/0/26 Ethernet1/0/27 Ethernet1/0/28</td></tr></table>				VLAN Name	Type	Media	Ports	1 default	Static	ENET
VLAN Name	Type	Media	Ports								
1 default	Static	ENET	Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19 Ethernet1/0/20 Ethernet1/0/21 Ethernet1/0/22 Ethernet1/0/23 Ethernet1/0/24 Ethernet1/0/25 Ethernet1/0/26 Ethernet1/0/27 Ethernet1/0/28								



	100 VLAN0100	UserDynam	ENET

5.1.43. Ассоциация MAC-адреса с VLAN (mac-vlan)

Синтаксис	mac-vlan mac <mac-addrss> <mac-mask> vlan <vlan-id> priority <priority-id> no mac-vlan {mac <mac-addrss> <mac-mask> all}										
Параметр	<mac-addrss>/<mac-mask>	Формат mac-адреса/mac-маски: XX-XX-XX-XX-XX-XX									
	<vlan-id>	vlan-id это идентификатор VLAN с допустимым диапазоном 1~4094									
	<priority-id>	priority-id это уровень приоритета, который используется в теге VLAN с допустимым диапазоном 0~7									
Состояние по умолчанию	По умолчанию ни один MAC-адрес не ассоциирован с VLAN										
Режим	Режим глобальной конфигурации										
Применение	С помощью этой команды пользователь может добавить указанный MAC-адрес в указанную VLAN. Если из порта коммутатора с указанного MAC-адреса поступает пакет данных без метки VLAN, ему будет присвоен указанный VLAN ID, и он будет отправлен в указанную VLAN. Тег VLAN у этих пакетов будет одним и тем же, независимо от того, с какого порта приняты пакеты. Команда не оказывает никакого влияния на пакеты данных с метками VLAN. Команда show mac-vlan выводит на экран настройки										
Пример	Добавить сетевое устройство с MAC-адресом 00-03-0f-11-22-33 в VLAN 100. Switch#config Switch(config)#mac-vlan vlan 100 Switch(config)#mac-vlan mac 00-03-0f-11-22-33 ff-ff-ff-ff-ff-ff vlan 100 priority 0 Switch#show mac-vlan <table><tr><td>Mac-Address</td><td>Mac-Mask</td><td>VLAN_ID</td><td>Priority</td></tr><tr><td>00-03-0f-11-22-33</td><td>ff-ff-ff-ff-ff-ff</td><td>100</td><td>0</td></tr></table>			Mac-Address	Mac-Mask	VLAN_ID	Priority	00-03-0f-11-22-33	ff-ff-ff-ff-ff-ff	100	0
Mac-Address	Mac-Mask	VLAN_ID	Priority								
00-03-0f-11-22-33	ff-ff-ff-ff-ff-ff	100	0								



5.1.44. Протоколы VLAN (protocol-vlan)

Синтаксис	<pre>protocol-vlan mode (ethernetII snap) etype <etype-id> vlan <vlan-id> [priority<priority-id>] protocol-vlan mode llc dsap <dsap-id> ssap <ssap-id> vlan <vlan-id> no protocol-vlan (mode ((ethernetII snap) etype <etype-id>) all} no protocol-vlan mode llc dsap <dsap-id> ssap <ssap-id></pre>													
Параметр	<etype-id>	etype-id это тип протокола пакета, диапазон значений 1536 – 65535												
	<vlan-id>	vlan-id — идентификатор VLAN, допустимый диапазон 1~4094												
	<priority-id>	priority-id - приоритет, диапазон 0~7												
	<dsap-id>/<ssap-id>	dsap-id это точка доступа назначения, ssap-id: точка доступа источника, диапазон значений 0 - 255												
Состояние по умолчанию	По умолчанию ни один протокол не ассоциирован с VLAN													
Режим	Режим глобальной конфигурации													
Применение	Эта команда используется для добавления в VLAN конкретных протоколов. Если пакеты указанных протоколов без тегов VLAN принимаются коммутатором, они проверяются на согласование с VLAN с идентификатором VLAN ID и затем передаются в этот VLAN. Тег VLAN у этих пакетов будет одним и тем же, независимо от того, с какого порта приняты пакеты. Когда эта команда введена, пакеты, уже имеющие теги VLAN, не будут изменены. Рекомендуется настраивать протокол ARP вместе с протоколом IP, иначе это может повлиять на работу некоторых приложений. Команда "show protocol -vlan" выведет на экран настройки													
Пример	Присвоить протокол IP-пакета данных, инкапсулированный в EthernetII сети LAN200. <pre>Switch#config Switch(config)#protocol-vlan mode ethernetII etype 1536 vlan 200 Switch#show protocol-vlan</pre> <table> <thead> <tr> <th>Protocol_Type</th><th>VLAN_ID</th><th>Priority</th></tr> </thead> <tbody> <tr> <td colspan="3">-----</td> </tr> <tr> <td>mode ethernetii etype 0x600</td><td>200</td><td>0</td> </tr> <tr> <td>mode ethernetii etype 0x60e</td><td>1</td><td>7</td> </tr> </tbody> </table>		Protocol_Type	VLAN_ID	Priority	-----			mode ethernetii etype 0x600	200	0	mode ethernetii etype 0x60e	1	7
Protocol_Type	VLAN_ID	Priority												

mode ethernetii etype 0x600	200	0												
mode ethernetii etype 0x60e	1	7												



	mode snap etype 0x613	1	1	
	mode llc dsap 0x1	ssap 0x1	1	0

5.1.45. Вывод данных о приоритетных динамических VLAN (show dynamic-vlan prefer)

Синтаксис	show dynamic-vlan prefer
Параметр	Отсутствует
Состояние по умолчанию	Mac Vlan/Voice Vlan
Режим	Привилегированный режим, режим конфигурации
Применение	Команда позволяет вывести на экран предпочтения динамических VLAN
Пример	Вывести на экран текущий приоритет динамических VLAN. Switch#show dynamic-vlan prefer Mac Vlan/Voice Vlan IP Subnet Vlan Protocol Vlan

5.1.46. Вывод данных VLAN на основе MAC-адресов (show mac-vlan interface)

Синтаксис	show mac-vlan interface
Параметр	Отсутствует
Состояние по умолчанию	Отсутствует
Режим	Привилегированный режим и другие режимы конфигурации
Применение	Команда выводит на экран порты, которые поддерживают VLAN на основе MAC-адресов, а символы в скобках указывают на режим работы порта: А - порты доступа, Т - магистральные порты и Н - гибридные порты
Пример	Вывести на экран порты, поддерживающие VLAN на основе MAC-адресов.



Switch#show mac-vlan
Ports

Ethernet1/0/1(A) Ethernet1/0/2(A) Ethernet1/0/3(A) Ethernet1/0/4(A)
Ethernet1/0/5(A) Ethernet1/0/6(A) Ethernet1/0/7(A) Ethernet1/0/8(A)
Ethernet1/0/9(A) Ethernet1/0/10(A) Ethernet1/0/11(A)
Ethernet1/0/12(A) Ethernet1/0/13(A) Ethernet1/0/14(A)
Ethernet1/0/15(A) Ethernet1/0/16(A) Ethernet1/0/17(A)
Ethernet1/0/18(A) Ethernet1/0/19(A) Ethernet1/0/20(A)
Ethernet1/0/21(A) Ethernet1/0/22(A) Ethernet1/0/23(A)
Ethernet1/0/24(A) Ethernet1/0/25(A) Ethernet1/0/26(A)
Ethernet1/0/27(A) Ethernet1/0/28(A)

5.1.47. Вывод данных протокола VLAN (show protocol-vlan)

Синтаксис	show protocol-vlan																		
Параметр	Отсутствует																		
Состояние по умолчанию	Отсутствует																		
Режим	Привилегированный режим и режим конфигурации																		
Применение	Команда выводит на экран конфигурирования VLAN на основе протокола на коммутаторе																		
Пример	Вывести на экран конфигурирования текущей сети VLAN на основе протокола. Switch#show protocol-vlan <table><thead><tr><th>Protocol_Type</th><th>VLAN_ID</th><th>Priority</th></tr></thead><tbody><tr><td>-</td><td></td><td></td></tr><tr><td>mode ethernetii etype 0x600</td><td>200</td><td>0</td></tr><tr><td>mode ethernetii etype 0x60e</td><td>1</td><td>7</td></tr><tr><td>mode snap etype 0x613</td><td>1</td><td>1</td></tr><tr><td>mode llc dsap 0x1 ssap 0x1</td><td>1</td><td>0</td></tr></tbody></table>	Protocol_Type	VLAN_ID	Priority	-			mode ethernetii etype 0x600	200	0	mode ethernetii etype 0x60e	1	7	mode snap etype 0x613	1	1	mode llc dsap 0x1 ssap 0x1	1	0
Protocol_Type	VLAN_ID	Priority																	
-																			
mode ethernetii etype 0x600	200	0																	
mode ethernetii etype 0x60e	1	7																	
mode snap etype 0x613	1	1																	
mode llc dsap 0x1 ssap 0x1	1	0																	

5.1.48. Вывод данных подсети VLAN (show subnet-vlan)

Синтаксис	show subnet-vlan
Параметр	Отсутствует



Состояние по умолчанию	Отсутствует								
Режим	Привилегированный режим и другие режимы конфигурации								
Применение	Команда выводит на экран конфигурирования VLAN на основе IP-подсетей на коммутаторе								
Пример	Вывести на экран конфигурирования текущей VLAN на основе IP-подсетей. Switch#show subnet-vlan <table><thead><tr><th>IP-Address</th><th>Mask</th><th>VLAN_ID</th><th>Priority</th></tr></thead><tbody><tr><td>192.168.5.2</td><td>255.255.255.0</td><td>100</td><td>0</td></tr></tbody></table>	IP-Address	Mask	VLAN_ID	Priority	192.168.5.2	255.255.255.0	100	0
IP-Address	Mask	VLAN_ID	Priority						
192.168.5.2	255.255.255.0	100	0						

5.1.49. Вывод интерфейса подсети VLAN (show subnet-vlan interface)

Синтаксис	show subnet-vlan interface																																
Параметр	Отсутствует																																
Состояние по умолчанию	Отсутствует																																
Режим	Привилегированный режим и другие режимы конфигурации																																
Применение	Команда выводит на экран порты, которые поддерживают VLAN на основе IP-подсетей; символы в скобках указывают на режим работы порта: А — порты доступа, Т — магистральные порты и Н — гибридные порты																																
Пример	Вывести на экран порты, поддерживающие VLAN на основе IP-подсетей в данный момент. Switch#show subnet-vlan interface Ports ----- <table><tr><td>Ethernet1/0/1(A)</td><td>Ethernet1/0/2(A)</td><td>Ethernet1/0/3(A)</td><td>Ethernet1/0/4(A)</td></tr><tr><td>Ethernet1/0/5(A)</td><td>Ethernet1/0/6(A)</td><td>Ethernet1/0/7(A)</td><td>Ethernet1/0/8(A)</td></tr><tr><td>Ethernet1/0/9(A)</td><td>Ethernet1/0/10(A)</td><td></td><td>Ethernet1/0/11(A)</td></tr><tr><td></td><td>Ethernet1/0/12(A)</td><td>Ethernet1/0/13(A)</td><td>Ethernet1/0/14(A)</td></tr><tr><td>Ethernet1/0/15(A)</td><td>Ethernet1/0/16(A)</td><td></td><td>Ethernet1/0/17(A)</td></tr><tr><td></td><td>Ethernet1/0/18(A)</td><td>Ethernet1/0/19(A)</td><td>Ethernet1/0/20(A)</td></tr><tr><td>Ethernet1/0/21(A)</td><td>Ethernet1/0/22(A)</td><td></td><td>Ethernet1/0/23(A)</td></tr><tr><td></td><td>Ethernet1/0/24(A)</td><td>Ethernet1/0/25(A)</td><td>Ethernet1/0/26(A)</td></tr></table>	Ethernet1/0/1(A)	Ethernet1/0/2(A)	Ethernet1/0/3(A)	Ethernet1/0/4(A)	Ethernet1/0/5(A)	Ethernet1/0/6(A)	Ethernet1/0/7(A)	Ethernet1/0/8(A)	Ethernet1/0/9(A)	Ethernet1/0/10(A)		Ethernet1/0/11(A)		Ethernet1/0/12(A)	Ethernet1/0/13(A)	Ethernet1/0/14(A)	Ethernet1/0/15(A)	Ethernet1/0/16(A)		Ethernet1/0/17(A)		Ethernet1/0/18(A)	Ethernet1/0/19(A)	Ethernet1/0/20(A)	Ethernet1/0/21(A)	Ethernet1/0/22(A)		Ethernet1/0/23(A)		Ethernet1/0/24(A)	Ethernet1/0/25(A)	Ethernet1/0/26(A)
Ethernet1/0/1(A)	Ethernet1/0/2(A)	Ethernet1/0/3(A)	Ethernet1/0/4(A)																														
Ethernet1/0/5(A)	Ethernet1/0/6(A)	Ethernet1/0/7(A)	Ethernet1/0/8(A)																														
Ethernet1/0/9(A)	Ethernet1/0/10(A)		Ethernet1/0/11(A)																														
	Ethernet1/0/12(A)	Ethernet1/0/13(A)	Ethernet1/0/14(A)																														
Ethernet1/0/15(A)	Ethernet1/0/16(A)		Ethernet1/0/17(A)																														
	Ethernet1/0/18(A)	Ethernet1/0/19(A)	Ethernet1/0/20(A)																														
Ethernet1/0/21(A)	Ethernet1/0/22(A)		Ethernet1/0/23(A)																														
	Ethernet1/0/24(A)	Ethernet1/0/25(A)	Ethernet1/0/26(A)																														



	Ethernet1/0/27(A)	Ethernet1/0/28(A)

5.1.50. subnet-vlan

Синтаксис	subnet-vlan ip-address <ipv4-addrss> mask <subnet-mask> vlan <vlan-id> priority <priority-id> no subnet-vlan {ip-address <ipv4-addrss> mask <subnet-mask> all}	
Параметр	<ipv4-addrss>	это IPv4-адрес, представленный десятично-точечной записью; допустимый диапазон каждой секции - 0~255;
	<subnet-mask>	код маски подсети в десятично-точечной записи; допустимый диапазон каждой секции - 0~255;
	<vlan-id>	идентификатор VLAN с допустимым диапазоном 1~4094
	<priority-id>	приоритет, применяемый в теге VLAN, допустимый диапазон 0~7;
Состояние по умолчанию	По умолчанию ни одна IP-подсеть не подключена к VLAN	
Режим	Режим глобальной конфигурации	
Применение	Эта команда используется для добавления в VLAN конкретных IP подсети. Если пакеты без тегов VLAN из указанного IP подсети принимаются коммутатором, они проверяются на согласование с заданным идентификатором VLAN ID и затем передаются в этот VLAN. Эти пакеты попадают в одну и ту же VLAN независимо от порта, с которого они поступают. Когда эта команда введена, пакеты, уже имеющие теги VLAN, не будут изменены. Команда show subnet-vlan выводит на экран настройки	
Пример	Добавить сетевое оборудование с IP-подсети 192.168.1.1/24 в VLAN 300 <pre>Switch#config Switch(config)#vlan 300 Switch(config-vlan300)#exit Switch(config)#subnet-vlan ip-address 192.168.1.1 mask 255.255.255.0 vlan 300 priority 0 Switch(config)#show subnet-vlan</pre>	



	IP-Address	Mask	VLAN_ID	Priority
	192.168.1.1	255.255.255.0	300	0

5.1.51. Настройка VLAN на основе MAC-адресов (switchport mac-vlan enable)

Синтаксис	switchport mac-vlan enable no switchport mac-vlan enable
Параметр	отсутствует
Состояние по умолчанию	Функция MAC-base VLAN включена на порту
Режим	Режим конфигурации порта
Применение	После добавления MAC-адреса в указанную VLAN функция MAC-based VLAN будет включена в режиме глобальной конфигурации. Эта команда отключает функцию MAC VLAN для указанного порта для специальных пользовательских приложений. Команда "show mac-vlan interface" выводит на экран настройки
Пример	Отключить функцию VLAN на основе MAC-адресов на порту1. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#no switchport mac-vlan enable Switch(config-if-ethernet1/0/1)#show mac-vlan interface Ports Ethernet1/0/2(A) Ethernet1/0/3(A) Ethernet1/0/4(A) Ethernet1/0/5(A) Ethernet1/0/6(A) Ethernet1/0/7(A) Ethernet1/0/8(A) Ethernet1/0/9(A) Ethernet1/0/10(A) Ethernet1/0/11(A) Ethernet1/0/12(A) Ethernet1/0/13(A) Ethernet1/0/14(A) Ethernet1/0/15(A) Ethernet1/0/16(A) Ethernet1/0/17(A) Ethernet1/0/18(A) Ethernet1/0/19(A) Ethernet1/0/20(A) Ethernet1/0/21(A) Ethernet1/0/22(A) Ethernet1/0/23(A) Ethernet1/0/24(A) Ethernet1/0/25(A) Ethernet1/0/26(A) Ethernet1/0/27(A) Ethernet1/0/28(A)

5.1.52. Настройка подсетей VLAN (switchport subnet-vlan enable)

Синтаксис	switchport subnet-vlan enable no switchport subnet-vlan enable
Параметр	отсутствует



Состояние по умолчанию	VLAN на основе IP-подсетей включена на порту по умолчанию
Режим	Режим конфигурации порта
Применение	После добавления IP-подсети в указанную VLAN функция VLAN на основе IP-подсетей будет включена в режиме глобальной конфигурации. Эта команда отключает функцию VLAN на основе IP-подсетей на указанном порту для специальных пользовательских приложений. Команда <code>show subnet-vlan interface</code> выводит на экран настройки
Пример	Отключить функцию VLAN на основе IP-подсетей на порту2. <pre>Switch#config Switch(config)# interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)#no switchport subnet-vlan enable Switch(config-if-ethernet1/0/2)#show subnet-vlan interface Ports ----- Ethernet1/0/1(A) Ethernet1/0/3(A) Ethernet1/0/4(A) Ethernet1/0/5(A) Ethernet1/0/6(A) Ethernet1/0/7(A) Ethernet1/0/8(A) Ethernet1/0/9(A) Ethernet1/0/10(A) Ethernet1/0/11(A) Ethernet1/0/12(A) Ethernet1/0/13(A) Ethernet1/0/14(A) Ethernet1/0/15(A) Ethernet1/0/16(A) Ethernet1/0/17(A) Ethernet1/0/18(A) Ethernet1/0/19(A) Ethernet1/0/20(A) Ethernet1/0/21(A) Ethernet1/0/22(A) Ethernet1/0/23(A) Ethernet1/0/24(A) Ethernet1/0/25(A) Ethernet1/0/26(A) Ethernet1/0/27(A) Ethernet1/0/28(A)</pre>

5.1.53. Вывод данных голосовой VLAN (show voice-vlan)

Синтаксис	<code>show voice-vlan</code>
Параметр	Отсутствует
Состояние по умолчанию	Отсутствует
Режим	Привилегированный режим и другие режимы конфигурации
Применение	Выводит на экран конфигурирование голосовой виртуальной локальной сети Voice VLAN (голосовой VLAN)



Пример	Вывести на экран текущую конфигурирование голосовой VLAN. Switch#show subnet-vlan			
	IP-Address	Mask	VLAN_ID	Priority
	-	-		
	192.168.5.2	255.255.255.0	100	0

5.1.54. Настройки голосовой VLAN (switchport voice-vlan enable)

Синтаксис	switchport voice-vlan enable no switchport voice-vlan enable
Параметр	отсутствует
Состояние по умолчанию	По умолчанию Voice VLAN включена
Режим	Режим конфигурации порта
Применение	По умолчанию голосовые виртуальные локальные сети Voice VLAN включаются в глобальном режиме конфигурации, когда голосовое устройство присоединяется к голосовой виртуальной локальной сети. Эта команда отключает Voice VLAN на указанных портах для заданных пользователем применений. Команда "show voice-vlan" выводит на экран настройки
Пример	Отключить функцию Voice VLAN на порту2. Switch#config Switch(config)# interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)#no switchport voice-vlan enable Switch(config-if-ethernet1/0/2)# show voice-vlan Voice VLAN ID: 100 Ports ----- Ethernet1/0/1(A) Ethernet1/0/3(A) Ethernet1/0/4(A) Ethernet1/0/5(A) Ethernet1/0/6(A) Ethernet1/0/7(A) Ethernet1/0/8(A) Ethernet1/0/9(A) Ethernet1/0/10(A) Ethernet1/0/11(A) Ethernet1/0/12(A) Ethernet1/0/13(A) Ethernet1/0/14(A) Ethernet1/0/15(A) Ethernet1/0/16(A) Ethernet1/0/17(A) Ethernet1/0/18(A) Ethernet1/0/19(A) Ethernet1/0/20(A) Ethernet1/0/21(A) Ethernet1/0/22(A) Ethernet1/0/23(A)



	Ethernet1/0/24(A) Ethernet1/0/25(A) Ethernet1/0/26(A) Ethernet1/0/27(A) Ethernet1/0/28(A)
	Voice name Mac-Address Mask Priority

5.1.55. Голосовая VLAN (voice-vlan)

Синтаксис	voice-vlan mac <mac-address> mask <mac-mask> priority <priority-id> [name <voice-name>] no voice-vlan {mac <mac-address> mask <mac-mask> name <voice-name> all}	
Параметр	<mac-address>	MAC-адрес голосового оборудования в формате "xx-xx-xx-xx-xx-xx"
	<mac-mask>	последние восемь цифр кода маски MAC-адреса, допустимые значения: 0xff, 0xfe, 0xfc, 0xf8, 0xf0, 0xe0, 0xc0, 0x80, 0x0
	<priority-id>	приоритет голосового трафика, допустимый диапазон: 0–7
	<voice-name>	имя голосового устройства для облегчения управления устройством
Состояние по умолчанию	Эта команда добавляет указанное голосовое устройство в Voice VLAN. Если пакет данных без VLAN-тегов для указанного голосового устройства поступает из порта коммутатора, пакет принадлежит Voice VLAN независимо от порта, из которого поступает пакет данных. Команда не меняет пакеты, уже имеющие теги VLAN	
Режим	Режим глобальной конфигурации	
Применение	Эта команда добавляет указанное голосовое устройство в Voice VLAN. Если пакет данных без VLAN-тегов для указанного голосового устройства поступает из порта коммутатора, пакет принадлежит Voice VLAN независимо от порта, из которого поступает пакет данных. Команда не меняет пакеты, уже имеющие теги VLAN. Команда show voice-vlan выводит на экран настройки	
Пример	Добавить 256 комплектов голосового оборудования отдела исследований и разработок с MAC-адресами от 00-03-0f-11-22-00 до 00-03-0f-11-22-ff в Voice VLAN. Switch#config Switch(config)#vlan 100 Switch(config-vlan100)#exit	



<pre>Switch(config)#voice-vlan vlan 100 Switch(config)#voice-vlan mac 00-03-0f-11-22-00 mask 0 priority 5 name R&D Switch(config)#show voice-vlan Voice VLAN ID: 100 Ports ----- Ethernet1/0/1(A) Ethernet1/0/3(A) Ethernet1/0/4(A) Ethernet1/0/5(A) Ethernet1/0/6(A) Ethernet1/0/7(A) Ethernet1/0/8(A) Ethernet1/0/9(A) Ethernet1/0/10(A) Ethernet1/0/11(A) Ethernet1/0/12(A) Ethernet1/0/13(A) Ethernet1/0/14(A) Ethernet1/0/15(A) Ethernet1/0/16(A) Ethernet1/0/17(A) Ethernet1/0/18(A) Ethernet1/0/19(A) Ethernet1/0/20(A) Ethernet1/0/21(A) Ethernet1/0/22(A) Ethernet1/0/23(A) Ethernet1/0/24(A) Ethernet1/0/25(A) Ethernet1/0/26(A) Ethernet1/0/27(A) Ethernet1/0/28(A) Voice name Mac-Address Mask Priority R&D 00-03-0f-11-22-00 00-00-00-00-00-00 5</pre>	

5.1.56. Настройка VLAN в качестве голосовой (voice-vlan vlan)

Синтаксис	<pre>voice-vlan vlan <vlan-id> no voice-vlan</pre>	
Параметр	<vlan-id>	номер указанной виртуальной локальной сети
Состояние по умолчанию	По умолчанию голосовая VLAN не настроена	
Режим	Режим глобальной конфигурации	
Применение	Команда задает указанную VLAN в качестве голосовой, одновременно может быть только одна голосовая VLAN. Голосовая VLAN не может применяться одновременно с VLAN на основе MAC-адресов. Команда show voice-vlan выводит на экран настройки	
Пример	Установить для VLAN100 значение Voice VLAN. <pre>Switch#config Switch(config)#vlan 100 Switch(config-vlan100)#exit Switch(config)#voice-vlan vlan 100</pre>	



Switch(config)#show voice-vlan Voice VLAN ID: 100			
Ports			

Ethernet1/0/1(A)	Ethernet1/0/3(A)	Ethernet1/0/4(A)	Ethernet1/0/5(A)
Ethernet1/0/6(A)	Ethernet1/0/7(A)	Ethernet1/0/8(A)	Ethernet1/0/9(A)
Ethernet1/0/10(A)	Ethernet1/0/11(A)		Ethernet1/0/12(A)
	Ethernet1/0/13(A)	Ethernet1/0/14(A)	Ethernet1/0/15(A)
Ethernet1/0/16(A)	Ethernet1/0/17(A)		Ethernet1/0/18(A)
	Ethernet1/0/19(A)	Ethernet1/0/20(A)	Ethernet1/0/21(A)
Ethernet1/0/22(A)	Ethernet1/0/23(A)		Ethernet1/0/24(A)
	Ethernet1/0/25(A)	Ethernet1/0/26(A)	Ethernet1/0/27(A)
Ethernet1/0/28(A)			
Voice name	Mac-Address	Mask	Priority



6. НАСТРОЙКА ПРОТОКОЛА ANTI-RING

6.1. Команды работы с протоколом MSTP

6.1.1. Прерывание (abort)

Команда	abort
Параметр	-
Значение по умолчанию	-
Режим	Режим настройки регионов MSTP
Руководство по использованию	Эта команда выполняет выход из режима настройки регионов MSTP без сохранения текущих настроек. При этом начинают использоваться предыдущие настройки региона MSTP
Пример	Выйти из режима настройки регионов MSTP без сохранения сделанных настроек. Switch(Config-Mstp-Region)#abort Switch(config)#

6.1.2. Выход (exit)

Команда	exit
Параметр	-
Значение по умолчанию	-
Режим	Режим настройки регионов MSTP
Руководство по использованию	Эта команда сохраняет сделанные настройки, а затем выполняет выход из режима настройки регионов MSTP
Пример	Выйти из режима настройки регионов MSTP с сохранением сделанных настроек. Switch(Config-Mstp-Region)#exit Switch(config)#



6.1.3. Экземпляры VLAN (instance vlan)

Команда	instance <instance-id> vlan <vlan-list> no instance <instance-id> [vlan <vlan-list>]	
Параметр	instance-id	задает номер экземпляра связующего дерева Диапазон значений от 0 до 64
	vlan-list	задает последовательность номеров VLAN, либо отдельные номера VLAN. символ "-" используется для ввода последовательности номеров, а символ ";" позволяет перечислить отдельные номера
Значение по умолчанию	До создания экземпляров связующего дерева имеется всего один экземпляр с номером 0, которому принадлежат все VLAN 1 - 4094	
Режим	Режим настройки регионов MSTP	
Руководство по использованию	Эта команда позволяет задать соответствие между VLAN и экземплярами связующего дерева. Коммутаторы считаются принадлежащими одному и тому же региону MSTP только в том случае, если одинаковы все заданные соответствия и другие атрибуты. До настройки экземпляров связующего дерева все VLAN принадлежат экземпляру 0. Протокол MSTP может поддерживать не более 48 экземпляров MSTI (не считая экземпляры общих связующих деревьев CIST). Общее связующее дерево CIST можно трактовать, как экземпляр дерева MSTI с номером 0. Все остальные экземпляры имеют номера с 1 по 48	
Пример	Поставить в соответствие VLAN 1-10 и VLAN 100-110 экземпляру связующего дерева 1. <pre>Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)#instance 1 vlan 1-10; 100-110</pre>	

6.1.4. Имя (name)

Команда	name <name> no name	
Параметр	name	имя региона MSTP. Длина имени не должна превышать 32 символа
Значение по умолчанию	Имя региона MSTP по умолчанию — MAC-адрес этого коммутатора	



Режим	Режим настройки регионов MSTP
Руководство по использованию	Команда используется для задания имени региона MSTP. Коммутаторы с одинаковыми именами региона MSTP и одинаковыми другими атрибутами рассматриваются, как один и тот же регион MSTP
Пример	Задать имя региона MSTP как mstp-test. Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)#name mstp-test

6.1.5. Номер версии (revision-level)

Команда	revision-level <level> no revision-level	
Параметр	level	номер версии. Допустимые значения – от 0 до 65 535
Значение по умолчанию	По умолчанию номер версии равен 0	
Режим	Режим настройки регионов MSTP	
Руководство по использованию	Эта команда позволяет задать номер версии настроек MSTP. Коммутаторы с одинаковыми именами региона MSTP и одинаковыми другими атрибутами рассматриваются, как один и тот же регион MSTP	
Пример	Установить номер версии 2000. Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)# revision-level 2000	

6.1.6. Протокол STP (spanning-tree)

Команда	spanning-tree no spanning-tree	
Параметр	-	
Значение по умолчанию	Протокол MSTP не включен	
Режим	Режим глобальной конфигурации, режим настройки портов	



Руководство по использованию	Если в режиме глобальной конфигурации протокол MSTP включен, то он включен на всех портах, за исключением тех, для которых использование MSTP выключено
Пример	Включить MSTP в режиме глобальной конфигурации, выключить MSTP в интерфейсе 0/0/2. <pre>Switch(config)#spanning-tree Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#no spanning-tree</pre>

6.1.7. Метрика протокола STP (spanning-tree cost)

Команда	spanning-tree cost <cost> no spanning-tree cost																									
Параметр	cost	указывает метрику маршрута. Допустимые значения – от 1 до 200 000 000																								
Значение по умолчанию	Метрика маршрута к порту соответствует пропускной способности порта <table> <tr> <td>Для агрегированных портов метрики маршрутов, используемые по умолчанию, следующие:</td><td>Метрика маршрута к порту, используемая по умолчанию</td><td>Предполагаемый диапазон</td></tr> <tr> <td>10Мбит/с</td><td>2000000</td><td>2000000-20000000</td></tr> <tr> <td>100Мбит/с</td><td>200000</td><td>200000-2000000</td></tr> <tr> <td>1ГМбит/с</td><td>20000</td><td>20000-200000</td></tr> </table> Для агрегированных портов метрики <table> <tr> <th>Тип</th><th>Допустимое число</th><th>Метрика</th></tr> <tr> <td>10 МБ</td><td>N</td><td>2 000 000</td></tr> <tr> <td>100 МБ</td><td>N</td><td>200 000</td></tr> <tr> <td>1 ГБ</td><td>N</td><td>20 000</td></tr> </table>		Для агрегированных портов метрики маршрутов, используемые по умолчанию, следующие:	Метрика маршрута к порту, используемая по умолчанию	Предполагаемый диапазон	10Мбит/с	2000000	2000000-20000000	100Мбит/с	200000	200000-2000000	1ГМбит/с	20000	20000-200000	Тип	Допустимое число	Метрика	10 МБ	N	2 000 000	100 МБ	N	200 000	1 ГБ	N	20 000
Для агрегированных портов метрики маршрутов, используемые по умолчанию, следующие:	Метрика маршрута к порту, используемая по умолчанию	Предполагаемый диапазон																								
10Мбит/с	2000000	2000000-20000000																								
100Мбит/с	200000	200000-2000000																								
1ГМбит/с	20000	20000-200000																								
Тип	Допустимое число	Метрика																								
10 МБ	N	2 000 000																								
100 МБ	N	200 000																								
1 ГБ	N	20 000																								
Режим	Режим конфигурации порта																									



Руководство по использованию	Установив метрику для порта, пользователи могут контролировать метрику маршрута от текущего порта до корневого моста для управления выбором порта и порта назначения для экземпляра связующего дерева
Пример	В порте 0/0/2 установить метрику MSTP 3000000. Switch(Config-If-Ethernet1/0/2)#spanning-tree cost 3000000

6.1.8. Использование партнерского порта (spanning-tree digest-snooping)

Команда	spanning-tree digest-snooping no spanning-tree digest-snooping
Параметр	-
Значение по умолчанию	Строка аутентификации партнерского порта не используется
Режим	Режим конфигурации порта
Руководство по использованию	В соответствии с протоколом MSTP, строка аутентификации региона автоматически генерируется алгоритмом MD5 с общедоступным ключом аутентификации, с ID экземпляра связующего дерева и VLAN ID. Некоторые производители не используют общедоступный ключ аутентификации, что является причиной несовместимости. После ввода команды порт сможет использовать строку аутентификации партнерского порта, что обеспечит совместимость с оборудованием этих производителей. Так как строка аутентификации зависит от ID экземпляра связующего дерева и VLAN ID, команда позволяет распознавать оборудования с отличающимися ID экземпляра связующего дерева и VLAN ID, как принадлежащие одному и тому же региону. Перед выполнением команды удостоверьтесь в правильности соответствий VLAN и экземпляра связующего дерева для всего оборудования. Если подключено более одного оборудования, эта команда должна быть выполнена на всех подключенных портах
Пример	Установить строку аутентификации партнерского порта. <pre>Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#spanning-tree digest-snooping Switch(Config-If-Ethernet1/0/2)#</pre>



6.1.9. Формат пакета STP (spanning-tree format)

Команда	spanning-tree format {standard privacy auto} no spanning-tree format	
Параметр	standard	формат пакета, соответствующий стандарту IEEE
	privacy	специальный формат пакета, совместимый с оборудованием CISCO
	auto	автоматическое определение формата пакета на основе принятых пакетов
Значение по умолчанию	Автоматическое определение формата пакета на основе принятых пакетов	
Режим	Режим конфигурации порта	
Руководство по использованию	Так как формат пакетов CISCO отличается от формата IEEE, многие компании поддерживают также и формат CISCO для совместимости. Наша компания поддерживает оба формата. Формат "standard" пакета разработан IEEE, формат "privacy" пакета поддерживает оборудование CISCO. Если Вы не имеете полной информации о том, какой формат пакетов используется на оборудовании других производителей, подключенном к коммутатору, настройка AUTO является более предпочтительной, при которой формат будет определен по принятым пакетам. По умолчанию установлено определение формата по принятым пакетам (AUTO) для лучшей совместимости с уже существующей продукцией и продукцией других компаний. Если установлен режим AUTO, то до первого принятого пакета будет использоваться специальный формат пакетов. Когда формат AUTO не выбран и принятый от партнеров пакет не согласуется с установленным форматом, для порта установлено состояние DISCARDING (отбрасывание пакетов), что приведет к отбрасыванию несогласующихся пакетов. Это предотвращает ситуацию, когда обе стороны считают, что у них находится корневой узел сети. Когда задан формат AUTO и к порту подключено несовместимое оборудование (например, оборудование подключено через концентратор (HUB), либо используется прозрачная передача BPDU по нескольким направлениям, в которых используется протокол MSTP), будут записаны счетчики изменения формата и порт будет выключен при достижении счетчиками некоторого порогового значения. Включить порт снова может только пользователь с правами администратора	
Пример	Установить для порта формат пакетов IEEE. <pre>Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#spanning-tree format standard Switch(Config-If-Ethernet1/0/2)#</pre>	



6.1.10. Время задержки передачи (spanning-tree forward-time)

Команда	spanning-tree forward-time <time> no spanning-tree forward-time	
Параметр	time	время задержки передачи в секундах. Допустимые значения – от 4 до 30
Значение по умолчанию	Установлено время задержки передачи 15 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Когда топология сети изменяется, состояние порта меняется с blocking (блокирующего) на состояние forwarding, в котором передача разрешена. Такая задержка называется задержкой передачи. Задержка передачи работает вместе с временем задержки "hello time" и максимальным сроком жизни "max age". Параметры должны отвечать следующим условиям, иначе MSTP может работать неправильно. $2 * (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$ $\text{Bridge\_Max\_Age} \geq 2 * (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})$	
Пример	В глобальном режиме конфигурации задать время задержки передачи MSTP 20 секунд. <pre>Switch(config)#spanning-tree forward-time 20</pre>	

6.1.11. Время приветствия STP (spanning-tree hello-time)

Команда	spanning-tree hello-time <time> no spanning-tree hello-time	
Параметр	time	время приветствия (hello time) в секундах. Допустимые значения – от 1 до 10
Значение по умолчанию	Значение Hello Time по умолчанию 2 секунды	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет установить интервала отправки bpdv коммутатором, команда «no spanning-tree hello-time» восстанавливает конфигурирование по умолчанию. Время hello time это интервал времени, по прошествии которого, коммутатор посылает сообщения BPDU. Время hello time связано с задержкой передачи (forward delay) и	



	максимальным сроком жизни (max age). Параметры должны отвечать следующим условиям, иначе MSTP будет работать неправильно. $2 * (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$ $\text{Bridge\_Max\_Age} \geq 2 * (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})$
Пример	Установить время hello time протокола MSTP 5 секунд в режиме глобальной конфигурации. <pre>Switch(config)#spanning-tree hello-time 5</pre>

6.1.12. Тип линии «точка-точка» (spanning-tree link-type p2p)

Команда	spanning-tree link-type p2p {auto force-true force-false} no spanning-tree link-type	
Параметр	auto	использовать автоматическое согласование
	force-true	принудительно устанавливает тип линии «точка-точка»
	force-false	принудительно устанавливает для линии тип «не точка-точка»
Значение по умолчанию	Установлен тип линии auto; MSTP определяет тип линии автоматически	
Режим	Режим конфигурации порта	
Руководство по использованию	При настройке типов соединений портов команда «no spanning-tree link-type» восстанавливает конфигурирование по умолчанию. Если порт работает в режиме полного дуплекса, MSTP устанавливает для линии порта типа "точка-точка"; Если порт работает в режиме полудуплекса, MSTP устанавливает для линии порта тип "разделяемая"	
Пример	Принудительно установить для порта 1/0/7-8 тип "точка-точка". <pre>Switch(config)#interface ethernet 1/0/7-8</pre> <pre>Switch(Config-Port-Range)#spanning-tree link-type p2p force-true</pre>	

6.1.13. Максимальный срок жизни (spanning-tree maxage)

Команда	spanning-tree maxage <time> no spanning-tree maxage	
Параметр	time	время максимального срока жизни в секундах. Допустимые значения – от 6 до 40



Значение по умолчанию	Установлен максимальный срок жизни 20 секунд
Режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для настройки максимального времени жизни bpdu, команда «no spanning-tree maxage» восстанавливает конфигурирование по умолчанию. Максимальный срок жизни связан с задержкой передачи (forward delay) и с задержкой hello time. Параметры должны отвечать следующим условиям, иначе MSTP будет работать неправильно. $2 * (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$ $\text{Bridge\_Max\_Age} \geq 2 * (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})$
Пример	В глобальном режиме конфигурации задать максимальный срок жизни адреса коммутатора 25 секунд. Switch(config)#spanning-tree maxage 25

6.1.14. Максимальное число хопов (spanning-tree max-hop)

Команда	spanning-tree max-hop <hop-count> no spanning-tree max-hop	
Параметр	hop-count	задает максимальное число хопов. Допустимые значения – от 1 до 40
Значение по умолчанию	Установлено максимальное число хопов, равное 20	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет задать максимальное число хопов BPDU в регионе MSTP, команда "no spanning-tree max-hop" восстанавливает значения, используемые по умолчанию. В протоколе MSTP для подсчета срока жизни BPDU используется максимальный срок жизни (max age). Кроме того, в протоколе MSTP для подсчета срока жизни BPDU используется и максимальное число хопов. Максимальное число хопов в сети уменьшается. Максимальное число хопов BPDU имеет максимальное значение при инициализации, выполняемой корневым мостом MSTI. После того, как сообщение BPDU принято, максимальное число хопов уменьшается на 1. После того, как порт примет сообщение BPDU при максимальном числе хопов равном 0, он отбрасывает это сообщение BPDU и объявляет себя портом назначения (designated port), чтобы посылать сообщения BPDU	
Пример	Установить максимальное число хопов 32. Switch(config)#spanning-tree max-hop 32	



6.1.15. Установка режима MSTP (spanning-tree mcheck)

Команда	spanning-tree mcheck
Параметр	-
Значение по умолчанию	Порт работает в режиме MSTP
Режим	Режим конфигурации порта
Руководство по использованию	Если сеть, которая подключена к текущему порту работает по протоколу IEEE 802.1D STP, порт автоматически преобразуется для работы в режиме STP. Команда используется для принудительной установки режима MSTP для порта. Однако, как только порт примет сообщение STP, он снова переключится в режим STP. Эта команда может использоваться только в том случае, когда коммутатор работает в режиме IEEE 802.1s MSTP. Если коммутатор работает в режиме IEEE 802.1D STP, то применение этой команды некорректно
Пример	Принудительно установить для порта 1/0/2 режим работы MSTP. Switch(Config-If-Ethernet1/0/2)#spanning-tree mcheck

6.1.16. Режим STP (spanning-tree mode)

Команда	spanning-tree mode {mstp stp rstp} no spanning-tree mode	
Параметр	mstp	устанавливает в коммутаторе режим IEEE 802.1s MSTP
	stp	устанавливает в коммутаторе режим IEEE 802.1D STP
	rstp	устанавливает в коммутаторе режим IEEE 802.1D RSTP
Значение по умолчанию	Коммутатор работает в режиме MSTP	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет установить на коммутаторе режим spanning-tree, а команда "no spanning-tree mode" восстанавливает настройки, используемые по умолчанию. Когда коммутатор работает в режиме IEEE 802.1D STP, он посылает сообщения BPDU стандарта IEEE 802.1D и TCN. Все BPDU протокола MSTP отбрасываются	



Пример	Установить на коммутаторе режим STP. Switch(config)#spanning-tree mode stp

6.1.17. Режим конфигурации MSTP (spanning-tree mst configuration)

Команда	spanning-tree mst configuration no spanning-tree mst configuration
Параметр	-
Значение по умолчанию	-
Режим	Режим глобальной конфигурации
Руководство по использованию	Независимо от того, находится ли коммутатор в режиме настройки регионов MSTP или в другом режиме, пользователи могут войти в режим конфигурации MSTP, настроить атрибуты и сохранить эти настройки. Когда коммутатор работает в режиме MSTP, система генерирует идентификатор конфигурирования MST, соответствующий конфигурирования MSTP. Только коммутаторы с одинаковыми идентификаторами конфигурирования MST считаются коммутаторами одного и того же региона MSTP
Пример	Войти в режим настройки регионов MSTP. Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)#

6.1.18. Метрика MSTP (spanning-tree mst cost)

Команда	spanning-tree mst <instance-id> cost <cost> no spanning-tree mst <instance-id> cost
Параметр	instance-id идентификатор экземпляра связующего дерева. Допустимый диапазон 0-64. cost метрика маршрута, различные форматы метрики имеют разные диапазоны. Для стандартного режима dot1t допустимый диапазон составляет 1-200 000 000, а для dot1d - 1-65535.
Значение по умолчанию	Метрика маршрута к порту соответствует пропускной способности порта.



Тип порта	Метрика маршрута к порту, используемая по умолчанию	Предполагаемый диапазон
10 Мбит/с	2000000	2000000-20000000
100 Мбит/с	200000	200000-2000000
1 ГМбит/с	20000	20000-200000
Для агрегированных портов, метрики маршрутов, используемые по умолчанию, следующие:		
Тип порта	Допустимое число агрегированных портов	Метрика маршрута, используемая по умолчанию
10 Мбит/с	N	2000000/N
100 Мбит/с	N	200000/N
1 ГМбит/с	N	20000/N
Скорость порта	Тип порта	Метка порта
		802.1D-2008 802.1T
0		65535 200000000
10Мбит/с	Полудуплекс	100 2 000 000
	Полный дуплекс	99 1,999,999
	агрегированный	95 1 000 000
	канал с 2 портами	95 666,666
	агрегированный	95 500000
	канал с 3 портами	
	агрегированный	
	канал с 4 портами	
100Мбит/с	Полудуплекс	19 200,000
	Полный дуплекс	18 199,999
	агрегированный	15 100 000
	канал	15 66,666
	с 2 портами	15 50,000
	агрегированный	
	канал	
	с 3 портами	
	агрегированный	
	канал	
	с 4 портами	



	1000Mbps	Полный дуплекс	4	20,000
		агрегированный канал	3	10 000
		с 2 портами	3	6,666
		агрегированный канал	3	5 000
		с 3 портами		
		агрегированный канал		
		с 4 портами		

6.1.19. Формат метрики MSTP (spanning-tree cost-format)

Команда	spanning-tree cost-format {dot1d dot1t}
	-
Значение по умолчанию	Стоимость пути задана в формате dot1t
Режим	Режима глобальной конфигурации
Руководство по использованию	Существует два формата метрики: dot1d, обозначенный в IEEE802.1d-2008, и dot1t, обозначенный в IEEE802.1t, но они имеют разные диапазоны стоимости пути: от 1 до 65535 для dot1d и от 1 до 200,000,000 для dot1t
Пример	Задать формат стоимости в глобальном режиме. Switch(config)#spanning-tree cost-format dot1d

6.1.20. Защита от закольцовывания MSTP (spanning-tree mst loopguard)

Команда	spanning-tree [mst <instance-id>] loopguard no spanning-tree [mst <instance-id>] loopguard	
Параметр	instance-id	идентификатор экземпляра MSTP
Значение по умолчанию	Функция выключена	
Режим	Режим конфигурации порта	



Руководство по использованию	Эта команда предотвращает смену корневого или заменяемого порта на порт назначения, если односторонняя связь недействительна. По истечении времени таймера приема настроенный порт с loopguard переходит в состояние блокировки
Пример	Задать для порта 1/0/2 режим loopguard для экземпляра 0. <pre>Switch(Config)#interface ethernet 1/0/2</pre> Switch(Config-Ethernet-1/0/2)#spanning-tree mst 0 loopguard <pre>Switch(Config-Ethernet-1/0/2)#</pre>

6.1.21. Приоритет порта (spanning-tree mst port-priority)

Команда	spanning-tree mst <instance-id> port-priority <port-priority> no spanning-tree mst <instance-id> port-priority	
Параметр	instance-id	идентификатор экземпляра связующего дерева. Диапазон значений от 0 до 64
	port-priority	задает приоритет порта. Допустимые значения — от 0 до 240. Значение должно быть кратно 16, например, 0, 16, 32...240
Значение по умолчанию	Установлен приоритет порта 128	
Режим	Режим конфигурации порта	
Руководство по использованию	Задавая приоритет порта, пользователи могут управлять ID порта экземпляра связующего дерева, чтобы управлять корневым портом и портом назначения этого экземпляра. Чем меньше значение приоритета порта, тем выше его приоритет	
Пример	Установить приоритет порта 32 на порту 0/0/2 экземпляра связующего дерева 1. <pre>Switch(config)#interface ethernet 1/0/2</pre> <pre>Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 1 port-priority 32</pre>	

6.1.22. Приоритет коммутатора MSTP (spanning-tree mst priority)

Команда	spanning-tree mst <instance-id> priority <bridge-priority> no spanning-tree mst <instance-id> priority	
Параметр	instance-id	идентификатор экземпляра связующего дерева. Допустимый диапазон значений от 0 до 64



	port-priority	приоритет коммутатора. Допустимый диапазон значений от 0 до 61440. Значение должно быть кратно 4096, например, 0, 4096, 8192...61440
Значение по умолчанию	Установлен приоритет порта 32768	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Задавая приоритет коммутатора, пользователи могут изменять ID коммутатора для указанного экземпляра связующего дерева. ID коммутатора может влиять на выбор корневого моста и порта назначения для указанного экземпляра связующего дерева	
Пример	Установить приоритет 4096 для экземпляра связующего дерева 2. Switch(config)#spanning-tree mst 2 priority 4096	

6.1.23. Защита коммутатора (spanning-tree mst rootguard)

Команда	spanning-tree [mst <instance-id>] rootguard no spanning-tree [mst <instance-id>] rootguard	
Параметр	instance-id	идентификатор экземпляра MSTP
Значение по умолчанию	Функция rootguard не включена	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда используется в режиме настройки порта. Если для порта указана функция rootguard, ему запрещено быть корневым портом дерева MSTP. Если от порта, для которого включена функция rootguard, принят пакет BPDU более высокого уровня иерархии, протокол MSTP не вычисляет связующее дерево, а просто задает состояние порта root_inconsistent (порт не может быть корневым) и блокирует порт. Если от заблокированного порта с функцией rootguard не принимаются пакеты BPDU более высокого уровня, состояние порта будет восстановлено на передачу и ему будет разрешена передача. Функция rootguard может использоваться для обслуживания относительно стабильных топологий связующего дерева при добавлении в сеть нового коммутатора	
Пример	Включить функцию rootguard для порта 1/0/2 экземпляра связующего дерева 0. Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 0 rootguard	



	Switch(Config-If-Ethernet1/0/2)#

6.1.24. Режим граничного порта (spanning-tree portfast)

Команда	spanning-tree portfast [bpdufilter bpduguard] [recovery <30-3600>] no spanning-tree portfast	
Параметр	bpdufilter	устанавливает в порту режим граничного порта для фильтрации пакетов BPDU
	bpduguard	устанавливает защиту BPDU для граничного порта
	recovery	задает автоматическое восстановление граничного порта после применения операции отключения при bpduguard
	<30-3600>	время восстановления. По умолчанию восстановление не выполняется
Значение по умолчанию	После включения протокола MSTP все порты не являются граничными портами	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда объявляет текущий порт граничным портом, выполняющим фильтрацию пакетов BPDU. Режим защиты BPDU может быть указан в команде, либо использоваться по умолчанию. Команда “no spanning-tree portfast” относит указанный порт к неграничному порту. Когда порт объявлен граничным портом, его состояние преобразуется из discarding (отбрасывание пакетов BPDU) в состояние, в котором разрешена передача (forwarding), при этом задержка передачи (forward delay) отсутствует. Как только граничный порт принимает пакет BPDU, он вновь становится неграничным портом	
Пример	Установить режим защиты BPDU с временем восстановления 60 секунд. <pre>Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#spanning-tree portfast bpduguard recovery 60 Switch(Config-If-Ethernet1/0/2)#</pre>	



6.1.25. Приоритет порта (spanning-tree port-priority)

Команда	spanning-tree port-priority <port-priority> no spanning-tree port-priority	
Параметр	port-priority	задает приоритет порта. Допустимые значения — от 0 до 240. Значение должно быть кратно 16, например, 0, 16, 32, 48...240
Значение по умолчанию	Установлен приоритет коммутатора 32768	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда устанавливает приоритет для назначенного порта. Чем меньше значение приоритета порта, тем выше его приоритет	
Пример	Установить для порта 1 приоритет 4096. Switch(Config-If-Ethernet1/0/1)#spanning-tree port-priority 4096	

6.1.26. Приоритет коммутатора (spanning-tree priority)

Команда	spanning-tree priority <bridge-priority> no spanning-tree priority	
Параметр	bridge-priority	приоритет мостового коммутатора. Его значение должно быть кратно 4096 между 0 и 61440, например, 0, 4096, 8192... 61440
Значение по умолчанию	Приоритет по умолчанию 32768	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Идентификатор моста может быть изменен путем изменения приоритета коммутатора. Приоритет коммутатора может влиять на выбор корневого моста и заданных портов. Чем меньше значение приоритета моста коммутатора, тем выше его приоритет	
Пример	Установить приоритет коммутатора равным 4096. Switch(config)#spanning-tree priority 4096	



6.1.27. Защита корневого порта (spanning-tree rootguard)

Команда	spanning-tree rootguard no spanning-tree rootguard
Параметр	-
Значение по умолчанию	Порт не является корневым
Режим	Режим конфигурации порта
Руководство по использованию	Команда используется в режиме настройки портов, если для порта включена функция rootguard, ему запрещено быть корневым портом дерева MSTP. Если от порта, для которого включена функция rootguard, принят пакет BPDU более высокого уровня иерархии, протокол MSTP не вычисляет связующее дерево, а просто задает состояние порта root_inconsistent (порт не может быть корневым) и блокирует порт. Если от заблокированного порта с функцией rootguard не принимаются пакеты BPDU более высокого уровня, состояние порта будет восстановлено на передачу и ему будет разрешена передача. Функция rootguard может использоваться для обслуживания относительно стабильных топологий связующего дерева при добавлении в сеть нового коммутатора
Пример	Включить для порта 1 режим корневого порта. Switch(Config-If-Ethernet1/0/1)#spanning-tree rootguard

6.1.28. Режим FLUSH STP (режим глобальной конфигурации) (spanning-tree tcflush (Global mode))

Команда	spanning-tree tcflush {enable disable protect} no spanning-tree tcflush	
Параметр	enable	связующее дерево строится сразу, как только изменяется топология
	disable	при изменении топологии связующее дерево не строится
	protect	связующее дерево строится через каждые 10 секунд
Значение по умолчанию	Включено	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда включает режим flush, в котором связующее дерево строится сразу, как только изменяется топология. Команда "no spanning-tree tcflush" восстанавливает значения по умолчанию. В соответствии с протоколом MSTP, когда топология изменяется, порт посылает сообщение об изменении, которое очищает таблицу MAC/ARP (FLUSH). Фактически, для некоторых сетей нет необходимости выполнять операцию FLUSH при каждом изменении топологии. Однако для предотвращения атак на сеть администратор сети с помощью этой команды может настроить режим FLUSH
Пример	Настроить режим "flush spanning-tree", чтобы при изменении топологии не выполнялось flush на tc. <pre>Switch(config)#spanning-tree tcflush disable Switch(config)#</pre>

6.1.29. Режим FLUSH STP (режим конфигурации порта) (spanning-tree tcflush (Port mode))

Команда	spanning-tree tcflush {enable disable protect} no spanning-tree tcflush	
Параметр	enable	связующее дерево строится сразу, как только изменяется топология
	disable	при изменении топологии связующее дерево не строится
	protect	связующее дерево строится через каждые десять секунд
Значение по умолчанию	Режим включения по умолчанию	
Режим	Режим конфигурации порта	
Руководство по использованию	Позволяет включить режим flush, в котором связующее дерево строится сразу, как только изменяется топология. Команда "no spanning-tree tcflush" восстанавливает значения по умолчанию. В соответствии с протоколом MSTP, когда топология изменяется, порт посылает сообщение об изменении, которое очищает таблицу MAC/ARP (FLUSH). Фактически, для некоторых сетей нет необходимости выполнять операцию FLUSH при каждом изменении топологии. Однако для предотвращения атак на сеть администратор сети с помощью этой команды может настроить режим FLUSH	
Пример	Настроить режим flush spanning-tree, чтобы при изменении топологии не выполнялось flush на tc. <pre>Switch(config)#spanning-tree tcflush disable</pre>	



6.1.30. Максимальное число отправки (spanning-tree transmit-hold-count)

Команда	spanning-tree transmit-hold-count < tx-hold-count-value> no spanning-tree transmit-hold-count	
Параметр	tx-hold-count-value	в диапазоне от 1 до 20, по умолчанию значение 10
Значение по умолчанию	10	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда задает максимальное число для отправки BPDU в течение интервала Hello Time, чтобы контролировать поток BPDU. Переменная применяется для всего моста MST	
Пример	Установить максимальное значение параметра "transmit-hold-count" равным 20. Switch(config)#spanning-tree transmit-hold-count 20	

6.1.31. Вывод данных текущего региона MSTP (show mst-pending)

Команда	show mst-pending	
Параметр	-	
Значение по умолчанию	-	
Режим	Привилегированный режим	
Руководство по использованию	В режиме настройки регионов MSTP позволяет вывести на экран настройки текущего региона MSTP: имя MSTP, номер версии, VLAN и привязки к экземплярам связующего дерева	
Пример	Вывести на экран настройки для текущего региона MSTP. Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)#show mst-pending Name switch Revision 0 Instance Vlans Mapped ----- 00 1-29, 31-39, 41-4093	



	03 30 04 40 05 4094 ----- Switch(Config-Mstp-Region)#

6.1.32. Вывод данных MSTP (show spanning-tree)

Команда	show spanning-tree [mst [<instance-id>]] [interface <interface-list>] [detail]	
Параметр	instance-id	список интерфейсов
	interface-list	идентификатор экземпляра связующего дерева. Диапазон значений от 0 до 64
	detail	вывод подробной информации о связующем дереве
Значение по умолчанию	-	
Режим	Привилегированный режим и режим конфигурации	
Руководство по использованию	С помощью этой команды на экран может быть выведена информация MSTP только для экземпляров связующего дерева текущего моста	
Пример	Вывести на экран мост MSTP. <pre>Switch#sh spanning-tree ***** Process 0 ***** -- MSTP Bridge Config Info -- Standard : IEEE 802.1s Bridge MAC : 00: 1f: ce: 10: b0: 1b Bridge Times : Max Age 20, Hello Time 2, Forward Delay 15 Force Version: 3 ##### Instance 0 ##### Self Bridge Id : 32768.00: 1f: ce: 10: b0: 1b Root Id : this switch Ext.RootPathCost : 0 Region Root Id : this switch Int.RootPathCost: 0</pre>	



	Root Port ID : 0 Current port list in Instance 0: Ethernet1/0/12 Ethernet1/0/20 (Total 2)

PortName	ID	Ext RPC	Int RPC	Stat e	Role	DsgBridge	DsgPort
Ethernet1/0/12	128.012	0	0	FW D	DSG N	32768.001fce10b01b	128.012
Ethernet1/0/20	128.020	0	0	FW D	DSG N	32768.001fce10b01b	128.020

Информация, отображаемая на экране	Описание
Информация о MSTP мосте	
Standard	Версия STP
Bridge MAC	MAC-адрес моста
Bridge Times	Максимальный срок жизни адреса, время hello time и задержка передачи моста
Force Version	Версия STP
Информация для экземпляра связующего дерева 0	
Self Bridge Id	Приоритет и MAC-адрес текущего моста для текущего экземпляра связующего дерева
Root Id	Приоритет и MAC-адрес корневого моста для текущего экземпляра связующего дерева
Ext.RootPathCost	Полная метрика для маршрута от текущего коммутатора до корневого узла всей сети
Int.RootPathCost	Метрика маршрута от текущего коммутатора до корневого узла текущего экземпляра связующего дерева
Root Port ID	Корневой порт текущего экземпляра связующего дерева на текущем мосту



Информация, отображаемая на экране	Описание
Список портов текущего экземпляра связующего дерева 0	
PortName	имя порта
ID	Приоритет порта и номер порта
ExtRPC	Метрика порта относительно корневого узла всей сети
IntRPC	Метрика маршрута от текущего порта до корневого узла текущего экземпляра связующего дерева
State Role	Состояние порта текущего экземпляра связующего дерева
DsgBridge	Восходящий коммутатор назначения для текущего порта в текущем экземпляре связующего дерева
DsgPort	Восходящий порт назначения для текущего порта в текущем экземпляре связующего дерева

6.1.33. Вывод параметров MSTP (show spanning-tree mst config)

Команда	show spanning-tree mst config
Параметр	-
Значение по умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	В привилегированном режиме эта команда позволяет вывести на экран параметры MSTP, например, имя MSTP, номер версии, VLAN и привязки к экземплярам связующего дерева



Пример	Вывести на экран настройки протокола MSTP. Switch#show spanning-tree mst config Название Revision 0 Instance Vlans Mapped ----- 00 1-4094

6.1.34. Процесс MSTP (spanning-tree process)

Команда	spanning-tree process <process-id> no spanning-tree process <process-id>	
Параметр	process-id	диапазон от 1 до 31
Значение по умолчанию	-	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда создает новый процесс MSTP. На одном устройстве может быть настроено несколько процессов MSTP, и каждый процесс является автономным. Процесс 0 существует только по умолчанию	
Пример	Создать новый процесс MSTP 1. Switch(config)#spanning-tree process 1	

6.1.35. MSTP-процесс 0 (spanning-tree tc-notify process0)

Команда	spanning-tree tc-notify process0 no spanning-tree tc-notify process0
Параметр	-
Значение по умолчанию	-
Режим	Режим процесса mstp
Руководство по использованию	Устройство получает пакет tc при изменении MSTP-процесса N, в то же время процесс N сообщает tc экземпляру MSTP-процесса 0 на общем канале. Это позволяет процессу 0 обновить записи в таблице, чтобы трафик не прерывался



Пример	Настроить уведомление TC процесса 1 для процесса 0. Switch(Config-Mstp-Process-1)#spanning-tree tc-notify process0

6.1.36. Процесс присоединения порта (spanning-tree binding-process)

Команда	spanning-tree binding-process <process-id> no spanning-tree binding-process <process-id>	
Параметр	process-id	диапазон от 1 до 31
Значение по умолчанию	Все порты относятся к процессу 0	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда устанавливает присоединение порта к указанному MSTP-процессу N. Порт переходит из процесса 0 в процесс N. Эта команда является взаимоисключающей с командой конфигурирования общего порта (link-share)	
Пример	Добавить Ethernet1/0/2 в процесс 1. Switch(Config-If-Ethernet1/0/2)#spanning-tree binding-process 1	

6.1.37. Присоединение общего порта (spanning-tree binding-process link-share)

Команда	spanning-tree binding-process < process-id > link-share no spanning-tree binding-process < process-id > link-share	
Параметр	process-id	диапазон от 1 до 31
Значение по умолчанию	Порт находится только в вычислении MSTP-процесса 0	
Режим	Режим конфигурации порта	
Руководство по использованию	Настроенные командой порты являются общими портами для процесса N. Настроенные порты могут находиться в вычислениях MSTP для нескольких процессов, кроме процесса 0, но статус порта может быть установлен только процессом 0. Эта команда может быть настроена несколько раз	
Пример	Настроить Ethernet1/0/2 как общий порт для процессов 1 и 0. Switch(Config-If-Ethernet1/0/2)#spanning-tree binding-process 1 link-share	



6.2. Команды настройки протокола ERPS

6.2.1. Настройка отправки уведомлений ERPS (ethernet tcn-propagation erps to {erps | stp})

Команда	ethernet tcn-propagation erps to {erps stp} no ethernet tcn-propagation erps to	
Параметр	erps	изменение топологии отправляет пакеты событий R-APS, чтобы уведомить кольцо соединения об этом устройстве
	stp	изменение топологии отправляет пакеты stp для уведомления топологии stp, подключенной к этому устройству
Значение по умолчанию	Изменение топологии кольца ERPS происходит только в этом кольце без отправки пакетов уведомлений	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда изменяет метод уведомления об изменении топологии, поддерживаемый этим устройством, на указанный метод. Экземпляр кольца ERPS отправляет пакеты уведомления, когда обнаруживает изменение топологии. Если настроен метод erps, он отправляет пакеты событий R-APS другим кольцам ERPS; если настроен метод stp, он отправляет пакеты stp	
Пример	Настроить отправку уведомления о событии R-APS в кольцо межсоединений после изменения топологии. <pre>Switch(config)#ethernet tcn-propagation erps to erps</pre> Настроить отправку уведомления STP на кольцо межсоединения после изменения топологии. <pre>Switch(config)#ethernet tcn-propagation erps to stp</pre> Удалить метод уведомления об изменении топологии. <pre>Switch(config)#no ethernet tcn-propagation erps to</pre>	



6.2.2. Имя кольца ERPS (erps-ring <ring-name>)

Команда	erps-ring < ring-name > no erps-ring < ring-name >	
Параметр	ring-name	созданное имя кольца ERPS. Максимальное количество символов 64, включающих буквы, цифры и подчеркивания. Первый и последний символы не могут быть подчеркиваниями
Значение по умолчанию	Кольцо ERPS не сконфигурировано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда создает кольцо ERPS и переходит в режим настройки кольца ERPS. Если кольцо ERPS уже существует, позволяет войти в режим настройки кольца ERPS. "no" перед началом команды удаляет кольцо ERPS	
Пример	Создать кольцо ERPS ring1 Switch(config)#erps-ring 1 Switch(config-erps-ring)# Удалить кольцо ERPS ring1 Switch(config)#no erps-ring 1	

6.2.3. Версия (version {v1 | v2})

Команда	version {v1 v2} no version	
Параметр	v1	для поддержки версии 1, выпущенной в 2008-06 и изменений (2009-04)
	v2	для поддержки версии 2, выпущенной в 2010-03 и изменений (2010-06)
Значение по умолчанию	V2	
Режим	Режим конфигурации кольца ERPS	



Руководство по использованию	Эта команда используется для настройки поддерживаемой версии кольца ERPS, в противном случае команда возвращается к состоянию по умолчанию v2. Если в кольце ERPS настроена поддержка версии v1, это кольцо не будет поддерживать многоэкземплядность. Экземпляр кольца ERPS не поддерживает команды управления, такие как MS, FS и т.д. и нереверсивное переключение не действует. Поддерживается только реверсивное переключение. Если кольцо ERPS настроено на поддержку v1, экземпляр этого кольца будет обрабатывать пакеты ERPS в соответствии с форматом v1. Упаковывать пакеты R-APS и разбирать поля в соответствии с форматом v1. Поля, определенные в формате v2, обрабатываться не будут
Пример	Настроить в ring1 кольца ERPS поддержку v1 <pre>Switch(config-erps-ring)#version v1</pre> Удалить поддержку v1 в ring1 кольца ERPS <pre>Switch(config)#erps-ring ring1</pre> <pre>Switch(config-erps-ring)#no version</pre>

6.2.4. Подкольцо открытого типа (open-ring)

Команда	open-ring no open-ring
Параметр	-
Значение по умолчанию	Конфигурирование по умолчанию - подкольцо ERPS
Режим	Режим конфигурации кольца ERPS
Руководство по использованию	Если на кольце был настроен экземпляр кольца ERPS, появится сообщение " Can't config open-ring on ERPS ring which has ERPS instance, please delete ERPS instance firstly! (Невозможно настроить открытое кольцо на кольце ERPS, которое имеет экземпляр ERPS, сначала удалите экземпляр ERPS) " В ином случае переходите к следующему шагу. Настройте этот тип кольца ERPS как подкольцо
Пример	Настроить кольцо ERPS ring1 как подкольцо открытого типа. <pre>Switch(config)#erps-ring 1</pre> <pre>Switch(config-erps-ring)#open-ring</pre> Удалить настройку типа подкольца как открытое. <pre>Switch(config)#erps-ring 1</pre>



	Switch(config-erps-ring)#no open-ring

6.2.5. Виртуальный канал R-APS (raps-virtual-channel {with | without})

Команда	raps-virtual-channel {with without}	
Параметр	with	виртуальный канал R-APS существует в этом кольце ERPS
	without	виртуальный канал R-APS отсутствует в этом кольце ERPS
Значение по умолчанию	Виртуального канала R-APS в этом кольце ERPS нет	
Режим	Режим конфигурации кольца ERPS	
Руководство по использованию	Устанавливает наличие виртуального канала R-APS в кольце ERPS в соответствии с конфигурацией. Ввод: Успешно или ошибка Если в кольце ERPS нет виртуального канала R-APS, то каналы R-APS всех экземпляров в кольце ERPS будут постоянно разблокированы и будут заблокированы только каналы данных; в противном случае будут заблокированы и каналы R-APS, и каналы данных	
Пример	Настроить наличие виртуального канала R-APS в подкольце ERPS ring1. <pre>Switch(config)#erps-ring ring1 Switch(config-erps-ring)#raps-virtual-channel with</pre>	

6.2.6. Порт 0 кольца ERPS (erps-ring <ring-name> port0 [port1-none])

Команда	erps-ring <ring-name> port0 [port1] no erps-ring <ring-name> port0	
Параметр	ring-name	имя кольца ERPS, максимальная строка — 64, состоит из букв, цифр и подчеркиваний; первый и последний символы не могут быть подчеркиваниями
	port1-none	на этом кольцевом узле ERPS есть только port0, port1 нет, и он является межсетевым узлом
Значение по умолчанию	port0 на кольце ERPS не сконфигурирован	
Режим	Режим конфигурации порта	



Руководство по использованию	Эта команда используется для настройки порта в качестве порта указанного кольца ERPS. Если это кольцо ERPS не является кольцом открытого типа, порт1-none не может быть сконфигурирован. Проверьте, завершена ли конфигурирование кольца ERPS; если завершена, проверьте, завершена ли конфигурирование экземпляра ERPS; если завершена, запустите экземпляр как активный и выполните протокол
Пример	Настроить e 1/0/1 как port0 кольца ERPS ring1 <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#erps-ring ring1 port0</pre> Удалить настройку e 1/0/1 в качестве port0 кольца ERPS ring1 <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#no erps-ring ring1 port0</pre>

6.2.7. Порт 1 кольца ERPS (erps-ring <ring-name> port1)

Команда	erps-ring <ring-name> port1 no erps-ring <ring-name> port1	
Параметр	ring-name	имя кольца ERPS, максимальная строка — 64, состоит из букв, цифр и подчеркиваний; первый и последний символы не могут быть подчеркиваниями
Значение по умолчанию	Не конфигурируйте port1 на кольце ERPS	
Режим	Режим конфигурации порта	
Руководство по использованию	Эта команда используется для настройки порта в качестве порта в указанного кольца ERPS. Проверьте, завершена ли конфигурирование кольца ERPS; если завершена, убедитесь, что завершена конфигурирование экземпляра ERPS; если завершена, запустите экземпляр как активный и выполните протокол	
Пример	Настроить e 1/0/1 в качестве port1 кольца ERPS ring1 <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#erps-ring ring1 port1</pre> Удалить настройку e 1/0/1 в качестве port1 кольца ERPS ring1 <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#no erps-ring ring1 port1</pre>	



6.2.8. Обнаружение неисправности (failure-detect {cc | physical-link-or-cc} domain <domain-name> service {< ma-name > | number < ma-num > | pvlan < vlan-id >} mep <mep-id> rmep<rmep-id>)

Команда	<pre>{port0 port1} failure-detect {cc physical-link-or-cc} domain <domain-name> service {< ma-name > number < ma-num > pvlan < vlan-id >} mep <mep-id> rmep<rmep-id> no {port0 port1} failure-detect</pre>	
Параметр	{port0 port1}	выбор параметра. Port0 означает тип обнаружения падения канала в port0. Port1 означает тип обнаружения падения канала в port1
	{cc physical-link-or-cc}	выбор параметра. cc означает, что обнаружение порта кольца ERPS выполняется отправкой отчетов о падении cc. physical-link-or-cc означает, что обнаружение порта кольца ERPS выполняется как с помощью падения физического порта, так и с помощью отправки отчетов cc
	<domain-name>	имя домена cfm для обнаружения порта кольца ERPS
	< ma-name >	имя службы, к которой принадлежит cfm, для обнаружения порта кольца ERPS
	<mep-id>	локальный идентификатор mep, который отслеживает cfm, для обнаружения порта кольца ERPS
	<rmep-id>	удаленный идентификатор mep, который отслеживает cfm, для обнаружения порта кольца ERPS
Значение по умолчанию	Порт кольца ERPS по умолчанию обнаруживает только неисправность физического канала	
Режим	Режим конфигурации кольца ERPS	
Руководство по использованию	Команда позволяет указать тип обнаружения неисправностей для порта кольца ERPS. Если обнаружение имеет тип cc, необходимо указать домен обслуживания, набор обслуживания, к которым принадлежит cc и канал мониторинга (это зависит от (mep-id, rmep-id)). Эта конфигурация предполагает, что соответствующий порт был добавлен в кольцо ERPS. "no" перед началом команды удаляет тип обнаружения неисправностей для порта кольца ERPS. Позволяет указать тип обнаружения неисправностей для порта кольца ERPS в качестве назначенного. Если указан тип cc, сохраняется	



	настроенная информация md, ma, mer и rmer для сравнения после получения уведомления о сбое cfm
Пример	Задать тип обнаружения ERPS ring1 port0 как cc. <pre>Switch(config)#erps-ring 1 Switch(config-erps-ring)#port0 failure-defect cc domain domain1 service servive1 mer 1 rmer 2</pre> Удалить настройку. <pre>Switch(config)#erps-ring 1 Switch(config-erps-ring)#no port0 failure-defect</pre>

6.2.9. Экземпляр кольца ERPS (erps-instance <instance-id>)

Команда	erps-instance <instance-id> no erps-instance <instance-id>	
Параметр	instance-id	идентификатор кольца ERPS, диапазон от 1 до 48
Значение по умолчанию	Экземпляр кольца ERPS не сконфигурирован	
Режим	Режим конфигурации кольца ERPS	
Руководство по использованию	Команда позволяет создать экземпляр кольца ERPS и войти в режим настройки экземпляра кольца ERPS. Если кольцо ERPS поддерживает версию 1, при настройке нескольких экземпляров ERPS появляется сообщение "Doesn't support multiple ERPS instance capability on the ring running version 1! (Не поддерживает возможность использования нескольких экземпляров ERPS на кольце с поддержкой версии 1!)"	
Пример	Настроить экземпляр 1 кольца ERPS на кольце ERPS ring1. <pre>Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#</pre> Удалить экземпляр 1 кольца ERPS на кольце ERPS ring1. <pre>Switch(config)#erps-ring 1 Switch(config-erps-ring)#no erps-instance 1</pre>	



6.2.10. Описание (description)

Команда	description <instance-name> no description <instance-name>	
Параметр	instance-name	имя экземпляра ERPS, максимальная строка - 64, состоит из букв, цифр и подчеркиваний; первый и последний символы не могут быть подчеркиваниями. no в начале команды удаляет имя экземпляра ERPS
Значение по умолчанию	Имя экземпляра ERPS по умолчанию не задано	
Режим	Режим конфигурации экземпляра ERPS	
Руководство по использованию	Команда конфигурирует строку описания для экземпляра ERPS	
Пример	Задать имя экземпляра1 ERPS на ring1 как instance1. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)# description instance1 Delete this name of instance1. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)# no description	

6.2.11. Идентификатор кольца ERPS (ring-id <ring-id>)

Команда	ring-id <ring-id> no ring-id <ring-id>	
Параметр	ring-id	идентификатор кольца ERPS, диапазон от 1 до 64
Значение по умолчанию	По умолчанию задан MAC-адрес 01-19-A7-00-00-01	
Режим	Режим конфигурации экземпляра ERPS	
Руководство по использованию	Команда позволяет настроить последний байт MAC-адреса назначения пакетов R-APS, отправляемых узлом кольца ERPS, на передачу идентификатора кольца. Если кольцо ERPS поддерживает v1, ring-id может быть сконфигурирован только как 1. Команда с no в своем начале не будет передавать ring-id, это означает, что MAC-адрес будет 01-19-A7-00-00-01	



Пример	Настроить последний байт MAC-адреса назначения пакетов R-APS, отправляемых экземпляром2 кольца ERPS ring1, так, чтобы он содержал ring-id 2. <pre>Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 2 Switch(config-erps-ring-inst-2)#ring-id 2</pre> Удалить из последнего байта MAC-адреса назначения пакетов R-APS, отправляемых экземпляром2 кольца ERPS ring1 ring-id, это означает, что MAC-адрес назначения будет 01-19-A7-00-00-01. <pre>Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 2 Switch(config-erps-ring-inst-2)#no ring-id</pre>

6.2.12. Роли RPL (rpl {port0 | port1} {owner | neighbour})

Команда	rpl {port0 port1} {owner neighbour} no rpl {port0 port1}	
Параметр	{port0 port1}	порты-члены кольца ERPS
	{owner neighbour}	Owner: узел защиты кольца (RPL owner) Neighbour: узел защиты кольца (RPL owner)
Значение по умолчанию	Отсутствует. Обычный тип узла передачи данных	
Режим	Режим конфигурации экземпляра ERPS	
Руководство по использованию	Команда позволяет настроить порты-члены экземпляра кольца ERPS в качестве RPL owner или RPL neighbour (с другой стороны канала), роли узлов RPL разных экземпляров одного кольца ERPS не могут быть заданы для одного порта-члена. "no" перед началом команды конфигурирует порт-член кольца ERPS в качестве обычного порта-члена передачи	
Пример	Настроить port0 кольца ERPS ring1 instance1 в качестве узла RPL owner. <pre>Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)# rpl port0 owner</pre>	



6.2.13. Реверсивный режим (non-revertive)

Команда	non-revertive no non-revertive
Параметр	-
Значение по умолчанию	Экземпляр кольца ERPS по умолчанию поддерживает реверсивный режим
Режим	Режим конфигурации экземпляра ERPS
Руководство по использованию	Выполняется конфигурирование экземпляра кольца ERPS как нереверсивного. Если это кольцо ERPS поддерживает v1, эта команда равна нулю и не может быть настроена. no в начале команды задает экземпляр кольца ERPS как реверсивный. Если это кольцо ERPS поддерживает v1, эта команда будет пустой. Эта команда может быть задана только на узле подкольца RPL owner
Пример	Настроить кольцо ERPS ring1 экземпляра1 для поддержки нереверсивного режима. Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#non-revertive

6.2.14. Таймер защиты (guard-timer <guard-times>)

Команда	guard-timer <guard-times> no guard-timer	
Параметр	guard-times	интервал — 10 мс, диапазон — от 10 мс до 2 с
Значение по умолчанию	500 мс	
Режим	Режим конфигурации экземпляра ERPS	
Руководство по использованию	Команда устанавливает таймер защиты, который используется узлом Ethernet для предотвращения обработки ошибок и замыкания цикла в соответствии с устаревшими пакетами R-APS. В начальный момент времени таймера все полученные R-APS-пакеты (кроме пакетов R-APS с Request/State=«1110») будут отброшены. "no" перед началом команды устанавливает значение таймера защиты по умолчанию	



Пример	Установить таймер защиты экземпляра кольца ERPS ring1 instance1 на 1 секунду. Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)guard-timer 100

6.2.15. Таймер задержки (holdoff-timer <holdoff-times>)

Команда	holdoff -timer <holdoff-times> no holdoff -timer	
Параметр	holdoff-times	интервал составляет 1 с, диапазон — от 0 до 10 с
Значение по умолчанию	0 секунд	
Режим	Режим конфигурации экземпляра ERPS	
Руководство по использованию	Эта команда используется для настройки таймера задержки, конфигурирование по умолчанию восстанавливается словом "No" в начале команды	
Пример	Настроить таймер Holdoff кольца ERPS ring1 instance1 на 5 секунд. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#holdoff -timer 5	

6.2.16. Таймер WTR (wtr-timer <wtr-times>)

Команда	wtr-timer <wtr-times> no wtr-timer	
Параметр	wtr-times	интервал — 1 мин, диапазон — от 1 до 12 мин
Значение по умолчанию	5 минут	
Режим	Режим конфигурации экземпляра ERPS	
Руководство по использованию	Команда настраивает таймер WTR, который используется для предотвращения частого переключения защиты узла RPL owner из-за периодических (прерывистых) сбоев. Когда порт RPL owner получает пакеты восстановления по умолчанию, через некоторое время проверяется, существует ли еще умолчание на других узлах, и предотвращается немедленная блокировка порта RPL owner. "no" перед началом команды устанавливает WTR timer по умолчанию	



Пример	Установить таймер WTR на ERPS ring1 instance1 на 10 минут. Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#wtr-timer 10

6.2.17. Экземпляр защиты (protected-instance)

Команда	protected-instance <instance-list> no protected-instance <instance-list>	
Параметр	instance-list	список экземпляров MSTP, защищенных экземпляром кольца ERPS, например, i, j-k. Количество экземпляров в списке не ограничено
Значение по умолчанию	Экземпляр кольца ERPS не защищает ни один экземпляр MSTP	
Режим	Режим конфигурации экземпляра ERPS	
Руководство по использованию	Команда настраивает экземпляр защиты экземпляра кольца ERPS. Экземпляр кольца ERPS может защищать все экземпляры MSTP. Один и тот же экземпляр не может быть воспроизводиться несколькими экземплярами кольца ERPS в одной топологии. В одном и том же экземпляре кольца ERPS выполните эту команду более одного раза для защиты экземпляра, результат будет накапливаться. но в начале команды удаляет экземпляр защиты экземпляра кольца ERPS	
Пример	Установить экземпляр защиты кольца ERPS ring1 instance1 как instance 2. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#protected-instance 2	

6.2.18. Уровень канала R-APS (raps-mel <level-value>)

Команда	raps-mel <level-value> no raps-mel	
Параметр	level-value	значение уровня пакетов APS, диапазон от 0 до 7
Значение по умолчанию	Уровень 7	
Режим	Режим конфигурации экземпляра ERPS	



Руководство по использованию	Команда позволяет задать указанный в ней уровень канала R-APS для экземпляра кольца ERPS. При успешной настройке поле mel пакетов R-APS, отправляемых этим экземпляром кольца ERPS, будет добавлено к указанному уровню, и будут пропускаться только пакеты R-APS с уровнем, большим или равным указанному, в противном случае будет выдано уведомление об ошибке. "No" перед началом команды устанавливает уровень по умолчанию 7. Поле MEL в пакетах протокола используется для определения того, может ли пройти текущий пакет
Пример	Установить уровень канала R-APS для ERPS ring1 instance1 на 5. <pre>Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)rap-mel 5</pre>

6.2.19. Управляющая сеть VLAN (control-vlan <vlan-id>)

Команда	control-vlan <vlan-id> no control-vlan	
Параметр	vlan-id	идентификатор VLAN для пакетов R-APS, диапазон от 2 до 4094
Значение по умолчанию	Управляющая сеть VLAN не задана	
Режим	Режим конфигурации экземпляра ERPS	
Руководство по использованию	Команда позволяет установить управляющую сеть VLAN для пакетов R-APS канала R-APS. В экземпляре кольца ERPS эта VLAN используется только для передачи пакетов протокола ERPS, но не для пересылки пользовательских бизнес-пакетов. Это повышает безопасность протокола ERPS. Пользователь обеспечивает уникальность конфигурирования. Эта VLAN используется как VLAN tag при отправке пакетов R-APS. Конфигурирование защитной VLAN на всех узлах экземпляра должно быть идентично. "no" перед началом команды удаляет управляющую VLAN	
Пример	Настроить управляющую VLAN на ERPS ring1 instance1 как vlan10. <pre>Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)control-vlan 10</pre>	



6.2.20. Принудительное переключение (forced-switch {port0 | port1})

Команда	forced-switch {port0 port1}	
Параметр	port0	означает запуск конфигурирования принудительного переключения на port0 узла кольца
	port1	означает запуск конфигурирования принудительного переключения на port1 узла кольца
Значение по умолчанию	Принудительное переключение в экземпляре кольца ERPS отсутствует	
Режим	Режим конфигурации экземпляра ERPS	
Руководство по использованию	Команда выполняет принудительное переключение на порту узла кольца ERPS. Экземпляр кольца ERPS допускает одновременное выполнение двух или более принудительных переключений. Однако узел кольца может иметь только одну команду принудительного переключения. Пользователям следует избегать использования нескольких команд принудительного переключения в экземпляре кольца ERPS, чтобы избежать разделения экземпляра кольца ERPS. Если переключение происходит принудительно по текущему наивысшему приоритету, блокируется канал данных и канал R-APS данного экземпляра кольца ERPS на указанном порту-члене (port0 или port1) и разблокируются остальные порты-члены данного узла кольца; если конфигурирование данного экземпляра не завершена, и он находится в неактивном состоянии, появится сообщение "The request is rejected because the ERP instance in unactive state! (Запрос отклонен, так как экземпляр ERP в неактивном состоянии!)" в ином случае, можно переходить к следующему этапу	
Пример	Запустить конфигурирование принудительного переключения на port0 кольца ERPS ring1 instance1. <pre>Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#force-switch port0</pre>	

6.2.21. Ручное переключение (manual-switch {port0 | port1})

Команда	manual-switch {port0 port1}	
Параметр	port0	означает запуск ручного переключения на port0 узла кольца
	port1	означает запуск ручного переключения на port1 узла кольца



Значение по умолчанию	Ручное переключение на экземпляре кольца ERPS отсутствует
Режим	Режим конфигурации экземпляра ERPS
Руководство по использованию	Команда выполняет ручное переключение на порту узла кольца ERPS. Для экземпляра кольца ERPS разрешено только одно ручное переключение, при условии, что у экземпляра кольца ERPS отсутствуют сбои SF или команды FS. Если конфигурирование данного экземпляра не завершено, и он находится в неактивном состоянии, появится сообщение "The request is rejected because the ERP instance in unactive state! (Запрос отклонен, так как экземпляр ERP в неактивном состоянии!)" в ином случае, можно переходить к следующему этапу;
Пример	Выполнить ручное переключение на port0 ERPS ring1 instance1. <pre>Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#manual-switch port0</pre>

6.2.22. Очистка команд (clear command)

Команда	clear command
Параметр	-
Значение по умолчанию	В экземпляре кольца ERPS нет очистки команд
Режим	Режим конфигурации экземпляра ERPS
Руководство по использованию	Выполнение команды clear на порту-члене узла кольца ERPS очищает локально активные административные команды: команду принудительного переключения и команду ручного переключения; также может быть использован для запуска переключения соединения в реверсивном режиме до истечения времени WTR или WTB; а также для переключения канала с резервного канала RPL обратно на внутренний канал в нереверсивном режиме после восстановления падения связи. Если на узле данного экземпляра кольца существовала команда принудительного или ручного переключения, команда переключения снимается, а канал данных и канал R-APS заблокированного порта-члена остаются в заблокированном состоянии. Передача пакетов R-APS (NR) на обоих портах-участниках сохраняется стабильной до тех пор, пока не будет получен пакет R-APS (NR, RB) и не станет известно, что RPL заблокирован. Или в кольце возникает запрос более высокого уровня (например, SF). Если на узлах данного экземпляра кольца



	существует локальное принудительное или ручное переключение, снимите команду, а затем снова получите пакеты R-APS (NR) с идентификатором узла, превышающим идентификатор локального узла. Разблокируйте все порты кольца, на которых нет неисправностей SF, и прекратите передачу пакетов R-APS (NR) на обоих портах-участниках
Пример	Очистить конфигурирование на кольце ERPS ring1 instance1. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#clear command

6.2.23. Вывод данных о кольце ERPS (show erps ring {<ring-name> | brief})

Команда	show erps ring {<ring-name> brief}	
Параметр	ring-name	имя кольца ERPS
	brief	показать основную информацию о кольце ERPS
Значение по умолчанию	-	
Режим	Привилегированный режим	
Руководство по использованию	Команда позволяет прочесть информацию о кольце ERPS	
Пример	Показать всю информацию о кольцах ERPS. Switch#show erps ring brief ethernet tcn-propagation erps to none. Ring-Name Ring-topo Port0 Port1 Version Inst-Count ----- -- ring1 major-ring - - V2 0	



6.2.24. Вывод данных экземпляра кольца ERPS (show erps instance [ring <ring-name> [instance <instance-id>]])

Команда	show erps instance [ring <ring-name> [instance <instance-id>]]		
Параметр	ring-name	имя кольца ERPS	
	instance-id	идентификатор экземпляра кольца ERPS, диапазон от 1 до 48. Если он не назначен, выводится информация обо всех экземплярах кольца ERPS	
Значение по умолчанию	-		
Режим	Привилегированный режим		
Руководство по использованию	Команда показывает информацию об экземпляре кольца ERPS		
Пример	Показать информацию об экземплярах кольца ERPS. Switch#show erps instance		
	ERPS Ring: 1		
	Instance: 1		
	Description: -		
	Protected Instance: -		
	Revertive mode: revertive		
	R-APS MEL: 7		
	R-APS Virtual-Channel: with		
	Control Vlan: -		
	Ring ID: 1		
Guard Timer(10ms): 50			
Holdoff Timer(seconds): 0			
WTR Timer(min): 5			
	Port	Role	Port-Status
	Port0	common	blocked
	Port1	common	blocked
	Информация на экране	Описание	
	Description	Имя экземпляра кольца ERPS	



Protected Instance	Экземпляр MSTP, защищенный экземпляром кольца ERPS
Revertive mode	Режим связи кольца ERPS: реверсивная, нереверсивная
R-APS MEL	Уровень канала R-APS, пакет пакетов R-APS
R-APS Virtual-Channel	Если кольцо ERPS является подкольцом, виртуальный канал R-APS наследуемого кольца: с, без
Ring ID	Номер идентификатора кольца, передаваемый пакетами, отправленными экземпляром кольца ERPS, диапазон от 1 до 64
Contral Vlan	R-APS канал vlan, R-APS пакеты для меток пакетов
WTR_Timer	Таймер ожидания восстановления, диапазон от 1 до 12 минут
Guard_Timer	Таймер защиты, диапазон от 10 мс до 2 с
Holdoff_Timer	Таймер удержания, диапазон от 0 до 10
Port	Информация о порте кольца ERPS: port0, port1
Role	Роли узлов кольца ERPS: RPL Owner, RPL neighbor, Common
Port-Status	Blocked: порт находится в состоянии блокировки forwarding: порт находится в состоянии отправки

6.2.25. Вывод состояния экземпляра кольца ERPS (show erps status [ring <ring-name> [instance <instance-id>]])

Команда	show erps status [ring <ring-name> [instance <instance-id>]]	
Параметр	ring-name	имя кольца ERPS
	instance-id	идентификатор экземпляра кольца ERPS, диапазон от 1 до 48. Если он не назначен, выводится информация о состоянии всех экземпляров кольца ERPS
Значение по умолчанию	-	
Режим	Привилегированный режим	



Руководство по использованию	Отображение информации о состоянии экземпляра кольца ERPS																																																																												
Пример	Показать информацию о состоянии всех экземплярах кольца ERPS Switch#show erps status ERPS ring: 1 instance: 1 status: Active: 0 Node State: - Time last topology change: Jan 00 00: 00: 00 1900 <table><tr><td>Port</td><td>Interface</td><td>Port-Status</td><td>Signal-Status</td><td>R-APS-NodeId</td></tr><tr><td colspan="5">BPR</td></tr><tr><td colspan="5">-----</td></tr><tr><td>Port0</td><td>-</td><td>-</td><td>-</td><td>-</td></tr><tr><td colspan="5">-</td></tr><tr><td>Port1</td><td>-</td><td>-</td><td>-</td><td>-</td></tr><tr><td colspan="5">-</td></tr></table> ERPS ring: 1 instance: 2 status: Active: 0 Node State: - Time last topology change: Jan 00 00: 00: 00 1900 <table><tr><td>Port</td><td>Interface</td><td>Port-Status</td><td>Signal-Status</td><td>R-APS-NodeId</td></tr><tr><td colspan="5">BPR</td></tr><tr><td colspan="5">-----</td></tr><tr><td>Port0</td><td>-</td><td>-</td><td>-</td><td>-</td></tr><tr><td colspan="5">-</td></tr><tr><td>Port1</td><td>-</td><td>-</td><td>-</td><td>-</td></tr><tr><td colspan="5">-</td></tr></table> <table><tr><td>Информация на экране</td><td>Описание</td></tr><tr><td>Active</td><td>Текущее активное состояние экземпляра кольца ERPS: 1, 0</td></tr><tr><td>Node State</td><td>Текущее состояние экземпляра кольца ERPS: Idle (статус при нормальном режиме работы), Protection (статус кольца в случае разрыва), Forced-switch (принудительное переключение),</td></tr></table>	Port	Interface	Port-Status	Signal-Status	R-APS-NodeId	BPR					-----					Port0	-	-	-	-	-					Port1	-	-	-	-	-					Port	Interface	Port-Status	Signal-Status	R-APS-NodeId	BPR					-----					Port0	-	-	-	-	-					Port1	-	-	-	-	-					Информация на экране	Описание	Active	Текущее активное состояние экземпляра кольца ERPS: 1, 0	Node State	Текущее состояние экземпляра кольца ERPS: Idle (статус при нормальном режиме работы), Protection (статус кольца в случае разрыва), Forced-switch (принудительное переключение),
Port	Interface	Port-Status	Signal-Status	R-APS-NodeId																																																																									
BPR																																																																													

Port0	-	-	-	-																																																																									
-																																																																													
Port1	-	-	-	-																																																																									
-																																																																													
Port	Interface	Port-Status	Signal-Status	R-APS-NodeId																																																																									
BPR																																																																													

Port0	-	-	-	-																																																																									
-																																																																													
Port1	-	-	-	-																																																																									
-																																																																													
Информация на экране	Описание																																																																												
Active	Текущее активное состояние экземпляра кольца ERPS: 1, 0																																																																												
Node State	Текущее состояние экземпляра кольца ERPS: Idle (статус при нормальном режиме работы), Protection (статус кольца в случае разрыва), Forced-switch (принудительное переключение),																																																																												



	Manual-switch (ручное переключение), Pending (статус кольца, когда проблемный линк восстановлен)
Time last topology change	Последнее переключение тоологии
Port-Status	Blocked: порт находится в состоянии блокировки Forwarding: порт находится в состоянии отправки
Signal-Status	Состояние неисправности порта кольца ERPS: Non-failed: сбоя нет Failed: произошел сбой
R-APS-NodeId	Информация об идентификаторе узла, т.е. последний бит MAC-адреса
BPR	Информация о заблокированной связи, передаваемая принимающим последним R-APS, сохраненная на порту кольца ERPS, это заблокированный port0 или port1.

6.2.26. Вывод статистики экземпляра кольца ERPS (show erps statistics [ring <ring-name> [instance <instance-id>]])

Команда	show erps statistics [ring <ring-name> [instance <instance-id>]]	
Параметр	ring-name	имя кольца ERPS
	instance-id	идентификатор экземпляра кольца ERPS, диапазон от 1 до 48. Если оно не задано, показывается статистическая информация обо всех экземплярах кольца ERPS этого устройства
Значение по умолчанию	-	
Режим	Привилегированный режим	
Руководство по использованию	Отображает статистическую информацию об экземпляре кольца ERPS	
Пример	Показать статистическую информацию об экземпляре кольца ERPS. Switch#show erps statistics	



Statistics for ERPS ring: 1 instance 1:				
R-APS	Port0(Tx/Rx)	Port1(Tx/Rx)		
-				
NR: 0	/0	0	/0	
NR,RB:	0	/0	0	/0
SF: 0	/0	0	/0	
MS: 0	/0	0	/0	
FS: 0	/0	0	/0	
EVENT:	0	/0	0	/0
-				
TOTAL:	0	/0	0	/0
Statistics for ERPS ring: 1 instance 2:				
R-APS	Port0(Tx/Rx)	Port1(Tx/Rx)		
-				
NR: 0	/0	0	/0	
NR,RB:	0	/0	0	/0
SF: 0	/0	0	/0	
MS: 0	/0	0	/0	
FS: 0	/0	0 /0		
EVENT:	0	/0	0 /0	
-				
TOTAL:	0	/0	0	/0

6.2.27. Удаление статистики экземпляра кольца ERPS (clear erps statistics [ring <ring-name> [instance <instance-id>]])

Команда	clear erps statistics [ring <ring-name> [instance <instance-id>]]	
Параметр	ring-name	имя кольца ERPS
	instance-id	идентификатор экземпляра кольца ERPS, диапазон от 1 до 48. Если оно не задано, удаляется статистическая информация обо всех экземплярах кольца ERPS этого устройства
Значение по умолчанию	-	
Режим	Привилегированный режим	



Руководство по использованию	Позволяет очистить статистическую информацию ERPS
Пример	Очистить статистическую информацию о ERPS ring1 instance1. Switch#clear erps statistics ring 1 instance 1



7. КАЧЕСТВО ОБСЛУЖИВАНИЯ (QOS)

7.1. Команды для настройки качества обслуживания (QOS)

7.1.1. Статистика (accounting)

Синтаксис	Accounting no accounting
Параметр	отсутствует
Состояние по умолчанию	Функции статистики не установлены
Режим	Конфигурирование карты правил
Применение	Задаёт функции статистики для классифицированного трафика. После включения этой функции в режиме политики классов, добавляет статистику трафика по карте политики классов, при применении политики сообщения может отображаться только в красном или зеленом цвете. При печати статистики информация в пакете указывает на номер классифицированного пакета и не поддерживает цветовую классификацию
Пример	Подсчитать пакеты, удовлетворяющие правилу c1. <pre>Switch#config Switch(config)#class-map c1 Switch(config-classmap-c1)#exit Switch(config)#policy-map p1 Switch(config-policymap-p1)#class c1 Switch(config-policymap-p1-class-c1)#accounting Switch(config-policymap-p1-class-c1)#exit Switch(config-policymap-p1)#exit Switch(config)#</pre>

7.1.2. Класс (class)

Синтаксис	class <class-map-name> [insert-before <class-map-name>] no class <class-map-name>		
Параметр	<class-map-name>	< class-map-name>	имя карты классов, используемое классом



	insert-before <class-map-name>	insert-before < class-map-name > вставить новый сконфигурированный класс перед существующим классом, чтобы повысить приоритет нового класса
Состояние по умолчанию	Классы правил не заданы	
Режим	Конфигурирование карты правил	
Применение	Привязывает класс к карте правил и переходит в режим карты класса правил; "no" перед началом команды удаляет установленный класс. До настройки правил классов должна быть создана карта правил и включен режим карты правил. В режиме карты правил классификация и настройка pexthor могут быть применены для пакетного трафика, классифицированного по карте классов	
Пример	После добавления карты класса c1 в карту правил добавить карту класса c2 и вставить ее перед c1. <pre>Switch(config)#class-map c1 Switch(config-classmap-c1)#exit Switch(config)#class-map c2 Switch(config-classmap-c2)#exit Switch(config)#policy-map p1 Switch(config-policymap-p1)#class c1 Switch(config-policymap-p1-class-c1)#exit Switch(config-policymap-p1)#class c2 insert-before c1 Switch(config-policymap-p1-class-c2)#exit</pre>	

7.1.3. Карта классов (class-map)

Синтаксис	class-map <class-map-name> no class-map <class-map-name>	
Параметр	<class-map-name>	имя карты классов
Состояние по умолчанию	Карты классов не заданы	
Режим	Режим глобальной конфигурации	
Применение	Позволяет создать карту классов и включить режим карты классов. "no" перед началом команды удаляет указанную карту классов	



Пример	Создать, а затем удалить карту класса с именем "c1". Switch#config Switch(config)#class-map c1 Switch(config-classmap-c1)#exit Switch(config)#no class-map c1

7.1.4. Удаление статистики карт правил (clear mls qos statistics)

Синтаксис	clear mls qos statistics (interface [ethernet] <interface-name>) (vlan <vlan-id>)	
Параметр	<vlan-id>	VLAN ID
	<interface-name>	имя интерфейса
Состояние по умолчанию	Действия не заданы	
Режим	Привилегированный режим	
Применение	Позволяет очистить данные статистики указанных портов или карты правил VLAN. При отсутствии параметров выполняется удаление данных статистики всех карт правил	
Пример	Очистить статистику карты правил для VLAN 100. Switch#clear mls qos statistics vlan 100	

7.1.5. Отбрасывание (drop)

Синтаксис	drop no drop
Параметр	отсутствует
Состояние по умолчанию	Отсутствует
Режим	Конфигурирования карты классов в карте политик
Применение	После ввода этой команды выполняется действие отбрасывания для указанных пакетов



Пример	Отбросить пакет, удовлетворяющий c1. Switch#config Switch(config)#policy-map p1 Switch(config-policymap-p1)#class c1 S witch(config-policymap-p1-class-c1)#drop Switch(config-policymap-p1-class-c1)#exit Switch(config-policymap-p1)#exit

7.1.6. Согласование (match)

Синтаксис	match (access-group <acl-index-or-name> ip dscp <dscp-list> ip precedence <ip-precedence-list> ipv6 access-group <acl-index-or-name> ipv6 dscp <dscp-list> ipv6 flowlabel <flowlabel-list> vlan <vlan-list> cos <cos-list>) no match {access-group ip dscp ip precedence ipv6 access-group ipv6 dscp ipv6 flowlabel vlan cos)	
Параметр	<acl-index-or-name>	согласование с указанным списком доступом ACL: IP ACL, MAC ACL или IPv6 standard ACL MAC-IP ACL, параметром является номер или имя списка ACL
	<dscp-list>	согласование с указанным значением DSCP, параметром является список значений DSCP, содержащий не более 8 значений DSCP; диапазон от 0 до 63;
	<ip-precedence-list>	согласование с указанным значением IP Precedence, параметром является список IP Precedence, содержащий не более 8 значений IP Precedence, каждое из которых задано в пределах 0~7;
	ipv6 access-group <acl-index-or-name>	согласование с указанным списком доступом IPv6 ACL, параметром является номер или имя списка IPv6 ACL;
	<flowlabel-list>	согласование с указанной меткой потока IPv6, является значение метки потока IPv6, допустимое значение - от 0 до 1048575;
	<vlan-list>	согласование с указанным VLAN ID, параметром является список VLAN ID, содержащий не более 8 VLAN ID, диапазон от 1 до 4094



	<cos-list>	согласование с указанным значением Cos, параметром является список Cos, содержащий не более 8 значений Cos
Состояние по умолчанию	Стандарт согласования не задан	
Режим	Режим карты классов	
Применение	Позволяет задать стандарт соответствия карте классов. "no" перед началом команды удаляет указанный стандарт согласования. Для карты классов может быть задан только один стандарт согласования. При настройке согласования со списком доступа ACL, доступно только правило permit (разрешить). Запрет правил является исключительной опцией и не применяется в действиях карты правил. (Правила запрета не поддерживаются в PBR, поэтому старайтесь избегать их). Если после установки правила согласования задать другое правило согласования, операция завершится неудачей, но установка того же правила согласования отменит предыдущее правило	
Пример	Создать карту классов с именем c1, задать правило класса для этой карты, устанавливающее согласование для пакетов с IP Precedence 0. <pre>Switch(config)#class-map c1 Switch(config-classmap-c1)#match ip precedence 0 Switch(config-classmap-c1)#exit</pre>	

7.1.7. Значение CoS (mls qos cos)

Синтаксис	<pre>mls qos cos <default-cos> no mls qos cos</pre>	
Параметр	<default-cos>	значение CoS для порта, используемое по умолчанию, в пределах от 0 до 7
Состояние по умолчанию	Задано значение CoS 0	
Режим	Режим конфигурации порта	
Применение	Позволяет задать значение CoS, используемое портом по умолчанию. Команда "no mls qos cos" восстанавливает значение по умолчанию. Позволяет задать значения CoS для порта коммутатора, используемые по умолчанию. В настройках по умолчанию, если сообщение имеет тег, cos входа сообщения для этого порта имеет значение по умолчанию.	



	Если сообщение не тегировано, используется значение cos сообщения для тега
Пример	Установить значение CoS по умолчанию 7 для порта Ethernet 1/0/1. Т.е. пакетам, проходящим через порт, по умолчанию будет присвоено значение CoS 7, если не задано иного значения CoS. <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mls qos cos 7</pre>

7.1.8. Карта соответствия значений (mls qos map)

Синтаксис	<pre>mls qos map (cos-intp <intp1...intp8> cos-dp <dp1...dp8> dscp-intp <in-dscp list> to <intp> dscp-dp <in-dscp list> to <dp> dscp-dscp <in-dscp list> to <out-dscp>)</pre> <pre>no mls qos map (cos-intp cos-dp dscp-intp dscp-dp dscp-dscp)</pre>	
Параметр	cos-intp <intp1...intp8>	карта соответствия значений CoS значениям intp (очереди) <intp1...intp8> 8 значений intp, соответствующие значениям CoS от 0 до 7, каждое значение intp разделено пробелами, в пределах от 0 до 7;
	cos-dp <dp1...dp8>	определяет соотнесение от cos к intp (очереди), <dp1...dp8> это 8 приоритетов отбрасывания, соответствующих значениям Cos от 0 до 7, каждое значение intp разделено пробелами, в пределах от 0 до 2;
	dscp-intp	определяет соответствие между DSCP и intp (очередью)
	dscp-dp	определяет соответствие между dscp и приоритетом отбрасывания
	dscp-dscp	определяет соответствие между входящим dscp и направляемым dscp, <in-dscp list> входное значение dscp, наибольшим является 8, отделены друг от друга пробелом и находятся в диапазоне от 0 до 63, <out-dscp> выходное значение dscp в диапазоне от 0 до 63
Состояние по умолчанию	Используются следующие значения соответствия:	
	Карта CoS-TO-INTP по умолчанию	



COS:	0	1	2	3	4	5	6	7		
INTP:	0	1	2	3	4	5	6	7		
Карта CoS-TO-DP по умолчанию										
CoS	0	1	2	3	4	5	6	7		
DP	0	0	0	0	0	0	0	0		
Карта DSCP-TO-INTP по умолчанию										
d1 : d2	0	1	2	3	5	6	7	8	9	
4										
0:	0	0	0	0	0	0	0	0	1	1
1:	1	1	1	1	1	1	2	2	2	2
2:	2	2	2	2	3	3	3	3	3	3
3:	3	3	4	4	4	4	4	4	4	4
4:	5	5	5	5	5	5	5	5	6	6
5:	6	6	6	6	6	6	7	7	7	7
6:	7	7	7	7						
Карта DSCP-TO-DP по умолчанию										
d1 : d2	0	1	2	3	5	6	7	8	9	
4										
0:	0	0	0	0	0	0	0	0	0	0
1:	0	0	0	0	0	0	0	0	0	0
2:	0	0	0	0	0	0	0	0	0	0
3:	0	0	0	0	0	0	0	0	0	0
4:	0	0	0	0	0	0	0	0	0	0
5:	0	0	0	0	0	0	0	0	0	0



	6: 0 0 0 0								
	Карта DSCP-TO-DSCP по умолчанию								
	d1 : d2 4	0	1	2	3	5	6	7	8 9
	0:	0	1	2	3 4	5	6	7	8 9
	1:	10 14	11	12	13	15	16	17	18 19
	2:	20 24	21	22	23	25	26	27	28 29
	3:	30 34	31	32	33	35	36	37	38 39
	4:	40 44	41	42	43	45	46	47	48 49
	5:	50 54	51	52	53	55	56	57	58 59
	6:	60	61	62	63				
Режим	Режим глобальной конфигурации								
Применение	INTP означает внутреннюю настройку приоритета для микросхемы. Поскольку внутренних значений DSCP 64, а внутренних приоритетов (очереди) только 8, то для сопоставления dscp-intp необходимо 8 внутренних dscp сопоставить с тем же INTP								
Пример	Установить значения сопоставления CoS-to-INTP по умолчанию 0 8 16 24 32 40 48 56 на 0 1 2 3 4 5 6 7. Switch(config)#mls qos map cos-intp 0 1 2 3 4 5 6 7								

7.1.9. Пропускная способность очереди (mls qos queue bandwidth)

Синтаксис	mls qos queue <queue-id> bandwidth <maximum-bandwidth> no mls qos queue <queue-id> bandwidth	
Параметр	<queue-id>	идентификатор очереди используется для установки гарантированной пропускной способности.



		Разные чипы поддерживают разное количество очередей с диапазоном от 1 до 8
	<maximum-bandwidth>	максимальная пропускная способность, в диапазоне от 0 до 128 000, при вводе 0 функция максимальной пропускной способности не действует. Значение минимальной пропускной способности не должно быть выше максимального значения
Состояние по умолчанию	Пропускная способность очереди не гарантируется	
Режим	Режим конфигурации порта	
Применение	Минимальная гарантированная пропускная способность и максимальное ограничение пропускной способности могут быть установлены для разных или одной и той же очереди. Гарантированная пропускная способность для очереди на выход зависит от режима управления, например, порт имеет очередь со строгим приоритетом, и сейчас самый высокий приоритет у очереди 8, когда происходит блокировка, она будет выполнять трафик этой очереди. Однако, если пользователи хотят, чтобы очередь с более низким приоритетом имела пропускную способность, они могут зарезервировать пропускную способность с помощью этой команды, чтобы сначала удовлетворить минимальную пропускную способность очереди с более низким приоритетом, а затем регулировалась дополнительная пропускная способность в соответствии с SP	
Пример	Настроить максимальную пропускную способность 128 кбит/с для ethernet1/0/2 queue1. <pre>Switch(config)#interface ethernet 1/0/2</pre> <pre>Switch(config-if-ethernet1/0/2)# mls qos queue 1 bandwidth 128</pre>	

7.1.10. Доверие меткам COS (mls qos trust)

Синтаксис	mls qos trust (cos dscp) no mls qos trust (cos dscp)	
Параметр	dscp	порт доверяет значению DSCP
	cos	порт доверяет значению COS
Состояние по умолчанию	По умолчанию установлено доверие меткам COS	
Режим	Режим конфигурации порта	



Применение	Переводит текущий порт в режим доверия; "no" перед началом команды отменяет текущий режим доверительности на порту. Режим trust dscp: настраивает поле intp на основе сопоставления dscp и intp. Режим trust cos: настраивает поле intp на основе сопоставления cos и intp
Пример	Установить режим trust dscp для порта 1/0/1, вместо trust cos. <pre>Switch(config)#interface ethernet 1/0/1 Switch(config-if-ehternet1/1)# mls qos trust dscp Switch(config-if-ehternet1/1)#no mls qos trust cos</pre>

7.1.11. Карта правил (Policy-map)

Синтаксис	<pre>policy-map <policy-map-name> no policy-map <policy-map-name></pre>	
Параметр	<policy-map-name>	имя карты правил
Состояние по умолчанию	Карты правил не заданы	
Режим	Режим глобальной конфигурации	
Применение	Позволяет создать карту правил и включить режим карты правил; Команда " no policy-map < policy-map-name> " удаляет указанную карту правил. Работа с картой класса правил может быть выполнена в режиме конфигурации карты правил	
Пример	Создать и удалить карту правил с именем "p1". <pre>Switch(config)#policy-map p1 Switch(config-policymap-p1)#exit Switch(config)#no policy-map p1</pre>	



7.1.12. Применение карты правил (service-policy input)

Синтаксис	service-policy input <policy-map-name> no service-policy input {<policy-map-name>}	
Параметр	input <policy-map-name>	input <policy-map-name > применяет указанную карту правил к входному порту коммутатора перед началом команды удаляет все карты правил на входе порта, при условии, что отсутствует имя указанной карты правил
Состояние по умолчанию	Карты правил не привязаны к портам	
Режим	Режим конфигурации порта	
Применение	Позволяет применить карту правил на указанном порту. "no" перед началом команды удаляет указанную карту правил, применяемую на порте или удаляет все карты правил на направлении входа порта. К каждому направлению передачи порта или интерфейса VLAN может быть применена только одна карта правил	
Пример	Привязать правило p1 к входному Ethernet-порту 1/1 Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#service-policy input p1	

7.1.13. Применение карты правил на указанном VLAN-интерфейсе (service-policy input vlan)

Синтаксис	no service-policy input {<policy-map-name>} vlan <vlan-list>	
Параметр	input <policy-map-name>	input <policy-map-name > применяет указанную карту правил к входному направлению интерфейса VLAN коммутатора
	vlan <vlan-list>	vlan <vlan-list> список vlan карты политики привязки
Состояние по умолчанию	По умолчанию ни одна карта политики не привязана к интерфейсу VLAN	
Режим	Режим глобальной конфигурации	



Применение	Позволяет применить карту правил на указанном VLAN-интерфейсе. "no" перед началом команды удаляет указанную карту правил, примененную к интерфейсу VLAN, или удаляет все карты, примененные в направлении входа интерфейса vlan. К каждому направлению передачи порта или интерфейса VLAN может быть применена только одна карта правил
Пример	Привязать политику p1 к входу интерфейса VLAN 2-4,6 <pre>Switch(config)#service-policy input p1 vlan 2-4; 6</pre>

7.1.14. Настройка значений (set)

Синтаксис	<pre>set (ip dscp <new-dscp> ip precedence <new-precedence> internal priority <new-inp> drop precedence <new-dp> cos <new-cos>) no set (ip dscp ip precedence internal priority drop precedence cos)</pre>	
Параметр	ip dscp <new-dscp>	новое значение DSCP, без различия между v4 и v6
	ip precedence <new-precedence>	новое значение IP Precedence
	cos <new-cos>	новое значение IP Precedence
Состояние по умолчанию	Не присвоено	
Режим	Режим карты классов-правил	
Применение	Позволяет задать для классифицированного трафика новые значения DSCP и IP Precedence, "no" перед началом команды удаляет новые присвоенные значения. Новые значения будут присвоены только классифицированному трафику, соответствующему стандарту сопоставления	
Пример	Задать значение IP DSCP 3 для пакетов, согласующихся с классом правил c1. <pre>Switch(config)#policy-map p1 Switch(Config-PolicyMap-p1)#class c1 Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 3 Switch(Config-PolicyMap-p1-Class-c1)#exit Switch(Config-PolicyMap-p1)#exit</pre>	



7.1.15. Вывод карты классов (show class-map)

Синтаксис	show class-map [<class-map-name>]	
Параметр	[<class-map-name>]	имя карты классов
Состояние по умолчанию	Отсутствует	
Режим	Привилегированный режим	
Применение	Команда выводит на экран все настроенные карты классов или информацию о указанной карте классов	
Пример	Switch#show class-map Class map name: cm, used by 1 time(s) match cos: 0 Class map name: color, used by 0 time(s) match cos: 0	
	Информация, отображаемая на экране	Пояснение
	Class map name: c1	Имя карты классов
	used by 1 times	Количество раз использования
	match acl name: 1	Правило классификации для этой карты классов.

7.1.16. Вывод карты правил (show policy-map)

Синтаксис	show policy-map [<policy-map-name>]	
Параметр	<policy-map-name>	имя карты правил
Состояние по умолчанию	Отсутствует	
Режим	Привилегированный режим	
Применение	Команда выводит на экран все настроенные карты правил или информацию о указанной карте правил	



Пример	Switch#show policy-map Policy Map 1, used by 0 time(s) Class Map name: cm Policy Map p1, used by 0 time(s) Class Map name: c1 drop set ip precedence 3 policy CIR: 2000 CBS: 512 conform-action: transmit exceed-action: drop	
	Информация, отображаемая на экране	Пояснение
	Policy map name: c1	Имя карты правил
	Class Map name: c1	Имя карты класса
	policy 20000 512	Примененное правило
	used by 0 port	Количество портов, на которых применяется правило

7.1.17. Вывод интерфейса QoS (show mls qos interface)

Синтаксис	show mls qos {interface [<interface-id>] [policy queuing] vlan <vlan-id>} [begin include exclude <regular-expression>]	
Параметр	<interface-id>	идентификатор порта
	<vlan-id>	идентификатор VLAN
	<regular-expression>	Обычное выражение
Состояние по умолчанию	Отсутствует	
Режим	Привилегированный режим	
Применение	Позволяет вывести на экран информацию о настройках QoS порта. Пакет может быть только зеленым или красным при применении политики. В распечатанной информации указывается классификационный номер пакета, вывод статистики по цветам не поддерживается	



Пример	<pre>Switch#show mls qos interface ethernet 1/0/1 Ethernet1/0/1: Default COS: 0 Trust: DSCP Attached Policy Map for Ingress: p1 Egress Internal-Priority-TO-Queue map: INTP: 0 1 2 3 4 5 6 7 Queue: 0 1 2 3 4 5 6 7 Queue Algorithm: WRR Queue weights: Queue 1 2 3 4 5 6 7 8 WrrWeight 1 2 3 4 5 6 7 8 WdrrWeight 10 10 20 20 40 40 80 80 Bandwidth Guarantee Configuration: Queue 1 2 3 4 5 6 7 8 MinBW(K) 0 0 0 0 0 0 0 0 MaxBW(K) 0 0 0 0 0 0 0 0</pre>							
	Информация, отображаемая на экране	Пояснение						
	Ethernet1/0/1	имя порта						
	default cos: 0	Значение CoS, выбираемое в порту по умолчанию.						
	Trust: COS	Состояние доверия для порта						
	Attached Policy Map for Ingress: p1	Имя правила, привязанного к порту						
	ClassMap	Имя карты класса						
	classified	Общее количество пакетов данных, соответствующих этой карте классов. Если для карты класса нет функции статистики, отображается NA						
	in-profile	Общее количество пакетов данных входящего профиля, соответствующих этой карте классов. Если для карты класса нет функции статистики, отображается NA						
	out-profile	Общее количество пакетов данных исходящего профиля, соответствующих этой карте классов. Если для карты класса нет функции статистики, отображается NA						



	Internal-Priority-TO-Queue map: :	Внутренний приоритет для сопоставления с очередью
	Queue Algorithm:	метод выстраивания очереди WRR, WDDR или PQ
	Queue weights	Конфигурация веса очереди
	Bandwidth Guarantee Configuration	Конфигурация гарантии пропускной способности

Switch(config)#show mls qos interface ethernet 1/0/1 queuing Ethernet1/0/1:

Egress Internal-Priority-TO-Queue map:

INTP: 0	1	2	3	4	5	6	7
Queue: 0	1	2	3	4	5	6	7

Queue Algorithm:

WRR Queue weights:

Queue	1	2	3	4	5	6	7	8
WrrWeight	1	2	3	4	5	6	7	8
WdrWeight	10	10	20	20	40	40	80	80

Bandwidth Guarantee Configuration:

Queue	1	2	3	4	5	6	7	8
MinBW(K)	0	0	0	0	0	0	0	0
MaxBW(K)	0	0	0	0	0	0	0	0

Информация, отображаемая на экране	Пояснение
Internal-Priority-TO-Queue map: :	Внутренний приоритет для сопоставления с очередью
Queue Algorithm:	метод выстраивания очереди WRR, WDDR или PQ



Queue weights	Конфигурирование веса очереди
Bandwidth Guarantee Configuration	Конфигурирование гарантии пропускной способности

Switch # show mls qos interface ethernet 1/0/1 policy

Ethernet1/0/1:

Attached Policy Map for Ingress: p1

Информация, отображаемая на экране	Пояснение
Ethernet1/0/1	имя порта
Attached Policy Map for Ingress: p1	Имя правила, привязанного к порту
ClassMap	имя карты классов
classified	Общее количество пакетов данных, соответствующих этой карте классов
in-profile	Общее количество пакетов данных входящего профиля, соответствующих этой карте классов
out-profile	Общее количество пакетов данных исходящего профиля, соответствующих этой карте классов

7.1.18. Вывод данных о настройках политики (show mls qos in (interface <interface-name> policy) | (vlan <vlan-id>))

Синтаксис	show mls qos in (interface <interface-name> policy) (vlan <vlan-id>)	
Параметр	<interface-name>	имя порта
	<vlan-id>	VLAN ID
Состояние по умолчанию	Отсутствует	
Режим	Привилегированный режим	



Применение	Позволяет вывести на экран информацию о настройках политики для входящего порта или vlan. Позволяет вывести на экран информацию о настройках политики для входящего трафика
Пример	Показать информацию о настройках политики для входящего трафика. Switch#show mls qos in interface ethernet1/0/1 policy Ethernet1/0/1: Attached Policy Map for Ingress: p1

7.1.19. Вывод данных о настройках карт (show mls qos maps)

Синтаксис	show mls qos maps [cos-intp cos-dp dscp-intp dscp-dp dscp-dscp] [begin include exclude <regular-expression>]	
Параметр	cos-intp	сопоставление входящего L2 CoS с внутренним приоритетом
	cos-dp	сопоставление входящего L2 CoS с приоритетом отбрасывания
	dscp-intp	сопоставление входящего DSCP с внутренним приоритетом
	dscp-dp	сопоставление входящего DSCP с приоритетом отбрасывания
	dscp-dscp	сопоставление внутреннего исходящего трафика с приоритетом DSCP
Состояние по умолчанию	Отсутствует	
Режим	Привилегированный режим и режим конфигурации	
Применение	Позволяет вывести на экран информацию о настройках карт QoS	
Пример	Вывести на экран информацию о конфигурировании таблицы сопоставления . Switch#show mls qos maps Ingress COS-TO-Internal-Priority map:	

COS: 0 1 2 3 4 5 6 7

INTP: 0 1 2 3 4 5 6 7

Ingress DSCP-TO-Internal-Priority map:



d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	7	1	7	7	7	0	7	7	7	1
1:	1	1	1	1	1	1	2	1	2	2
2:	2	2	2	2	3	1	3	3	3	3
3:	3	3	4	1	4	4	4	4	4	4
4:	5	1	5	5	5	5	5	5	6	1
5:	6	6	6	6	6	6	7	1	7	7
6:	7	7	7	7						

Ingress COS-T0-Drop-Precedence map:

COS: 0 1 2 3 4 5 6 7
 DP: 0 0 0 0 0 0 0 0

Ingress DSCP-T0-DSCP map:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	1	2	3	4	5	6	7	8	9
1:	10	11	12	13	14	15	16	17	18	19
2:	20	21	22	23	24	25	26	27	28	29
3:	30	31	32	33	34	35	36	37	38	39
4:	40	41	42	43	44	45	46	47	48	49
5:	50	51	52	53	54	55	56	57	58	59
6:	60	61	62	63						

Ingress DSCP-T0-Drop-Precedence map:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	0	0	0	0	0	0	0	7	1
1:	0	0	0	0	0	0	0	0	2	2



2:	0	0	0	0	0	0	0	0	3	3
3:	0	0	0	0	0	0	0	0	4	4
4:	0	0	0	0	0	0	0	0	6	1
5:	0	0	0	0	0	0	0	0	7	7
6:	0	0	0	0						

7.1.20. Вывод данных о конфигурировании QOS VLAN (show mls qos vlan)

Синтаксис	show mls qos vlan <v-id>	
Параметр	<v-id>	идентификатор VLAN
Состояние по умолчанию	Отсутствует	
Режим	Привилегированный режим	
Применение	Позволяет вывести на экран информацию о конфигурировании QOS VLAN	
Пример	Switch#show mls qos vlan 1 Vlan 1: Attached Policy Map for Ingress: 1 Classmap classified (in packets) c1 0 Rule ID classified (in packets)	

7.1.21. Передача (transmit)

Синтаксис	transmit no transmit	
Параметр	отсутствует	
Состояние по умолчанию	Не задавайте действие	
Режим	Конфигурирования карты классов в карте политик	
Применение	Передача пакета осуществляется сразу после настройки этой команды	



Пример	Отправить пакет, который удовлетворяет c1. <pre>Switch#config Switch(config)#policy-map p1 Switch(config-policy-map-p1)#class c1 Switch(config-policy-map-p1-class-c1)#transmit Switch(config-policy-map-p1-class-c1)#exit Switch(config-policy-map-p1)#exit</pre>

7.1.22. Перенаправление на основе трафика (access-group redirect to interface ethernet)

Синтаксис	<pre>access-group <aclname> redirect to interface [ethernet] <IFNAME> no access-group <aclname> redirect</pre>	
Параметр	<aclname>	имя потока, поддерживает только цифровой стандарт IP ACL, цифровой расширенный IP ACL, номенклатурный стандарт IP ACL, номенклатурный расширенный IP ACL, цифровой стандарт MAC ACL, цифровой расширенный MAC ACL, номенклатурный стандарт MAC ACL, номенклатурный расширенный MAC, цифровой стандарт IPv6 ACL и номенклатурный стандарт IPv6 ACL. Параметры Timerange и Portrange не могут быть установлены в ACL; тип ACL должен быть Permit
	<IFNAME>	<IFNAME > порт назначения переадресации
Состояние по умолчанию	Отсутствует	
Режим	Режим конфигурации порта	
Применение	Команда определяет перенаправление на основе трафика; для удаления перенаправления на основе трафика используется команда "no access-group <aclname> redirect". Функция перенаправления на основе трафика позволяет коммутатору отправлять кадры данных, удовлетворяющие определенным условиям, на другой указанный порт. Примечание: Перенаправление не поддерживает перенаправление трафика на порт	
Пример	Перенаправить кадры с IP-адресом источника 192.168.1.111, полученные с порта 1, на порт 6 <pre>Switch(config)#access-list 1 permit host 192.168.1.111 Switch(config)# interface ethernet 1/0/1</pre>	



	Switch(config-if-ethernet1/0/1)#access-group 1 redirect to interface ethernet 1/0/6

7.1.23. Перенаправлении трафика для системы/порта (show flow-based-redirect)

Синтаксис	show flow-based-redirect [interface [ethernet] <IFNAME>]	
Параметр	<IFNAME>	Отображает информацию о перенаправлении трафика, настроенном для портов, перечисленных в списке интерфейсов
Состояние по умолчанию	отсутствует	
Режим	Привилегированный режим, режим конфигурации	
Применение	Эта команда используется для отображения текущей информации о перенаправлении трафика для системы/порта	
Пример	Switch(config)#show flow-based-redirect Flow-based-redirect config on interface Ethernet1/0/1: RX flow (access-list 1) is redirected to interface Ethernet1/0/6	

7.1.24. Добавление (add)

Синтаксис	add s-vid <new-vid> no add s-vid	
Параметр	s-vid <new-vid>	s-vid <new-vid> назначенный VID туннельного VLAN Tag
Состояние по умолчанию	По умолчанию тег не добавляется	
Режим	Режим настройки таблицы классификации политик	
Применение	Добавляет указанную туннельную метку к пакетам в таблице классификации отображения, но в начале команды отменяет настройку. После настройки этой команды указанная туннельная метка или внутренняя метка добавляется к пакетам в таблице классификации соответствия. При использовании функции QinQ отправляемые пакеты имеют только внутренний тег VLAN или не имеют его, тогда	



	необходимо добавить указанную туннельную метку VLAN с помощью команды add s-vid, иначе данные не будут иметь внутреннего тега
Пример	Добавить метку VLAN Tag, VID которой равен 2, к пакетам, удовлетворяющим правилу классификации c1. Switch#config Switch(config)#policy-map p1 Switch(config-policy-map-p1)#class c1 Switch(config-policy-map-p1-class-c1)#add s-vid 2

7.1.25. Согласование (match)

Синтаксис	match {access-group <acl-index-or-name> ip dscp <dscp-list> ip precedence <ip-precedence-list> ipv6 access-group <acl-index-or-name> ipv6 dscp <dscp-list> ipv6 flowlabel <flowlabel-list> vlan <vlan-list> cos <cos-list> } no match {access-group ip dscp ip precedence ipv6 access-group ipv6 dscp no match {access-group ip dscp ip precedence ipv6 access-group ipv6 dscp ipv6 flowlabel vlan cos }}	
Параметр	access-group <acl-index-or-name>	согласование с указанным IP ACL, MAC-IP ACL или стандартным IPV6 ACL, параметрами являются номер или имя ACL
	ip dscp <dscp-list>	согласование с указанным значением DSCP, параметром является список DSCP, состоящий максимум из 8 значений DSCP, в диапазоне от 0 до 63
	ip precedence <ip-precedence-list>	согласование с указанным значением IP Precedence, параметр представляет собой список IP Precedence, состоящий максимум из 8 значений IP Precedence с диапазоном от 0 до 7
	ipv6 access-group <acl-index-or-name>	согласование с указанным списком доступом IPv6 ACL, параметром является номер или имя IPv6 ACL
	ipv6 flowlabel <flowlabel-list>	согласование с указанной меткой потока IPv6, параметром является значение метки потока IPv6, допустимое значение - от 0 до 1048575;



	vlan <vlan-list>	согласование с указанным VLAN ID внешнего VLAN Tag, параметром является список VLAN ID, содержащий не более 8 VLAN ID, диапазон от 1 до 4094
	cos <cos-list>	согласование с указанным значением Cos, параметром является список Cos, содержащий не более 8 значений Cos в диапазоне от 0 до 7
Состояние по умолчанию	Стандарт согласования не задан	
Режим	Режим карты классов	
Применение	Позволяет задать стандарт соответствия карте классов. "no" перед началом команды удаляет указанный стандарт соответствия карте классов. Для карты классов может быть задан только один стандарт согласования. При настройке согласования ACL разрешающее правило является параметром соответствия, который применяет действия карты правил. Правило запрета - это опция исключения, которая не применяет действия карты правил. Если было настроено другое правило соответствия, действие не будет выполнено, но установка того же правила соответствия отменяет предыдущее	
Пример	Создать class-map с именем c1 и настроить правило класса в class-map на соответствие пакетам с IP Precedence, равным 0. <pre>Switch(config)#class-map c1 Switch(config-classmap-c1)#match ip precedence 0 Switch(config-classmap-c1)#exit</pre>	

7.1.26. Карта политики (service-policy)

Синтаксис	<pre>service-policy <policy-map-name> in no service-policy <policy-map-name> in</pre>	
Параметр	<policy-map-name>	указанное имя карты политики flexible QinQ
Состояние по умолчанию	Карта правила не привязана к порту	
Режим	Режим конфигурации порта	



Применение	Привязывает указанные правила flexible QinQ к входу порта, а команда с "no" в начале команды отменяет привязку. Только одна карта правил может быть привязана к каждому порту, функция начинает действовать после привязки карты к порту. В настоящее время конфигурирование с помощью команд "add" и "delete" не поддерживается
Пример	Применить policy-map p1 (p1 соответствует действию, изменяющему s-vid) к Ethernet port 1/0/1 для flexible QinQ. <pre>Switch(config-if-ethernet1/0/1)#dot1q-tunnel enable Switch(config-if-ethernet1/0/1)#service-policy p1 in</pre>

7.1.27. Установка (set)

Синтаксис	<pre>set {s-vid <new-vid> cos <cos-list> drop-precedence <dp-list> internal-priority <inp-list> ip {dscp <dscp-list> precedence <pri-list>} s-tpid <tpid-list> } no set{s-vid cos drop-precedence internal-priority ip {dscp precedence} s-tpid }</pre>	
Параметр	<new-vid>	изменить туннельный VID тега VLAN
	<cos-list>	изменить значения cos для пакетов
	<dp-list>	изменить приоритет отбрасывание
	<inp-list>	изменить внутренний приоритет
	<dscp-list> <pri-list>	изменить значение ip dscp или значение прецедента
	<tpid-list>	изменение значения tpid туннельных пакетов
Состояние по умолчанию	Значение не изменяется	
Режим	Конфигурирования карты классов в карте политик	
Применение	Команда присваивает новые значения cos и vid пакетам, соответствующие карте классов, "no" перед началом команды отменяет действие. Повторно меняет новые значения только для классифицированного трафика, который соответствует критериям сопоставления	



Пример	Установить тег VID внешней VLAN как 3 для пакета, который удовлетворяет правилу класса c2. <pre>Switch(config)#policy-map p1 Switch(config-policy-map-p1)#class c2 Switch(config-policy-map-p1-class-c2)#set s-vid 3 Switch(config-policy-map-p1-class-c2)#exit</pre>



8. КОМАНДЫ ДЛЯ ПРОТОКОЛОВ FORWARD И ARP УРОВНЯ 3

8.1. Команды для настройки интерфейса уровня 3

8.1.1. Описание (description)

Команда	description < text > no description	
Параметр	text	это описательная информация интерфейса VLAN, длина которой не должна превышать 256 символов
Значение по умолчанию	Не настроен	
Режим	Режим интерфейса VLAN	
Руководство по использованию	Информация об описании интерфейса VLAN отображается под настроенной VLAN	
Пример	Настроить информацию описания интерфейса VLAN как test vlan. Switch(config)#interface vlan 2 Switch(config-if-vlan2)#description test vlan	

8.1.2. Интерфейс VLAN (interface vlan)

Команда	interface vlan <vlan-id> no interface vlan <vlan-id>	
Параметр	vlan-id	идентификатор VLAN, присвоенный VLAN, в пределах от 1 до 4094
Значение по умолчанию	Заводские настройки для интерфейса уровня отсутствуют	
Режим	Режим глобальной конфигурации	
Руководство по использованию	эта команда позволяет создать для создания 3-уровневого интерфейса, "no" перед началом команды удаляет указанный интерфейс уровня 3	
Пример	Создать интерфейс VLAN (интерфейс уровня 3). Switch(config)#interface vlan 1	



	Switch(Config-if-Vlan1)#

8.1.3. Удаление интерфейса (no interface IFNAME)

Команда	no interface IFNAME	
Параметр	IFNAME	имя интерфейса
Значение по умолчанию	-	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда используется для удаления интерфейса третьего уровня. Она позволяет справиться с ситуациями, когда имя интерфейса пишется особым образом. IFNAME может соответствовать нескольким вариантам, например, vlan1, Vlan1, v1, V1 и т. д.	
Пример	Удалить интерфейс vlan1. (config)# no interface vlan1	

8.1.4. Вывод данных маршрутизации (show ip route)

Команда	show ip route [database]	
Параметр	database	информация из базы данных
Значение по умолчанию	-	
Режим	Привилегированный режим	
Руководство по использованию	Отображает таблицу маршрутизации ядра, включая: тип маршрута, сеть назначения, маску, адрес следующего узла и интерфейс	
Пример	Показать таблицу маршрутизации. Switch#show ip route Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default	



C 127.0.0.0/8 is directly connected, Loopback tag: 0 Total routes are : 1 item(s)		
Информация, отображаемая на экране	Пояснение	
C –connected	Прямой маршрут, а именно сегмент, непосредственно соединенный с коммутатором уровня 3	
S –static	Статический маршрут, вручную настроенный пользователями	
R - RIP derived	Маршрут RIP, полученный коммутатором уровня 3 по протоколу RIP.	
O - OSPF derived	Маршрут OSPF, полученный от коммутаторов уровня 3 по протоколу OSPF.	
A- OSPF ASE	Маршрут, введенный OSPF	
B- BGP derived	Маршруты BGP, полученные по протоколу BGP.	

8.2. Команды для настройки протоколов IPv4/v6

8.2.1. Очистка статистической информации IP-протокола (clear ip traffic)

Команда	clear ip traffic
Параметр	-
Значение по умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	Команда очищает статистическую информацию о приеме и отправке пакетов для протокола ядра IP, включая статистику приема пакетов, отправки пакетов и сброса пакетов, а также информацию об ошибках при приеме и отправке пакетов для протокола IP, протокола ICMP, протокола TCP и протокола UDP
Пример	Удалить статистической информации IP-протокола. Switch#clear ip traffic



8.2.2. Очищение адресов соседних устройств (clear ipv6 neighbor)

Команда	clear ipv6 neighbors
Параметр	-
Значение по умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	Команда не очищает статические адреса соседних устройств
Пример	Очистить список соседних устройств. Switch#clear ipv6 neighbors

8.2.3. IP-адрес (ip address)

Команда	ip address <ip-address> <mask> [secondary] no ip address [<ip-address> <mask>] [secondary]	
Параметр	ip-address	IP-адрес; десятично-точечная запись;
	mask	маска подсети; десятично-точечная запись;
	secondary	указывает, что IP-адрес настроен, как вторичный IP-адрес
Значение по умолчанию	По умолчанию IP-адрес в системе не задан	
Режим	Режим конфигурации интерфейса VLAN	
Руководство по использованию	Эта команда используется для установки IP-адреса интерфейса VLAN вручную. Если дополнительный параметр secondary не задан, то IP-адрес будет настроен как первичный IP-адрес интерфейса VLAN; если дополнительный параметр secondary задан, это означает, что IP-адрес является вторичным IP-адресом VLAN. Интерфейс VLAN может иметь только один первичный IP-адрес и несколько вторичных IP-адресов. Первичный и вторичный IP-адреса могут использоваться для управления по SNMP/Web/Telnet. Кроме того, для управления по SNMP/Web/Telnet можно использовать как первичный, так и вторичный IP-адреса	



Пример	IP-адрес интерфейса VLAN1 коммутатора установить на 192.168.1.10/24. Switch(Config-if-Vlan1)#ip address 192.168.1.10 255.255.255.0

8.2.4. IPv6-адрес (ipv6 address)

Команда	ipv6 address <ipv6-address>[prefix-length] [eui-64] no ipv6 address <ipv6-address>[prefix-length] [eui-64]	
Параметр	ipv6-address	префикс IPv6-адреса, параметр
	prefix-length	длина префикса IPv6-адреса, которая находится в диапазоне 3-128
	eui-64	означает, что IPv6-адрес генерируется автоматически на основе идентификатора интерфейса eui64
Значение по умолчанию	-	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Префикс адреса IPv6 не может быть адресом multicast или любым другим конкретным адресом IPv6, а разные интерфейсы уровня 3 не могут иметь один и тот же префикс адреса. Для глобального unicast адреса длина префикса должна быть больше или равна 3. Для локального адреса сайта и локального адреса канала длина префикса должна быть больше или равна 10	
Пример	Настроить IPv6-адрес на интерфейсе 3-го уровня VLAN1: префикс 2001:3f:ed8::99, а длина префикса 64. Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64	



8.2.5. Число сообщений оповещения соседних устройств (ipv6 nd dad attempts)

Команда	ipv6 nd dad attempts <value> no ipv6 nd dad attempts	
Параметр	value	число сообщений оповещения соседних устройств, последовательно посылаемых интерфейсом при настройке обнаружения дублированных адресов, значение <value> должно быть в пределах от 0 до 10 NO перед началом команды восстанавливает значение по умолчанию 1
Значение по умолчанию	Номер сообщения запроса по умолчанию равен 1	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Когда конфигурируется IPv6-адрес, необходимо обрабатывать протокол IPv6 Duplicate Address Detection (обнаружение дублированных адресов). Эта команда используется для установки числа сообщений ND, посылаемых при обнаружении дублированных адресов; если value выбрано равным 0, то обнаружение дублированных адресов выполняться не будет	
Пример	Установить число сообщений оповещения соседних устройств, последовательно посылаемых интерфейсом при настройке обнаружения дублированных адресов равным 3. Switch(Config-if-Vlan1)# ipv6 nd dad attempts 3	

8.2.6. Интервал отправки сообщений (ipv6 nd ns-interval)

Команда	ipv6 nd ns-interval <seconds> no ipv6 nd ns-interval	
Параметр	seconds	интервал отправки сообщений запроса соседних устройств, значение <seconds> должно быть в пределах от 1 до 3600 секунд, по в начале команды восстанавливает значение по умолчанию 1 секунда
Значение по умолчанию	По умолчанию интервал времени сообщения запроса составляет 1 секунду	
Режим	Режим конфигурации интерфейса	



Руководство по использованию	Задаваемое значение должно учитывать условия работы на всех участках маршрута, по которым интерфейс посылает сообщения оповещения. В большинстве случаев не рекомендуется использовать очень малый временной интервал
Пример	Установить интервал отправки интерфейсом Vlan1 сообщений запроса соседних устройств равным 8 секунд. Switch(Config-if-Vlan1)#ipv6 nd ns-interval 8

8.2.7. ipv6 neighbor

Команда	ipv6 neighbor <ipv6-address> <hardware-address> interface <interface-type interface-name> no ipv6 neighbor <ipv6-address>		
Параметр	ipv6-address	статический устройства	IPv6-адрес соседнего
	hardware-address	статический устройства	аппаратный адрес соседнего
	interface-type	тип Ethernet,	
	interface-name	имя интерфейса уровня 2	
Значение по умолчанию	Статические адреса соседних устройств в таблице адресов не заданы		
Режим	Режим конфигурации интерфейса		
Руководство по использованию	IPv6- и multicast-адреса, предназначенные для специальных целей, а также локальные адреса, не могут быть использованы в качестве адресов соседних устройств		
Пример	Задать статический адрес соседнего устройства 2001:1:2::4 в порту E0/0/1 и аппаратный MAC-адрес 00-03-0f-89-44-bc. Switch(Config-if-Vlan1)#ipv6 neighbor 2001:1:2::4 00-03-0f-89-44-bc interface Ethernet 1/0/1		



8.2.8. Вывод данных интерфейса VLAN (show ip interface)

Команда	show ip interface [< ifname > vlan <vlan-id>] brief										
Параметр	ifname	имя интерфейса									
	vlan-id	идентификатор VLAN									
Значение по умолчанию	Показывает всю краткую информацию о сконфигурированном интерфейсе уровня 3, если параметр не указан										
Режим	Все режимы										
Руководство по использованию	Эта команда используется для просмотра краткой информации о сконфигурированном интерфейсе уровня 3										
Пример	Просмотреть краткую информацию о конфигурировании интерфейса VLAN1. Switch#show ip interface vlan 1 brief <table><tr><td>Index</td><td>Interface</td><td>IP-Address</td><td>Protocol</td></tr><tr><td>11001</td><td>Vlan1</td><td>192.168.2.1</td><td>up</td></tr></table>			Index	Interface	IP-Address	Protocol	11001	Vlan1	192.168.2.1	up
Index	Interface	IP-Address	Protocol								
11001	Vlan1	192.168.2.1	up								

8.2.9. Вывод данных трафика пакетов IP (show ip traffic)

Команда	show ip traffic
Параметр	-
Значение по умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	Выводит на экран статистику полученных/отправленных пакетов IP, ICMP, TCP, UDP
Пример	Вывести на экран статистику по IP-пакетам. <pre>Switch#show ip traffic</pre> IP statistics: Rcvd: 3249810 total, 3180 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards Frgs: 0 reassembled, 0 timeouts



0 fragment rcvd, 0 fragment dropped
 0 fragmented, 0 couldn't fragment, 0 fragment sent
 Sent: 0 generated, 3230439 forwarded
 0 dropped, 0 no route ICMP statistics:
 Rcvd: 0 total 0 errors 0 time exceeded
 0 redirects, 0 unreachable, 0 echo, 0 echo replies
 0 mask requests, 0 mask replies, 0 quench
 0 parameter, 0 timestamp, 0 timestamp replies
 Sent: 0 total 0 errors 0 time exceeded
 0 redirects, 0 unreachable, 0 echo, 0 echo replies
 0 mask requests, 0 mask replies, 0 quench
 0 parameter, 0 timestamp, 0 timestamp replies
 TCP statistics:
 TcpActiveOpens 0, TcpAttemptFails 0
 TcpCurrEstab 0, TcpEstabResets 0
 TcpInErrs 0, TcpInSegs 3180
 TcpMaxConn 0, TcpOutRsts 3
 TcpOutSegs 0, TcpPassiveOpens 8
 TcpRetransSegs 0, TcpRtoAlgorithm 0
 TcpRtoMax 0, TcpRtoMin 0
 UDP statics:
 UdpInDatagrams 0, UdpInErrors 0
 UdpNoPorts 0, UdpOutDatagrams 0

Информация на экране	Пояснение
IP statistics:	Статистика по IP-пакетам
Rcvd: 3249810 total, 3180 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards	Статистика общего количества полученных пакетов, количество пакетов, достигших локального пункта назначения, количество пакетов с ошибками в заголовке, количество ошибочных адресов, количество пакетов неизвестных протоколов; количество отброшенных пакетов
Frags : 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't	Статистика фрагментации: количество повторно собранных пакетов, тайм-ауты, полученные фрагменты, отброшенные фрагменты, пакеты, которые не могут быть фрагментированы,



	fragment, 0 fragment sent	количество отправленных фрагментов и т. д
	Sent : 0 generated, 0 forwarded 0 dropped, 0 no route	Статистика общего количества отправленных пакетов, включая количество локальных пакетов, переадресованных пакетов, отброшенных пакетов и пакетов без маршрута
	ICMP statistics :	Статистика ICMP-пакетов
	Rcvd : 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Статистика общего количества полученных ICMP-пакетов и классифицированной информации
	Sent : 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Статистика общего количества отправленных ICMP-пакетов и классифицированной информации
	TCP statistics:	Статистика пакетов TCP
	UDP statistics:	Статистика пакетов UDP

8.2.10. Вывод данных интерфейса IPv6 (show ipv6 interface)

Команда	show ipv6 interface {brief <interface-name> }	
Параметр	brief	краткое изложение состояния и конфигурирования IPv6



	interface-name	имя интерфейса уровня 3
Значение по умолчанию	-	
Режим	Привилегированный режим и режим конфигурации	
Руководство по использованию	Если указан только параметр "brief", то отображается информация обо всех L3, также можно указать конкретный интерфейс уровня 3	
Пример	Просмотреть информацию о ipv6 интерфейса vlan1. <pre>Switch#show ipv6 interface Vlan1</pre> Vlan1 is up, line protocol is up, dev index is 2004 Device flag 0x1203(UP BROADCAST ALLMULTI MULTICAST) IPv6 is enabled Link-local address(es): fe80: : 203: fff: fe00: 10 PERMANENT Global unicast address(es): 3001: : 1 subnet is 3001: : 1/64 PERMANENT Joined group address(es): ff02: : 1 ff02: : 16 ff02: : 2 ff02: : 5 ff02: : 6 ff02: : 9 ff02: : d ff02: : 1: ff00: 10 ff02: : 1: ff00: 1 MTU is 1500 bytes ND DAD is enabled, number of DAD attempts is 1 ND managed_config_flag is unset ND other_config_flag is unset ND NS interval is 1 second(s) ND router advertisements is disabled ND RA min-interval is 200 second(s) ND RA max-interval is 600 second(s) ND RA hoplimit is 64 ND RA lifetime is 1800 second(s)	

ND RA MTU is 0



ND advertised reachable time is 0 millisecond(s)

ND advertised retransmit time is 0 millisecond(s)

Информация на экране	Пояснение
Vlan1	Имя интерфейса уровня 3
[up/up]	Состояние интерфейса уровня 3
dev index	Номер внутреннего индекса
fe80::203:fff:fe00:10	Автоматически заданный IPv6-адрес интерфейса уровня 3
3001::1	Сконфигурированный IPv6-адрес интерфейса уровня 3

8.2.11. Вывод данных маршрутизации IPv6 (show ipv6 route)

Команда	show ipv6 route [database]	
Параметр	database	база данных маршрутизатора
Значение по умолчанию	-	
Режим	Привилегированный режим и режим конфигурации	
Руководство по использованию	Команда show ipv6 route отображает только таблицу маршрутизации ядра IPv6 (таблица маршрутизации в tcpip), а в базе данных отображаются все маршрутизаторы, кроме локального	
Пример	Отобразить таблицу маршрутизации IPv6. Switch#show ipv6 route IPv6 Routing Table Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP Timers: Uptime C :: 1/128 via :: , Loopback, 02: 55: 37 tag: 0	
	Информация на экране	Пояснение
	IPv6 Routing Table	Статус таблицы маршрутизации IPv6



	Codes: K - kernel route, C - Сокращенное обозначение connected, S - static, R - RIP, каждой записи O - OSPF, I - IS-IS, B - BGP > - selected route

8.2.12. Вывод данных устройств IPv6 (show ipv6 neighbors)

Команда	show ipv6 neighbors [{vlan ethernet} interface - number interface-name address <ipv6address>]					
Параметр	{vlan ethernet} interface - number		задает поиск на основе интерфейса			
	ipv6address		задает поиск на основе IPv6-адреса. Если параметры не заданы, на экран выводится вся таблица адресов соседних устройств			
Значение по умолчанию	-					
Режим	Привилегированный режим и режим конфигурации					
Руководство по использованию	Команда выводит на экран таблицу адресов соседних устройств. Если параметры не заданы, на экран выводится вся таблица адресов соседних устройств					
Пример	Проверить информацию таблицы соседних устройств ipv6. Switch#show ipv6 neighbors IPv6 neighbour unicast items: 2, valid: 1, matched: 1, incomplete: 0, delayed: 0. manage items: 0 IPv6 Address Hardware Addr					
	IPv6 Address	Hardware Addr	Interface	Port	State	Age-time(sec)
	fe80::d8e4:a662:88e4:dc24	00-e0-4c-21-00-34	Vlan1	Ethernet1/0/18	reachable	563
	IPv6 neighbour table: 1 entries					



Информация на экране	Пояснения
IPv6 Address	IPv6-адрес соседнего устройства
Hardware Addr	MAC-адрес соседнего устройства
Interface	Имя выходного интерфейса
Port	Имя выходного интерфейса.
State	Состояние соседнего устройства (досягаемое, стабильное, задержка, тестируется, постоянное, неполное, неизвестное)

8.2.13. Вывод данных трафика IPv6 (show ipv6 traffic)

Команда	show ipv6 traffic
Параметр	-
Значение по умолчанию	-
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Позволяет вывести на экран статистическую информацию о передаче IPv6-пакетов
Пример	Вывести на экран статистическую информацию о передаче IPv6-пакетов. <pre>Switch#show ipv6 traffic</pre> IPv6 statistics: Rcvd: 27 total, 21 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards Frgs: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent Sent: 24 generated, 0 forwarded 0 dropped, 0 no route ICMPv6 statistics: Rcvd: 21 total, 0 errors 0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems 0 echo requests, 0 echo replies



0 group queries, 0 group responses, 0 group reduces 0 router solicits, 0 router adverts, 0 redirects 9 neighbor solicits, 12 neighbor adverts Sent: 24 total, 0 errors 0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems 0 echo requests, 0 echo replies 0 group queries, 0 group responses, 0 group reduces 0 router solicits, 0 router adverts, 0 redirects 9 neighbor solicits, 9 neighbor adverts TCP statistics: Rcvd: 0 total segments, 0 errors Sent: 0 total segments, 0 retransmitted segments UDP statics: Rcvd: 0 total, 0 errors, 0 no port Sent: 0 total	
Информация на экране	Пояснения
IPv6 statistics:	Статистика IPv6-данных
Rcvd: 27 total, 21 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards	Статистика принятых IPv6-пакетов
Frag: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	Статистика фрагментирования IPv6-пакетов
Sent: 24 total, 0 errors 0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems 0 echo requests, 0 echo replies 0 group queries, 0 group responses, 0 group reduces 0 router solicits, 0 router adverts, 0 redirects 9 neighbor solicits, 9 neighbor adverts	Статистика переданных IPv6-пакетов



8.2.14. IP-адрес маршрутизации (ip route)

Команда	ip route {< ip-prefix > < mask > < ip-prefix >/< prefix-length >} {< gateway-address > null0} [< distance >] no ip route { <ip-prefix> <mask> <ip-prefix > /<prefix-length> } [<gateway-address> undefined<gateway-interface>undefinedundefined] [undefinedundefined<distance>undefinedundefined]undefined	
Параметр	ip-prefix	Адрес назначения маршрутизации, например: 1.1.1.1
	mask	Маска подсети адреса назначения маршрутизации, например, 255.255.255.0
	prefix-length	Префикс адреса назначения при маршрутизации
	gateway-address	Адрес IP следующего хопа, например, 1.1.1.1
	null0	Интерфейс передачи
	distance	Приоритет маршрутизации, диапазон размеров: 1-255
Значение по умолчанию	Статическая маршрутизация по умолчанию имеет приоритет 1	
Режим	Режима глобальной конфигурации	
Руководство по использованию	Эта команда используется для настройки статической маршрутизации коммутатора. При настройке следующего хопа статического маршрута, указывая IP-адрес следующего хопа в пакете маршрутизации, можно использовать адрес и интерфейс передачи	
Пример	Добавить статическую маршрутизацию в коммутатор. Switch(config)#ip route 192.168.2.8/24 null0	



8.3. Команды для настройки ARP

8.3.1. Записи ARP (arp)

Команда	arp <ip_address> <mac_address> {interface [ethernet] < portName >} no arp <ip_address>	
Параметр	ip_address	IP-адрес в том же поле, что и адрес интерфейса
	mac_address	MAC-адрес
	ethernet	Ethernet-порт
	portName	имя порта второго уровня
Значение по умолчанию	Статическая запись ARP не задана	
Режим	Режим настройки интерфейса VLAN	
Руководство по использованию	Команда позволяет создавать на коммутаторе статические записи ARP	
Пример	Создать статическую запись ARP для интерфейса VLAN1. Switch(Config-if-Vlan1)#arp 1.1.1.1 00-03-0f-f0-12-34 interface eth 1/0/2	

8.3.2. Удаление содержимого таблицы ARP (clear arp-cache)

Команда	clear arp-cache
Параметр	-
Значение по умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	Команда очищает содержимое таблицы ARP
Пример	Удалить содержимое таблицы ARP. Switch#clear arp-cache



8.3.3. Очищение данных трафика ARP (clear arp traffic)

Команда	clear arp traffic
Параметр	-
Значение по умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	Команда позволяет очистить статистическую информацию сообщений ARP коммутатора. бокс-коммутаторов, эта команда очищает только статистику ARP-сообщений, полученных и отправленных с текущей карты
Пример	Удалить статистическую информацию сообщений ARP коммутатора. Switch#clear arp traffic

8.3.4. Вывод текущей таблицы ARP (show arp)

Команда	show arp [< ipaddress >] [< vlan-id >] [< hw-addr >] [type {static dynamic}] [count] [vrf word]	
Параметр	ipaddress	заданный IP-адрес
	vlan-id	идентификатор Vlan
	hw-addr	для записи с указанным MAC-адресом
	static	запись ARP является статической
	dynamic	запись ARP является динамической
	count	число записей ARP
	vrf word	заданное имя vrf
Значение по умолчанию	-	
Режим	Привилегированный режим	
Руководство по использованию	Позволяет вывести на экран содержимое текущей таблицы ARP: IP- и MAC-адреса, тип аппаратуры, имя интерфейса и т. д	



Пример

Вывести на экран информацию о текущем содержимом таблицы ARP.

Switch#show arp

ARP Unicast Items: 7, Valid: 7, Matched: 7, Verifying: 0, Incomplete: 0.

Failed: 0, None: 0

Address	Hardware Addr	Interface	Port	Flag
50.1.1.6	00-0a-eb-51-51-38	Vlan50	Ethernet1/0/11	Dynamic
50.1.1.9	00-00-00-00-00-09	Vlan50	Ethernet1/0/1	Static
150.1.1.2	00-00-58-fc-48-9f	Vlan150	Ethernet1/0/4	Dynamic

Информация на экране	Пояснения
Total arp items	Общее число записей ARP.
Valid	Число записей ARP, согласующихся с условиями фильтра и атрибутами легальных состояний.
Matched	Число записей ARP, согласующихся с условиями фильтра.
Verifying	Число записей ARP, используемых при верификации правильности ARP
InCompleted	Число записей ARP, для которых запрос ARP был послан, но ответа на него не поступило
Failed	Число записей ARP в состоянии сбоя
None	Число записей ARP в состоянии начала поиска
Address	IP-адрес записи ARP
Hardware Address	MAC-адрес записи ARP
Interface	Интерфейс уровня 3, соответствующий записи ARP
Port	Физический интерфейс (уровня 2), соответствующий записи ARP
Flag	Указывает, какой является запись ARP статической или динамической



8.3.5. Вывод трафика сообщений ARP (show arp traffic)

Команда	show arp traffic
Параметр	-
Значение по умолчанию	-
Режим	Привилегированный режим и конфигурирования
Руководство по использованию	Позволяет вывести на экран статистическую информацию получаемых и отправляемых сообщений ARP
Пример	Вывести на экран текущую статистику ARP. <pre>Switch#show arp traffic</pre> ARP statistics: Rcvd: 0 request, 0 response Sent: 0 request, 0 response

8.4. Команды для настройки защиты от arp-сканирования

8.4.1. Включение защиты от ARP-сканирования (anti-arpscan enable)

Команда	anti-arpscan enable no anti-arpscan enable
Параметр	-
Значение по умолчанию	Функция защиты от ARP-сканирования выключена
Режим	Режим глобальной конфигурации конфигурирования
Руководство по использованию	При удаленном управлении коммутатором, например, по telnet, пользователи должны до включения функции защиты от ARP-сканирования установить в uplink-порту режим супербезопасного порта (Super Trust port) для того, чтобы предотвратить выключение порта при приеме слишком большого числа ARP-сообщений. После выключения функции защиты от ARP-сканирования порт вернется к атрибутам по умолчанию и станет небезопасным портом
Пример	Включить функцию защиты от ARP-сканирования коммутатора. <pre>Switch(config)#anti-arpscan enable</pre>



8.4.2. Пороговое значение защиты от ARP-сканирования (anti-arpscan port-based threshold)

Команда	anti-arpscan port-based threshold <threshold-value> no anti-arpscan port-based threshold	
Параметр	threshold-value	пороговое значение скорости поступления пакетов, в пределах от 2 до 200
Значение по умолчанию	10 пакетов в секунду	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Пороговое значение защиты от ARP-сканирования на основе портов должно быть больше порогового значения защиты от ARP-сканирования на основе IP-адресов, иначе защита от ARP-сканирования на основе IP-адресов даст сбой	
Пример	Задать пороговое значение защиты от ARP-сканирования на основе портов, равное 10 пакетов/секунда. Switch(config)#anti-arpscan port-based threshold 10	

8.4.3. Пороговое значение защиты от ARP-сканирования на основе IP-адресов (anti-arpscan ip-based threshold)

Команда	anti-arpscan ip-based threshold <threshold-value> no anti-arpscan ip-based threshold	
Параметр	threshold-value	пороговое значение скорости поступления пакетов, в пределах от 2 до 200
Значение по умолчанию	3 пакета в секунду	
Режим	Режим глобальной конфигурации конфигурирования	
Руководство по использованию	Пороговое значение защиты от ARP-сканирования на основе портов должно быть больше порогового значения защиты от ARP-сканирования на основе IP-адресов, иначе защита от ARP-сканирования на основе IP-адресов даст сбой	
Пример	Задать пороговое значение защиты от ARP-сканирования на основе IP-адресов 6 пакетов/секунду. Switch(config)#anti-arpscan ip-based threshold 6	



8.4.4. Настройка безопасного порта (anti-arpscan trust)

Команда	anti-arpscan trust [port supertrust-port] no anti-arpscan trust [port supertrust-port]
Параметр	-
Значение по умолчанию	Все порты считаются небезопасными
Режим	Режим настройки порта
Руководство по использованию	Если порт настроен безопасным, функция защиты от ARP-сканирования не будет работать на этом порту даже в том случае, если скорость поступления ARP-сообщений превысит заданное пороговое значение, порт не будет закрыт, но небезопасные IP-адреса этого порта будут продолжать проверяться. Если порт объявлен супербезопасным, то никакая защита от ARP-сканирования не будет работать. Если порт выключен защитой от ARP-сканирования, то после объявления его безопасным портом он будет снова включен
Пример	Объявить порт ethernet 0/0/5 коммутатора безопасным портом. Switch(Config-If-Ethernet4/5)# anti-arpscan trust port

8.4.5. Настройка безопасного IP-адреса (anti-arpscan trust ip)

Команда	anti-arpscan trust ip <ip-address> [<netmask >] no anti-arpscan trust ip < ip-address> [<netmask >]	
Параметр	ip-address	безопасный IP-адрес
	netmask	маска сети IP-адреса
Значение по умолчанию	Все IP-адреса считаются небезопасными. По умолчанию используется маска 255.255.255.255	
Режим	Режим глобальной конфигурации конфигурирования	
Руководство по использованию	Если порт объявлен безопасным, функция защиты от ARP-сканирования не будет работать на этом порту даже в том случае, если скорость поступления ARP-сообщений превысит заданное пороговое значение, порт при этом не закрывается. Если порт был выключен защитой от ARP-сканирования, его трафик будет немедленно восстановлен	



Пример	Объявить 192.168.1.0/24 безопасным IP-адресом. Switch(config)#anti-arp scan trust ip 192.168.1.0 255.255.255.0

8.4.6. Включение автоматического восстановления (anti-arp scan recovery enable)

Команда	anti-arp scan recovery enable no anti-arp scan recovery enable	
Параметр	-	
Значение по умолчанию	Функция автоматического восстановления включена	
Режим	Режим глобальной конфигурации конфигурирования	
Руководство по использованию	Эта функция позволяет восстановить нормальный режим работы после закрытия порта или отключения IP на определенный период времени	
Пример	Включить на коммутаторе функцию автоматического восстановления. Switch(config)#anti-arp scan recovery enable	

8.4.7. Время автоматического восстановления (anti-arp scan recovery time)

Команда	anti-arp scan recovery time <seconds> no anti-arp scan recovery time	
Параметр	seconds	время автоматического восстановления, в пределах от 5 до 86 400 секунд
Значение по умолчанию	300 секунд	
Режим	Режим глобальной конфигурации конфигурирования	
Руководство по использованию	команда позволяет задать время автоматического восстановления, по в начале команды восстанавливает значение времени, заданное по умолчанию	
Пример	Задать время автоматического восстановления 3600 секунд. Switch(config)#anti-arp scan recovery time 3600	



8.4.8. Включение регистрации защиты от ARP-сканирования (anti-arpscan log enable)

Команда	anti-arpscan log enable no anti-arpscan log enable
Параметр	-
Значение по умолчанию	Функция регистрации защиты от ARP-сканирования включена
Режим	Режим глобальной конфигурации конфигурирования
Руководство по использованию	Когда функция регистрации системных сообщений защиты от ARP-сканирования включена, пользователям доступна подробная информация о выключенных и автоматически восстановленных портах, заблокированных и восстановленных IP-адресах. Регистрация имеет уровень значимости "Предупреждение"
Пример	Включить функцию регистрации защиты от ARP-сканирования на коммутаторе. Switch(config)#anti-arpscan log enable

8.4.9. Включение SNMP Trap защиты от ARP-сканирования (anti-arpscan trap enable)

Команда	anti-arpscan trap enable no anti-arpscan trap enable
Параметр	-
Значение по умолчанию	Функция SNMP Trap защиты от ARP-сканирования выключена
Режим	Режим глобальной конфигурации конфигурирования
Руководство по использованию	Когда функция SNMP Trap защиты от ARP-сканирования включена, пользователи будут принимать сообщение Trap, если защитой от ARP-сканирования выключен или восстановлен порт, либо заблокирован или восстановлен IP-адрес
Пример	Включить в коммутаторе функцию SNMP Trap защиты от ARP-сканирования. Switch(config)#anti-arpscan trap enable



8.4.10. Вывод данных защиты от ARP-сканирования (show anti-arpscan)

Команда	show anti-arpscan [trust [ip port supertrust-port] prohibited [ip port]]																																																																																				
Параметр	-																																																																																				
Значение по умолчанию	Выводит на дисплей информацию о портах – являются ли они безопасными, включены или выключены. Если порт закрыт, будет показано время, в течение которого он находится в выключенном состоянии. На дисплей выводится информация о всех безопасных и заблокированных IP																																																																																				
Режим	Привилегированный режим																																																																																				
Руководство по использованию	Команду "show anti-arpscan trust port" следует использовать, если необходимо проверить безопасные порты. Перезагрузка происходит по тому же правилу																																																																																				
Пример	Проверить работу защиты от ARP-сканирования после ее включения. Switch#show anti-arpscan Total port: 28 <table><tr><th>Name</th><th>Port-property</th><th>beShut</th><th>shutTime(seconds)</th></tr><tr><td>Ethernet1/0/1</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/2</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/3</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/4</td><td>trust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/5</td><td>trust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/6</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/7</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/8</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/9</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/10</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/11</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/12</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/13</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/14</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/15</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/16</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/17</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/18</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/19</td><td>untrust</td><td>N</td><td>0</td></tr><tr><td>Ethernet1/0/20</td><td>untrust</td><td>N</td><td>0</td></tr></table>	Name	Port-property	beShut	shutTime(seconds)	Ethernet1/0/1	untrust	N	0	Ethernet1/0/2	untrust	N	0	Ethernet1/0/3	untrust	N	0	Ethernet1/0/4	trust	N	0	Ethernet1/0/5	trust	N	0	Ethernet1/0/6	untrust	N	0	Ethernet1/0/7	untrust	N	0	Ethernet1/0/8	untrust	N	0	Ethernet1/0/9	untrust	N	0	Ethernet1/0/10	untrust	N	0	Ethernet1/0/11	untrust	N	0	Ethernet1/0/12	untrust	N	0	Ethernet1/0/13	untrust	N	0	Ethernet1/0/14	untrust	N	0	Ethernet1/0/15	untrust	N	0	Ethernet1/0/16	untrust	N	0	Ethernet1/0/17	untrust	N	0	Ethernet1/0/18	untrust	N	0	Ethernet1/0/19	untrust	N	0	Ethernet1/0/20	untrust	N	0
Name	Port-property	beShut	shutTime(seconds)																																																																																		
Ethernet1/0/1	untrust	N	0																																																																																		
Ethernet1/0/2	untrust	N	0																																																																																		
Ethernet1/0/3	untrust	N	0																																																																																		
Ethernet1/0/4	trust	N	0																																																																																		
Ethernet1/0/5	trust	N	0																																																																																		
Ethernet1/0/6	untrust	N	0																																																																																		
Ethernet1/0/7	untrust	N	0																																																																																		
Ethernet1/0/8	untrust	N	0																																																																																		
Ethernet1/0/9	untrust	N	0																																																																																		
Ethernet1/0/10	untrust	N	0																																																																																		
Ethernet1/0/11	untrust	N	0																																																																																		
Ethernet1/0/12	untrust	N	0																																																																																		
Ethernet1/0/13	untrust	N	0																																																																																		
Ethernet1/0/14	untrust	N	0																																																																																		
Ethernet1/0/15	untrust	N	0																																																																																		
Ethernet1/0/16	untrust	N	0																																																																																		
Ethernet1/0/17	untrust	N	0																																																																																		
Ethernet1/0/18	untrust	N	0																																																																																		
Ethernet1/0/19	untrust	N	0																																																																																		
Ethernet1/0/20	untrust	N	0																																																																																		



Ethernet1/0/21	untrust	N	0
Ethernet1/0/22	untrust	N	0
Ethernet1/0/23	untrust	N	0
Ethernet1/0/24	untrust	N	0
Ethernet1/0/25	untrust	N	0
Ethernet1/0/26	untrust	N	0
Ethernet1/0/27	untrust	N	0
Ethernet1/0/28	untrust	N	0
No prohibited IP.			
192.168.1.0 255.255.255.0			

8.5. Команды для настройки защиты от подмены ARP

8.5.1. Автоматическое обновление ARP (ip arp-security updateprotect)

Команда	ip arp-security updateprotect no ip arp-security updateprotect
Параметр	-
Значение по умолчанию	Автоматическое обновление таблиц ARP включено
Режим	Режим глобальной конфигурации конфигурирования, режим настройки интерфейсов
Руководство по использованию	Если автоматическое обновление таблицы ARP запрещено, будут отбрасываться пакеты ARP, конфликтующие с текущей записью ARP (например, с тем же IP-адресом, но отличающимся MAC-адресом или портом), остальные пакеты будут приниматься для обновления таймера времени жизни или для создания новой записи). В результате текущая запись ARP не изменится, вместе с тем будет продолжаться и обучение
Пример	Запретить автоматическое обновление таблицы ARP. Switch(Config-if-Vlan1)#ip arp-security updateprotect. Switch(config)#ip arp-security updateprotect



8.5.2. Автоматическое обучение ARP (ip arp-security learnprotect)

Команда	ip arp-security learnprotect no ip arp-security learnprotect
Параметр	-
Значение по умолчанию	Обучение ARP включено
Режим	Режим глобальной конфигурации конфигурирования/режим настройки интерфейсов
Руководство по использованию	Команда позволяет отключить автоматическое обучение и обновление ARP. В отличие от защиты, даваемой командой ip arp-security updateprotect, эта команда устанавливает таймер даже в том случае, если коммутатор продолжает посылать сообщения запросов и ответов
Пример	Запретить функцию обучения ARP для версии IPv4. Switch(config)# ip arp-security learnprotect

8.5.3. Преобразование записей ARP (ip arp-security convert)

Команда	ip arp-security convert
Параметр	-
Значение по умолчанию	-
Режим	Режим глобальной конфигурации конфигурирования/режим настройки интерфейсов
Руководство по использованию	Команда позволяет преобразовать все динамические записи ARP в статические, что в сочетании с выключением автоматического обучения может помешать привязке ARP. Сразу после ввода команда прекращает свое действие
Пример	Преобразовать все динамические записи ARP в статические. Switch(config)#ip arp -security convert

8.5.4. Удаление записей ARP (clear ip arp dynamic)

Команда	clear ip arp dynamic
Параметр	-



Значение по умолчанию	-
Режим	Режим настройки интерфейсов
Руководство по использованию	Команда позволяет очистить динамические записи перед привязкой ARP. Сразу после ввода команда прекращает свое действие
Пример	Очистить динамические записи ARP на интерфейсе. Switch(Config-if-Vlan1)#clear ip arp dynamic

8.5.5. Удаление записей ND (clear ipv6 nd dynamic)

Команда	clear ipv6 nd dynamic
Параметр	-
Значение по умолчанию	-
Режим	Режим интерфейса VLAN
Руководство по использованию	Команда позволяет очистить таблицу динамических записей перед привязкой ND. Сразу после выполнения команда прекращает свое действие
Пример	Очистить все динамические ND в портах. Switch(Config-if-Vlan1)#clear ipv6 nd dynamic

8.6. Команды для настройки защиты ARP (ARP Guard)

8.6.1. Настройка ip-адреса (arp-guard ip)

Команда	arp-guard ip <addr> no arp-guard ip <addr>		
Параметр	Addr	защищенный IP-адрес в десятичном представлении с точками	
Состояние по умолчанию	Адрес ARP GUARD не задан		
Режим	Режим настройки порта		



Руководство по использованию	После настройки адреса ARP GUARD, ARP-сообщения, принятые от портов, на которых сконфигурирован ARP GUARD, будут фильтроваться. Если IP-адреса источников ARP-сообщений согласуются с адресами ARP GUARD, заданными на этом порту, они будут считаться подмененными ARP-сообщениями и вместо отправки на CPU коммутатора или пересылки будут отброшены. Для каждого порта можно задать 16 адресов ARP GUARD
Пример	Задать адрес ARP GUARD 100.1.1.1 для порта Ethernet0/0/1 switch(config)#interface ethernet1/0/1 switch(Config-If-Ethernet 1/0/1)#arp-guard ip 100.1.1.1

8.7. Команды для настройки самообращенных запросов (Gratuitous ARP)

8.7.1. Включение самообращенного ARP и настройка интервала обновления (ip gratuitous-arp)

Команда	ip gratuitous-arp [< interval-time >] no ip gratuitous-arp	
Параметр	interval-time	интервал обновления запросов gratuitous ARP, диапазон значений — от 5 до 1200 с, значение по умолчанию 300 с
Состояние по умолчанию	По умолчанию запросы Gratuitous ARP выключены	
Режим	Режим глобальной конфигурации и режим конфигурации интерфейса vlan	
Руководство по использованию	Если запросы gratuitous ARP включены в режиме глобальной конфигурации, все интерфейсы уровня 3 коммутатора способны посылать запросы gratuitous ARP. Если запросы gratuitous ARP включены в режиме настройки интерфейсов, их сможет посылать только указанный интерфейс. При конфигурировании gratuitous ARP, интервал обновления, заданный в режиме настройки интерфейсов, имеет больший приоритет, чем этот же интервал, но заданный в режиме глобальной конфигурации	
Пример	Включить запросы gratuitous ARP в режиме глобальной конфигурации, установить интервал обновления 400 секунд. Switch#config Switch(config)#ip gratuitous-arp 400	



8.7.2. Отображение конфигурации самообращенного ARP (show ip gratuitous-arp)

Команда	show ip gratuitous-arp [interface vlan <vlan-id>]	
Параметр	vlan-id	идентификатор VLAN
Состояние по умолчанию	-	
Режим	Все режимы конфигурации	
Руководство по использованию	Позволяет вывести на дисплей информацию о настройках запросов gratuitous ARP	
Пример	Вывести на дисплей информацию о настройках запросов gratuitous ARP. Switch#show ip gratuitous-arp Gratuitous ARP send is Global enabled, Interval-Time is 300(s) Gratuitous ARP send enabled interface vlan information: Name Interval-Time(seconds) Vlan1 400 Vlan10 350	

8.8. Команды настройки функции контроля динамических ARP (Dynamic ARP Inspection)

8.8.1. Включение функции ARP (ip arp inspection)

Команда	ip arp inspection vlan <vlan-id> no ip arp inspection vlan <vlan-id>	
Параметр	vlan-id	vlan, в котором включена функция динамической проверки ARP
Состояние по умолчанию	Отключено	
Режим	Режим глобальной конфигурации	
Руководство по использованию	После настройки функции динамической проверки ARP в режиме глобальной конфигурации администратор может перехватывать, записывать и отбрасывать пакеты данных ARP, содержащие недопустимые MAC-адреса/IP-адреса	



Пример	Включите функцию динамической проверки ARP для vlan10. <pre>Switch(config)# Switch(config)#ip arp inspection vlan 10 Switch(config)#exit</pre>

8.8.2. Настройка доверенного порта (ip arp inspection trust)

Команда	ip arp inspection trust no ip arp inspection trust
Параметр	-
Состояние по умолчанию	По умолчанию все порты являются ненадежными
Режим	Режим конфигурации порта
Руководство по использованию	Если эта команда задана в режиме порта, сконфигурированный порт не будет проверять входящие ARP-пакеты и будет пересылать их напрямую. Если ARP-пакеты поступают с ненадежного порта, коммутатор будет пересылать только разрешенные пакеты данных. Неразрешенные данные будут отброшены, данное действие будет записано
Пример	Настроить порт 1/0/1 в качестве доверенного. <pre>Switch(config)# Switch(config)#in e 1/0/1 Switch(config-if-ethernet1/0/1)#ip arp inspection trust</pre>

8.8.3. Частота получаемых запросов (ip arp inspection limit-rate)

Команда	ip arp inspection limit-rate <rate> no ip arp inspection limit-rate	
Параметр	rate	настроенная ограниченная скорость передачи ARP-пакета для ненадежного порта, единица измерения pps
Состояние по умолчанию	Скорость передачи ARP-пакетов для доверенных и ненадежных портов не ограничена	
Режим	Режим конфигурации порта	



Руководство по использованию	Команда позволяет ограничить скорость передачи ARP-пакетов ненадежного порта. Скорость пересылки разрешенных пакетов данных ARP находится в ограниченном диапазоне
Пример	Настроить скорость передачи ARP-пакета на ненадежном порту 1/0/1 равной 100pps. Switch(config)# Switch(config)#interface eth 1/0/1 Switch(config-if-ethernet1/0/1)# ip arp inspection limit-rate 100 Switch(config-if-ethernet1/0/1)#exit



9. DHCP

9.1. Команды для настройки DHCP

9.1.1. Настройка загрузочного файла (bootfile)

Синтаксис	Bootfile <filename> no bootfile	
Параметр	<filename>	имя импортируемого файла, допустимая длина не более 255 символов
По умолчанию	Отсутствует	
Режим	Режим настройки пула адресов DHCP	
Руководство по использованию	Позволяет задать имя файла, импортируемого клиентом. Обычно эта команда используется для рабочих станций, не имеющих жесткого диска, которым при загрузке им необходимо загрузить файл с настройками сервера. Эта команда используется вместе с командой "next server"	
Пример	Путь и имя импортируемого файла "temp\nos.img" Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#bootfile \temp\nos.img	

9.1.2. Удаление записи привязки IP-адреса (clear ip dhcp binding)

Синтаксис	clear ip dhcp binding (<A.B.C.D> all)	
Параметр	<A.B.C.D>	IP-адрес, имеющий запись о привязке, в десятичном формате
	all	все IP-адреса, имеющие запись о привязке
По умолчанию	Отсутствует	
Режим	Привилегированный режим	



Руководство по использованию	Команда "show ip dhcp binding" применяется для просмотра привязок IP-адресов к аппаратным DHCP клиентам. Если DHCP-сервер получил информацию о том, что DHCP-клиент по некоторым причинам не использует присвоенный IP-адрес до того, как истекает срок жизни адреса, то DHCP-сервер не удаляет автоматически информацию привязки. Администратор системы может использовать эту команду для удаления такой привязки IP-адреса к аппаратному адресу клиента вручную. Если выбран параметр "all", то записи автоматической привязки будут удалены, а соответствующие адреса пула DHCP перераспределены
Пример	Удалить все записи привязок IP-адресов к аппаратным адресам Switch#clear ip dhcp binding all

9.1.3. Удаление записи обнаруженных конфликтов адресов (clear ip dhcp conflict)

Синтаксис	clear ip dhcp binding (<A.B.C.D> all)	
Параметр	<A.B.C.D>	IP-адрес, для которого имеется запись о конфликте
	all	все адреса, для которых имеются записи о конфликте
По умолчанию	Отсутствует	
Режим	Привилегированный режим	
Руководство по использованию	Команда "show ip dhcp conflict" позволяет проверить, какие IP-адреса конфликтуют. Используя команду "clear ip dhcp conflict" можно удалить записи обнаруженных конфликтов адресов. Параметр "all" в команде удаляет все записи о конфликте в журнале. После того, как записи будут удалены, соответствующие адреса будут снова доступны для распределения DHCP-сервером	
Пример	Администратор сети обнаружил, что для адреса 10.1.128.160 имеется запись о конфликте, и он больше не используется пользователями, поэтому требуется удалить запись о конфликте адресов из журнала. Switch#clear ip dhcp conflict 10.1.128.160	

9.1.4. Удаление статистики DHCP-сервера (clear ip dhcp server statistics)

Синтаксис	clear ip dhcp server statistics
Параметр	Отсутствует



По умолчанию	Отсутствует
Режим	Привилегированный режим
Руководство по использованию	Статистику подсчета DHCP можно просмотреть с помощью команды “show ip dhcp server statistics”, выводится вся информация. С помощью команды “clear ip dhcp server statistics” можно переустановить счетчик DHCP-сервера
Пример	Переустановить счетчик DHCP-сервера. Switch#clear ip dhcp server statistics

9.1.5. Настройка идентификатора пользователя (client-identifier)

Синтаксис	client-identifier <unique-identifier> no client-identifier	
Параметр	<unique-identifier>	идентификатор пользователя в шестнадцатеричном формате
По умолчанию	Отсутствует	
Режим	Режим настройки пула адресов DHCP	
Руководство по использованию	Команда используется вместе с командой “host” при привязке адреса вручную. Если запрашиваемый идентификатор клиента совпадает с идентификатором, указанным в команде, DHCP-сервер присваивает клиенту IP-адрес, указанный в команде “host”	
Пример	При привязке адреса вручную задать привязку IP-адреса 10.1.128.160 к пользователю с уникальным id 00-10-5a-60-af-12. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#client-identifier 00-10-5a-60-af-12 Switch(dhcp-1-config)#host 10.1.128.160 24	

9.1.6. Настройка шлюза по умолчанию (default-router)

Синтаксис	default-router <A.B.C.D> [<A.B.C.D>[...<A.B.C.D>]] no default-router	
Параметр	<A.B.C.D>	IP-адрес, в десятичном формате
По умолчанию	Шлюз для DHCP-клиентов не задан	



Режим	Режим настройки пула адресов DHCP
Руководство по использованию	IP-адрес шлюза (или шлюзов), назначаемых по умолчанию, должен принадлежать той же подсети, что и IP-адрес DHCP-клиента. Коммутатор поддерживает до 8 адресов шлюзов. Адрес шлюза, присвоенный первым, имеет наивысший приоритет, поэтому адрес 1 имеет наивысший приоритет, адрес 2 - второй по значимости и т. д.
Пример	Задать шлюзы, назначаемые по умолчанию для DHCP-клиентов: 10.1.128.2 и 10.1.128.100. <pre>Switch#config Switch(config) # ip dhcp pool 1 Switch(dhcp-1-config)#default-router 10.1.128.2 10.1.128.100</pre>

9.1.7. Настройка DNS-серверов (dns-server)

Синтаксис	dns-server <A.B.C.D> [<A.B.C.D>[...<A.B.C.D>]] no dns-server	
Параметр	<A.B.C.D>	IP-адрес, в десятичном формате
По умолчанию	DNS-сервер для DHCP-клиентов не задан	
Режим	Режим настройки пула адресов DHCP	
Руководство по использованию	Может быть задано до 8 адресов DNS-серверов. Адрес DNS-сервера, присвоенный первым, имеет наивысший приоритет, поэтому адрес 1 имеет наивысший приоритет, адрес 2 – второй по значимости и т. д.	
Пример	Установить 10.1.128.2 в качестве адреса DNS-сервера для DHCP-клиентов. Switch#config <pre>Switch(config) # ip dhcp pool 1 Switch(dhcp-1-config)#dns-server 10.1.128.2</pre>	

9.1.8. Доменное имя для DHCP-клиентов (domain-name)

Синтаксис	domain-name <domain> no domain-name	
Параметр	<domain>	доменное имя, допустимая длина не более 255 символов
По умолчанию	Отсутствует	



Режим	Режим настройки пула адресов DHCP
Руководство по использованию	Позволяет задать доменное имя для клиента
Пример	Задать "node1.qtech.ru" в качестве доменного имени DHCP-клиента. <pre>Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#domain-name node1.qtech.ru</pre>

9.1.9. Аппаратный адрес пользователя (hardware-address)

Синтаксис	<pre>hardware-address <hardware-address> [Ethernet IEEE802 <type-number>] no hardware-address</pre>	
Параметр	<hardware-address>	аппаратный адрес в шестнадцатеричном формате;
	Ethernet IEEE802	тип протокола Ethernet,
	<type-number>	Номер RFC, определенный для типов протоколов, в диапазоне от 1 до 255, например, 0 для Ethernet и 6 для IEEE 802
По умолчанию	Задан тип протокола Ethernet	
Режим	Режим настройки пула адресов DHCP	
Руководство по использованию	Команда используется вместе с командой "host" при привязке адреса вручную. Если запрашиваемый аппаратный адрес клиента совпадает с аппаратным адресом, указанным в команде, DHCP-сервер присваивает клиенту IP-адрес, указанный в команде "host"	
Пример	При привязке вручную задать IP-адрес 10.1.128.160 для пользователя с аппаратным адресом 00-00-e2-3a-26-04. <pre>Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#hardware 00-00-e2-3a-26-04 Switch(dhcp-1-config)#host 10.1.128.160 24</pre>	



9.1.10. Настройка IP-адреса для пользователя (host)

Синтаксис	host < address > [< mask > < prefix-length >]	
Параметр	<address>	IP-адрес в десятичном формате
	<prefix-length>	маска задана префиксом. Например, маска 255.255.255.0 имеет префикс “24”, а маска 255.255.255.252 — префикс “30”
По умолчанию	Отсутствует	
Режим	Режим настройки пула адресов DHCP	
Руководство по использованию	Если при настройке IP-адреса маска и префикс не заданы и в пуле IP-адресов информация о маске отсутствует, система присвоит маску автоматически в соответствии с классом IP-адреса. При привязке адресов вручную, эта команда используется вместе с командами “hardware address” или “client-identifier”. Если запрашиваемый аппаратный адрес клиента совпадает с указанным в команде идентификатором или аппаратным адресом, DHCP-сервер присваивает клиенту IP-адрес, указанный в команде “host”	
Пример	При привязке вручную задать IP-адрес 10.1.128.160 для пользователя с аппаратным адресом 00-10-5a-60-af-12. <pre>Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12 Switch(dhcp-1-config)#host 10.1.128.160 24</pre>	

9.1.11. Регистрация конфликтов адресов (ip dhcp conflict logging)

Синтаксис	ip dhcp conflict logging no ip dhcp conflict logging
Параметр	отсутствуют
По умолчанию	Ведение записи о конфликтах адресов включено
Режим	Режим глобальной конфигурации



Руководство по использованию	Когда включено ведение записи, то после обнаружения конфликта адресов сервером DHCP конфликтующий адрес будет занесен в журнал. Адреса, для которых обнаружен конфликт, не будут динамически выделяться DHCP-сервером до тех пор, пока не будут удалены записи о конфликте
Пример	Выключить создание записей DHCP-сервером. Switch#config Switch(config)#no ip dhcp conflict logging

9.1.12. Выключение сервисов DHCP на интерфейсе (ip dhcp disable)

Синтаксис	ip dhcp disable no ip dhcp disable	
Параметр	отсутствуют	
По умолчанию	Выключено	
Режим	Настройка портов	
Руководство по использованию	После отключения портом служб DHCP, все пакеты DHCP, отправленные портом, отбрасываются	
Пример	Порт отключает службы DHCP. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#ip dhcp disable	

9.1.13. Удаление динамически распределяемых адресов (ip dhcp excluded-address)

Синтаксис	ip dhcp excluded-address <low-address> [<high-address>] no ip dhcp excluded-address <low-address> [<high-address>]	
Параметр	<low-address>	начальный IP-адрес
	<high-address>	конечный IP-адрес
По умолчанию	Можно исключить только один индивидуальный адрес	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда позволяет исключить один или несколько последовательных адресов в пуле из числа адресов, распределяемых динамически. Исключенные адреса могут быть использованы администратором для других целей
Пример	Зарезервировать адрес 1.1.1.1 из числа распределяемых динамически. Switch#config Switch(config)#ip dhcp excluded-address 1.1.1.1

9.1.14. Пул DHCP-адресов (ip dhcp pool)

Синтаксис	ip dhcp pool <name> no ip dhcp pool <name>	
Параметр	<name>	имя пула адресов, допустимая длина не более 32 символов
По умолчанию	Отсутствует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда используется для настройки пула DHCP-адресов в глобальном режиме конфигурации	
Пример	Задать пул адресов с именем "1". Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#	

9.1.15. Ping-обнаружение конфликтов на DHCP-сервере (ip dhcp conflict ping-detection enable)

Синтаксис	ip dhcp conflict ping-detection enable no ip dhcp conflict ping-detection enable	
Параметр	Отсутствует	
По умолчанию	ping-обнаружение конфликтов на DHCP-сервере выключено	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Перед тем, как включать Ping-обнаружение конфликтов, необходимо включить регистрацию конфликтующих адресов, поскольку если эта функция отключена, Ping-обнаружение конфликтов также будет отключено. Если клиенту не удалось принять сообщения с Ping-запросами (например, они заблокированы межсетевым экраном), эта функция проверит соответствие назначенного IP-адреса локальной записи ARP: если назначенный IP-адрес имеет соответствующую запись ARP, то существует конфликт адресов, в противном случае, IP-адрес назначается клиенту
Пример	Включить Ping-обнаружение конфликта. Switch#config Switch(config)#ip dhcp conflict ping-detection enable

9.1.16. Количество направляемых ping-пакетов (ip dhcp ping packets)

Синтаксис	ip dhcp ping packets <request-num> no ip dhcp ping packets	
Параметр	<request num>	количество посылаемых сообщений запросов ping при обнаружении конфликта
По умолчанию	Отправляется не более двух запросов	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Устанавливает максимальное количество ping-пакетов (Echo Request), которые DHCP-сервер будет отправлять в случае Ping-обнаружения конфликтов. По умолчанию количество запросов — 2. "no" в начале команды восстанавливает значение по умолчанию	
Пример	Установить число посылаемых ping-запросов (Echo Request) при обнаружении конфликтов на сервере DHCP равным 3. Switch#config Switch(config)#ip dhcp ping packets 3	

9.1.17. Тайм-аут ping-пакета (ip dhcp ping timeout)

Синтаксис	ip dhcp ping timeout <timeout-value> no ip dhcp ping timeout	
Параметр	<timeout-value>	<timeout-value> период ожидания ответного сообщения после каждого сообщения запроса Ping при Ping-обнаружении конфликта



По умолчанию	500 миллисекунд
Режим	Режим глобальной конфигурации
Руководство по использованию	Позволяет задать время ожидания (в мс) ответного сообщения (Echo Request), которое должно приниматься после отправки каждого ping-пакета при обнаружении конфликта на DHCP сервере. По умолчанию, задано время ожидания 500 миллисекунд. Действие "no" в данной команде восстанавливает значение по умолчанию
Пример	Установить период ожидания (в мс) каждого ответного сообщения (Echo Request) при Ping-обнаружении конфликта на DHCP-сервере равным 600 мс. Switch#config Switch(config)#ip dhcp ping timeout 600

9.1.18. Срок аренды адресов пула (lease)

Синтаксис	lease (<days> [<hours>][<minutes>] infinite) no lease	
Параметр	<days>	количество дней, от 0 до 365
	<hours>	количество часов, от 0 до 23
	<minutes>	количество минут, от 0 до 59
	infinite	постоянное использование
По умолчанию	Продолжительность аренды адресов составляет 1 сутки	
Режим	Режим настройки пула адресов DHCP	
Руководство по использованию	Протокол DHCP позволяет распределять сетевые адреса динамически, вместо распределения их на постоянной основе, что обуславливает срок жизни адресов. Настройки срока жизни адресов должны учитывать условия работы сети: слишком большой срок аренды адресов ухудшает гибкость протокола DHCP, но при этом слишком короткий срок жизни адресов приводит к увеличению сетевого трафика и потребления ресурсов. По умолчанию срок жизни адресов составляет 1 сутки	
Пример	Задать срок аренды адресов пула DHCP с именем "1" 3 дня 12 часов 30 минут. Switch#config Switch(config)#ip dhcp pool sd	



	Switch(dhcp-sd-config)#lease 3 12 30

9.1.19. Максимальное время аренды адреса (max-lease-time)

Синтаксис	max-lease-time (<days> [<hours>][<minutes>] infinite) no max-lease-time	
Параметр	<days>	количество дней, от 0 до 365
	<hours>	количество часов, от 0 до 23
	<minutes>	количество минут, от 0 до 59
	infinite	постоянное использование
По умолчанию	Срок аренды адресов составляет 1 сутки	
Режим	Режим настройки пула адресов DHCP	
Руководство по использованию	Эта команда используется для пакетов запроса DHCP, содержащих опцию 51. Если время аренды (запрос адреса пользователем) превышает установленное максимальное время аренды, время аренды, назначенное этому адресу DHCP-сервером, будет равно установленному максимальному времени аренды. Если время аренды, запрошенное пользователем, меньше максимального заданного времени аренды, то время аренды, которое DHCP-сервер назначает адресу, равно времени аренды, запрошенному пользователем. Максимальное время аренды может быть установлено администратором в соответствии с фактическими условиями сети, по умолчанию максимальное время аренды составляет 1 день	
Пример	Установить максимальное время аренды пула адресов DHCP "1" на 3 дня 12 часов и 30 минут. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#max-lease-time 3 12 30	

9.1.20. Адрес WINS-сервера (netbios-name-server)

Синтаксис	netbios-name-server <address1> [address2[...<address8>]] no netbios-name-server	
Параметр	<address1>...<address8>	IP-адрес, в десятичном формате



По умолчанию	WINS-сервер не включен
Режим	Режим настройки пула адресов DHCP
Руководство по использованию	Команда позволяет задать для клиента WINS-сервер. Может быть задано до 8 адресов WINS-серверов. Адрес WINS-сервера, присвоенный первым, имеет наивысший приоритет. Поэтому адрес 1 имеет высший приоритет, адрес 2 – второй по значимости и т. д
Пример	Задать адрес сервера пула DHCP «1» как 192.168.1.1. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#netbios-name-server 192.168.1.1

9.1.21. Тип узла для порта (netbios-node-type)

Синтаксис	netbios-node-type {b-node h-node m-node p-node <type-number>} no netbios-node-type	
Параметр	b-node	узел вещания
	h-node	гибридный узел, который может осуществлять вещание после разрыва соединения точка-точка
	m-node	гибридный узел, после вещания может устанавливать соединение точка-точка
	p-node	узел точка-точка
	<type-number>	тип узла в шестнадцатеричной форме, от 0 до FF
По умолчанию	Тип клиентского узла не задан	
Режим	Режим настройки пула адресов DHCP	
Руководство по использованию	Если тип клиентского узла задан, рекомендуется установить его h-node, чтобы после разрыва соединения точка-точка он осуществлял вещание	
Пример	Задать тип узла клиента пула 1 как узла, осуществляющего вещание. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#netbios-node-type-node	



9.1.22. Диапазон присваиваемых адресов (network-address)

Синтаксис	network-address <network-number> [<mask> <prefix-length>] no network-address	
Параметр	<network-number>	номер сети
	<mask>	маска подсети в десятичном формате
	<prefix-length>	маска в форме префикса. Например, маска 255.255.255.0 в префиксе - это «24», а маска 255.255.255.252 в префиксе - это «30». Примечание: При использовании DHCP-сервера маска пула должна быть больше или равна маске IP-адреса интерфейса уровня 3 соответствующем сегменте
По умолчанию	Если маска не задана, то по умолчанию будет присвоена маска, соответствующая классу адреса	
Режим	Режим настройки пула адресов DHCP	
Руководство по использованию	Команда позволяет задать диапазон адресов, который DHCP-сервер может использовать в процессе динамического распределения адресов; один пул адресов может соответствовать только одному сегменту. Эта команда исключает использование привязки адресов вручную с помощью команд "hardware address" и "host"	
Пример	Задать присваиваемый адрес в пуле как 10.1.128.0/24. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#network-address 10.1.128.0 24	

9.1.23. Адрес сервера хранения файла, импортируемого клиентом (next-server)

Синтаксис	next-server <address1>[<address2>[...<address8>]] no next-server	
Параметр	<address1>...<address 8>	IP-адреса в десятичном формате
По умолчанию	Отсутствует	
Режим	Режим настройки пула адресов DHCP	



Руководство по использованию	Команда позволяет задать адрес сервера, на котором хранится файл, импортируемый клиентом. Обычно эта команда используется для рабочих станций, не имеющих жесткого диска, которым при загрузке им необходимо загрузить файл с сервера. Эта команда используется вместе с командой "bootfile"
Пример	Задать адрес сервера хостинга 10.1.128.4. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#next-server 10.1.128.4

9.1.24. Настройка параметра сети (option)

Синтаксис	option <code> {ascii <string> hex <hex> ipaddress <ipaddress> } no option <code>	
Параметр	<code>	код сетевого параметра
	<string>	строка ASCII, длиной не более 255 символов
	<hex>	шестнадцатеричное значение, большее 510, с четной длиной
	<ipaddress>	IP-адрес в десятичном формате, может быть задано до 63 IP-адресов
По умолчанию	отсутствуют	
Режим	Режим настройки пула адресов DHCP	
Руководство по использованию	В коммутаторе имеются команды для настройки сетевых параметров, а также различные команды, полезные для настройки сети в соответствии с требованиями пользователя. Определения опциональных кодов подробно описаны в RFC2123	
Пример	Задать адрес WWW-сервера как 10.1.128.240. Switch#config Switch(config)# ip dhcp pool 1 Switch(dhcp-1-config)#option 72 ip 10.1.128.240	



9.1.25. Включение службы DHCP (service dhcp)

Синтаксис	service dhcp no service dhcp
Параметр	Отсутствует
По умолчанию	Служба DHCP выключена
Режим	Режим глобальной конфигурации
Руководство по использованию	В службу DHCP входят DHCP-сервер и функция DHCP-relay. Когда служба DHCP включена, включены и DHCP-сервер, и DHCP-relay. Коммутатор может назначать IP-адреса DHCP-клиентам и включать функцию DHCP-relay только тогда, когда включен DHCP-сервер
Пример	Включить DHCP-сервер. Switch#config Switch(config)#service dhcp

9.1.26. Вывод информации о привязках (show ip dhcp binding)

Синтаксис	show ip dhcp binding [[<ip-addr>] [type {all manual dynamic}] [count]]	
Параметр	<ip-addr>	заданный IP-адрес
	all	все типы привязок (введенные вручную и назначенные динамически)
	manual	привязки, введенные вручную
	dynamic	привязки, назначенные динамически
	count	отображение статистики привязок адресов в записях DHCP
По умолчанию	Отсутствует	
Режим	Привилегированный режим и режим конфигурации	
Руководство по использованию	Позволяет вывести на экран информацию привязок IP-MAC	



Пример	Switch# show ip dhcp binding		
	IP address Hardware address Lease expiration Type		
	10.1.1.233 00-00-E2-3A-26-04 Infinite Manual		
	10.1.1.254 00-00-E2-3A-5C-D3 60 Automatic		
	Информация, отображаемая на экране		Пояснение
	IP address	IP-адрес, присвоенный DHCP-клиенту	
	Hardware address	MAC-адрес DHCP-клиента	
	Lease expiration	Период времени, в течение которого DHCP-клиент может владеть IP-адресом	
	Type	Тип присвоения: привязка вручную или динамическое распределение	

9.1.27. Вывод информации по конфликтующим адресам (show ip dhcp conflict)

Синтаксис	show ip dhcp conflict		
Параметр	отсутствуют		
По умолчанию	отсутствуют		
Режим	Привилегированный режим и режим конфигурации		
Руководство по использованию	Позволяет вывести на дисплей информацию по конфликтующим адресам		
Пример	Switch# show ip dhcp conflict		
	IP Address Detection method Detection Time		
	10.1.1.1 Ping FRI JAN 02 00: 07: 01 2002		
	Информация, отображаемая на экране		Пояснение
	IP address	Конфликтующий IP-адрес	
	Detection method	Метод обнаружения конфликта	
	Detection Time	Время и дата обнаружения конфликта.	



9.1.28. Отображение информации состоянии опции (show ip dhcp relay information option)

Синтаксис	show ip dhcp relay information option
Параметр	отсутствуют
по умолчанию	отсутствуют
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Команда позволяет вывести на экран информацию о состоянии опции 82 для DHCP Relay
Пример	Switch#show ip dhcp relay information option ip dhcp server relay information option(i.e. option 82) is enabled ip dhcp relay information option(i.e. option 82) is enabled

9.1.29. Вывести статистику для DHCP-сервера (show ip dhcp server statistics)

Синтаксис	show ip dhcp server statistics																
Параметр	отсутствуют																
По умолчанию	отсутствуют																
Режим	Привилегированный режим и режим конфигурации																
Руководство по использованию	Позволяет вывести на дисплей статистику для всех DHCP-пакетов DHCP-сервера																
Пример	<pre>Switch# show ip dhcp server statistics</pre> <table> <tr> <td>Address pools</td><td>1</td></tr> <tr> <td>Database agents</td><td>0</td></tr> <tr> <td>Automatic bindings</td><td>0</td></tr> <tr> <td>Manual bindings</td><td>0</td></tr> <tr> <td>Conflict bindings</td><td>0</td></tr> <tr> <td>Expired bindings</td><td>0</td></tr> <tr> <td>Malformed message</td><td>0</td></tr> <tr> <td>Message Message</td><td>Received</td></tr> </table>	Address pools	1	Database agents	0	Automatic bindings	0	Manual bindings	0	Conflict bindings	0	Expired bindings	0	Malformed message	0	Message Message	Received
Address pools	1																
Database agents	0																
Automatic bindings	0																
Manual bindings	0																
Conflict bindings	0																
Expired bindings	0																
Malformed message	0																
Message Message	Received																



	BOOTREQUEST	0
	DHCPDISCOVER	0
	DHCPREQUEST	0
	DHCPDECLINE	0
	DHCPRELEASE	0
	DHCPINFORM	0
	Message	Send
	BOOTREPLY	0
	DHCPOFFER	0
	DHCPACK	0
	DHCPNAK	0
	DHCPRELAY	0
	DHCPFORWARD	0
	Switch#	
	Информация, отображаемая на экране	Пояснение
	Address pools	Число сконфигурированных пулов адресов DHCP
	Database agents	Число агентов баз данных
	Automatic bindings	Количество адресов, привязанных автоматически
	Manual bindings	Количество адресов, привязанных вручную
	Conflict bindings	Количество конфликтующих адресов
	Expired bindings	Количество адресов, у которых истек срок жизни
	Malformed message	Количество сообщений об ошибках
	Message Received	Статистика по принятым пакетам DHCP
	BOOTREQUEST	Общее число принятых пакетов



	DHCPDISCOVER	Количество DHCPDISCOVER	пакетов
	DHCPREQUEST	Количество DHCPREQUEST	пакетов
	DHCPDECLINE	Количество DHCPDECLINE	пакетов
	DHCPRELEASE	Количество DHCPRELEASE	пакетов
	DHCPINFORM	Количество DHCPINFORM	пакетов
	Message Send	Статистика по переданным пакетам DHCP	
	BOOTREPLY	Общее число переданных пакетов	
	DHCPOFFER	Количество DHCPOFFER	пакетов
	DHCPACK	Количество DHCPACK	пакетов
	DHCPNAK	Количество DHCPNAK	пакетов
	DHCPRELAY	Количество DHCPRELAY	пакетов
	BOOTREPLY	Общее число переданных пакетов	

9.1.30. Подавление широковещательной рассылки DHCP (ip dhcp broadcast suppress)

Синтаксис	ip dhcp broadcast suppress no ip dhcp broadcast suppress
Параметр	отсутствуют
По умолчанию	Отключение
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда подключает функцию подавления широковещательной рассылки DHCP, "No" в начале команды отключает функцию подавления пересылки широковещательных пакетов DHCP, а именно, отбрасывание или копирование широковещательных пакетов DHCP на CPU



Пример	Включить функцию подавления широковещания DHCP. Switch# config Switch(config)#ip dhcp broadcast suppress

9.1.31. Настройка VLAN источника и назначения перенаправления (ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist>)

Синтаксис	ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist> no ip dhcp relay share-vlan	
Параметр	<vlanid>	VLAN ID для vlan назначения перенаправления
	<vlanlist>	перечень sub-vlan
По умолчанию	Отсутствует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет указать sub-vlan для share-vlan. "no" в начале команды отменяет sub-vlan. vlan назначения перенаправления share-vlan может включать множество sub-vlan, но sub-vlan соответствует только одному share-vlan. Когда DHCP-запрос поступает на устройство уровня 2 DHCP Relay, оно сначала определяет, есть ли VLAN с интерфейсом уровня 3 для приема пакета. Если в пакете есть интерфейс уровня 3, этот интерфейс используется для обработки DHCP Relay, в противном случае, если VLAN является sub-vlan для share-vlan, для обработки DHCP Relay используется интерфейс уровня 3 share-vlan	
Пример	Switch#config Switch(config)#ip dhcp relay share-vlan 2 sub-vlan 2-4	

9.1.32. Настройка DHCP-relay для перенаправления пакетов (ip forward-protocol udp bootps)

Синтаксис	ip forward-protocol udp bootps
	no ip forward-protocol udp bootps
Параметр	отсутствуют
По умолчанию	Перенаправление широковещательных пакетов UDP выключено
Режим	Режим глобальной конфигурации



Руководство по использованию	Указывает DHCP relay перенаправлять UDP-пакеты на порту. Команда "no ip forward-protocol udp bootps" отменяет действие. Адрес, на который перенаправляются пакеты задается командой "ip helper-address", которая описана далее
Пример	Настроить направление пакетов DHCP на 192.168.1.5. <pre>Switch#config Switch(config)#ip forward-protocol udp bootps Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip helper-address 192.168.1.5</pre>

9.1.33. Адрес DHCP сервера для перенаправления (ip helper-address)

Синтаксис	<pre>ip helper-address <ip-address> no ip helper-address <ip-address></pre>	
Параметр	ip-address	IP-адреса в десятичном формате
По умолчанию	отсутствуют	
Режим	Настройка портов	
Руководство по использованию	Устанавливает адрес назначения для DHCP relay для пересылки широковещательных пакетов UDP на порт; Команда "no ip helper-address <ip-address>" отменяет эту функцию. Адрес сервера пересылки DHCP relay соответствует порту пересылки UDP, т. е. DHCP relay пересылает соответствующие UDP-пакеты только на соответствующий сервер, а не все UDP-пакеты на все серверы. Когда эта команда выполняется после команды "ip forward-protocol udp <port>", адрес пересылки, настроенный этой командой, получает UDP-пакеты из <port>. Для настройки следует использовать комбинацию команды "ip forward-protocol udp <port>" и этой команды	
Пример	<pre>Switch#config Switch(config)#ip forward-protocol udp bootps Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip helper-address 192.168.2.5</pre>	



9.1.34. Отображение протокола перенаправления (show ip forward-protocol)

Синтаксис	show ip forward-protocol
Параметр	отсутствуют
По умолчанию	отсутствуют
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Отображает настроенный идентификатор порта для протокола, поддерживающего пересылку широковещательных пакетов, т.е. идентификатор порта для пересылки пакетов DHCP
Пример	Switch#show ip forward-protocol Forward protocol (UDP port): 67(active)

9.1.35. Вывод адреса сервера ретрансляции (show ip helper-address)

Синтаксис	show ip helper-address
Параметр	отсутствуют
По умолчанию	отсутствуют
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Отображает взаимосвязь между ID порта протокола (который может пересылать широковещательные пакеты), интерфейсом (который поддерживает пересылку) и IP-адресом назначения пересылки
Пример	Switch#show ip helper-address Forward protocol Interface Forward server 67(active) Vlan1 192.168.2.5



9.1.36. Удаление записи привязки IPv6-адреса (clear ipv6 dhcp binding)

Синтаксис	clear ipv6 dhcp binding [<ipv6-address>] [pd <ipv6-prefix prefix-length>]	
Параметр	<ipv6-address>	IPv6-адрес записи привязки
	<ipv6-prefix prefix-length>	IPv6-префикс с записью привязки; Позволяет удалить запись привязки указанного IPv6-адреса или все такие записи
По умолчанию	отсутствуют	
Режим	Привилегированный режим	
Руководство по использованию	Команда позволяет удалить указанную запись привязки адресов DHCPv6 или все записи привязки адресов IPv6. Информацию о привязке IPv6-адресов DHCPv6 можно вывести на экран с помощью команды show ipv6 dhcp binding. Если DHCPv6-клиент не использует выделенный DHCPv6 IPv6-адрес, но время жизни IPv6-адреса не заканчивается, DHCPv6-сервер не будет удалять привязку для этого адреса. В этом случае можно вручную удалить информацию о привязке адреса с помощью этой команды; если нет дополнительных параметров, эта команда удалит всю информацию о привязке адреса и затем переназначит все адреса и префиксы в пуле адресов DHCPv6	
Пример	Удалить все записи о привязке IPv6-адреса и префикса Switch#clear ipv6 dhcp binding	

9.1.37. Удаление информации о конфликтах ipv6-адресов (clear ipv6 dhcp conflict)

Синтаксис	clear ipv6 dhcp conflict [address]	
Параметр	address	определенный адрес с записью о конфликте, без указания адреса удаляются все записи о конфликтах
По умолчанию	отсутствуют	
Режим	Привилегированный режим	



Руководство по использованию	Команда удаляет адреса с записью о конфликтах в журнале. С помощью команды <code>show ipv6 dhcp conflict</code> пользователь может проверить, какие IP-адреса конфликтуют. Данная команда позволяет пользователю удалить записи о конфликтах адресов. Если не указан конкретный адрес, будут удалены записи о конфликтах для всех адресов в журнале. После очистки записей эти адреса могут снова использоваться сервером DHCPv6.
Пример	При проверке журнала записей конфликтов администратор сети обнаружил, что адрес 2001::1 с записью о конфликте не используется, нужно удалить запись из файлов конфликтов адреса. Switch#clear ipv6 dhcp conflict 2001::1

9.1.38. Удаление статистики ipv6 DHCP-сервера (clear ipv6 dhcp statistics)

Синтаксис	clear ipv6 dhcp statistics	
Параметр	отсутствуют	
По умолчанию	отсутствуют	
Режим	Привилегированный режим	
Руководство по использованию	Позволяет удалить статистику пакетов DHCPv6, обнуляет счетчик статистики пакетов DHCPv6. Используя команду <code>show ipv6 dhcp statistics</code> пользователь может просмотреть информацию счетчика пакетов DHCPv6, вся информация выводится как сводная информация. С помощью этой команды можно очистить счетчик для удобной проверки отладки.	
Пример	Сбросить счетчик пакетов DHCPv6. Switch#clear ipv6 dhcp statistics	

9.1.39. DNS-серверы для DHCPv6-клиентов (dns-server)

Синтаксис	dns-server <ipv6-address> no dns-server <ipv6-address>	
Параметр	<ipv6-address>	IPv6-адрес DNS-сервера
По умолчанию	отсутствуют	
Режим	Режим конфигурации пула адресов DHCPv6	



Руководство по использованию	Команда задает IPv6-адреса DNS-сервера для DHCPv6-клиентов; "no" в начале команды удаляет конфигурацию DNS. Для каждого пула адресов можно задать не более трех DNS-серверов, причем адреса DNS-серверов должны быть действительными IPv6-адресами
Пример	Задать адрес DNS-сервера DHCPv6-клиента как 2001: da8: : 1. Switch(dhcp-1-config)#dns-server 2001: da8: : 1

9.1.40. Доменное имя для DHCPv6-клиентов (domain-name)

Синтаксис	domain-name <domain-name> no domain-name <domain-name>	
Параметр	<domain-name>	доменное имя, допустимая длина – не более 32 символов
По умолчанию	Параметр доменного имени пула адресов по умолчанию не настроен	
Режим	Режим конфигурации пула адресов DHCPv6	
Руководство по использованию	Команда позволяет задать доменное имя для DHCPv6-клиентов. "no" в начале команды удаляет доменное имя. Может быть задано до 3 доменных имен для каждого пула адресов	
Пример	Задать node1.qtech.ru в качестве доменного имени DHCPv6-клиента. Switch(dhcp-1-config)#domain-name node1.qtech.ru	

9.1.41. Исключение адреса из раздачи (excluded-address)

Синтаксис	excluded-address <ipv6-address> no excluded-address <ipv6-address>	
Параметр	<ipv6-address>	IPv6-адрес, который будет исключен из распределения хостам в пуле адресов
По умолчанию	Отключено	
Режим	Режим конфигурации пула адресов DHCPv6	



Руководство по использованию	Позволяет указать IPv6-адрес, который необходимо исключить из пула адресов и исключить его из числа адресов, распределяемых хостам. "no" в начале команды отменяет настройку. Эта команда позволяет зарезервировать указанный адрес из распределения адресов DHCPv6
Пример	Исключить 2001: da8: 123: : 1 из распределения DHCPv6-адресов. Switch(config)#excluded-address 2001: da8: 123: : 1

9.1.42. Настройка IPv6-адреса (ipv6 address)

Синтаксис	ipv6 address <prefix-name> <ipv6-prefix/prefix-length> no ipv6 address <prefix-name> <ipv6-prefix/prefix-length>	
Параметр	<prefix-name>	строка длиной не более 32 символов, обозначающая или вручную конфигурирующая имя префикса адреса, определенного в пуле префиксов
	<ipv6-prefix/prefix-length>	оставшаяся часть IPv6-адреса, исключая префикс адреса и его длину
По умолчанию	Глобальный адрес не задан	
Режим	Настройка портов	
Руководство по использованию	Позволяет настроить определенный интерфейс на использование префиксов делегирования для распределения адресов. Форма "no" этой команды отключает использование префиксов для распределения адресов. IPv6-адреса состоит из двух частей: < prefix-name> и < ipv6-prefix>/<prefix-length >. Если включено объявление маршрутизации, будут объявляться первые 64 бита адресов. Адрес, сгенерированный комбинацией < prefix-name > и < ipv6-prefix/prefix-length > будет удален и объявление префикса будет отключено. Разрешается настроить только один < ipv6-prefix/prefix-length > для одного имени префикса	
Пример	Если имя префикса my-prefix обозначает 2001: da8: 221: : /48, применить следующую команду для добавления адреса 2001: da8: 221: 2008: : 2008 в интерфейс VLAN1. Switch(Config-if-Vlan1)# ipv6 address my-prefix 0: 0: 0: 2008: : 2008/64	



9.1.43. Сконфигурировать клиент назначения префикса (ipv6 dhcp client pd)

Синтаксис	ipv6 dhcp client pd <prefix-name> [rapid-commit] no ipv6 dhcp client pd	
Параметр	<prefix-name>	строка длиной не более 32 символов, которая указывает имя префикса
	rapid-commit	Если указан параметр rapid-commit и на сервере назначения префикса включена функция rapid-commit, сервер назначения префикса будет отвечать клиенту непосредственно сообщением REPLY. Запрос на делегирование префикса будет осуществляться путем однократного обмена сообщениями
По умолчанию	DHCPv6-клиент назначения префикса выключен	
Режим	Настройка портов	
Руководство по использованию	Данная команда используется для настройки DHCPv6-клиента назначения префикса на определенном интерфейсе. "no" в начале команды отключает назначение префиксов DHCPv6-клиента и удаляет выделенный префикс адреса. Данная команда используется для настройки клиента назначения префикса на указанном интерфейсе. Интерфейс с подключенным делегированием префикса будет посылать пакеты SOLICIT для того, чтобы получить префикс адреса с сервера. Если префикс получен правильно, префикс адреса в глобальном пуле адресов может быть использован командой ipv6 address для генерации действительного IPv6-адреса. Эта команда является взаимоисключающей с командами ipv6 dhcp server и ipv6 dhcp relay destination. Если клиент делегирования префиксов для интерфейса отключен, то префикс адреса, полученный от этого интерфейса через делегирование префиксов, будет удален из глобального пула адресов. Кроме того, адреса интерфейсов, сгенерированные клиентом делегирования префикса, также удаляются, а объявления о маршрутах, использующие этот префикс, отключаются. Если общие префиксы были настроены с помощью команды ipv6 general-prefix, тот же префикс, полученный от делегирования префикса, отвергается	
Пример	Switch(Config-if-Vlan1)#ipv6 dhcp client pd ClientA rapid-commit	



9.1.44. Назначить требуемый клиентом префикс (ipv6 dhcp client pd hint)

Синтаксис	ipv6 dhcp client pd hint <prefix prefix-length> no ipv6 dhcp client pd hint <prefix prefix-length>	
Параметр	<prefix prefix-length>	требуемый клиентом префикс и его длина
По умолчанию	По умолчанию в системе нет такой конфигурации	
Режим	Настройка портов	
Руководство по использованию	Позволяет назначить требуемый клиентом префикс и его длину. "no" в начале команды удалит этот префикс и его длину с указанного интерфейса. Система определяет префикс и его длину на интерфейсе для клиента. Если на интерфейсе включена функция запроса "client prefix-proxy", а на коммутаторе включена функция "hint", при назначении сервером префикса, пользователь имеет преимущественное право на префикс и длину префикса, который он запрашивает. В системе разрешен только один префикс подсказки "hint"	
Пример	Switch(vlan-1-config)#ipv6 dhcp client pd hint 2001: : /48	

9.1.45. Создание пула адресов DHCPv6 (ipv6 dhcp pool)

Синтаксис	ipv6 dhcp pool <poolname> no ipv6 dhcp pool <poolname>	
Параметр	<poolname>	имя пула адресов в DHCPv6, длина не более 32 символов
По умолчанию	DHCPv6 пул не создан	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Данная команда позволяет войти в режим конфигурации DHCPv6-пула адресов, в котором можно настроить соответствующие параметры, такие как префикс адреса, адреса DNS, имя домена. "no" в начале команды удалит конфигурацию пула адресов. Команду следует применять в режиме глобальной конфигурации, при успешном применении выполняется переход в режим конфигурации пула адресов DHCPv6. Чтобы удалить настроенный пул адресов, удаляются привязки интерфейсов, связанные с пулом адресов, и связанные с ними привязки адресов	



Пример	Чтобы определить пул адресов, задать имя 1. Switch#config Switch(config)#ipv6 dhcp pool 1

9.1.46. Адрес перенаправления запросов для DHCPv6 relay (ipv6 dhcp relay destination)

Синтаксис	ipv6 dhcp relay destination {[<ipv6-address>] [interface { < interface-name > vlan <1-4096> }] } no ipv6 dhcp relay destination { [<ipv6-address>] [interface { < interface-name > vlan < 1-4096 > }] }	
Параметр	<ipv6-address>	адрес, куда механизм DHCPv6 relay будет перенаправлять запросы
	<interface-name>	имя интерфейса перенаправления DHCPv6-запросов
	<1-4096>	идентификатор VLAN
Если < ipv6-address > является глобальным unicast-адресом, то параметр интерфейса не задается; Если < ipv6-address > является локальным адресом, параметр интерфейса задать необходимо; Адресом назначения для DHCPv6-сервера будет групповой адрес ALL_DHCP_Servers (FF05: : 1: 3) , если задан только параметр интерфейса		
по умолчанию	Адрес назначения для перенаправления DHCPv6 не настроен	
Режим	Настройка портов	
Руководство по использованию	Позволяет сконфигурировать адрес, куда функция DHCPv6 relay будет перенаправлять DHCPv6-запросы от клиентов, в качестве адреса назначения должен быть указан адрес внешнего DHCPv6-relay или DHCPv6-сервера. "no" в начале команды удаляет конфигурацию. Данная команда используется для настройки DHCPv6 relay для указанного интерфейса, адрес должен быть адресом другого DHCPv6 relay или адресом DHCPv6-сервера. Для одного интерфейса можно настроить не более трех адресов перенаправления. Следует отметить, что DHCPv6 relay перестает работать только в том случае, если все конфигурации адресов назначения перенаправления были удалены. Эта команда является взаимоисключающей для команд "ipv6 dhcp server" и "ipv6 dhcp client pd"	
Пример	Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ipv6 dhcp relay destination 2001:da8::1	



9.1.47. Включение функции DHCPv6 сервера (ipv6 dhcp server)

Синтаксис	ipv6 dhcp server <poolname> [preference <value>] [rapid-commit] [allow-hint] no ipv6 dhcp server <poolname>	
Параметр	<poolname>	имя создаваемого пула адресов DHCPv6
	<value>	Приоритет сервера DHCPv6, чем больше значение, тем выше приоритет, диапазон: 0-255, по умолчанию 0
	rapid-commit	Сервер DHCPv6 отправляет пакет REPLY клиенту сразу после получения пакета SOLICIT
	allow-hint	ожидаемое клиентом значение будет добавлено в его пакет запроса
По умолчанию	Пул адресов DHCPv6 на основе порта не настроен	
Режим	Настройка портов	
Руководство по использованию	Команда настраивает пул адресов, который будет выделяться сервером DHCPv6 через указанный интерфейс. "no" в начале команды удаляет настройку пула адресов. Эта команда настраивает пул адресов DHCPv6, который применяется сервером DHCPv6 для указанного интерфейса, а также дополнительные параметры. Одна VLAN может связывать множество пулов адресов DHCPv6 и назначать адреса для пакетов запроса DHCPv6 при прямом и ретрансляционном делегировании	
Пример	Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ipv6 dhcp server PoolA preference 80 rapid-commit allow-hint	

9.1.48. Настройка общего префикса адресов (ipv6 general-prefix)

Синтаксис	ipv6 general-prefix <prefix-name> <ipv6-prefix/prefix-length> no ipv6 general-prefix <prefix-name>	
Параметр	<prefix-name>	<prefix-name> строка длиной не более 32 символов, для использования в качестве имени общего префикса IPv6
	<ipv6-prefix/prefix-length>	<ipv6-prefix/prefix-length> определяется как общий префикс IPv6



По умолчанию	Общий префикс IPv6 по умолчанию не настроен
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда для конфигурирования общего префикса IPv6 адресов. "no" в начале команды отменяет настройку. Если IPv6-префикс задан, то при генерации IPv6-адреса будет использоваться указанный данной командой префикс. Обычно общий префикс используется для префикса IPv6 предприятия, и при вводе IPv6-адреса пользователям достаточно добавить к имени общего префикса суффикс адреса of. Сконфигурированный IPv6-префикс будет зарезервирован в пуле общих префиксов. Может быть сконфигурировано до 8 общих префиксов. При попытке удалить сконфигурированное имя общего префикса операция завершится неудачей, если какой-либо интерфейс использует сконфигурированный префикс. Имя префикса может иметь только один общий префикс. Общие префиксы не могут использовать одно и то же определение префикса с префиксами, полученными в результате делегирования префиксов
Пример	Задать префикс 2001:da8:221::/48 для общего префикса my-prefix. Switch#config Switch(config)# ipv6 general-prefix my-prefix 2001:da8:221::/48

9.1.49. Пул делегирования префиксов (ipv6 local pool)

Синтаксис	ipv6 local pool <poolname> <prefix/prefix-length> <assigned-length> no ipv6 local pool <poolname>	
Параметр	<poolname>	< poolname > имя пула IPv6-адресов выделения префиксов, длина строки не более 32 символов
	<prefix/prefix-length>	< prefix/prefix-length > префикс адреса и длина выделения префикса
	<assigned-length>	< assigned-length > это длина префикса в пуле адресов, который может быть получен клиентом, длина выделенного префикса должна быть не меньше параметра < prefix-length >
По умолчанию	Пул адресов делегирования префиксов IPv6 не настроен	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда конфигурирует пул для выделения префиксов адресов. "no" в начале команды удаляет конфигурацию делегирования префиксов IPv6. Эта команда должна быть использована совместно с командой "prefix delegation pool" для выделения префикса адресов клиентам. Если делегирование префиксов IPv6 будет удалено, соответствующая команда "prefix delegation" перестанет работать
Пример	<pre>Switch#config Switch(config)#ipv6 local pool 1 1100::1/24 24</pre>

9.1.50. Конфигурирование времени жизни (lifetime)

Синтаксис	lifetime {<valid-time> infinity} {<preferred-time> infinity} no lifetime	
Параметр	<valid-time>	действительное время жизни IPv6-адреса, выделенного в локальном пуле адресов, в диапазоне от 1 до 31536000 секунд, должно быть больше, чем <preferred-time>
	<preferred-time>	предпочитаемое время жизни IPv6-адреса, выделенного в локальном пуле адресов, в диапазоне от 1 до 31536000 секунд, должно быть меньше, чем <valid-time>
	infinity	максимальное время жизни
По умолчанию	Для действительного и предпочитаемого времени задано значение 2592000 секунд (30 дней) и 604800 секунд (7 дней) соответственно	
Режим	Режим конфигурации пула адресов DHCPv6	
Руководство по использованию	Команда позволяет сконфигурировать время жизни адресов и префиксов, выдаваемых DHCPv6. "no" в начале команды возвращает настройки по умолчанию	
Пример	Настроить действительное время жизни равным 1000 секундам, а предпочитаемое время жизни равным 600 секундам. <pre>Switch#config Switch(config)#lifetime 1000 600</pre>	



9.1.51. Настройка пула адресов (network-address)

Синтаксис	network-address <ipv6-pool-start-address> <ipv6-pool-end-address> <prefix-length> [eui-64]) no network-address	
Параметр	<ipv6-pool-start-address>	начальный адрес пула
	<ipv6-pool-end-address>	конечный адрес пула
	<prefix-length>	длина префикса адреса, в диапазоне от 3 до 128. По умолчанию длина 64
	eui-64	согласно стандарта eui-64, IPv6-адреса распределяются, а не назначаются в порядке очереди
По умолчанию	По умолчанию пул адресов не настроен	
Режим	Режим конфигурации пула адресов DHCPv6	
Руководство по использованию	Команда применяется для конфигурирования DHCPv6-пула адресов. "no" в начале команды удаляет конфигурацию пула адресов. Данная команда используется для конфигурирования пула адресов DHCPv6- сервера. Только один диапазон может быть сконфигурирован для каждого пула. Обратите внимание, что если включен сервер DHCPv6 и настроена длина префикса IPv6-адреса, то длина префикса в пуле адресов должна быть не меньше длины префикса IPv6-адреса соответствующих интерфейсов третьего уровня в коммутаторе. Если < ipv6-pool-end-address > длиннее, чем < ipv6-pool-start-address > , эта команда сразу возвращается	
Пример	Настроить диапазон адресов для пула адресов как 2001: da8: 123: : 100-2001: da8: 123: : 200. <pre>Switch#config Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#network-address 2001: Switch(dhcp-1-config)#network-address 2001: da8: 123: : 100 2001: da8: 123: : 200</pre>	



9.1.52. Выдача определенного префикса (prefix-delegation)

Синтаксис	prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>] [lifetime <valid-time> <preferred-time>] no prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>]	
Параметр	<ipv6-prefix/prefix-length>	< ipv6-prefix/prefix-length > длина префикса, выдаваемого клиенту
	<client-DUID>	<client-DUID> DUID клиента. Поддерживаются DUID типа DUID-LLT и DUID-LL, DUID типа DUID-LLT должен состоять из 14 символов;
	<iaid>	< iaid > значение, которое будет добавлено в поле IA_PD клиентского запроса
	<valid-time>	действительное время жизни (в секундах) IPv6-адреса, назначенного клиенту, в диапазоне 1-31536000, со значением по умолчанию 2592000. Должно быть больше, чем параметр preferred-time
	<preferred-time>	предпочитаемое время жизни (в секундах) IPv6-адреса, назначенного клиенту, в диапазоне от 1-31536000, со значением по умолчанию 604800. Должно быть меньше, чем параметр valid-time
По умолчанию	Отключено	
Режим	Настройка портов	
Руководство по использованию	Команда применяется для конфигурирования выдачи определенного префикса указанному пользователю. "no" в начале команды удаляет делегирование префикса. Эта команда устанавливает указанный префикс адреса IPv6 для привязки к указанному клиенту. Если IAID не задан, любой IA любого клиента может получить этот префикс адреса. В каждом пуле адресов может быть установлено до восьми статически привязанных префиксов адресов. При делегировании префикса приоритет статической привязки выше, чем у пула адресов префикса	
Пример	Назначить адрес 2001: da8: : /48 клиенту с DUID 0001000600000005000BBFAA2408 и IAID 12. Switch#config Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#prefix-delegation 2001: da8: : /48 0001000600000005000BBFAA240812	



9.1.53. Пул делегирования префиксов, используемый адресным пулом (prefix-delegation pool)

Синтаксис	prefix-delegation pool <poolname> [lifetime <valid-time> <preferred-time>] no prefix-delegation pool <poolname>	
Параметр	<poolname>	< poolname > имя пула префиксов адресов, длина не более 32 символов
	<valid-time>	действительное время жизни (в секундах) IPv6-адреса, назначенного клиенту, в диапазоне от 1-31536000, со значением по умолчанию 2592000. Должно быть больше, чем параметр preferred-time
	<preferred-time>	предпочитаемое время жизни IPv6-адреса, назначенного клиенту (в секундах), в диапазоне от 1-31536000, со значением по умолчанию 604800. Должно быть меньше, чем параметр valid-time
По умолчанию	Имя делегирования префикса, используемое пулом адресов DHCPv6. Не задано	
Режим	Режим конфигурации пула адресов DHCPv6	
Руководство по использованию	Команда применяется для конфигурирования имени пула назначения префикса, используемого DHCPv6-пулом. "no" в начале команды удаляет конфигурацию. Данная команда задает имя пула префиксов адресов, используемого для назначения адресов. Если задана команда, адреса в пуле префиксов назначаются клиентам. Эту команду можно использовать вместе с командой ipv6 local pool. К пулу адресов может быть привязан только один пул делегирования префиксов. При попытке удалить конфигурацию префиксных имен служба делегирования префиксов на сервере будет недоступна, если пул адресов не связан с пулом делегирования префиксов и не включена статическая привязка делегирования префиксов	
Пример	<pre>Switch#show subnet-vlan Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#prefix-delegation pool abc</pre>	

9.1.54. Включение службы DHCPv6 (service dhcpv6)

Синтаксис	service dhcpv6 no service dhcpv6
Параметр	отсутствуют



По умолчанию	Отключено
Режим	Режим глобальной конфигурации
Руководство по использованию	Включает службу DHCPv6 сервера. "no" в начале команды отменяет конфигурацию. В службу DHCPv6 входят DHCPv6-сервер, DHCPv6-relay и DHCPv6-назначение префиксов. Все вышеуказанные службы настраиваются на портах. Назначение IP-адресов DHCPv6-клиента, DHCPv6-relay и делегирование префиксов DHCPv6 может быть настроено на порту только при включенной функции сервера DHCPv6
Пример	Включить DHCPv6-сервер. <pre>Switch#config Switch(config)# service dhcpv6</pre>

9.1.55. Вывод настроек сервера DHCPv6 (show ipv6 dhcp)

Синтаксис	show ipv6 dhcp
Параметр	отсутствуют
По умолчанию	отсутствуют
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Команда выводит на экран коммутатор подключения и идентификатор DUID службы DHCPv6. Для вывода коммутатора и идентификатора DUID службы DHCPv6, опции идентификатора сервера используют только DUID типа DUID-LLT
Пример	<pre>Switch#show ipv6 dhcp DHCPv6 is enabled LLT DUID is <00: 01: 00: 01: 43: b7: 1b: 81: 00: 03: 0f: 01: 5f: 9d> LL DUID is <00: 03: 00: 01: 00: 03: 0f: 01: 5f: 9d></pre>

9.1.56. Вывод привязки адресов и префиксов службы DHCPv6 (show ipv6 dhcp binding)

Синтаксис	show ipv6 dhcp binding [<ipv6-address>] pd <ipv6-prefix prefix-length>[count]	
Параметр	ipv6-address	указанный IPv6-адрес;



	count	количество отображаемых DHCPv6-привязок
По умолчанию	отсутствуют	
Режим	Привилегированный режим и режим конфигурации	
Руководство по использованию	Отображает все привязки адресов и префиксов DHCPv6, включая тип, DUID, IAID, префикс, срок жизни и т.д.	
Пример	Switch#show ipv6 dhcp binding Client: iatype IANA, iauid 0x0e001d92 DUID: 00: 01: 00: 01: 0f: 55: 82: 4f: 00: 19: e0: 3f: d1: 83 IANA leased address: 2001: da8: : 10 Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds Lease obtained at %Jan 01 01: 34: 44 1970 Lease expires at %Jan 31 01: 34: 44 1970 (2592000 seconds left) Число DHCPv6-привязок: 1	

9.1.57. Вывод всех конфликтов адресов, зарегистрированных сервером DHCPv6 (show ipv6 dhcp conflict)

Синтаксис	show ipv6 dhcp conflict	
Параметр	отсутствуют	
По умолчанию	отсутствуют	
Режим	Привилегированный режим и режим конфигурации	
Руководство по использованию	Команда выводит на экран журнал адресов, для которых есть запись о конфликте	
Пример	Switch#show ipv6 dhcp DHCPv6 is enabled LLT DUID is <00: 01: 00: 01: 43: b7: 1b: 81: 00: 03: 0f: 01: 5f: 9d> LL DUID is <00: 03: 00: 01: 00: 03: 0f: 01: 5f: 9d>	

9.1.58. Вывод информации DHCPv6 для интерфейса (show ipv6 dhcp interface)

Синтаксис	show ipv6 dhcp interface [<interface-name>]	
Параметр	<interface-name>	<interface-name> название и номер интерфейса, если параметр <interface-name> не указан, то



		будет выведена информация обо всех интерфейсах
По умолчанию	отсутствуют	
Режим	Привилегированный режим и режим конфигурации	
Руководство по использованию	Команда выводит на экран информацию об интерфейсе DHCPv6, включая режимы работы портов (делегируемые префиксы клиенту, DHCPv6-сервер, DHCPv6 relay) и информацию об относительном соответствии для каждого режима	
Пример	<pre>Switch#show ipv6 dhcp interface vlan10 Vlan10 is in server mode Using pool: poolv6 Preference value: 20 Rapid-Commit is disabled</pre>	

9.1.59. Проверка имени DHCPv6-пула и его параметры (show ipv6 dhcp pool)

Синтаксис	show ipv6 dhcp pool [poolname]	
Параметр	[poolname]	<poolname> это имя пула адресов DHCPv6, сконфигурированного на данный момент, длина не больше 32 символов. Если параметр <poolname> не указан, отображается вся информация о пуле адресов DHCPv6
По умолчанию	отсутствуют	
Режим	Привилегированный режим и режим конфигурации	
Руководство по использованию	Команда позволяет вывести информацию о конфигурации и динамическом назначении пула адресов DHCPv6, включая имя пула адресов DHCPv6, префикс пула адресов DHCPv6, исключенный адрес, конфигурацию DNS-сервера, информацию об относительном префиксе и т.д. Применяется для вывода на экран назначенного номера привязки адреса для пула адресов, используемого в качестве сервера распределения адресов. Для вывода номера назначенного префикса пула адресов, который используется в качестве сервера делегирования префиксов	
Пример	Switch#show ipv6 dhcp pool poolv6	



9.1.60. Статистика DHCPv6-сервера (show ipv6 dhcp statistics)

Синтаксис	show ipv6 dhcp statistics					
Параметр	отсутствуют					
По умолчанию	отсутствуют					
Режим	Привилегированный режим и режим конфигурации					
Руководство по использованию	Отображает статистику по всем типам DHCPv6 пакетов для DHCPv6-сервера					
Пример	Switch#show ipv6 dhcp statistics Address pools 1					
	Active bindings 0					
	Expired bindings 0					
	Malformed message 0					
	Message	Received	Send			
	DHCP6SOLICIT	0	0			
	DHCP6ADVERTISE	0	0			
	DHCP6REQUEST	0	0			
	DHCP6REPLY	0	0			
	DHCP6RENEW	0	0			
	DHCP6REBIND	0	0			
	DHCP6RELEASE	0	0			
DHCP6DECLINE	0	0				
DHCP6CONFIRM	0	0				
DHCP6RECONFIGURE	0	0				
DHCP6INFORMREQ	0	0				
DHCP6RELAYFORW	0	0				
DHCP6RELAYREPLY	0	0				
<table><tr><td>Информация, отображаемая на дисплее</td><td>Пояснение</td></tr><tr><td>Address pools</td><td>Число сконфигурированных пулов адресов DHCPv6;</td></tr></table>			Информация, отображаемая на дисплее	Пояснение	Address pools	Число сконфигурированных пулов адресов DHCPv6;
Информация, отображаемая на дисплее	Пояснение					
Address pools	Число сконфигурированных пулов адресов DHCPv6;					



	Active bindings	Количество адресов с автоматическим назначением;
	Expired bindings	Количество привязок с истекшим сроком действия;
	Malformed message	Количество ошибочных сообщений;
	Message Recieved	Статистика полученных пакетов DHCPv6
	DHCP6SOLICIT	Количество пакетов SOLICIT в DHCPv6
	DHCP6ADVERTISE	Количество пакетов ADVERTISE в DHCPv6
	DHCPv6REQUEST	Количество пакетов REQUEST в DHCPv6
	DHCP6REPLY	Количество пакетов REPLY в DHCPv6
	DHCP6RENEW	Количество пакетов RENEW в DHCPv6
	DHCP6REBIND	Количество пакетов REBIND в DHCPv6
	DHCP6RELEASE	Количество пакетов RELEASE в DHCPv6
	DHCP6DECLINE	Количество пакетов DECLINE в DHCPv6
	DHCP6CONFIRM	Количество пакетов CONFIRM в DHCPv6
	DHCP6RECONFIGURE	Количество пакетов RECONFIGURE в DHCPv6
	DHCP6INFORMREQ	Количество пакетов INFORMREQ в DHCPv6
	DHCP6RELAYFORW	Количество пакетов RELAYFORW в DHCPv6
	DHCP6RELAYREPLY	Количество пакетов RELAYREPLY в DHCPv6

9.1.61. Вывод информации, общей для префикса IPv6-пула (show ipv6 general-prefix)

Синтаксис	show ipv6 general-prefix
Параметр	отсутствуют
По умолчанию	отсутствуют
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Команда выводит на экран информацию общую для префикса IPv6-пула, включая количество префиксов в общем пуле префиксов, имя каждого префикса и значение префикса



Пример	Switch#show ipv6 general-prefix IPv6 Prefix my, acquired via Manual configuration 2001: da8: 221: : /48

9.1.62. Вывести информацию для DHCPv6 пула префиксов (show ipv6 local pool)

Синтаксис	show ipv6 local pool
Параметр	отсутствуют
По умолчанию	отсутствуют
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Команда выводит информацию для DHCPv6 пула префиксов, включая имя пула префиксов, префикс и длину префикса, количество назначенных префиксов и информацию в пуле адресов DHCPv6
Пример	Switch#show ipv6 local pool Pool Prefix Free In use a 2010: : 1/0/48 65536 0

9.1.63. Включение добавления опции 82 ретрансляции DHCP (ip dhcp relay information option)

Синтаксис	ip dhcp relay information option no ip dhcp relay information option
Параметр	отсутствуют
По умолчанию	По умолчанию система отключает функцию option82
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда подключает функцию option82 агента ретрансляции коммутатора. Команда “ no ip dhcp relay information option ” используется для отключения функции option82 агента ретрансляции коммутатора. Только агенты ретрансляции DHCP, настроенные с помощью этой команды, могут добавлять option82 в сообщение запроса DHCP и позволять серверу обрабатывать его. Перед включением этой функции пользователи должны убедиться, что служба DHCP включена и агент ретрансляции будет передавать широковещательные сообщения udp с портом назначения 67
Пример	Подключить функцию option82 ретранслирующего агента коммутатора.



	<pre>Switch#config Switch(config)#service dhcp Switch(config)# ip forward-protocol udp bootps Switch(config)# ip dhcp relay information option</pre>

9.1.64. Настройка разделителя (ip dhcp relay information option delimiter)

Синтаксис	<pre>ip dhcp relay information option delimiter [colon dot slash space] no ip dhcp relay information option delimiter</pre>	
Параметр	отсутствуют	
По умолчанию	косая чёрта ("/")	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда настраивает разделитель каждого параметра субопций в опции 82 в глобальном режиме. Команда с "no" в начале восстанавливает разделитель по умолчанию. Разделяет параметры с помощью настроенных разделителей после определения их пользователями, которые используются для создания суб-опций (remot-de, circuit-id) опции 82 в глобальном режиме	
Пример	Установить разделители параметров в виде точек («.») для субопций опции 82. <pre>Switch#config Switch(config)#ip dhcp relay information option delimiter dot</pre>	

9.1.65. Настройка Remote ID опции 82 (ip dhcp relay information option remote-id)

Синтаксис	<pre>ip dhcp relay information option remote-id {standard <remote-id>} no ip dhcp relay information option remote-id</pre>	
Параметр	standard	standard означает формат MAC-адреса VLAN по умолчанию
	<remote-id>	<remote-id> означает содержимое remote-id в опции 82, указанное пользователями, его длина не может превышать 64 символов
По умолчанию	Применяется стандартный формат для установки remote-id опции 82	



Режим	Режим глобальной конфигурации
Руководство по использованию	Устанавливает формат суб-опции 2 (опция remote ID) опции 82, добавляемой пакетами запроса DHCP (принимаются интерфейсом). Команда "no" установит стандартный формат. Добавочная информация опции 82 необходима для связи со сторонним DHCP-сервером и используется пользователями для указания содержимого remote-id, когда стандартный формат remote-id не удовлетворяет требованиям сервера
Пример	Установить подпараметр remote-id опции DHCP82 как street-1-1. <pre>Switch#config Switch(config)#ip dhcp relay information option remote-id street-1-1</pre>

9.1.66. Настройка формата Remote ID опции 82 (ip dhcp relay information option remote-id format)

Синтаксис	ip dhcp relay information option remote-id format {default vs-hp}	
Параметр	default	означает, что remote-id - это MAC-адрес VLAN в шестнадцатеричном формате
	vs-up	означает, что remote-id совместим с форматом remote-id производителя HP
По умолчанию	Состояние по умолчанию	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда устанавливает формат remote-id опции 82 ретранслирующего агента. Формат remote-id по умолчанию определен следующим образом: Тип опции <table><tr><td>Type</td><td>Lenght</td><td></td></tr><tr><td>2</td><td>6</td><td>MAC</td></tr><tr><td>1 байт</td><td>1 байт</td><td>6 байт</td></tr></table> MAC означает MAC-адрес виртуальной локальной сети. Формат remote-id совместимый с производителем HP определен следующим образом: Тип опции <table><tr><td>Type</td><td>Lenght</td><td></td></tr><tr><td>2</td><td>4</td><td>IP</td></tr><tr><td>1 байт</td><td>1 байт</td><td>4 байт</td></tr></table> IP означает основной IP-адрес интерфейса уровня 3, с которого поступают DHCP-пакеты	Type	Lenght		2	6	MAC	1 байт	1 байт	6 байт	Type	Lenght		2	4	IP	1 байт	1 байт	4 байт
Type	Lenght																		
2	6	MAC																	
1 байт	1 байт	6 байт																	
Type	Lenght																		
2	4	IP																	
1 байт	1 байт	4 байт																	
Пример	Задать remote-id опции 82 ретранслирующего агента в качестве совместимого формата с производителем HP. Switch#config Switch(config)#ip dhcp relay information option remote-id format vs-hp																		

9.1.67. Пользовательские параметры remote-id для опции 82 (ip dhcp relay information option self-defined remote-id)

Синтаксис	ip dhcp relay information option self-defined remote-id {hostname mac string WORD} no ip dhcp relay information option self-defined remote-id	
Параметр	WORD	WORD это самостоятельно определяемая строка remote-id с максимальной длиной 64
По умолчанию	Используется стандартный метод	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда задает способ создания опции82 и позволяет пользователю определить параметры суб-опции remote-id. После установки этой команды, если пользователи не настроили remote-id на интерфейсе, она создаст суб-опцию remote-id для опции82 в соответствии с самостоятельно определенным методом. Для мас, если пакет в формате ascii, используется формат 00-02-d1-2e-3a-0d, но шестнадцатеричный формат занимает 6 байт. Каждая опция заполняет пакет в том порядке, которым заданы команды, и разделяется разделителем (разделителем является конфигурация ip dhcp relay information option delimiter)
Пример	Установить метод самоопределения и строку символов подпараметра remote-id - hostname и abc соответственно для опции82. <pre>Switch#config Switch(config)# ip dhcp relay information option self-defined remote-id hostname string abc</pre>

9.1.68. Формат представления данных remote-id для опции 82 (ip dhcp relay information option self-defined remote-id format)

Синтаксис	ip dhcp relay information option self-defined remote-id format [ascii hex]
Параметр	отсутствуют
По умолчанию	ascii
Режим	Режим глобальной конфигурации
Руководство по использованию	Устанавливает формат представления remote-id для опции 82. Пользовательский формат использует тип self-defined remote-id опции ip dhcp relay information для создания формата remote-id
Пример	Задать шестнадцатеричный формат представления remote-id для ретрансляции опции 82. <pre>Switch#config Switch(config)# ip dhcp relay information option self-defined remote-id format hex</pre>



9.1.69. Пользовательские параметры subscriber-id для опции 82 (ip dhcp relay information option self-defined subscriber-id)

Синтаксис	ip dhcp relay information option self-defined subscriber-id {vlan port id (switch-id (mac hostname) remote-mac) string WORD } no ip dhcp relay information option self-defined subscriber-id	
Параметр	WORD	самостоятельно определяемая строка символов circuit-id, максимальная длина 64 символа
По умолчанию	Используется стандартный метод	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда задает способ создания опции82, чтобы пользователь мог самостоятельно определить параметры субопции circuit-id. После установки этой команды, если пользователи не настроили circuit-id на интерфейсе, она создаст суб-опцию circuit-id для опции82 в соответствии с самостоятельно определенным методом. Формат пользовательского circuit-id: если указан формат представления данных ascii, то для vlan запись представляет собой "Vlan2", для порта это "Ethernet1/0/1", записи для mac и remote-mac это "00-02-d1-2e-3a-0d". если пользователь указывает шестнадцатиричный формат hex, запись vlan занимает 2 байта, port занимает 4 байта, байт означает слот (для шасси-коммутатора - ID слота, для бокс-коммутатора - 1), байт означает Module (по умолчанию - 0), два байта означают ID порта, начиная с 1, mac и remote-mac занимают 6 байт. Каждая опция будет заполнять пакеты в соответствии с настроенным порядком команд и разделяться разделителем (разделителем является конфигурация ip dhcp relay information option delimiter)	
Пример	Задать пользовательский метод суб-опции circuit-id как port, mac для опции82. <pre>Switch#config Switch(config)#ip dhcp relay information option self-defined subscriber-id port id switch-id mac</pre>	

9.1.70. Пользовательский формат subscriber-id (ip dhcp relay information option self-defined subscriber-id format)

Синтаксис	ip dhcp relay information option self-defined subscriber-id format [ascii hex]	
Параметр	отсутствуют	
По умолчанию	ascii	



Режим	Режим глобальной конфигурации
Руководство по использованию	Задаёт самостоятельно определяемый формат circuit-id для опции82. Самостоятельно определяемый формат использует тип self-defined subscriber-id опции ip dhcp relay information для создания формата circuit-id
Пример	Задать самостоятельно определяемый формат circuit-id как шестнадцатеричный для опции82. <pre>Switch#config Switch(config)#ip dhcp relay information option self-defined subscriber-id format hex</pre>

9.1.71. Содержание опции subscriber-id (ip dhcp relay information option subscriber-id)

Синтаксис	ip dhcp relay information option subscriber-id {standard <circuit-id>} no ip dhcp relay information option subscriber-id	
Параметр	<circuit-id>	<circuit-id> содержание circuit-id опции82, указанное пользователем, длина строки не более 64 символов
	standard	standard означает стандартный формат имени vlan и имени физического порта
По умолчанию	По умолчанию система использует стандартный формат для установки circuit-id опции 82	
Режим	Настройка портов	
Руководство по использованию	Поскольку новая информация опции 82, добавленная в коммутатор, должна работать с DHCP-серверами сторонних производителей, если стандартный формат circuit-id коммутатора не соответствует требованиям сервера, предусмотрен этот метод, позволяющий пользователю указать содержимое circuit-id в соответствии с ситуацией на сервере	
Пример	Установить суб-опцию circuit-id опции DHCP82 как foobar. <pre>Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip dhcp relay information option subscriber-id foobar</pre>	



9.1.72. Формат представления данных опции subscriber-id (ip dhcp relay information option subscriber-id format)

Синтаксис	ip dhcp relay information option subscriber-id format {hex ascii vs-hp}																																																			
Параметр	hex	hex означает, что subscriber-id это информация о VLAN и порте в шестнадцатеричном формате																																																		
	ascii	ascii означает, что subscriber-id это информация о VLAN и порте в формате ASCII																																																		
	vs-hp	vs-hp означает, что subscriber-id совместим с форматом производителя HP																																																		
По умолчанию	ascii																																																			
Режим	Режим глобальной конфигурации																																																			
Руководство по использованию	Команда устанавливает формат subscriber-id опции 82 ретранслирующего агента. Информация о VLAN и порте в формате ASCII записывается как "Vlan1+Ethernet1/0/11", запись информации о VLAN и порте в шестнадцатеричном формате показана ниже: <table><tr><td>Suboption type</td><td>Length</td><td>Circuit ID type</td><td>Length</td><td></td><td></td><td></td><td></td></tr><tr><td>↓</td><td>↓</td><td>↓</td><td>↓</td><td></td><td></td><td></td><td></td></tr><tr><td>1</td><td>8</td><td>0</td><td>6</td><td>VLAN</td><td>Slot</td><td>Module</td><td>Port</td></tr><tr><td>1 byte</td><td>1 byte</td><td>1 byte</td><td>1 byte</td><td>2 byte</td><td>1 byte</td><td>1 byte</td><td>2 byte</td></tr></table> В поле VLAN заполняется идентификатор VLAN. Для стоечного коммутатора Slot означает номер слота, для коммутатора в коробке Slot это 1; по умолчанию Module - 0; Port означает номер порта, который начинается с 1. Формат subscriber-id, совместимый с форматом производителя HP, определен следующим образом: <table><tr><td>Suboption type</td><td>Length</td><td></td></tr><tr><td>↓</td><td>↓</td><td></td></tr><tr><td>1</td><td>2</td><td>Port</td></tr><tr><td>1 byte</td><td>1 byte</td><td>2 byte</td></tr></table> Port означает номер порта, который начинается с 1								Suboption type	Length	Circuit ID type	Length					↓	↓	↓	↓					1	8	0	6	VLAN	Slot	Module	Port	1 byte	1 byte	1 byte	1 byte	2 byte	1 byte	1 byte	2 byte	Suboption type	Length		↓	↓		1	2	Port	1 byte	1 byte	2 byte
Suboption type	Length	Circuit ID type	Length																																																	
↓	↓	↓	↓																																																	
1	8	0	6	VLAN	Slot	Module	Port																																													
1 byte	1 byte	1 byte	1 byte	2 byte	1 byte	1 byte	2 byte																																													
Suboption type	Length																																																			
↓	↓																																																			
1	2	Port																																																		
1 byte	1 byte	2 byte																																																		
Пример	Задать шестнадцатеричный формат представления subscriber-id опции82 ретранслирующего агента. Switch#config Switch(config)#ip dhcp relay information option subscriber-id format hex																																																			



9.1.73. Политика ретрансляции сообщения (ip dhcp relay information policy)

Синтаксис	ip dhcp relay information policy {drop keep replace} no ip dhcp relay information policy	
Параметр	drop	режим drop означает, что если сообщение содержит опцию 82, система отбросит его без обработки;
	keep	режим keep означает, что система сохранит исходный сегмент опции 82 в сообщении и передаст его на сервер для обработки
	replace	режим replace означает, что система заменит сегмент опции 82 в существующем сообщении своей собственной опцией 82 и передаст сообщение на сервер для обработки
По умолчанию	Система применяет режим replace для замены сегмента опции 82 на собственную опцию 82	
Режим	Настройка портов	
Руководство по использованию	Эта команда используется для установки политики ретрансляции системы для полученного сообщения запроса DHCP, содержащего опцию 82. Команда "no ip dhcp relay information policy" установит политику ретрансляции DHCP-сообщения с опцией 82 как "replace". Поскольку сообщения DHCP-клиента могут проходить через несколько агентов ретрансляции DHCP при передаче на DHCP-сервер, последующие агенты ретрансляции на этом пути должны установить политики обработки опции 82, добавленной агентами ретрансляции до них. При выборе политики повторной передачи опции 82 следует учитывать политику конфигурации DHCP-сервера	
Пример	Установить политику повторной передачи DHCP-сообщений опции 82 как keep. <pre>Switch#config Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip dhcp relay information policy keep</pre>	



9.1.74. Включение опции 82 DHCP сервера (ip dhcp server relay information enable)

Синтаксис	ip dhcp server relay information enable no ip dhcp server relay information enable
Параметр	отсутствуют
По умолчанию	По умолчанию система отключает функцию идентификации опции82
Режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда позволяет DHCP серверу коммутатора идентифицировать опцию 82. Команда “no ip dhcp server relay information enable” заставит сервер игнорировать опцию 82. Эту команду необходимо задать, если вы хотите, чтобы DHCP-сервер коммутатора распознавал опцию82 и возвращал информацию об опции82 в ответных сообщениях, в противном случае DHCP-сервер коммутатора будет игнорировать опцию82
Пример	Настроить DHCP-сервер на поддержку опции82 <pre>Switch#config Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip dhcp server relay information enable</pre>

9.1.75. Вывод информации о состоянии опции 82 (show ip dhcp relay information option)

Синтаксис	show ip dhcp relay information option
Параметр	отсутствуют
По умолчанию	отсутствуют
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Эта команда отображает информацию о состоянии опции 82 DHCP в системе, включая опцию 82 разрешающего коммутатора, политику ретрансляции интерфейса, режим идентификатора цепи и опцию 82 разрешающего коммутатора DHCP-сервера. Используйте эту команду для проверки информации о состоянии опции 82 агента ретрансляции во время работы
Пример	<pre>Switch#show ip dhcp relay information option</pre> ip dhcp server relay information option(i.e. option 82) is disabled



	ip dhcp relay information option(i.e. option 82) is enabled Vlan2: ip dhcp relay information policy keep ip dhcp relay information option subscriber-id standard Vlan3: ip dhcp relay information policy replace ip dhcp relay information option subscriber-id foobar

9.1.76. Установка опции 43 в формате ASCII (option 43 ascii LINE)

Синтаксис	option 43 ascii LINE no option 43	
Параметр	LINE	настройка строки опции 43 в формате ascii, длиной от 1 до 255 символов
По умолчанию	Строка символов опции 43 не настроена	
Режим	Режим настройки пула адресов DHCP	
Руководство по использованию	Позволяет настроить строки символов опции 43 с форматом ascii в режиме ip dhcp pool. "no" в начале команды удаляет настройку опции 43	
Пример	Задать для опции 43 формат ascii как "AP 1000". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 43 ascii AP 1000	

9.1.77. Задать опцию 43 в формате HEX (option 43 hex WORD)

Синтаксис	option 43 hex WORD no option 43	
Параметр	WORD	сконфигурированная строка символов опции 43 в шестнадцатеричном формате, например, a1241b
По умолчанию	Опция 43 не сконфигурирована	
Режим	Режим настройки пула адресов DHCP	
Руководство по использованию	Настройка строки символов опции 43 в шестнадцатеричном формате в режиме ip dhcp pool. "no" в начале команды удаляет настройку опции 43.	



	При установке шестнадцатеричного метода настройки опции 43 строка должна быть записана в соответствии с форматом TLV (Type-Length-Value (Тип-Длина-Значение)). Например, если через опцию 43 выдается IP-адрес 10.1.1.1, шестнадцатеричная строка здесь должна быть 01040A010101; Type=0x01 это IP-адрес; Length=0x04 это IP-адрес длиной 4 байта; и Value=0x0A010101 означает шестнадцатеричный формат 10.1.1.1
Пример	Настроить опцию 43 в шестнадцатеричном формате "01040a010101". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 43 hex 01040a010101

9.1.78. Задать опцию 43 в формате IP-адреса (option 43 ip A.B.C.D)

Синтаксис	option 43 ip A.B.C.D no option 43	
Параметр	A.B.C.D	Настройка опции 43 в символьной строке в формате IP, например, 192.168.1.1
По умолчанию	Опция 43 не сконфигурирована	
Режим	Режим настройки пула адресов DHCP	
Руководство по использованию	Задаёт символьную строку опции 43 в формате IP-адреса в режиме ip dhcp pool. "no" в начале команды удаляет настройку опции 43. При применении команды для настройки опции 43, например, "192.168.1.1", опция 43 будет записываться в пакетах как "C0A80101"	
Пример	Задать опцию 43 в формате IP-адреса "192.168.1.1". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 43 ip 192.168.1.1	

9.1.79. Задать опцию 60 в формате ASCII (option 60 ascii LINE)

Синтаксис	option 60 ascii LINE no option 60	
Параметр	LINE	Настройка символьной строки опции 60 в формате ascii длиной от 1 до 255 символов
По умолчанию	Строка символов опции 60 не задана	



Режим	Режим настройки пула адресов DHCP
Руководство по использованию	Настройка строки символов опции 60 с форматом ascii в режиме ip dhcp pool. "no" в начале команды удаляет настройку опции 60
Пример	Задать для опции 60 формат ascii как "AP 1000". <pre>Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 60 ascii AP 1000</pre>

9.1.80. Задать опцию 60 в формате HEX (option 60 hex WORD)

Синтаксис	option 60 hex WORD no option 60	
Параметр	WORD	Настройка символьной строки опции 60 в формате hex, например, a1241b
По умолчанию	Опция 60 не сконфигурирована	
Режим	Режим настройки пула адресов DHCP	
Руководство по использованию	Настройка строки символов опции 60 в шестнадцатеричном формате в режиме ip dhcp pool. "no" в начале команды удаляет настройку опции 60	
Пример	Настроить опцию 60 в шестнадцатеричном формате "01040a010101". <pre>Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 60 hex 01040a010101</pre>	

9.1.81. Задать опцию 60 в формате IP-адреса (option 60 ip A.B.C.D)

Синтаксис	option 60 ip A.B.C.D no option 60	
Параметр	A.B.C.D	Настройка символьной строки опции 60 в формате IP-адреса, например, 192.168.1.1
По умолчанию	Опция 60 не сконфигурирована	
Режим	Режим настройки пула адресов DHCP	



Руководство по использованию	Задаёт символьную строку опции 60 в формате IP-адреса в режиме ip dhcp pool. "no" в начале команды удаляет настроенную опцию 60. При использовании этой команды для настройки опции 60 как, например, "192.168.1.1", опция 60 пакетов, сопоставленных с настроенной опцией 60, будет "C0A80101"
Пример	Настроить опцию 60 в символьной строке в формате IP-адреса "192.168.1.1". <pre>Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 60 ip 192.168.1.1</pre>

9.1.82. Диапазон адресов адресного пула (address range)

Синтаксис	address range <start-ip> <end-ip> no address range <start-ip> <end-ip>	
Параметр	<start-ip>	определяет начальный адрес пула адресов
	<end-ip>	определяет конечный адрес пула адресов
По умолчанию	Отсутствует	
Режим	Режиме конфигурации адресного пула DHCPv6	
Руководство по использованию	Эта команда используется для задания диапазона адресов для класса DHCPv6 в режиме конфигурации пула адресов DHCPv6. "no" в начале команды удаляет диапазон адресов. Форма записи prefix/plen (префикс/длина) не поддерживается. Необходимо проверить диапазон адресов, назначенный классу, чтобы убедиться, что он не превышает диапазон адресов связанного с ним пула адресов. Классу назначается только один диапазон адресов, и диапазоны адресов, назначенные разным классам в одном пуле адресов, могут пересекаться. Если не применять эту команду для назначения диапазона адресов классу DHCPv6, по умолчанию диапазон будет состоять из всей подсети пула адресов	
Пример	Привязать класс DHCPv6 с именем CLASS1 к пулу dhcpv6 1 и назначить диапазон адресов от 2001: da8: 100: 1: : 2 до 2001: da8: 100: 1: : 30 для CLASS1. <pre>Switch#config Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#class CLASS1</pre>	



	Switch(dhcp-1-class-CLASS1-config)#address range 2001:da8:100:1::2 2001:da8:100:1::30

9.1.83. Конфигурация класса в пуле адресов (class)

Синтаксис	class <class-name> no class <class-name>	
Параметр	<class-name>	имя класса DHCPv6
По умолчанию	отсутствуют	
Режим	Режиме конфигурации адресного пула DHCPv6	
Руководство по использованию	Эта команда связывает класс с пулом адресов в режиме конфигурации пула адресов DHCPv6 и переводит в режим конфигурации класса в пуле адресов. Для удаления связи используйте команду с "no" в начале. Рекомендуется сначала определить этот класс с помощью глобальной команды класса IPv6 DHCP. Если ввести несуществующее имя класса, класс не будет создан	
Пример	Привязать класс DHCPv6 с именем CLASS1 к пулу dhcpv6 1. <pre>Switch(Config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#class CLASS1</pre>	

9.1.84. Создание dhcpv6 класс (ipv6 dhcp class)

Синтаксис	ipv6 dhcp class <class-name> no ipv6 dhcp class <class-name>	
Параметр	<class-name>	имя класса DHCPv6, представляющее собой строку длиной менее 32 символов
По умолчанию	отсутствуют	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда определяет класс DHCPv6 и переводит в режим конфигурации класса DHCPv6. Операция с "no" в начале этой команды удаляет этот класс DHCPv6. Команда настраивает группу опций 37 или 38, или обе опции 37 и 38 одновременно в классе DHCPv6. Эту команду можно использовать, только если сервер поддерживает класс DHCPv6	



Пример	Определить класс DHCPv6 с именем CLASS1. Switch(config)#ipv6 dhcp class CLASS1

9.1.85. Настройка добавления опции 37 (ipv6 dhcp relay remote-id)

Синтаксис	ipv6 dhcp relay remote-id <remote-id> no ipv6 dhcp relay remote-id		
Параметр	<remote-id>	содержимое	опции 37, определяемое пользователем
По умолчанию	В качестве содержимого remote-id используется MAC-адрес vlan, например, "00-01-ac-12-23", с дефисом '-'		
Режим	Настройка портов		
Руководство по использованию	Эта команда настраивает форму включения опции 37 во входящие пакеты запроса DHCPv6, где <remote-id> - определяемый пользователем remote-id в опции 37 строкой длиной не более 128. Операция по этой команды восстанавливает remote-id в опции 37 на enterprise-number вместе с MAC-адресом vlan. Поскольку информация опции 37, добавляемая коммутатором, может связываться со сторонними DHCPv6-серверами, пользователи могут указать содержимое remote-id в зависимости от состояния сервера, если remote-id по умолчанию коммутатора не удовлетворяет требованиям сервера. По умолчанию в качестве remote-id используется enterprise-number вместе с MAC-адресом vlan		
Пример	Включить abc в качестве remote-id опции 37 DHCPv6. Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)# ipv6 dhcp relay remote-id abc		

9.1.86. Включение поддержки опции 37 в DHCPv6-relay (ipv6 dhcp relay remote-id option)

Синтаксис	ipv6 dhcp relay remote-id option no ipv6 dhcp relay remote-id option
Параметр	отсутствуют
По умолчанию	Опция отключена
Режим	Режим глобальной конфигурации



Руководство по использованию	Эта команда включает поддержку опции 37 в ретрансляторе коммутатора, форма по этой команды отключает ее. Только после настройки этой команды агент ретрансляции DHCPv6 может добавлять опцию 37 в пакеты запроса DHCPv6 перед отправкой их на сервер или следующему агенту ретрансляции. Перед выполнением этой команды необходимо убедиться, что служба DHCPv6 включена
Пример	Включить поддержку опции 37 на ретрансляторе коммутатора. <pre>Switch#config Switch(config)#service dhcpv6 Switch(config)#ipv6 dhcp relay remote-id option</pre>

9.1.87. Настройка добавления опции 38 в DHCPv6-relay (ipv6 dhcp relay subscriber-id)

Синтаксис	<pre>ipv6 dhcp relay subscriber-id <subscriber-id> no ipv6 dhcp relay subscriber-id</pre>	
Параметр	<subscriber-id>	содержание опции 38, определенное пользователем
По умолчанию	subscriber-id в опции 38 задан на имя vlan вместе с именем порта	
Режим	Настройка портов	
Руководство по использованию	Эта команда используется для настройки формы опции 38, которая будет добавлена в полученный пакет запроса DHCPv6, где <subscriber-id> - это определяемый пользователем идентификатор абонента в опции 38, который представляет собой строку длиной не более 128. Поскольку информация опции 38, добавляемая коммутатором, может связываться со сторонними DHCPv6-серверами, пользователи могут указать содержимое subscriber-id в зависимости от состояния сервера, если subscriber-id по умолчанию коммутатора не удовлетворяет требованиям сервера. По умолчанию в качестве идентификатора абонента для опции 38 используется имя vlan и имя физического порта	
Пример	Включите abc в качестве subscriber-id в опции 38 DHCPv6. <pre>Switch#config Switch(config) # interface vlan 1 Switch(config-if-vlan1)# ipv6 dhcp relay subscriber-id abc</pre>	



9.1.88. Включение поддержки опции 38 в DHCPv6-relay (ipv6 dhcp relay subscriber-id option)

Синтаксис	ipv6 dhcp relay subscriber-id option no ipv6 dhcp relay subscriber-id option
Параметр	отсутствуют
По умолчанию	Опция 38 отключена
Режим	Режим глобальной конфигурации
Руководство по использованию	Только после установки этой команды агент ретрансляции DHCPv6 может добавлять опцию 38 в пакеты запроса DHCPv6 перед отправкой их на сервер или следующему агенту ретрансляции. Перед выполнением этой команды убедитесь, что служба DHCPv6 включена. По умолчанию опция 38 ретрансляции коммутатора отключена
Пример	Включить на ретрансляторе поддержку опции 38. Switch#config Switch(config) # service dhcpv6 Switch(Config)#ipv6 dhcp relay subscriber-id option

9.1.89. Выбор разделителя наименований для опции 38 DHCPv6 ретранслятора (ipv6 dhcp relay subscriber-id select delimiter)

Синтаксис	ipv6 dhcp relay subscriber-id select (sp sv pv spv) delimiter WORD (delimiter WORD) no ipv6 dhcp relay subscriber-id select delimiter	
Параметр	(sp sv pv spv)	данная опция позволяет выбрать комбинации слота, порта, vlan, где sp означает слот и порт, sv означает слот и vlan, pv означает порт и vlan, а spv означает слот, порт и vlan
	WORD	разделитель между полями slot, port и vlan. Возможны варианты (# . , ; : /\space). Обратите внимание, что здесь есть два разделителя WORD, первый - между слотом и портом, второй - между портом и vlan
По умолчанию	Значение отсутствует	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Настраивает пользовательскую конфигурацию опций subscriber-id. Команда "no" восстанавливает конфигурацию по умолчанию, т.е. название vlan вместе с названием порта. Команда не действует на порты с самоопределяемым subscriber-id. Если пользователь переопределит subscriber-id порта после применения этой команды, то приоритет будет иметь идентификатор, заданный пользователем. По умолчанию эта конфигурация равна нулю
Пример	<pre>Switch#config Switch(config)#ipv6 dhcp relay subscriber-id select sp delimiter #</pre>

9.1.90. Поддержка опции 37 в DHCPv6-сервере (ipv6 dhcp server remote-id option)

Синтаксис	<pre>ipv6 dhcp server remote-id option no ipv6 dhcp server remote-id option</pre>
Параметр	Отсутствует
По умолчанию	Опция 37 не поддерживается
Режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда включает поддержку идентификации опции 37 сервером DHCPv6, форма "no" этой команды отключает поддержку. Задайте эту команду, если ожидается, что сервер DHCPv6 будет распознавать и обрабатывать опцию 37, в противном случае она будет игнорироваться. По умолчанию опция 37 не поддерживается
Пример	Включить поддержку опции 37 DHCPv6 сервером. <pre>Switch#config Switch(config)#ipv6 dhcp server remote-id option</pre>

9.1.91. Выбор между опциями 37 и 38 на DHCPv6-сервере (ip dhcp server select relay-forw)

Синтаксис	<pre>ipv6 dhcp server select relay-forw no ipv6 dhcp server select relay-forw</pre>
Параметр	отсутствуют
По умолчанию	Выбор опции 37 и опции 38 из оригинальных пакетов



Режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда позволяет серверу DHCPv6 поддерживать выбор при наличии нескольких опций 37 или 38, и выбирать опции 37 и 38 внутреннего уровня. Команда "no" возвращает настройку по умолчанию, т.е. выбор опций 37 и 38 оригинальных пакетов. Перед использованием этой команды необходимо убедиться, что на сервере включена поддержка опции 37 и опции 38. По умолчанию система выбирает опцию 37 и опцию 38 из исходных пакетов
Пример	Настроить для интерфейса vlan1 сервера DHCPv6 выбор опции 37 и опцию 38 relay-forw на внутреннем уровне. <pre>Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)# ipv6 dhcp server select relay-forw</pre>

9.1.92. Выбор между опциями 37 и 38 на DHCPv6-сервере (ip dhcp server select relay-forw)

Синтаксис	<pre>ipv6 dhcp server select relay-forw no ipv6 dhcp server select relay-forw</pre>
Параметр	отсутствуют
По умолчанию	Выбор опции 37 и опции 38 из оригинальных пакетов
Режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда позволяет серверу DHCPv6 поддерживать выбор при наличии нескольких опций 37 или 38, и выбирать опции 37 и 38 внутреннего уровня. Команда "no" возвращает настройку по умолчанию, т.е. выбор опций 37 и 38 оригинальных пакетов. Перед использованием этой команды необходимо убедиться, что на сервере включена поддержка опции 37 и опции 38. По умолчанию система выбирает опцию 37 и опцию 38 из исходных пакетов
Пример	Настроить для интерфейса vlan1 сервера DHCPv6 выбор опции 37 и опцию 38 relay-forw на внутреннем уровне. <pre>Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)# ipv6 dhcp server select relay-forw</pre>



9.1.93. Поддержка опции 38 в DHCPv6 сервере (ipv6 dhcp server subscriber-id option)

Синтаксис	ipv6 dhcp server subscriber-id option no ipv6 dhcp server subscriber-id option
Параметр	отсутствуют
По умолчанию	Опция 38 не поддерживается
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда включает поддержку опции 38 в DHCPv6 сервере. Команда с "no" в начале выключает поддержку. Команда задается, если ожидается, что сервер DHCPv6 будет распознавать и обрабатывать опцию 38, в противном случае она игнорируется. По умолчанию опция 38 не поддерживается
Пример	Включить поддержку опции 38 на DHCPv6 сервере. Switch#config Switch(config)#ipv6 dhcp server subscriber-id option

9.1.94. Формат представления данных remote-id опции 37 ретранслирующего агента (ipv6 dhcp snooping information option remote-id format)

Синтаксис	ipv6 dhcp snooping information option remote-id format {hex ascii }	
Параметр	hex	Hex означает, что remote-id - это MAC-адрес VLAN шестнадцатеричного формата
	ascii	ascii означает, что remote-id - это MAC-адрес VLAN формата ascii
По умолчанию	ascii	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда позволяет настроить формат remote-id опции 37 ретранслирующего коммутатора DHCPv6. Ниже приведено определение шестнадцатеричного формата remote-id:	



	Тип опции Remote Длина MAC - это MAC-адрес VLAN коммутатора
Пример	Настройте формат remote-id по умолчанию для опции 37 DHCPv6 агента ретрансляции коммутатора. Switch#config Switch(config)#ipv6 dhcp snooping information option remote-id format ascii

9.1.95. Формат представления данных subscribe-id для опции 38 DHCPv6 snooping (ipv6 dhcp snooping information option subscriber-id format)

Синтаксис	ipv6 dhcp snooping information option subscriber-id format {hex ascii }	
Параметр	hex	hex означает, что subscriber-id это шестнадцатеричная информация о VLAN и порте
	ascii	ascii означает, что subscriber-id это информация о VLAN и порте в формате ACSII
По умолчанию	ascii	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда задает формат subscribe-id по умолчанию для опции 38 DHCPv6 snooping коммутатора. Информация о VLAN и порте в формате ACSII имеет вид Vlan1+Ethernet1/0/11. Шестнадцатеричная информация о VLAN и порте определяется следующим образом: В поле VLAN записывается идентификатор VLAN коммутатора. Для стоечного коммутатора Slot означает номер слота, для кассетного это 1. По умолчанию модуль равен 0. Port означает номер порта, начиная с 1	
Пример	Задать формат subscribe-id опции 38 DHCPv6 snooping коммутатора в шестнадцатеричном формате. Switch#config	



	Switch(config)#ipv6 dhcp snooping information option subscriber-id format hex

9.1.96. Форма добавления опции 37 в DHCPv6 snooping (ipv6 dhcp snooping remote-id)

Синтаксис	ipv6 dhcp snooping remote-id <remote-id> no ipv6 dhcp snooping remote-id		
Параметр	<remote-id>	содержимое	опции 37, определяемое пользователем
По умолчанию	В качестве содержимого remote-id используется MAC-адрес vlan, например, "00-01-ac-12-23", с дефисом '-'		
Режим	Настройка портов		
Руководство по использованию	Эта команда настраивает форму включения опции 37 во входящие пакеты запроса DHCPv6, где <remote-id> это содержимое remote-id, определяемое пользователем в опции 37 строкой длиной не более 128. Форма по этой команды возвращает remote-id в опции 37 к заводскому номеру вместе с VLAN MAC-адреса. Поскольку информация опции 37, добавляемая коммутатором, может связываться со сторонними DHCPv6-серверами, пользователи могут указать содержимое remote-id в зависимости от состояния сервера, если стандартный remote-id коммутатора не удовлетворяет требованиям сервера. По умолчанию в качестве remote-id используется заводской номер вместе с MAC-адресом vlan		
Пример	Включить abc в качестве remote-id опции 37 DHCPv6. <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-Ethernet1/0/1)#ipv6 dhcp snooping remote-id abc</pre>		

9.1.97. Поддержка опции 37 в DHCPv6 snooping (ipv6 dhcp snooping remote-id option)

Синтаксис	ipv6 dhcp snooping remote-id option no ipv6 dhcp snooping remote-id option		
Параметр	отсутствуют		
По умолчанию	Отключено		



Режим	Режим глобальной конфигурации
Руководство по использованию	Команда включает поддержку опции 37 в DHCPv6 snooping, форма команды с "no" выключает поддержку. Только после настройки этой команды DHCPv6 SNOOPING может добавлять опцию 37 в пакеты DHCPv6 перед отправкой их на сервер или агенту ретрансляции. Перед выполнением этой команды необходимо убедиться, что функция DHCPv6 SNOOPING включена. По умолчанию система отключает опцию 37 DHCPv6 SNOOPING
Пример	Включить опцию 37 в DHCPv6 SNOOPING. <pre>Switch#config Switch(config)#ipv6 dhcp snooping enable Switch(config)#ipv6 dhcp snooping remote-id option</pre>

9.1.98. Политика пересылки пакетов, содержащих опцию 37 (ipv6 dhcp snooping remote-id policy)

Синтаксис	ipv6 dhcp snooping remote-id policy {drop keep replace} no ipv6 dhcp snooping remote-id policy	
Параметр	drop	система просто отбросит пакеты с опцией 37
	keep	система сохранит исходную опцию 37 и перешлет пакет
	replace	система заменит поле опции 37 в существующем сообщении своей и перешлет сообщение серверу
По умолчанию	Применяется режим replace для замены опции 37 текущего пакета системной опцией	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Поскольку клиентские пакеты DHCPv6 могут уже содержать информацию опции 37, требуется соответствующая политика обработки DHCPv6 SNOOPING. Если политика пересылки установлена как replace, опция 37 должна быть включена заранее. При использовании режима replace по умолчанию опция 37 текущего пакета будет заменена собственной опцией 37 системы	



Пример	Настроить политику перенаправления пакетов DHCPv6 с опцией 37 как keep для DHCPv6 SNOOPING Switch#config Switch(config)#ipv6 dhcp snooping remote-id policy keep

9.1.99. Форма добавления опции 38 в DHCPv6-snooping (ipv6 dhcp snooping subscriber-id)

Синтаксис	ipv6 dhcp snooping subscriber-id <subscriber-id> no ipv6 dhcp snooping subscriber-id		
Параметр	<subscriber-id>	содержание	опции 38, определенное пользователем
По умолчанию	subscriber-id в опции 38 задан на имя vlan вместе с именем порта		
Режим	Настройка портов		
Руководство по использованию	Эта команда используется для настройки формы опции 38, которая будет добавлена в полученный пакет запроса DHCPv6, где <subscriber-id> - это определяемый пользователем идентификатор абонента в опции 38, который представляет собой строку длиной не более 128. Оператор "no" в начале команды восстанавливает subscriber-id в опции 38 по умолчанию, т.е. название vlan вместе с названием порта, например, "Vlan2+Ethernet1/2". Поскольку информация опции 38, добавляемая коммутатором, может связываться со сторонними DHCPv6-серверами, пользователи могут указать содержимое subscriber-id в зависимости от состояния сервера, если стандартный subscriber-id коммутатора не удовлетворяет требованиям сервера. По умолчанию имя vlan и имя физического порта используются в subscriber-id в опции 38		
Пример	Включить abc в качестве subscriber-id для опции 38 DHCPv6. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#ipv6 dhcp snooping subscriber-id abc		

9.1.100. Поддержка опции 38 в DHCPv6-snooping (ipv6 dhcp snooping subscriber-id option)

Синтаксис	ipv6 dhcp snooping subscriber-id option no ipv6 dhcp snooping subscriber-id option
Параметр	отсутствуют



По умолчанию	Опция 38 в DHCPv6 SNOOPING отключена
Режим	Режим настройки пула адресов DHCP
Руководство по использованию	Эта команда включает поддержку опции 38 в DHCPv6-snooping, форма команды с "no" выключает поддержку. Только после настройки этой команды функция DHCPv6-snooping может добавлять опцию 38 в пакеты DHCPv6 перед отправкой их серверу или агенту ретрансляции. Перед выполнением этой команды убедитесь, что функция отслеживания DHCPv6 включена. По умолчанию система отключает параметр 38 для отслеживания DHCPv6
Пример	Включить опцию 38 в DHCPv6-snooping. <pre>Switch#config Switch(config)#ipv6 dhcp snooping enable Switch(config)#ipv6 dhcp snooping subscriber-id option</pre>

9.1.101. Политика пересылки пакетов, содержащих опцию 38 (ipv6 dhcp snooping subscriber-id policy)

Синтаксис	ipv6 dhcp snooping subscriber-id policy {drop keep replace} no ipv6 dhcp snooping subscriber-id policy	
Параметр	drop	система просто отбросит пакеты с опцией 38
	keep	система сохранит опцию 38 без изменений и перешлет пакет
	replace	система заменит поле существующей опции 38 своей и перешлет пакет серверу
По умолчанию	Применяется режим replace для замены опции 38 текущего пакета системной опцией	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Поскольку клиентские пакеты DHCPv6 могут уже содержать информацию опции 38, требуется соответствующая политика обработки DHCPv6 SNOOPING. Если политика пересылки установлена как replace, опция 38 должна быть включена заранее. По умолчанию система отключает опцию 38 DHCPv6 SNOOPING	



Пример	Настроить политику перенаправления пакетов DHCPv6 с опцией 38 как keep для DHCPv6 SNOOPING Switch#config Switch(config)#ipv6 dhcp snooping subscriber-id policy keep

9.1.102. Выбор разделителя наименований для опции 38 DHCPv6 snooping (ipv6 dhcp snooping subscriber-id select delimiter)

Синтаксис	ipv6 dhcp snooping subscriber-id select (sp sv pv spv) delimiter WORD (delimiter WORD) no ipv6 dhcp snooping subscriber-id select delimiter	
Параметр	(sp sv pv spv)	данная опция позволяет выбрать комбинации слота, порта, vlan, где sp означает слот и порт, sv означает слот и vlan, pv означает порт и vlan, а spv означает слот, порт и vlan
	WORD	разделитель между полями slot, port и vlan. Возможны варианты (# . , ; : /\space). Обратите внимание, что здесь есть два разделителя WORD, первый - между слотом и портом, второй - между портом и vlan
По умолчанию	null	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Настраивает пользовательскую конфигурацию опций subscriber-id. Команда "no" восстанавливает конфигурацию по умолчанию, т.е. название vlan вместе с названием порта. Эта команда не работает для портов с самостоятельно определяемым subscriber-id. Если пользователь переопределит subscriber-id порта после настройки команды, то приоритет будет иметь пользовательский идентификатор. По умолчанию используется значение null	
Пример	Switch#config Switch(config)#ipv6 dhcp snooping subscriber-id select sv delimiter #	

9.1.103. Поддержка классов для DHCPv6 адресов (ipv6 dhcp use class)

Синтаксис	ipv6 dhcp use class no ipv6 dhcp use class
Параметр	отсутствуют



По умолчанию	Сервер DHCPv6 поддерживает класс DHCPv6 при назначении адресов
Режим	Режим глобальной конфигурации
Руководство по использованию	Включает на DHCPv6 сервере поддержку использования DHCPv6 классов при присвоении адресов. Команда по умолчанию включает это, не удаляя настройки классов DHCPv6. По умолчанию серверы DHCPv6 поддерживают классы DHCPv6 при назначении адресов, и команда "no" не удаляет информацию о настройках классов DHCPv6. Перед использованием этой команды убедитесь, что служба DHCPv6 включена. По умолчанию сервер DHCPv6 поддерживает класс DHCPv6 при назначении адресов
Пример	Настроить сервер DHCPv6 для поддержки класса DHCPv6 при назначении адресов. <pre>Switch#config Switch(config)# ipv6 dhcp use class</pre>

9.1.104. Настройка опций, соответствующих классу (remote-id subscriber-id)

Синтаксис	<pre>{remote-id [*] <remote-id> [*] subscriber-id [*] <subscriber-id> [*]} no {remote-id [*] <remote-id> [*] subscriber-id [*] <subscriber-id> [*]}</pre>	
Параметр	<remote-id>	строка длиной от 1 до 128 байт используется для соотнесения remote-id в опции 37
	<subscriber-id>	строка длиной от 1 до 128 байт используется для соотнесения subscriber-id в опции 38
	[*]	соответствуют нулю или нескольким символам
По умолчанию	Отсутствует	
Режим	Режим конфигурации DHCPv6 класса	
Руководство по использованию	Настраивает опции 37 и 38, которые соответствуют классу в режиме конфигурации DHCPv6 класса. Эта команда задает режим, соответствующий уже определенному классу DHCPv6, причем для одного класса DHCPv6 можно задать несколько команд. Если эта команда игнорируется и в режиме конфигурации DHCPv6 класса не задан режим, то любой remote-id или subscriber-id будет считаться соответствующим классу DHCPv6, при этом remote-id или subscriber-id должны присутствовать в пакете DHCPv6	



Пример	Настроить какой-либо remote-id или subscriber-id, принадлежащий классу DHCPv6 с именем CLASS1. <pre>Switch#config Switch(config)#ipv6 dhcp class CLASS1 Switch(dhcpv6-class-class1-config)#remote-id abc* subscriber-id bcd* Switch(dhcpv6-class-class1-config)#remote-id edf* Switch(dhcpv6-class-class1-config)#subscriber-id *mmn</pre>

9.1.105. Вывод конфигурации ретранслятора (show ipv6 dhcp relay option)

Синтаксис	show ipv6 dhcp relay option
Параметр	отсутствуют
По умолчанию	отсутствуют
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Команда позволяет проверить состояния конфигурации агентов ретрансляции для опции 37 и опции 38
Пример	<pre>Switch#show ipv6 dhcp relay option remote-id option enable subscriber-id option enable Interface Vlan 1: remote-id option configure "abc"</pre>

9.1.106. Просмотр опций DHCPv6 Snooping (show ipv6 dhcp snooping option)

Синтаксис	show ipv6 dhcp snooping option
Параметр	отсутствуют
По умолчанию	отсутствуют
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Используйте эту команду для проверки состояния конфигурации snooping для опции 37 и опции 38
Пример	<pre>Switch#show ipv6 dhcp snooping option remote-id option enable subscriber-id option enable</pre>



	The slot port vlan select option is : port and vlan The delimiter is : #

9.1.107. Включение ключа шифрования DES для частных пакетов (enable trustview key)

Синтаксис	enable trustview key {0 7} <password> no enable trustview key	
Параметр	<password>	<password> символьная строка длиной не более 16 символов, ключ шифра
	{0 7}	0 означает, что пароли шифроваться не будут, 7 - что будут шифроваться
По умолчанию	Отключено	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет настроить ключ шифрования по алгоритму DES для частных пакетов, кроме того, эта команда включает на коммутаторе шифрование частных пакетов и использование хеш-функции пакетов. Коммутатор связывается с системой управления TrustView с помощью частных протоколов. По умолчанию эти пакеты не шифруются. Во избежание перехвата, можно задать шифрование этих пакетов. Одновременно с этим, на сервере TrustView должны быть установлены те же пароли	
Пример	Включить шифрование частных сообщений и использование для них хеш-функции Switch#config Switch(config)# enable trustview key 0 switch	

9.1.108. Включение функции DHCP Snooping (ip dhcp snooping)

Синтаксис	ip dhcp snooping enable no ip dhcp snooping enable
Параметр	отсутствуют
По умолчанию	Протокол DHCP Snooping не включен
Режим	Режим глобальной конфигурации



Руководство по использованию	Команда включает функцию DHCP Snooping. Когда эта функция включена, выполняется контроль всех пакетов DHCP-сервера для небезопасных портов
Пример	Включить функцию DHCP Snooping Switch#config Switch(config)#ip dhcp snooping enable

9.1.109. Установить действия защиты (ip dhcp snooping action)

Синтаксис	ip dhcp snooping action {shutdown blackhole} [recovery <second>] no ip dhcp snooping action	
Параметр	shutdown	когда порт обнаруживает фальшивый DHCP-сервер, порт выключается
	blackhole	когда порт обнаруживает фальшивый DHCP-сервер, vid и MAC-адрес фальшивого пакета будут использованы для блокирования трафика с этого MAC-адреса
	recovery	Пользователи могут задать выполнение восстановления после выполнения защитной операции (не выключая порты и не удаляя соответствующую блокировку)
	<second>	пользователи могут задать период времени между выполнением защитной операции и восстановлением. Единица измерения секунда, диапазон от 10 до 3600
По умолчанию	Защитная операция не задана	
Режим	Настройка портов	
Руководство по использованию	Позволяет задать или удалить защитную операцию, выполняемую при атаке на порт. Эта команда может задаваться только в том случае, если DHCP Snooping включено в глобальном режиме конфигурации. Безопасный порт не будет обнаруживать фальшивый DHCP-сервер, а значит соответствующая защитная операция не будет выполняться. Когда состояние порта меняется с небезопасного на безопасный, защитная операция порта автоматически удаляется	



Пример	На порту ethernet0/0/1 задать оборонительную операцию DHCP Snooping "blackhol", время восстановления 30 секунд. <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(Config-Ethernet1/0/1)#ip dhcp snooping action blackhole recovery 30</pre>

9.1.110. Задать число оборонительных операций (ip dhcp snooping action MaxNum)

Синтаксис	ip dhcp snooping action {<maxNum> default}	
Параметр	<maxNum>	число оборонительных операций на каждом порту, в диапазоне от 1 до 200, значение по умолчанию 10
	default	восстанавливает значение, заданное по умолчанию
По умолчанию	Значение по умолчанию 10	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать число одновременно выполняемых оборонительных операций. Задаёт максимальное число оборонительных операций, чтобы не растрачивать ресурсы при атаках на коммутатор. Если число аварийных сообщений больше установленного значения, будет принудительно восстановлено защитное действие, которое было выполнено раньше всех для отправки новых защитных действий	
Пример	Задать число оборонительных операций порта 100. <pre>Switch#config Switch(config)#ip dhcp snooping action 100</pre>	

9.1.111. Включение функции привязки DHCP Snooping (ip dhcp snooping binding)

Синтаксис	<pre>ip dhcp snooping binding enable no ip dhcp snooping binding enable</pre>
Параметр	отсутствуют
По умолчанию	Привязки DHCP Snooping не включены
Режим	Режим глобальной конфигурации



Руководство по использованию	Команда включает функцию привязки DHCP Snooping Когда эта функция включена, будет сохраняться информация о привязках, назначенных DHCP-сервером всем безопасным портам. Функция привязки может быть включена только после того, как будет включена функция DHCP SNOOPING
Пример	Включить функцию привязки DHCP Snooping. Switch#config Switch(config)#ip dhcp snooping binding enable

9.1.112. Включение функции привязки DOT1X для DHCP Snooping (ip dhcp snooping binding dot1x)

Синтаксис	ip dhcp snooping binding dot1x no ip dhcp snooping binding dot1x
Параметр	отсутствуют
По умолчанию	Функция привязки DOT1X выключена на всех портах
Режим	Настройка портов
Руководство по использованию	Когда эта функция включена, DHCP SNOOPING будет уведомлять модуль DOT1X о захваченной информации привязок для пользователей, осуществляющих управление DOT1X. Эта команда является взаимоисключающей с командой ip dhcp snooping binding user-control". Функция привязки dot1x может быть включена только после того, как будет включена функция привязки DHCP SNOOPING
Пример	Включить функцию привязки DOT1X на порту ethernet1/0/1. Switch#config Switch(config) #interface ethernet 1/0/1 switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding dot1x

9.1.113. Настройка статической привязки (ip dhcp snooping binding user)

Синтаксис	ip dhcp snooping binding user <mac> address <ipaddress> vlan <vlan-id> interface [Ethernet] <ifname> no ip dhcp snooping binding user <mac> interface [Ethernet] <ifname>	
Параметр	<mac>	MAC-адрес пользователя со статической привязкой, индекс пользователя с привязкой



	<ipaddress>	IP-адрес и маска пользователя со статической привязкой
	<vlan-id>	идентификатор VLAN ID, которой принадлежит пользователь со статической привязкой
	<ifname>	интерфейс доступа пользователя со статической привязкой
По умолчанию	DHCP Snooping не имеет списка статических привязок	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Работа с пользователями со статической привязкой осуществляется так же, как и с пользователями, привязки которых получены динамически, перехваченными с помощью DHCP SNOOPING, в частности, разрешены следующие операции: уведомление DOT1X для пользователей, работающих под управлением DOT1X, прямое добавление пользователей в список безопасных пользователей, добавление в список привязок ARP. Для пользователей со статической привязкой срок жизни адресов не ограничен, они имеют более высокий приоритет, чем пользователи с динамической привязкой. Пользователи со статической привязкой включаются только после того, как будет включена функция привязки DHCP SNOOPING	
Пример	Настроить пользователей со статической привязкой. Switch#config Switch(config)#ip dhcp snooping binding user 00-11-22-33-44-55 address 1.1.1.1 vlan 1 interface ethernet 1/0/14	

9.1.114. Включение функции привязки пользователя (ip dhcp snooping binding user-control)

Синтаксис	ip dhcp snooping binding user-control no ip dhcp snooping binding user-control
Параметр	Отсутствует
По умолчанию	Функция привязки пользователя выключена на всех портах
Режим	Настройка портов
Руководство по использованию	Когда эта функция включена, DHCP SNOOPING будет считать, что вся захваченная информация о привязках относится к безопасным пользователям, которым разрешен доступ ко всем ресурсам. Эта



	команда является взаимоисключающей с командой "ip dhcp snooping binding dot1x". Функция привязки ARP может быть включена только после того, как будет включена функция привязки DHCP SNOOPING. На эту команду не распространяется ограничение "ip dhcp snooping" для VLAN, а только глобальной командой "ip dhcp snooping enable"
Пример	Включить функцию привязки USER на порту ethernet1/0/1. <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding user-control</pre>

9.1.115. Максимальное число пользователей с разрешенным доступом (ip dhcp snooping binding user-control max-user)

Синтаксис	<pre>ipv6 dhcp snooping binding user-control max-user <number> no ip dhcp snooping binding user-control max-user</pre>	
Параметр	<number>	<number> максимальное число пользователей, которым разрешен доступ к порту, в пределах от 0 до 1024
По умолчанию	Максимальное число пользователей, которым разрешен доступ, на каждом порту равно 1024	
Режим	Настройка портов	
Руководство по использованию	Команда позволяет задать максимальное число пользователей, которым разрешен доступ к порту, когда включена функция DHCP Snooping для привязки пользователей. "no" в начале команды восстанавливает значение по умолчанию. Команда позволяет задать максимальное число безопасных пользователей в соответствии с информацией привязок, при этом для порта должна быть выполнена команда ip dhcp snooping binding user-control enabled on the port. По умолчанию, число пользователей равно 1024. Так как аппаратные ресурсы коммутатора ограничены, реальное число безопасных пользователей зависит от количества ресурсов. Если этой командой установлено большое максимальное число пользователей, DHCP Snooping в соответствии с информацией привязок перераспределит ресурсы аппаратуры так, что большая их часть будет выделена безопасным пользователям, а оставшая часть, при наличии ресурсов, небезопасным. Если новое введенное максимальное число пользователей будет меньше, DHCP Snooping вновь перераспределит ресурсы в соответствии с изменившейся информацией привязок. Когда число привязок станет предельно допустимым, новые DHCP-привязки для безопасных пользователей	



	выделяться не будут, они не будут также выделяться для доступа через коммутатор к другим сетевым ресурсам
Пример	Включить функцию для привязки пользователей DHCP Snooping на порту ethernet1/0/1, задать максимальное число пользователей при доступе к порту Ethernet0/0/1 равным 5. <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-ethernet 1/0/1)#ip dhcp snooping binding user-control max-user 5</pre>

9.1.116. Включение функции опции 82 DHCP Snooping (ip dhcp snooping information enable)

Синтаксис	<pre>ip dhcp snooping information enable no ip dhcp snooping information enable</pre>
Параметр	отсутствуют
По умолчанию	Функция option 82 DHCP Snooping выключена
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда позволяет включить функцию option 82 DHCP Snooping. Выключение функции выполняется при "no" в начале команды. Только с помощью этой команды DHCP Snooping может добавить стандартную опцию 82 к сообщениям запроса DHCP и передать их. Формат опции1 в опции 82 (опция Circuit ID) - это стандартное имя vlan плюс имя физического порта, например, vlan1+ethernet1/0/12. Формат опции2 в опции 82 (опция remote ID) - это MAC-адрес процессора коммутатора, например, 00030f023301. Если получено сообщение запроса DHCP с опцией 82, DHCP Snooping заменит эти опции в сообщении на свои собственные. Если получено ответное сообщение DHCP с параметрами опции 82, DHCP Snooping сбросит эти опции в сообщении и перешлет его
Пример	Включить функцию коммутатора опция82 DHCP Snooping <pre>Switch#config Switch(config)#ip dhcp snooping enable Switch(config)# ip dhcp snooping binding enable Switch(config)# ip dhcp snooping information enable</pre>



9.1.117. Разрешение передачи DHCP-запросов с недоверенных портов (ip dhcp snooping information option allow-untrusted (replace))

Синтаксис	ip dhcp snooping information option allow-untrusted (replace) no ip dhcp snooping information option allow-untrusted (replace)	
Параметр	(replace)	при установке параметра "replace" разрешается заменять опцию82
По умолчанию	DHCP-запросы с добавленной опцией 82, полученные с недоверенных портов отбрасываются	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Данная команда разрешает недоверенным портам DHCP snooping принимать DHCP пакеты с опцией 82. При отключении данной команды все недоверенные порты будут отбрасывать DHCP пакеты с опцией82. Обычно коммутатор с функцией DHCP snooping подключается непосредственно к конечному пользователю, поэтому параметр allow-untrusted по умолчанию отключен, чтобы пользователи не могли добавить опцию82 в частном порядке. При включении функции DHCP snooping на порту для каскадирования установите этот порт в качестве доверенного порта	
Пример	Включите функцию, принимающую DHCP-пакеты с опцией 82 Switch#config Switch(config)#ip dhcp snooping information option allow-untrusted	

9.1.118. Разделитель для параметров суб-опций опции 82 (ip dhcp snooping information option delimiter)

Синтаксис	ip dhcp snooping information option delimiter [colon dot slash space] no ip dhcp snooping information option delimiter	
Параметр	отсутствуют	
По умолчанию	косая черта ("/")	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда настраивает разделитель каждого параметра субопций в опции 82 в глобальном режиме. Команда с "no" в начале восстанавливает разделитель по умолчанию.	



	После того как пользователь определит параметры, они разделяются с помощью разделителей, которые используются для создания суб-опций (remote-id, circuit-id) опции 82 в режиме глобальной конфигурации
Пример	Установить разделители параметров в виде точек («.») для субопций опции 82. Switch#config Switch(config)#ip dhcp snooping information option delimiter dot

9.1.119. Содержание суб-опции remote-id опции 82 (ip dhcp snooping information option remote-id)

Синтаксис	ip dhcp snooping information option remote-id {standard <remote-id>} no ip dhcp snooping information option remote-id	
Параметр	standard	означает формат MAC VLAN по умолчанию
	<remote-id>	<remote-id> содержание опции 82, заданное пользователем, не более 64 символов
По умолчанию	Применяется стандартный формат настройки remote-id	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Добавочная информация опции 82 необходима для связи со сторонним DHCP-сервером и используется пользователями для указания содержимого remote-id, когда стандартный формат remote-id не удовлетворяет требованиям сервера	
Пример	Установить подпараметр remote-id опции DHCP82 как street-1-1. Switch#config Switch(config)#ip dhcp snooping information option remote-id street-1-1	

9.1.120. Настройка пользовательских параметров суб-опции remote-id в опции 82 (ip dhcp snooping information option self-defined remote-id)

Синтаксис	ip dhcp snooping information option self-defined remote-id {hostname mac string WORD} no ip dhcp snooping information option self-defined remote-id	
Параметр	WORD	WORD строка символов для remote-id, заданная самостоятельно, максимальная длина 64 символа



По умолчанию	Используется стандартный метод
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда задает способ создания опции82 и позволяет пользователю определить параметры суб-опции remote-id. После установки этой команды, если пользователь не задал опцию ip dhcp snooping information remote-id в глобальном режиме конфигурации, она создаст суб-опцию remote-id для опции82 в соответствии с заданным методом. Для mac, если пакет записывается в формате ascii, используется формат 00-02-d1-2e-3a-0d, а шестнадцатеричный формат занимает 6 байт. Каждая опция будет заполнять пакеты в соответствии с настроенным порядком команд и разделяться разделителем (разделителем является конфигурация ip dhcp snooping information option delimiter)
Пример	Установить метод самоопределения и строку символов суб-опции remote-id - mac и abc соответственно для опции82. <pre>Switch#config Switch(config)#ip dhcp snooping information option self-defined remote-id mac string abc</pre>

9.1.121. Формат представления данных заданной пользователем суб-опции remote-id (ip dhcp snooping information option self-defined remote-id format)

Синтаксис	ip dhcp snooping information option self-defined remote-id format [ascii hex]	
Параметр	hex	шестнадцатеричный формат представления информации о VLAN и порте
	ascii	информация о VLAN и порте в remote-id дана в формате ASCII
По умолчанию	ascii	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда позволяет выбрать формат представления данных remote-id в опции 82 DHCP Snooping. Самостоятельно определяемый формат использует тип self-defined remote-id опции ip dhcp snooping information для создания формата remote-id	



Пример	Установить шестнадцатеричный формат представления данных в remote-id для опции82 snooping. <pre>Switch#config Switch(config)#ip dhcp snooping information option self-defined remote-id format hex</pre>

9.1.122. Настройка пользовательских параметров суб-опции subscriber-id в опции 82 (ip dhcp snooping information option self-defined subscriber-id)

Синтаксис	<pre>ip dhcp snooping information option self-defined subscriber-id {vlan port id (switch-id (mac hostname) remote-mac) string WORD} no ip dhcp snooping information option type self-defined subscriber-id</pre>	
Параметр	WORD	WORD строка символов circuit-id, заданная пользователем максимальная длина 64 символа
По умолчанию	Используется стандартный метод	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда задает способ создания опции82, чтобы пользователь мог самостоятельно определить параметры субопции circuit-id. После установки этой команды, если пользователи не настроили circuit-id на порту, она создаст суб-опцию circuit-id для опции82 в соответствии с самостоятельно определенным методом. Формат пользовательского circuit-id: если для subscriber-id указан формат представления данных ascii, то для vlan запись представляет собой "Vlan2", для порта это "Ethernet1/0/1", записи для mac и remote-mac это "00-02-d1-2e-3a-0d". если пользователь указывает шестнадцатеричный формат hex, запись vlan занимает 2 байта, port занимает 4 байта, байт означает слот (для шасси-коммутатора - ID слота, для бокс-коммутатора - 1), байт означает Module (по умолчанию - 0), два байта означают ID порта, начиная с 1, mac и remote-mac занимают 6 байт. Каждая опция заполняет пакет в том порядке, котором заданы команды, и разделяется разделителем (разделителем является ip dhcp snooping information option delimiter)	
Пример	Задать метод самоопределения суб-опции circuit-id как vlan, port, mac и remote-mac для опции82. <pre>Switch#config Switch(config)#ip dhcp snooping information option self-defined subscriber-id vlan port id remote-mac</pre>	



9.1.123. Формат представления данных заданной пользователем суб-опции subscriber-id (ip dhcp snooping information option self-defined subscriber-id)

Синтаксис	ip dhcp snooping information option self-defined subscriber-id format [ascii hex]	
Параметр	hex	hex означает, что subscriber-id это информация о VLAN и порте в шестнадцатеричном формате
	ascii	ascii означает, что subscriber-id это информация о VLAN и порте в формате ASCII
По умолчанию	ascii	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Настроить формат представления данных circuit для опции 82 DHCP Snooping. Эта команда позволяет выбрать формат представления данных circuit-id в опции 82 DHCP Snooping	
Пример	Установить шестнадцатеричный формат представления данных в circuit-id для опции 82 snooping. Switch#config Switch(config)#ip dhcp snooping information option self-defined subscriber-id format	

9.1.124. Содержание опции subscriber-id опции 82 DHCP snooping (ip dhcp snooping information option subscriber-id)

Синтаксис	ip dhcp snooping information option subscriber-id {standard <circuit-id>} no ip dhcp snooping information option subscriber-id	
Параметр	standard	означает стандартный формат имени VLAN и имени физического порта, например, Vlan2+Ethernet1/0/12
	<circuit-id>	<circuit-id> содержание circuit-id опции 82, указанное пользователем, не более 64 символов
По умолчанию	Применяется стандартный формат настройки circuit-id	
Режим	Настройка портов	



Руководство по использованию	Устанавливает формат суб-опции 1 (опция circuit ID) опции 82, добавляемой пакетами запроса DHCP (принимаются портом). "no" в начале команды устанавливает стандартный формат суб-опции 1 (опция circuit ID) опции 82. Добавочная информация опции 82 необходима для связи со сторонним DHCP-сервером и используется пользователями для указания содержимого circuit-id, когда стандартный формат circuit-id не соответствует требованиям сервера
Пример	Установить суб-опцию circuit-id опции DHCP82 как P2 <pre>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#ip dhcp snooping information option subscriber-id P2</pre>

9.1.125. Формат представления данных subscribe-id для опции 82 DHCPv6 snooping (ipv6 dhcp snooping information option subscriber-id format)

Синтаксис	ip dhcp snooping information option subscriber-id format {hex ascii vs-hp}																						
Параметр	hex	hex означает, что subscriber-id это информация о VLAN и порте в шестнадцатеричном формате																					
	ascii	ascii означает, что subscriber-id это информация о VLAN и порте в формате ASCII																					
	vs-hp	vs-hp означает, что subscriber-id совместим с форматом изготовителя HP																					
По умолчанию	ascii																						
Режим	Режим глобальной конфигурации																						
Руководство по использованию	Эта команда позволяет выбрать формат представления данных subscriber-id в опции 82 DHCP Snooping. Информация о VLAN и порте в формате ASCII записывается как "Vlan1+Ethernet1/0/11", запись информации о VLAN и порте в шестнадцатеричном формате показана ниже: Suboption type Length Circuit ID type Length ↓ ↓ ↓ ↓ <table><tr><td>1</td><td>8</td><td>0</td><td>6</td><td>VLAN</td><td>Slot</td><td>Module</td><td>Port</td></tr><tr><td>1 byte</td><td>1 byte</td><td>1 byte</td><td>1 byte</td><td>2 byte</td><td>1 byte</td><td>1 byte</td><td>2 byte</td></tr></table>							1	8	0	6	VLAN	Slot	Module	Port	1 byte	1 byte	1 byte	1 byte	2 byte	1 byte	1 byte	2 byte
1	8	0	6	VLAN	Slot	Module	Port																
1 byte	1 byte	1 byte	1 byte	2 byte	1 byte	1 byte	2 byte																



	В поле VLAN указан идентификатор VLAN. Для стоечного коммутатора Slot означает номер слота, для коммутатора в коробке Slot это 1; по умолчанию Module - 0; Port означает номер порта, который начинается с 1. Формат subscriber-id, совместимый с форматом производителя HP, определен следующим образом: Suboption type Length 1 2 Port 1 byte 1 byte 2 byte Port означает номер порта, который начинается с 1
Пример	Установить шестнадцатеричный формат представления данных в subscriber-id для опции82 snooping. Switch#config Switch(config)#ip dhcp snooping information option subscriber-id format hex

9.1.126. Предельная скорость поступления сообщений DHCP (ip dhcp snooping limit-rate)

Синтаксис	ip dhcp snooping limit-rate <pps> no ip dhcp snooping limit-rate	
Параметр	<pps>	число сообщений DHCP, передаваемых в минуту, в диапазоне от 0 до 100. По умолчанию задано 100. 0 означает, что сообщения DHCP передаваться не будут
По умолчанию	По умолчанию задано 100	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать предельную скорость поступления сообщений DHCP. Когда DHCP snooping включено, коммутатор осуществляет мониторинг всех сообщений DHCP и с помощью ПО выполняет их передачу. Производительность программного обеспечения зависит от типа коммутатора, от текущей нагрузки на него и т. д.	
Пример	Задать скорость передачи сообщений 50pps. Switch#config Switch(config)# ip dhcp snooping limit-rate 50	



9.1.127. Атрибуты безопасности DHCP Snooping для порта (ip dhcp snooping trust)

Синтаксис	ip dhcp snooping trust no ip dhcp snooping trust
Параметр	отсутствуют
По умолчанию	Все порты считаются небезопасными
Режим	Настройка портов
Руководство по использованию	Позволяет установить или удалить атрибуты безопасности DHCP Snooping для порта. Эта команда может задаваться только в том случае, если DHCP Snooping включено в глобальном режиме конфигурации. Когда порт превращается из небезопасного в безопасный, исходные защитные операции порта будут автоматически удалены, будут очищены и все записи из архива записей безопасности (за исключением системных сообщений)
Пример	Задать порт ethernet 1/0/1 как безопасный порт DHCP Snooping. <pre>Switch#config Switch(config)#interface ethernet 1/0/1 switch(config- ethernet 1/0/1)#ip dhcp snooping trust</pre>

9.1.128. Функция DHCP snooping для VLAN (ip dhcp snooping vlan)

Синтаксис	ip dhcp snooping vlan (WORD) no ip dhcp snooping vlan (WORD)	
Параметр	WORD	идентификатор VLAN
По умолчанию	Отключение	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда включает функцию dhcp snooping для VLAN. Команда no ip dhcp snooping vlan <vlan-id> отключает функцию dhcp snooping на соответствующем vlan	
Пример	Включить функцию DHCP snooping. <pre>Switch#config Switch(config)#ip dhcp snooping vlan 10</pre>	



	Switch(config)#no ip dhcp snooping vlan 10

9.1.129. Настройка адреса и порта HELPER-сервера (ip user helper-address)

Синтаксис	ip user helper-address <svr_addr> [port <udp_port>] source <src_addr> [secondary] no ip user helper-address [secondary]	
Параметр	<svr_addr>	IP-адрес HELPER-сервера в десятичном представлении с точками
	<udp_port>	Порт UDP HELPER-сервера, в диапазоне 1-65535, значение по умолчанию 9119
	<src_addr>	IP-адрес локального управления коммутатором в десятичном представлении с точками
	[secondary]	указывает, является ли этот адрес сервера вторичным или нет
По умолчанию	Адрес HELPER-сервера не задан	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать адрес и порт HELPER-сервера. DHCP SNOOPING будет посылать контролируемую информацию привязок на HELPER-сервер для ее сохранения. Если запуск коммутатора произошел со сбоями, коммутатор может восстановить данные привязок с HELPER-сервера. Функция HELPER-сервера обычно интегрирована в пакет DCBI. DHCP SNOOPING и HELPER-сервер используют для связи протокол UDP и гарантируют прибытие данных, переданных повторно. Кроме того, HELPER-сервер может использоваться для отправки с сервера данных DOT1X-пользователя, подробнее об этом см. в разделе настройки dot1x. Допускается два адреса HELPER-сервера, в первую очередь DHCP SNOOPING будет пытаться подключиться к первичному серверу. Только в том случае, если первичный сервер недоступен, коммутатор с HELPER-сервером будет пытаться подключиться к вторичному серверу. Обратите внимание: адрес источника является действующим IP-адресом управления коммутатором, если он изменяется, эту настройку необходимо своевременно обновить	
Пример	Задать для порта как значения по умолчанию: IP-адрес локального управления 100.1.1.1, адрес первичного HELPER-сервера 100.1.1.100. <pre>Switch#config switch(config)#interface vlan 1</pre>	



	<pre>Switch(config-if-vlan1)#ip address 100.1.1.1 255.255.255.0 switch(config-if-vlan1)exit switch(config)#ip user helper-address 100.1.1.100 source 100.1.1.1</pre>

9.1.130. Установить на коммутаторе версию 2 частных пакетов (ip user private packet version two)

Синтаксис	<pre>ip user private packet version two no ip user private packet version two</pre>
Параметр	отсутствуют
По умолчанию	На коммутаторе установлена версия 1 частных пакетов для связи с DCBI
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда позволяет установить на коммутаторе версию 2 частных пакетов для связи с trustview. Если применяется управление доступом DCBI, то для связи с DCBI-сервером на коммутаторе должно быть установлено использование частного протокола версии 1. Однако, если применяется TrustView, должна применяться версия 2
Пример	Задать на коммутаторе использование частных пакетов версии 2 для связи с фоновой системой управления безопасностью. <pre>Switch#config Switch(config)#ip user private packet version two</pre>

9.1.131. Вывод информации о текущих настройках dhcp snooping (show ip dhcp snooping)

Синтаксис	show ip dhcp snooping [interface [ethernet] <interfaceName>]	
Параметр	<interfaceName>	Имя указанного порта
По умолчанию	отсутствуют	
Режим	Привилегированный режим и режим конфигурации	
Руководство по использованию	Если порт не указан, на дисплей выводятся текущие настройки dhcp snooping, в противном случае, отображаются записи о защитных операциях для указанного порта	



Пример	Switch#show ip dhcp snooping User primary helper server 1.1.1.1: 9119, source 100.1.1.1, socket 0 seq no 0, connection 0, retry 0, renew 0, binding count 0 00: 00: 00 retry, 01: 16: 57 keep alive, 00: 00: 00 dead Get PrivateDESMD5 Ack 0, Get FreeResource Ack 0, Get HttpRedirPage Ack 0, Get Binding Ack 0 DHCP Snooping is enabled DHCP Snooping maxnum of action info: 100 DHCP Snooping limit rate is 100 pps, switch ID 10-f0-13-f1-72-3a DHCP Snooping dropped packets 0, discarded packets 0 DHCP Snooping alarm count 0, binding count 1, static binding count 1, from shell 1, from server 0 expired binding 0, request binding 0					
	interface	trust	action	recovery	alarm num	bind num
	Ethernet1/0/1	trust	none	0	0	0
	Ethernet1/0/2	untrust	none	0	0	0
	Ethernet1/0/3	untrust	none	0	0	0
	Ethernet1/0/4	untrust	none	0	0	0
	Ethernet1/0/5	untrust	none	0	0	0
	Ethernet1/0/6	untrust	none	0	0	0
	Ethernet1/0/7	untrust	none	0	0	0
	Ethernet1/0/8	untrust	none	0	0	0
	Ethernet1/0/9	untrust	none	0	0	0
	Ethernet1/0/10	untrust	none	0	0	0
	Ethernet1/0/11	untrust	none	0	0	0
	Ethernet1/0/12	untrust	none	0	0	0
	Ethernet1/0/13	untrust	none	0	0	0
	Ethernet1/0/14	untrust	none	0	0	1
	Ethernet1/0/15	untrust	none	0	0	0
	Ethernet1/0/16	untrust	none	0	0	0
	Ethernet1/0/17	untrust	none	0	0	0
	Ethernet1/0/18	untrust	none	0	0	0



Ethernet1/0/19	untrust	none	0	0	0
Ethernet1/0/20	untrust	none	0	0	0
Ethernet1/0/21	untrust	none	0	0	0
Ethernet1/0/22	untrust	none	0	0	0
Ethernet1/0/23	untrust	blackhole	30	0	0
Ethernet1/0/24	untrust	none	0	0	0
Ethernet1/0/25	untrust	none	0	0	0
Ethernet1/0/26	untrust	none	0	0	0
Ethernet1/0/27	untrust	none	0	0	0
Ethernet1/0/28	untrust	none	0	0	0

Информация, отображаемая на экране	Пояснение
DHCP Snooping is enable	Включено или выключено DHCP Snooping в режиме глобальной конфигурации конфигурирования.
DHCP Snooping binding arp	Включена или выключена функция привязки ARP.
DHCP Snooping maxnum of action info	Максимальное число защитных действий порта
DHCP Snooping limit rate	Предельно допустимое число принятых пакетов
switch ID	ID коммутатора, используемый для его идентификации, обычно используется MAC-адрес CPU
DHCP Snooping dropped packets	Число отброшенных сообщений после того как число принятых DHCP-сообщений превысило установленное предельно допустимое число.
discarded packets	Число отброшенных пакетов, обусловленное сбоями связи в системе. Это может происходить, если CPU коммутатора занят обработкой задач DHCP SNOOPING и не успевает обрабатывать принятые DHCP-сообщения.
DHCP Snooping alarm count:	Число аварийных сообщений.



	binding count	Число привязок.
	expired binding	Число привязок, которые уже устарели, но пока не удалены. Причина, по которой истекшая информация не удаляется сразу, в том, что коммутатору необходимо было передать эту информацию на helper-сервер, однако helper-сервер к этому моменту еще не прислал подтверждения о ее получении.
	request binding	Число пакетов с запросами REQUEST
	interface	Имя порта
	trust	Атрибут безопасности порта
	action	Автоматическое защитное действие порта
	recovery	Автоматическое время восстановления порта
	alarm num	Число записей в истории событий автоматического выполнения защитных действий в порту.
	bind num	Число привязок для порта.

9.1.132. Вывод информации о созданных привязках (show ip dhcp snooping binding all)

Синтаксис	show ip dhcp snooping binding all
Параметр	отсутствуют
По умолчанию	отсутствуют
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Эта команда позволяет проверить глобальную информацию о привязке DHCP snooping, выводимая информация для каждой записи включает соответствующий MAC-адрес, IP-адрес, имя порта, идентификатор VLAN и флаг состояния привязки. Для применения данной команды DHCP Snooping должен быть включен в глобальном режиме конфигурации
Пример	Switch#show ip dhcp snooping binding all ip dhcp snooping static binding count: 1, dynamic binding count: 0 MAC IP address Interface Vlan ID



	Flag 00-11-22-33-44-55 SE	1.1.1.1	Ethernet1/0/14	1

9.1.133. Вывод информации о пакетах от TrustView (show trustview status)

Синтаксис	show trust status
Параметр	отсутствуют
По умолчанию	отсутствуют
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Команда используется для отладочных сообщений связи между коммутатором и TrustView-сервером, например, уведомлении о версии протокола, согласование шифрования, общедоступные ресурсы, число сообщений о принудительном выходе из системы (log-off), количество принудительных обновлений учета
Пример	Switch#show trustview status Primary trustview Server 1.1.1.1: 9119 trustview version2 message inform failed trustview inform free resource failed trustview inform web redirect address failed trustview inform user binding data failed trustview version 2 message encrypt/digest not enabled Rcvd 0 force log-off packets Rcvd 0 force accounting update packets using version two private packet

9.1.134. Включить функцию option 82 DHCP Snooping (ip dhcp snooping information enable)

Синтаксис	ip dhcp snooping information enable no ip dhcp snooping information enable
Параметр	отсутствуют
По умолчанию	Функция option 82 DHCP Snooping выключена
Режим	Режим глобальной конфигурации
Руководство по использованию	Только с помощью этой команды DHCP Snooping может добавить стандартную опцию 82 к сообщениям запроса DHCP и передать их. Формат опции1 в опции 82 (опция Circuit ID) - это стандартное имя vlan плюс имя физического порта, например, "vlan1+ethernet1/0/12". Формат опции2 в опции 82 (опция remote ID) - это MAC-адрес процессора



	коммутатора, например, "00030f023301". Если получено сообщение запроса DHCP с опцией 82, DHCP Snooping заменит эти опции в сообщении на свои собственные. Если получено ответное сообщение DHCP с параметрами опции 82, DHCP Snooping сбросит эти опции в сообщении и перешлет его
Пример	Включить функцию коммутатора опция 82 DHCP Snooping Switch#config Switch(config)#ip dhcp snooping enable Switch(config)#ip dhcp snooping binding enable Switch(config)#ip dhcp snooping information enable



10. ПРОТОКОЛ МНОГОАДРЕСНОЙ ПЕРЕДАЧИ

10.1. Настройка протокола многоадресной передачи IPv4

10.1.1. Список доступа (access-list (управление назначением группового трафика))

Синтаксис	access-list <6000-7999> (((add delete) profile-id WORD) ((deny permit) ip ((<source> <wildcard-bit>) (host-source <source-host-ip> [range <2-65535>]) any-source) ((<destination> <wildcard-bit>) (host-destination <destination-host-ip> [range <2-255>]) any-destination))) no access-list <6000-7999> {deny permit} ip ((<source> <source-wildcard>) (host-source <source-host-ip> [range <2-65535>]) any-source) ((<destination> <destination-wildcard>) (host-destination <destination-host-ip> [range <2-255>]) any-destination)	
Параметр	<6000-7999>	номера списка доступа для управления назначением
	add delete	добавить или удалить профиль
	WORD	идентификатор файла
	deny permit	разрешить или запретить
	<source>	адрес источника многоадресной передачи
	<wildcard-bit>	специальный символ адреса
	<source-host-ip>	адрес хоста источника многоадресной передачи
	<2-65535>	диапазон хостов-источников многоадресной передачи
	<destination>	адрес назначения многоадресной передачи
	<destination-host-ip >	адрес хоста назначения многоадресной передачи
	<2-255>	диапазон хостов назначения многоадресной передачи
По умолчанию	отсутствуют	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Запись ACL списка управления многоадресной рассылкой контролируется указанным номером ACL в диапазоне от 6000 до 7999, и эта команда используется для настройки этого ACL. Для управления списком доступа ACL назначения многоадресной передачи необходимо только задать IP-адрес источника и IP-адрес назначения (групповой IP-адрес). Процедура настройки в основном такая же, как и для других списков доступа ACL. Для настройки диапазона адресов, а также для указания адреса хоста, либо всех адресов используется длина маски. Имейте в виду, что опция “all address” (все адреса) соответствует групповому IP-адресу 224.0.0.0/4, а не 0.0.0.0/0, как в других списках доступа. А добавление или удаление profile-id можно использовать для изменения ACL управления назначением многоадресной рассылки
Пример	<pre>Switch#config Switch(config)#access-list 6000 permit ip 10.1.1.1 0.0.0.255 232.0.0.0 0.0.0.255 Switch(config)#access-list 6000 add profile-id 1 profile id 1 is not exist % Operation failed Switch(config)#</pre>

10.1.2. Список доступа (управление источником группового трафика) (access-list (Multicast Source Control))

Синтаксис	access-list <5000-5099> (deny permit) ip ((<source> <wildcard-bit>) (host <source-host-ip>) any-source) ((<destination> <wildcard-bit>) (host-destination <destination-host-ip>) any-destination) <destination-host-ip> any-destination} no access-list <5000-5099> (deny permit) ip ((<source> <wildcard-bit>) (host <source-host-ip>) any-source) ((<destination> <wildcard-bit>) (host-destination <destination-host-ip>) any-destination)	
Параметр	<5000-5099>	номера списка доступа для управления источником
	deny permit	разрешить или запретить
	<source>	адрес источника многоадресной рассылки
	<wildcard-bit>	символ подстановки адреса группового источника
	<source-host-ip>	адрес хоста источника многоадресной передачи
	<destination>	адрес назначения многоадресной передачи



	<destination-host-ip >	адрес хоста назначения многоадресной передачи
По умолчанию	Отсутствует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Разделу списка доступа ACL группового источника присвоены специальные номера ACL от 5000 до 5099. Эта команда используется для настройки соответствующего раздела ACL. Для управления списком доступа ACL группового источника необходимо только задать IP-адрес источника и IP-адрес назначения (групповой IP-адрес). Процедура настройки в основном такая же, как и для других списков доступа ACL. Символ подстановки используется для настройки диапазона адресов, а также для указания адреса хоста, либо всех адресов. Имейте в виду, что опция "all address" (все адреса) соответствует групповому IP-адресу 224.0.0.0/4, а не 0.0.0.0/0, как в других списках доступа	
Пример	Switch(config)#access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255	

10.1.3. Список доступа для управления назначением (ip multicast destination-control access-group)

Синтаксис	ip multicast destination-control access-group <6000-7999> no ip multicast destination-control access-group <6000-7999>	
Параметр	<6000-7999>	номер списка доступа для управления назначением
По умолчанию	Отсутствует	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Команда работает, только когда управление назначением групповых данных включено в глобальном режиме конфигурации. После применения команды, если включен IGMP-SPOOFING, при добавлении интерфейса к группе, он будет проверен на согласование с настройками списка доступа, например, наличие разрешения, при этом, если согласование достигнуто, новый член будет добавлен в группу	
Пример	Switch#config Switch(config)#interface ethernet 1/0/4 Switch(config-if-ethernet1/0/4)#ip multicast destination-control access-group 6000 Switch(config-if-ethernet1/0/4)#	



10.1.4. Список доступа для управления назначением на указанном сегменте (ip multicast destination-control access-group (sip))

Синтаксис	ip multicast destination-control <IPADDRESS/M> access-group <6000-7999> no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>	
Параметр	<IPADDRESS/M>	IP-адрес и длина маски
	<6000-7999>	номер списка доступа для управления назначением
По умолчанию	Отсутствует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда работает только когда управление назначением групповых данных активировано в глобальном режиме конфигурации. Если оно включено и включен протокол IGMP-SPOOPING, возможно добавление членов в группу. Если управление назначением групповых данных в сегменте сети, указанном в сообщении igmp-report настроено, то проверяется согласование со списком доступа, при этом, если согласование достигнуто, интерфейс добавляется в группу, если нет – не добавляется. Если до ввода этой команды была задана соответствующая группа или источник, выводимый командой ip igmp groups detail, предварительно необходимо в привилегированном режиме с помощью команды clear ip igmp groups уничтожить соответствующие группы	
Пример	Switch#config Switch(config)#ip multicast destination-control 10.1.1.0/24 access-group 6000	

10.1.5. Список доступа для управления назначением на указанной сети (ip multicast destination-control access-group (vmac))

Синтаксис	ip multicast destination-control <1-4094> <macaddr > access-group <6000-7999> no ip multicast destination-control <1-4094> <macaddr > access-group <6000-7999>	
Параметр	<1-4094>	идентификатор VLAN
	<macaddr >	MAC-адрес источника, переданный в сообщении IGMP-REPORT в формате "xx-xx-xx-xx-xx-xx";



	<6000-7999>	номер списка доступа для управления назначением
По умолчанию	Отсутствует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда работает, только когда управление назначением групповых данных включено в глобальном режиме конфигурации. При применении команды, если включен протокол IGMP SPOOFING, возможно добавление членов в группу многоадресной рассылки. Если управление назначением групповых данных по MAC-адресу источника, полученного в сообщении igmp-report настроено, то проверяется согласование со списком доступа, например, разрешение (permit), при этом, если согласование достигнуто, интерфейс будет добавлен в группу	
Пример	Switch#config Switch(config)#ip multicast destination-control 1 00-01-03-05-07-09 access-group 6000	

10.1.6. Политика обслуживания группового трафика (ip multicast policy)

Синтаксис	ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority> no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos	
Параметр	<IPADDRESS/M>	групповой адрес источника, длина маски, адрес назначения, отдельная длина маски
	<priority>	заданный приоритет, в диапазоне от 0 до 7
По умолчанию	Отсутствует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет изменить настройки, одновременно устанавливая один и тот же приоритет для указанного в ней потока групповых данных и типа обслуживания (TOS). Имейте в виду, что приоритет пакетов, переданных в режиме UNTAG (без меток), изменен не будет	
Пример	Switch(config)#ip multicast policy 10.1.1.0/24 225.1.1.0/24 cos 7	



10.1.7. Управление групповым источником (ip multicast source-control)

Синтаксис	ip multicast source-control no ip multicast source-control
Параметр	Отсутствует
По умолчанию	Отключено
Режим	Режим глобальной конфигурации
Руководство по использованию	Управление источником по списку доступа применяется к интерфейсу только тогда, когда управление групповым источником включено в глобальном режиме конфигурации, и подключает контроль без необходимости настраивать списки доступа на каждом интерфейсе. После ввода команды групповые данные, принятые от интерфейсов и не согласующиеся со списком доступа для группового источника, будут отброшены коммутатором. Только групповые данные, согласующиеся с параметром PERMIT будут приняты коммутатором и переданы в соответствующие интерфейсы
Пример	Switch(config)#ip multicast source-control

10.1.8. Управление источником групповых данных (ip multicast source-control access-group)

Синтаксис	ip multicast source-control access-group <5000-5099> no ip multicast source-control access-group <5000-5099>	
Параметр	<5000-5099>	номера списка доступа для управления источником
По умолчанию	Отсутствует	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Команда работает, только когда управление источником групповых данных включено в глобальном режиме конфигурации. После этого команда будет сопоставлять сообщения многоадресной рассылки, импортируемые с интерфейса, в соответствии с настроенным списком доступа, например, permit, сообщение будет получено и передано; в противном случае сообщение будет отброшено	
Пример	Switch (config)#interface ethernet1/0/4 Switch (config-if-ethernet1/0/4)#ip multicast source-control access-group 5000 Switch (config-if-ethernet1/0/4)#	



10.1.9. Управление назначением многоадресной рассылки (ip multicast destination-control)

Синтаксис	ip multicast destination-control
Параметр	Отсутствует
По умолчанию	Отключено
Режим	Режим глобальной конфигурации
Руководство по использованию	Только после того, как управление назначением multicast-трафика включено в глобальном режиме конфигурации, станут работать остальные настройки управления назначением; список доступа назначения может применяться к портам, VLAN-MAC и SIP. После ввода данной команды IGMP-SNOOPING и IGMP будут выполнять проверку на соответствие правилам, при попытке добавления интерфейса после получения сообщения IGMP REPORT
Пример	Switch(config)#ip multicast destination-control

10.1.10. Добавление правила profile-id (Список правил управления многоадресной рассылкой) (profile-id (Multicast Destination Control Rule List))

Синтаксис	profile-id <1-50> (deny permit) ip ((<source> <wildcard-bit>) (host-source <source-host-ip> [range <2-65535>]) any-source) ((<destination> <wildcard-bit>) (host-destination <destination-host-ip> [range <2-255>]) any-destination) no profile-id <1-50>	
Параметр	<1-50>	profile-id
	deny permit	решить или запретить
	<source>	адрес источника многоадресной передачи
	<wildcard-bit>	символ подстановки адреса группового источника
	<source-host-ip>	адрес хоста источника многоадресной передачи
	<2-65535>	диапазон хостов источника многоадресной рассылки



	<destination>	адрес назначения многоадресной передачи
	<destination-host-ip>	адрес хоста назначения многоадресной передачи
	<2-255>	диапазон хостов назначения многоадресной рассылки
По умолчанию	отсутствуют	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Список профилей из списка управления многоадресной рассылкой контролируется определенным номером profile-id от 1 до 50, команда применяется для настройки этого профиля и добавления его в ACL. Для управления многоадресной рассылкой требуется задать только IP-адрес источника и IP-адрес назначения (IP-адрес группы) Метод настройки в основном такой же, как и в ACL, с использованием длины маски для задания диапазона адресов, также можно указать адрес хоста или все адреса. Имейте в виду, что опция “all address” (все адреса) соответствует групповому IP-адресу 224.0.0.0/4, а не 0.0.0.0/0, как в других списках доступа	
Пример	switch(config)# profile-id 1 deny ip any-source host-destination 224.1.1.2	

10.1.11. Вывод настроек назначения (show ip multicast destination-control)

Синтаксис	<pre>show ip multicast destination-control [detail] show ip multicast destination-control interface <Interfacename> [detail] show ip multicast destination-control host-address <ipaddress> [detail] show ip multicast destination-control <vlan-id> <mac-address> [detail]</pre>	
Параметр	detail	задает, выводить ли детальную информацию
	<Interfacename>	имя интерфейса или имя группы интерфейсов, например, Ethernet1/0/1, port-channel 1 или ethernet1/0/1
	<ipaddress>	IP адрес
	<vlan-id>	идентификатор VLAN
	<mac-address>	Mac-адрес



По умолчанию	Отсутствует
Режим	Привилегированный режим и глобальной конфигурации
Руководство по использованию	Команда выводит на экран настройки правил управления назначением группового трафика, в том числе, когда выбрана опция detail, детальную информацию о них, а также детальную информацию о списке доступа
Пример	Switch#show ip multicast destination-control ip multicast destination-control is enabled multicast destination-control access-group 6000 used on interface Ethernet1/0/4

10.1.12. Вывод настроек списка доступа для управления назначением (show ip multicast destination-control access-list)

Синтаксис	show ip multicast destination-control access-list show ip multicast destination-control access-list <6000-7999>	
Параметр	<6000-7999>	номер списка доступа
По умолчанию	Отсутствует	
Режим	Привилегированный режим и глобальной конфигурации	
Руководство по использованию	Команда отображает настройки списка доступа для управления назначением многоадресного трафика	
Пример	Switch#show ip multicast destination-control access-list access-list 6000 permit ip 10.1.1.1 0.0.0.255 232.0.0.0 0.0.0.255	

10.1.13. Вывод списка профилей для контроля назначения (show ip multicast destination-control filter-profile-list)

Синтаксис	show ip multicast destination-control filter-profile-list show ip multicast destination-control filter-profile-list <1-50>	
Параметр	<1-50>	profile-id
По умолчанию	Отсутствует	
Режим	Привилегированный режим и глобальной конфигурации	



Руководство по использованию	Эта команда может показать список настроенных правил профиля управления назначения
Пример	Switch#show l2-address-table multicast vlan 1 Vlan Address Insert Тип Creator Ports

10.1.14. Вывести информацию о настройках политики обслуживания группового трафика (show ip multicast policy)

Синтаксис	show ip multicast policy
Параметр	Отсутствует
По умолчанию	Отсутствует
Режим	Привилегированный режим и глобальной конфигурации
Руководство по использованию	Команда выводит информацию о настройках политики обслуживания группового трафика
Пример	<pre>Switch#show ip multicast policy</pre> <pre>ip multicast-policy 10.1.1.0/24 225.0.0.0/8 cos 5</pre>

10.1.15. Вывод настроек управления групповым трафиком (show ip multicast source-control)

Синтаксис	<pre>show ip multicast source-control [detail]</pre> <pre>show ip multicast source-control interface <Interfacename> [detail]</pre>	
Параметр	detail	задает, выводить ли детальную информацию
	<Interfacename>	имя интерфейса, например, ethernet 1/0/1 или ethernet1/0/1
По умолчанию	Отсутствует	
Режим	Привилегированный режим и глобальной конфигурации	
Руководство по использованию	Команда выводит на дисплей настройки правил управления групповым источником, в том числе, когда выбрана опция detail, детальную информацию о списке доступа	



Пример	Switch#show ip multicast source-control detail ip multicast source-control is enabled Interface Ethernet1/0/13 use multicast source control access-list 5000 access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255 access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255	
Параметр	<5000-5099>	номер списка доступа
По умолчанию	Отсутствует	
Режим	Привилегированный режим и глобальной конфигурации	
Руководство по использованию	Команда выводит настройки списка доступа многоадресного трафика для управления источником группового трафика	
Пример	Switch#show ip multicast source-control access-list access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255 access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255	

10.1.16. Удаление записи о группе в vlan (clear ip igmp snooping vlan)

Синтаксис	clear ip igmp snooping vlan <1-4094> groups [A.B.C.D]	
Параметр	<1-4094>	идентификатор VLAN
	[A.B.C.D]	адрес группы
По умолчанию	Отсутствует	
Режим	Привилегированный режим	
Руководство по использованию	Используйте команду с "show" в начале для контроля удаления записи о группе	
Пример	Switch#clear ip igmp snooping vlan 1 groups	

10.1.17. Удаление mrouter-порт в vlan (clear ip igmp snooping vlan <1-4094> mrouter-port)

Синтаксис	clear ip igmp snooping vlan <1-4094> mrouter-port [ethernet] IFNAME	
Параметр	<1-4094>	идентификатор VLAN



	IFNAME	имя порта
По умолчанию	Отсутствует	
Режим	Привилегированный режим	
Руководство по использованию	Используйте команду для контроля удаления информации о порте mrouter в указанном vlan	
Пример	Удалить порт mrouter port в vlan 1. Switch#clear ip igmp snooping vlan 1 mrouter-port	

10.1.18. Включение функции IGMP Snooping (ip igmp snooping)

Синтаксис	ip igmp snooping no ip igmp snooping
Параметр	отсутствуют
По умолчанию	Протокол IGMP Snooping не включен
Режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду для активации IGMP Snooping. После этого можно будет настроить работу IGMP snooping на каждом vlan. Команда " no ip igmp snooping " отключает данную функцию
Пример	Включить протокол IGMP Snooping. Switch#config Switch(config)#ip igmp snooping Switch(config)#

10.1.19. Включить функцию IGMP Snooping proxy (ip igmp snooping proxy)

Синтаксис	ip igmp snooping proxy no ip igmp snooping proxy
Параметр	отсутствуют
По умолчанию	Выключено
Режим	Режим глобальной конфигурации



Руководство по использованию	Команда включает функцию IGMP Snooping проху, команда с "no" в начале отменяет это действие
Пример	Switch#config Switch(config)#no ip igmp snooping proxy Switch(config)#

10.1.20. Настроить igmp snooping на указанном vlan (ip igmp snooping vlan)

Синтаксис	ip igmp snooping vlan <vlan-id> no ip igmp snooping vlan <vlan-id>	
Параметр	<vlan-id>	идентификатор VLAN
По умолчанию	Протокол IGMP Snooping не включен	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Для того, чтобы настроить IGMP Snooping на указанном VLAN, необходимо сначала активировать IGMP Snooping глобально. Отключение IGMP Snooping на указанном VLAN выполняется командой "no ip igmp snooping vlan <vlan-id> "	
Пример	Включить IGMP Snooping для VLAN 100 в глобальном режиме конфигурации. Switch#config Switch(config)#ip igmp snooping vlan 100	

10.1.21. Включение функции быстрого выхода для VLAN (ip igmp snooping vlan immediate-leave)

Синтаксис	ip igmp snooping vlan <vlan-id> immediate-leave no ip igmp snooping vlan <vlan-id> immediate-leave	
Параметр	<vlan-id>	идентификатор VLAN
По умолчанию	Функция выключена	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Включает функцию быстрого выхода IGMP Snooping для указанного vlan. "no" в начале команды выключает функцию быстрого выхода IGMP Snooping
Пример	Включить для VLAN 100 функцию быстрого выхода IGMP Snooping. Switch#config Switch(config)#ip igmp snooping vlan 100 immediate-leave

10.1.22. Включение функции быстрого выхода по mac-адресам (ip igmp snooping vlan <id> immediately-leave mac-based)

Синтаксис	ip igmp snooping vlan <vlan-id> immediately-leave mac-based no ip igmp snooping vlan <vlan-id> immediately-leave mac-based	
Параметр	<vlan-id>	идентификатор VLAN
По умолчанию	Функция выключена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет удалить существующие записи таблицы igmp snooping в соответствии с mac источника пакета leave, когда коммутатор с включенной функцией igmp snooping получает пакет leave. Только если полученные данные порта, mac-адреса источника и группа многоадресной рассылки пакета leave совпадают с портом, хостом mac и группой многоадресной рассылки существующей записи таблицы igmp snooping, запись таблицы snooping может быть удалена. Если эта команда не настроена, существующие записи таблицы igmp snooping удаляются на основании порта и группы многоадресной рассылки, пакета leave. Чтобы команда начала работать, необходимо задать быстрый выход immediate-leave в том же vlan, чтобы эта команда начала работать. В этом случае, необходимо работать с хостом mac-адреса порта	
Пример	Используйте следующую конфигурацию для удаления записи в таблице в соответствии с хостом mac-адреса порта. <pre>Switch#config Switch(config)#ip igmp snooping vlan 12 immediate-leave Switch(config)#ip igmp snooping vlan 12 immediately-leave mac-based</pre>	



10.1.23. Установка vlan как маршрутизатор уровня 2 (ip igmp snooping vlan l2-general-querier)

Синтаксис	ip igmp snooping vlan < vlan-id > l2-general-querier no ip igmp snooping vlan < vlan-id > l2-general-querier	
Параметр	<vlan-id>	номер VLAN, в пределах <1-4094>
По умолчанию	VLAN не является маршрутизатором IGMP Snooping уровня 2	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Рекомендуется конфигурировать маршрутизатор уровня 2 на сегменте. Если функция IGMP Snooping ранее на этой vlan была выключена, после ввода этой команды она будет включена. После выключения функции маршрутизатора уровня 2 функция IGMP Snooping не будет выключена. Эта команда в основном используется для регулярной отправки общих запросов, помогающих коммутаторам внутри этого сегмента обучать порты mrouter	
	Комментарий: Существует три метода обучения mrouter при igmp snooping: 1. Порт принимает сообщения запросов IGMP 2. Порт принимает пакеты группового протокола и поддерживает DVMRP, PIM 3. Порт сконфигурирован статически	
Пример	Switch(config)#ip igmp snooping vlan 1 l2-general-querier	

10.1.24. Установка адреса источника для маршрутизатора (ip igmp snooping vlan l2-general-querier-source)

Синтаксис	ip igmp snooping vlan < vlan-id > l2-general-querier-source <A.B.C.D> no ip igmp snooping vlan <vlanid> l2-general-querier-source	
Параметр	<vlan-id>	идентификатор VLAN
	<A.B.C.D>	<A.B.C.D> адрес источника операции запроса
По умолчанию	0.0.0.0	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Операционные системы Win2000/XP при запросе не поддерживают адрес 0.0.0.0, поэтому они не определяют адрес источника при запросе уровня 2. Клиент прекратит отправку запрашивающих дейтаграмм после того, как одна из них будет отправлена. И через некоторое время он не сможет получать многоадресные дейтаграммы
Пример	Switch(config)#ip igmp snooping vlan 2 L2-general-query-source 192.168.1.2

10.1.25. Настройка версии маршрутизатора (ip igmp snooping vlan l2-general-querier-version)

Синтаксис	ip igmp snooping vlan <vlanid> l2-general-querier-version <version>	
Параметр	<vlan-id>	идентификатор VLAN
	<version>	номер версии, в пределах <1 — 3>
По умолчанию	версия 3	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Когда коммутатор подключен к среде, поддерживающей V1 и V2, для VLAN, имеющих второй уровень источника настройки запроса, VLAN может быть запрошена только в том случае, если указан номер версии. Эта команда используется для запроса номера версии второго уровня	
Пример	Switch(config)#ip igmp snooping vlan 2 l2-general-querier-version 2	

10.1.26. Максимальное число групп и их источников (ip igmp snooping vlan limit)

Синтаксис	ip igmp snooping vlan <vlanid> limit {group <g_limit> source <s_limit>} no ip igmp snooping vlan <vlan-id> limit	
Параметр	<vlan-id>	идентификатор VLAN
	<g_limit>	<1 — 65535>, максимальное число создаваемых групп
	<s_limit>	<1-65535>, максимальное количество записей источников в каждой группе, состоящей из включаемых и исключаемых источников
По умолчанию	Не более 50 групп, в каждой группе может быть не более 40 источников	



Режим	Режим глобальной конфигурации
Руководство по использованию	Когда число вступивших в группу достигнет заданного предельного значения, новые запросы на вступление в группу будут отвергаться для предотвращения сетевых атак. Для того, чтобы эту команду можно было использовать, на VLAN должна быть включена IGMP snooping. При вводе формы команды с “no” в начале, будут восстановлены настройки по умолчанию, при этом они отличаются от настройки “no limit” (число вступающих в группу не ограничено). По соображениям безопасности в этой команде не следует использовать опцию “no limit”. Рекомендуется использовать настройки по умолчанию и максимально точно следовать настройкам IGMP, если активен Layer 3 IGMP
Пример	Switch(config)#ip igmp snooping vlan 2 limit group 300

10.1.27. Максимальное количество групп и их источников для интерфейса IFNAME (ip igmp snooping vlan interface (ethernet | port-channel) IFNAME limit)

Синтаксис	ip igmp snooping vlan <vlanid> interface (ethernet port-channel) IFNAME limit {group <g_limit> source <s_limit>} strategy (replace drop) no ip igmp snooping vlan <1-4094> interface (ethernet port-channel) IFNAME limit group source strategy	
Параметр	<vlan-id>	Идентификатор VLAN
	IFNAME	Название интерфейса
	<g_limit>	<1-65535>, максимальное количество групп, которым разрешено присоединиться
	<s_limit>	<1-65535>, максимальное количество записей в таблице источников в каждой группе, с учетом включения в группу и исключения из нее
	replace	заменить информацию о группе и источнике
	drop	сбросить информацию о группе и источнике
По умолчанию	Ограничений не установлено	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Если количество групп, добавленных для порта, или количество источников для этой группы превысит установленный лимит, это будет обработано в соответствии с заданной политикой. Если задано drop,	



	новая группа и информация об источнике отбрасываются; Если задано replace, определяются динамические группы и источники в порту, удаляются и заменяются, а затем добавляется новая информация о группах и источниках. Для применения этой команды необходимо чтобы в данной VLAN была включена функция IGMP Snooping. Отсутствие команды настраивается как «без ограничений»
Пример	Switch(config)#ip igmp snooping vlan 2 interface ethernet 1/0/11 limit group 300 source 200 strategy replace

10.1.28. Статический порт mrouter на vlan (ip igmp snooping vlan mrouter-port interface)

Синтаксис	ip igmp snooping vlan <vlanid> mrouter-port interface [ehternet port-channel] <ifname> no ip igmp snooping vlan <vlan-id> mrouter-port interface[<ehternet> <port-channel>] <ifname>	
Параметр	<vlan-id>	идентификатор VLAN
	IFNAME	имя интерфейса
По умолчанию	Статический порт mrouter на vlan отсутствует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Когда порт является статическим портом mrouter и одновременно с этим – динамическим портом mrouter, он должен использоваться как статический порт mrouter. Удаление статического порта mrouter может быть выполнено только "no" в начале команды	
Пример	Switch(config)#ip igmp snooping vlan 2 mrouter-port interface ethernet1/0/13	

10.1.29. Динамическое добавление Mrouter порта для VLAN (ip igmp snooping vlan mrouter-port learnpim)

Синтаксис	ip igmp snooping vlan <vlanid> mrouter-port learnpim no ip igmp snooping vlan <vlan-id> mrouter-port learnpim	
Параметр	<vlan-id>	идентификатор VLAN
По умолчанию	Выключено	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда включает функцию, при которой указанная VLAN узнает mrouter-port (в соответствии с пакетами pim). Когда порт получает пакет pim, он настраивается как порт mrouter для автоматического обучения
Пример	Отключить функцию, при которой vlan 100 узнает mrouter-port (в соответствии с пакетами pim). Switch(config)#no ip igmp snooping vlan 100 mrouter-port learnpim

10.1.30. Задать срок жизни порта mrouter (ip igmp snooping vlan mrpt)

Синтаксис	ip igmp snooping vlan <vlanid> mrpt <value> no ip igmp snooping vlan <vlan-id> mrpt	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне <1-4094>
	<value>	срок жизни порта mrouter в диапазоне <1-65535> секунд
По умолчанию	255 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда корректна только для динамических портов mrouter. Для того, чтобы эту команду можно было использовать, на vlan должен быть включен IGMP snooping	
Пример	Switch(config)#ip igmp snooping vlan 2 mrpt 100	

10.1.31. Задать интервал отправки запросов (ip igmp snooping vlan query-interval)

Синтаксис	ip igmp snooping vlan <vlanid> query-interval < value > no ip igmp snooping vlan < vlan-id > query-interval	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне <1-4094>
	<value>	интервал выдачи запросов, в пределах <1-65535> секунд
По умолчанию	125 секунд	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Рекомендуется использовать настройку, заданную по умолчанию. По возможности согласуйте эту настройку с настройками IGMP, если протокол IGMP уровня 3 включен
Пример	Switch(config)#ip igmp snooping vlan 2 query-interval 130

10.1.32. Максимальный интервал времени ожидания ответа (ip igmp snooping vlan query-mrsp)

Синтаксис	ip igmp snooping vlan <vlanid> query-mrsp < value > no ip igmp snooping vlan < vlan-id > query-mrspt	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне <1-4094>
	<value>	интервал в пределах <1-25> секунд
По умолчанию	10 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Рекомендуется использовать настройку, заданную по умолчанию. По возможности согласуйте эту настройку с настройками IGMP, если протокол IGMP уровня 3 включен	
Пример	Switch(config)#ip igmp snooping vlan 2 query-mrsp 18	

10.1.33. Задать надежность запроса (ip igmp snooping vlan query-robustness)

Синтаксис	ip igmp snooping vlan <vlanid> query-robustness <value> no ip igmp snooping vlan <vlan-id> query-robustness	
Параметр	<vlan-id>	идентификатор VLAN
	<value>	диапазон <2-10>
По умолчанию	2с	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Рекомендуется использовать настройку, заданную по умолчанию. По возможности согласуйте эту настройку с настройками IGMP, если протокол IGMP уровня 3 включен	



Пример	Switch(config)#ip igmp snooping vlan 2 query-robustness 3

10.1.34. IP-адрес источника при перенаправлении IGMP сообщений (ip igmp snooping vlan report source-address)

Синтаксис	ip igmp snooping vlan <vlanid> report source-address <A.B.C.D> no ip igmp snooping vlan <vlan-id> report source-address	
Параметр	<vlan-id>	идентификатор VLAN
	<A.B.C.D>	IP-адрес, может быть 0.0.0.0
По умолчанию	Отключено	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Рекомендуется настройка по умолчанию. Если необходимо настроить IGMP snooping, адрес источника для пересылаемых IGMP-сообщений может быть 0.0.0.0. Если вышестоящие устройства требуют в IGMP сообщениях одинаковый адрес сети, то адрес источника IGMP сообщений необходимо задать такой же как вышестоящий	
Пример	Switch(config)#ip igmp snooping vlan 2 report source-address 10.1.1.1	

10.1.35. Максимальное время ответа на запросы принадлежности (ip igmp snooping vlan specific-query-mrsp)

Синтаксис	ip igmp snooping vlan <vlanid> specific-query-mrsp <value> no ip igmp snooping vlan <vlan-id> specific-query-mrspt	
Параметр	<vlan-id>	конкретный идентификатор VLAN, диапазон от 1 до 4094
	<value>	максимальное время ответа на запрос, единица измерения - секунда, диапазон от 1 до 25, по умолчанию 1
По умолчанию	Выключено	
Режим	Режим глобальной конфигурации	
Руководство по использованию	После включения vlan snooping в глобальном режиме ввод этой команды позволит настроить максимальное время ответа на запрос для определенной группы	



Пример	Настроить/отменить specific-query-mrsp для vlan3 как 2 секунды. Switch(config)#ip igmp snooping vlan 3 specific-query-mrsp 2 Switch(config)#no ip igmp snooping vlan 3 specific-query-mrsp

10.1.36. Задать статическую группу на указанном порту vlan (ip igmp snooping vlan static-group)

Синтаксис	ip igmp snooping vlan <vlanid> static-group <A.B.C.D> [source <A.B.C.D>] interface [ethernet port-channel] <IFNAME> no ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>] interface [ethernet port-channel] <IFNAME>	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне <1-4094>
	<A.B.C.D>	адрес группы или источника
	<IFNAME>	имя интерфейса
По умолчанию	Отсутствует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет задать статическую группу на указанном порту vlan. "no" в начале команды отменяет данную конфигурацию. Когда порт является статическим портом и одновременно с этим динамическим портом, он должен использоваться как статический порт. Удалить статическую группу можно только формой команды с "no" в начале команды	
Пример	Switch(config)#ip igmp snooping vlan 1 static-group 224.1.1.1 source 192.168.1.1 interface ethernet 1/0/1	

10.1.37. Задать время подавления запроса (ip igmp snooping vlan suppression-query-time)

Синтаксис	ip igmp snooping vlan <vlanid> suppression-query-time <value> no ip igmp snooping vlan <vlan-id> suppression-query-time	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне <1-4094>
	<value>	в диапазоне <1 — 65535> секунд
По умолчанию	255 секунд	



Режим	Режим глобальной конфигурации
Руководство по использованию	Команда позволяет задать время подавления запроса. Команда " по ip igmp snooping vlan < vlan-id > suppression-query-time " возвращает значение по умолчанию. Эта команда может быть выдана только для маршрутизатора уровня 2. Команда Suppression-query-time устанавливает период, на который задается состояние подавления, в котором маршрутизатор включается, когда он принимает запрос от IGMP уровня 3 в сегментах
Пример	Switch(config)#ip igmp snooping vlan 2 suppression-query-time 270

10.1.38. Вывод информации о сконфигурированных параметрах IGMP Snooping (show ip igmp snooping)

Синтаксис	show ip igmp snooping [vlan <vlan-id>]	
Параметр	<vlan-id>	идентификатор VLAN
По умолчанию	отсутствуют	
Режим	Привилегированный режим	
Руководство по использованию	Если номер VLAN не указан, будет показано, включен ли протокол igmp snooping в глобальном режиме конфигурации, в каком VLAN настроена функция I2-general-querier. Если номер VLAN указан, на дисплей будут выведены детальные сообщения IGMP для этой vlan	
Пример	1. Показать сводные сообщения IGMP Snooping для коммутатора Switch(config)#show ip igmp snooping Global igmp snooping status: Enabled L3 multicasting: running Igmp snooping is turned on for vlan 1(querier) Igmp snooping is turned on for vlan 2	
	Информация, отображаемая на экране	Пояснение
	Global igmp snooping status	Включен ли igmp snooping в глобальном режиме конфигурирования коммутатора
	L3 multicasting	Включен ли multicast-протокол уровня 3 коммутатора



Igmp snooping is turned on for vlan 1(querier)

На каких vlan коммутатора включена функция igmp snooping коммутатора и какие из них являются маршрутизаторами уровня 2

2.Вывести на дисплей детальную информацию IGMP Snooping для vlan1. Switch#show ip igmp snooping vlan 1

Igmp snooping information for vlan 1

Igmp snooping L2 general querier : Yes(COULD_QUERY)

Igmp snooping query-interval : 125(s)

Igmp snooping max reponse time : 10(s)

Igmp snooping robustness : 2

Igmp snooping mrouter port keep-alive time : 255(s)

Igmp snooping query-suppression time : 255(s)

IGMP Snooping Connect Group Membership

Note: *-All Source, (S)- Include Source, [S]-Exclude Source Groups
Sources Ports Exptime System Level 238.1.1.1 (192.168.0.1)

Ethernet1/0/8 00: 04: 14 V2

(192.168.0.2) Ethernet1/0/8 00: 04: 14 V2

Igmp snooping vlan 1 mrouter port Note: "! "-static mrouter port

! Ethernet1/0/2

Информация, отображаемая на экране	Пояснение
Igmp snooping L2 general querier	Включена ли для vlan функция маршрутизатора уровня 2, статус маршрутизатора: разрешены или подавлены запросы
Igmp snooping query-interval	Интервал запроса, установленный на vlan
Igmp snooping max reponse time	Максимальное время ответа vlan
Igmp snooping robustness	Надежность IGMP Snooping заданная на vlan
Igmp snooping mrouter port keep-alive time	Срок жизни динамического порта mrouter на vlan
Igmp snooping query-suppression time	Интервал времени подавления запросов VLAN когда она работает в качестве маршрутизатора уровня 2



	IGMP Snooping Connect Group Membership	Группа в данной VLAN, т.е. соответствие между портом и (S,G)
	Igmp snooping vlan 1 mrouter port	Порт mrouter vlan: статический и динамический

10.1.39. Удаление записи о группе в указанном vlan (clear ipv6 mld snooping vlan)

Синтаксис	clear ipv6 mld snooping vlan <1-4094> groups [X: X: : X: X]	
Параметр	<1-4094>	идентификатор VLAN
	[X: X: : X: X]	указанный адрес группы
По умолчанию	Отсутствует	
Режим	Привилегированный режим	
Руководство по использованию	Команда удаляет запись о группе в указанном VLAN. Используйте команду с "show" в начале для контроля удаления записи о группе	
Пример	Удалить все группы. Switch#clear ipv6 mld snooping vlan 1 groups	

10.1.40. Удаление порта mrouter в указанном vlan (clear ipv6 mld snooping vlan <1-4094> mrouter-port)

Синтаксис	clear ipv6 mld snooping vlan <1-4094> mrouter-port [ethernet] IFNAME	
Параметр	<1-4094>	идентификатор VLAN
	IFNAME	имя порта
По умолчанию	Отсутствует	
Режим	Привилегированный режим	
Руководство по использованию	Удаляет mrouter-порт в указанном VLAN. Используйте команду с "show" в начале для контроля удаления записи о группе	



Пример	Удалить mrouter-порт в vlan 1. Switch#clear ipv6 mld snooping vlan 1 mrouter-port

10.1.41. Включение функции MLD Snooping (ipv6 mld snooping)

Синтаксис	ipv6 mld snooping no ipv6 mld snooping
Параметр	Отсутствует
По умолчанию	Функция MLD Snooping выключена
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда позволяет в глобальном режиме конфигурации включить функцию MLD Snooping на коммутаторе, позволяет настроить MLD Snooping на каждой VLAN. "no" в начале команды отключит MLD Snooping на всех VLAN и глобально
Пример	Включить функцию MLD Snooping в глобальном режиме конфигурации. Switch(config)#ipv6 mld snooping

10.1.42. Включение MLD Snooping в указанной VLAN (ipv6 mld snooping vlan)

Синтаксис	ipv6 mld snooping vlan <vlan-id> no ipv6 mld snooping vlan <vlan-id>	
Параметр	<vlan-id>	идентификатор VLAN с действующим диапазоном <1-4094>
По умолчанию	Функция MLD Snooping в VLAN выключена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда включает MLD Snooping в указанной VLAN. "no" в начале команды отключает MLD Snooping на указанной VLAN. Для того, чтобы настроить MLD Snooping на указанной vlan, необходимо сначала включить MLD Snooping в глобальном режиме конфигурации. Команда "no ipv6 mld snooping vlan vid" отключает MLD Snooping на указанной vlan	



Пример	Включить MLD snooping в VLAN 100 в глобальном режиме конфигурации. Switch(config)#ipv6 mld snooping vlan 100

10.1.43. Функция быстрого выхода протокола MLD для указанной vlan (ipv6 mld snooping vlan immediate-leave)

Синтаксис	ipv6 mld snooping vlan <vlan-id> immediate-leave no ipv6 mld snooping vlan <vlan-id> immediate-leave	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне <1-4094>
По умолчанию	Функция отключена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда включает функцию быстрого выхода протокола MLD для указанной VLAN. “no” в начале команды отключает функцию быстрого выхода протокола MLD. Команда включения функции быстрого выхода протокола MLD ускоряет процесс выхода multicast-группы из порта, при этом указанной группе запрос не посылается, а просто непосредственно удаляется порт	
Пример	Включить для VLAN 100 функцию быстрого выхода протокола MLD. Switch(config)#ipv6 mld snooping vlan 100 immediate-leave	

10.1.44. Установить указанный vlan, как маршрутизатор уровня 2 (ipv6 mld snooping vlan l2-general-querier)

Синтаксис	ipv6 mld snooping vlan <vlan-id> l2-general-querier no ipv6 mld snooping vlan <vlan-id> l2-general-querier	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне <1-4094>
По умолчанию	VLAN не является маршрутизатором уровня 2 для протокола MLD Snooping	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Рекомендуется конфигурировать маршрутизатор уровня 2 на сегменте. Если до ввода этой команды MLD snooping не включен для этой VLAN, то описываемая команда выполнена не будет. После выключения функции маршрутизатора уровня 2 протокол MLD вместе с ней выключен не будет. Основная задача этой команды – формирование	



	периодических запросов, помогающих коммутатору сегмента обучить порт mrouter. Комментарий: В MLD Snooping имеется три способа обучения порта mrouter: 1. Порт принимает сообщения с запросами MLD. 2. Порт принимает пакеты multicast-протокола и поддерживает PIM. 3. Порт сконфигурирован статически
Пример	Установить VLAN 100 как маршрутизатор уровня 2. <pre>Switch(config)#ipv6 mld snooping vlan 100 l2-general-querier</pre>

10.1.45. Максимальное число групп MLD snooping и их источников (ipv6 mld snooping vlan limit)

Синтаксис	<pre>ipv6 mld snooping vlan <vlan-id> limit {group <g_limit> source <s_limit>} no ipv6 mld snooping vlan < vlan-id > limit</pre>	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне <1-4094>
	<g_limit>	максимальное количество присоединенных групп, в диапазоне: 1-65535
	<s_limit>	максимальное число источников в группе, состоящих из источников внутри группы и внешних источников группы, в диапазоне: 1-65535
По умолчанию	Не более 50 групп, в каждой группе может быть не более 40 источников	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Когда число вступивших в группу достигнет заданного предельного значения, новые запросы на вступление в группу будут отвергаться для предотвращения сетевых атак. Для того, чтобы эту команду можно было использовать, MLD snooping должен быть включен на VLAN. При вводе формы команды с "no" в начале, будут восстановлены настройки по умолчанию, при этом они отличаются от настройки "no limit" (число вступающих в группу не ограничено). По соображениям безопасности в этой команде не следует использовать опцию "no limit". Если включен протокол MLD уровня 3, рекомендуется использовать настройку по умолчанию, при этом она, насколько возможно, должна соответствовать конфигурации протокола MLD	
Пример	<pre>Switch(config)#ipv6 mld snooping vlan 2 limit group 300</pre>	



10.1.46. Установка статического порта mrouter для VLAN (ipv6 mld snooping vlan mrouter-port interface)

Синтаксис	ipv6 mld snooping vlan <vlan-id> mrouter-port interface [ethernet port-channel] <ifname> no ipv6 mld snooping vlan <vlan-id> mrouter-port interface [ethernet port-channel] <ifname>	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне <1-4094>
	<ifname>	имя интерфейса
По умолчанию	Если в порту одновременно имеется и статический, и динамический порт mrouter, предпочтительнее использовать статический mrouter. Удаление статического порта mrouter выполняется формой команды с "no" в начале	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать статический порт mrouter для VLAN. "no" в начале команды отменяет конфигурацию	
Пример	Switch(config)#ipv6 mld snooping vlan 2 mrouter-port interface ethernet1/0/13	

10.1.47. Получение информации о mrouter-порт на основе пакетов IPv6 PIM (ipv6 mld snooping vlan mrouter-port learnpim6)

Синтаксис	ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6 no ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6	
Параметр	<vlan-id>	идентификатор VLAN в диапазоне от 1 до 4094
По умолчанию	Выключено	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает функцию, которая позволяет указанной сети VLAN получить информацию о порте многоадресного маршрутизатора (на основе пакетов PIMv6). После того как порт получит пакеты pimv6, он будет настроен как порт mrouter для реализации автоматического обучения	
Пример	Отключите функцию, при которой vlan 100 обучает mrouter-port (на основе пакетов pimv6). Switch(config)#ipv6 mld snooping vlan 2 mrouter-port learnpim6	



10.1.48. Настройка срока жизни порта mrouter (ipv6 mld snooping vlan mrpt)

Синтаксис	ipv6 mld snooping vlan <vlan-id> mrpt <value> no ipv6 mld snooping vlan <vlan-id> mrpt	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне <1-4094>
	<value>	срок жизни порта mrouter, в пределах <1-65535> секунд
По умолчанию	255 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать срок жизни порта mrouter. Эта команда может быть применена к динамическому порту mrouter, но не к статическому. Для того, чтобы эту команду можно было использовать, на vlan должен быть включен протокол MLD snooping	
Пример	Switch(config)#ipv6 mld snooping vlan 2 mrpt 100	

10.1.49. Задать интервал отправки запросов (ipv6 mld snooping vlan query-interval)

Синтаксис	ipv6 mld snooping vlan <vlan-id> query-interval <value> no ipv6 mld snooping vlan <vlan-id> query-interval	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне <1-4094>
	<value>	интервал отправки запросов, диапазон: <1-65535> секунд
По умолчанию	125 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет задать интервал отправки запросов. Если включен протокол MLD уровня 3, рекомендуется использовать настройку по умолчанию, при этом она, по возможности, должна соответствовать конфигурации протокола MLD	
Пример	Switch(config)#ipv6 mld snooping vlan 2 query-interval 130	



10.1.50. Максимальный интервал времени ожидания ответа (ipv6 mld snooping vlan query-mrsp)

Синтаксис	ipv6 mld snooping vlan <vlan-id> query-mrsp <value> no ipv6 mld snooping vlan <vlan-id> query-mrspt	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне <1-4094>
	<value>	в диапазоне <1-25> секунд
По умолчанию	10 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет настроить максимальный интервал времени ожидания ответа. “no” в начале команды восстанавливает значение по умолчанию. Если включен протокол MLD уровня 3, рекомендуется использовать настройку по умолчанию, при этом она, по возможности, должна соответствовать конфигурации протокола MLD	
Пример	Switch(config)#ipv6 mld snooping vlan 2 query-mrsp 18	

10.1.51. Количество MLD Query без ответа до удаления MLD snooping для VLAN (ipv6 mld snooping vlan query-robustness)

Синтаксис	ipv6 mld snooping vlan <vlan-id> query-robustness <value> no ipv6 mld snooping vlan <vlan-id> query-robustness	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне <1-4094>
	<value>	в диапазоне <2-10>
По умолчанию	2с	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда задает надежность запроса. “no” в начале команды восстанавливает значения по умолчанию. Если включен протокол MLD уровня 3, рекомендуется использовать настройку по умолчанию, при этом она, по возможности, должна соответствовать конфигурации протокола MLD	
Пример	Switch(config)#ipv6 mld snooping vlan 2 query-robustness 3	



10.1.52. Задать в указанном порту VLAN статическую группу (ipv6 mld snooping vlan static-group)

Синтаксис	ipv6 mld snooping vlan <vlan-id> static-group <X: X: : X: X> [source< X: X: : X: X>] interface [ethernet port-channel] <IFNAME> no ipv6 mld snooping vlan <vlan-id> static-group <X: X: : X: X> [source< X: X: : X: X>] interface [ethernet port-channel] <IFNAME>	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне 1-4094
	<X: X: : X: X>	Адрес группы или источника
	<IFNAME>	имя интерфейса
По умолчанию	Отсутствует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет задать статическую группу на указанном порту vlan. "no" в начале команды отменяет данную конфигурацию. Когда порт является статическим портом и одновременно с этим динамическим портом, он должен использоваться как статический порт. Удалить статическую статическую группу можно только формой команды с "no" в начале команды	
Пример	Switch(config)#ipv6 mld snooping vlan 2 static-group ff1e: : 15 source 2000: : 1 interface ethernet 1/0/1	

10.1.53. Задать время подавления запроса (ipv6 mld snooping vlan suppression-query-time)

Синтаксис	ipv6 mld snooping vlan <vlan-id> suppression-query-time <value> no ipv6 mld snooping vlan <vlan-id> suppression-query-time	
Параметр	<vlan-id>	идентификатор VLAN, в диапазоне: <1-4094>
	<value>	значение в диапазоне: <1-65535> секунд
По умолчанию	255 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать время подавления запроса. "no" в начале команды восстанавливает значение по умолчанию.	



	Эта команда может быть задана только для маршрутизатора уровня 2. Время подавления запроса Suppression-query-time определяет интервал времени, в течение которого будут подавляться принятые в сегменте запросы маршрутизатора уровня 3 протокола MLD. Для использования этой команды необходимо, чтобы интервалы запросов разных коммутаторов одного и того же сегмента сети совпадали. Рекомендуется использовать настройку, заданную по умолчанию.
Пример	Switch(config)#ipv6 mld snooping vlan 2 suppression-query-time 270

10.1.54. Вывод настроек MLD Snooping (show ipv6 mld snooping)

Синтаксис	show ipv6 mld snooping [vlan <vlan-id>]	
Параметр	<vlan-id>	идентификатор VLAN
По умолчанию	отсутствуют	
Режим	Привилегированный режим	
Руководство по использованию	Если номер VLAN не указан, будет выведена информация о том, включен ли протокол MLD snooping в глобальном режиме конфигурации и multicast-протокол уровня 3, а также на каком VLAN включен протокол MLD Snooping и сконфигурирован маршрутизатор уровня 2. Если номер VLAN указан, на дисплей будет выведена подробная информация протокола MLD Snooping для этого VLAN.	
Пример	1. Вывести сводную информацию для протокола MLD snooping коммутатора Switch(config)#show ipv6 mld snooping Global mld snooping status: Enabled L3 multicasting: running Mld snooping is turned on for vlan 1(querier) Mld snooping is turned on for vlan 2	



Информация, отображаемая на экране	Пояснение
Global mld snooping status	Включен или нет протокол MLD Snooping в глобальном режиме конфигурирования на коммутаторе
L3 multicasting	Включен или нет multicast-протокол уровня 3 на коммутаторе
Mld snooping is turned on for vlan 1(querier)	На какой VLAN коммутатора включен протокол MLD Snooping, является ли VLAN маршрутизатором уровня 2

2.Вывести подробную информацию для протокола MLD snooping интерфейса vlan1.

```
Switch#show ipv6 mld snooping vlan 1
Mld snooping information for vlan 1
Mld snooping L2 general querier : Yes(COULD_QUERY)
Mld snooping query-interval : 125(s)
Mld snooping max reponse time : 10(s)
Mld snooping robustness : 2
Mld snooping mrouter port keep-alive time : 255(s)
Mld snooping query-suppression time : 255(s)
MLD Snooping Connect Group Membership
Note: *-All Source, (S)- Include Source, [S]-Exclude Source Groups Sources
Ports Exptime System Level
Ff1e: : 15 (2000: : 1) Ethernet1/0/8 00: 04: 14 V2
(2000: : 2) Ethernet1/0/8 00: 04: 14 V2

Mld snooping vlan 1 mrouter port Note: "! "-static mrouter port
! Ethernet1/0/2
```

Информация, отображаемая на экране	Пояснение
Mld snooping L2 general querier	Включен или нет маршрутизатор уровня 2 на VLAN, подавлены или посылаются запросы маршрутизатора
Mld snooping query-interval	Интервал отправки запросов в VLAN



	Mld snooping max reponse time	Максимальное время отклика для этого VLAN
	Mld snooping robustness	Надежность, заданная для VLAN
	Mld snooping mrouter port keep-alive time	Срок жизни динамического порта mrouter в этом vlan
	Mld snooping query-suppression time	Таймер VLAN подавления запросов маршрутизатора уровня 2 в состоянии подавления запросов
	MLD Snooping Connect Group Membership	Группа в данной VLAN, т.е. соответствие между портом и (S,G)
	Mld snooping vlan 1 mrouter port	Порт mrouter vlan: статический и динамический

10.1.55. Включение функции Multicast VLAN на VLAN (multicast-vlan)

Синтаксис	multicast-vlan no multicast-vlan
Параметр	отсутствуют
По умолчанию	Функция групповой VLAN не включена
Режим	Режим настройки VLAN
Руководство по использованию	Включает на VLAN функцию групповой (multicast) VLAN. “no” в начале команды отключает функцию групповой VLAN. Функция multicast VLAN не может быть включена для private VLAN. Для выключения на VLAN групповой функции VLAN, следует удалить ассоциативные связи с групповой VLAN. Имейте в виду, что с помощью этой команды не может быть сконфигурирована VLAN, назначаемая по умолчанию, и на коммутаторе допускается только одна групповая VLAN
Пример	<pre>Switch(config)#vlan 2 Switch(config-vlan2)# multicast-vlan</pre>



10.1.56. Ассоциация VLAN с Multicast VLAN (multicast-vlan association)

Синтаксис	multicast-vlan association <vlan-list> no multicast-vlan association <vlan-list>	
Параметр	<vlan-list>	<vlan-list> список идентификаторов VLAN ID, ассоциированных с групповой VLAN. <vlan-list> список идентификаторов VLAN ID, ассоциированных с групповой VLAN. Каждый VLAN может быть ассоциирован только с одним групповым VLAN, ассоциация будет успешной только в том случае, если VLAN, идентификатор которого (VLAN ID) указан в таблице, существует
По умолчанию	Групповой VLAN не ассоциирован с каким-либо VLAN	
Режим	Режим настройки VLAN	
Руководство по использованию	Ассоциирует несколько VLAN с групповой VLAN. “no” в начале команды отменяет ассоциированные связи. После того, как VLAN будет ассоциирован с групповым VLAN, когда приходит запрос на групповой трафик, многоадресные данные будут посылаться с групповой VLAN на этот порт, в результате трафик данных снизится. VLAN, ассоциированный с групповым VLAN, не должна быть private VLAN. После того, как включен групповой VLAN, обычный VLAN, кроме группового, может ассоциироваться только с другим обычным VLAN. На коммутаторе может быть настроен только один групповой VLAN	
Пример	Switch(config)#vlan 2 Switch(config-vlan2)# multicast-vlan association 3, 4	

10.1.57. Ассоциация Multicast VLAN с интерфейсом (multicast-vlan association interface)

Синтаксис	multicast-vlan association interface (ethernet port-channel) IFNAME out-tag <tag-id> no multicast-vlan association interface (ethernet port-channel) IFNAME	
Параметр	IFNAME	имя порта ethernet или порта канала
	<tag-id>	указывает vlan-тег многоадресных данных, пересылаемых связанным портом. tag-id действует только в том случае, если тег ассоциированного порта разрешает многоадресные VLAN. Диапазон от 1 до 4094



По умолчанию	Отсутствует
Режим	Режим настройки VLAN
Руководство по использованию	Команда ассоциирует указанный порт с групповой VLAN, чтобы связанные с ним порты могли принимать многоадресный поток. Команда с "no" в начале отменяет ассоциацию между портами и групповой VLAN. 'ассоциированный VLAN' и 'ассоциированный порт' групповой VLAN являются абсолютными и не влияют друг на друга в случае пересечения. Порты, являющиеся членами агрегации, не могут быть ассоциированы, но ассоциированные порты добавляться в группу портов и отменять ассоциацию. Настраиваемые типы портов включают порт-канал или порт Ethernet, порты конфигурируются только в режиме ACCESS. Порт (ассоциируемый) не может принадлежать к групповой VLAN, точно так же ассоциированный порт не может быть разделен в групповой VLAN. Если режим ассоциированного порта не установлен как ACCESS mode, режим не может быть изменен
Пример	<pre>Switch(config)#vlan 2 Switch(config-vlan2)#multicast-vlan association interface ethernet 1/2 Switch(config-vlan2)#multicast-vlan association interface port-channel 2 Switch(config-vlan2)#no multicast-vlan association interface ethernet 1/2 Switch(config-vlan2)#no multicast-vlan association interface port-channel 2</pre>

10.1.58. Выбор режима работы Multicast VLAN (multicast-vlan mode)

Синтаксис	multicast-vlan mode {dynamic compatible} no multicast-vlan mode {dynamic compatible}	
Параметр	dynamic	динамический режим
	compatible	режим совместимости
По умолчанию	Ни один из режимов не задан	
Режим	Режим настройки VLAN	
Руководство по использованию	Эта команда используется для настройки двух режимов работы многоадресного vlan; "no" в начале команды отменяет эту настройку. При настройке динамического режима порт mrouter не будет добавляться автоматически при выдаче многоадресных записей; при	



	настройке совместимого режима пакет отчета больше не будет передаваться на порт mrouter. Если настройки по умолчанию не заданы, порт mrouter будет добавляться при выдаче многоадресных записей, а пакет отчета будет передаваться на порт mrouter при его получении
Пример	Switch(config)#vlan 2 Switch(config-vlan2)# multicast vlan mode dynamic

10.1.59. Связь с Multicast Vlan на порте коммутатора (switchport association multicast-vlan)

Синтаксис	switchport association multicast-vlan <vlan-id> out-tag <tag-id> no switchport association multicast-vlan <vlan-id>	
Параметр	<vlan-id>	Многоадресная VLAN ассоциируется с портом. Каждый порт может быть связан только с одной многоадресной VLAN, ассоциация будет успешной, только если многоадресная VLAN существует
	<tag-id>	указывает vlan-тег многоадресных данных, пересылаемых связанным портом. tag-id действует только в том случае, если тег ассоциированного порта разрешает многоадресные VLAN. Диапазон от 1 до 4094
По умолчанию	По умолчанию порт не связан ни с одной многоадресной VLAN	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Связывает порт с указанной групповой VLAN. "no" в начале команды отменяет связь. После того, как VLAN будет ассоциирован с групповым VLAN, когда приходит запрос на групповой трафик, многоадресные данные будут посылаться с групповой VLAN на этот порт, в результате трафик данных снизится. Если ассоциированный порт настроен как магистральный и разрешены многоадресные VLAN, пересылается многоадресный трафик с указанным тегом vlan. Порт может быть связан с многоадресной VLAN только после того, как будет включена многоадресная VLAN	
Пример	Switch(config)#vlan 2 Switch(config-vlan2)# multicast-vlan Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode trunk Switch(config-if-ethernet1/0/1)#switchport association multicast-vlan 2 out-tag 5	



10.2. Команды настройки IGMP

10.2.1. Вывод информации таблицы маршрутизации многоадресной рассылки (show ip mroute)

Синтаксис	show ip mroute [<GroupAddr> [<SourceAddr>]] show IPv4 software multicast route table																									
Параметр	GroupAddr	показать записи многоадресной рассылки, относящиеся к данному групповому адресу																								
	SourceAddr	показать записи маршрутов многоадресной рассылки, относящиеся к данному адресу источника																								
По умолчанию	Нет																									
Режим	Привилегированный режим и режим глобальной конфигурации																									
Руководство по использованию																										
Пример	Показать все записи таблицы маршрутов многоадресной рассылки. <pre>Switch(config)#show ip mroute</pre> Name: Loopback, Index: 2002, State: 49 Name: null0, Index: 2003, State: 49 Name: sit0, Index: 2004, State: 80 Name: Vlan1, Index: 2005, State: 2005, State: 1043 Name: Vlan2, Index: 2006, State: 1002 Name: pimreg, Index: 2007, State: c1 The total matched ipmr active mfc entries is 1, unresolved ipmr entries is 0 Group The total matched ipmr active mfc entries is 1, unresolved ipmr entries is 0 <table><tr><td>Group</td><td>Origin</td><td>lif</td><td>Wrong</td><td>Wrong</td><td>Oif</td><td>TTL</td></tr><tr><td>225.1.1.1</td><td>192.168.1.136</td><td>vlan1</td><td>0</td><td></td><td>2006:</td><td>1</td></tr></table> <table><tr><td>Информация, отображаемая на экране</td><td>Пояснение</td></tr><tr><td>Name</td><td>имя интерфейса</td></tr><tr><td>Index</td><td>номер указателя интерфейса</td></tr><tr><td>State</td><td>статус интерфейса</td></tr><tr><td>The total matched ipmr active mfc entries</td><td>Общее количество совпавших активных записей mfc (кеш</td></tr></table>		Group	Origin	lif	Wrong	Wrong	Oif	TTL	225.1.1.1	192.168.1.136	vlan1	0		2006:	1	Информация, отображаемая на экране	Пояснение	Name	имя интерфейса	Index	номер указателя интерфейса	State	статус интерфейса	The total matched ipmr active mfc entries	Общее количество совпавших активных записей mfc (кеш
Group	Origin	lif	Wrong	Wrong	Oif	TTL																				
225.1.1.1	192.168.1.136	vlan1	0		2006:	1																				
Информация, отображаемая на экране	Пояснение																									
Name	имя интерфейса																									
Index	номер указателя интерфейса																									
State	статус интерфейса																									
The total matched ipmr active mfc entries	Общее количество совпавших активных записей mfc (кеш																									



		многоадресной пересылки) маршрутов IP multicast
	Unresolved ipmr entries	неразрешенные записи многоадресного маршрута IP
	Group	адрес назначения записей
	Origin Origin	адрес источника записей
	lif	входной интерфейс записей
	Wrong	пакеты, полученные с от the неправильного интерфейса
	Oif	выходной интерфейс записей
	TTL	значение TTL значение TTL

10.2.2. Вывод таблицы многоадресной маршрутизации ipv6 (show ipv6 mroute)

Синтаксис	show ipv6 mroute [<GroupAddr> [<SourceAddr>]] show IPv6 software multicast route table	
Параметр	GroupAddr	показать записи многоадресной рассылки, относящиеся к данному групповому адресу
	SourceAddr	показать записи маршрутов многоадресной рассылки, относящиеся к данному адресу источника
По умолчанию	Нет	
Режим	Привилегированный режим и режим глобальной конфигурации	
Руководство по использованию		
Пример	Показать все записи таблицы многоадресной маршрутизации IPv6 Switch(config)#show ipv6 mroute Name: Loopback, Index: 2002, State: 49 Name: Vlan1, Index: 2006, State: 1043 Name: Vlan11, Index: 2007, State: 1043 Name: Vlan12, Index: 2008, State: 1043 Name: Tunnel1, Index: 2009, State: d1 Name: Tunnel2, Index: 0, State: 0 Name: pim6reg, Index: 2010, State: c1	



Name: pimreg, Index: 2011, State: c1 The total matched ip6mr active mfc entries is 1, unresolved ip6mr entries is 1 Group Origin lif Wrong Oif: TTL ff2f: : 1 2014: 1: 2: 3: : 2 Tunnel1 0 2008: 1 ff3f: : 1 2012: 1: 2: 3: : 2 NULL 4 0: 0	
Информация, отображаемая на экране	Пояснение
Name	имя интерфейса
Index	номер указателя интерфейса
State	статус интерфейса
The total matched ipmr active mfc entries	Общее количество совпавших активных записей mfc (кеш многоадресной пересылки) маршрутов IP multicast
Unresolved entries ipmr	неразрешенные записи многоадресного маршрута IP
Group	адрес назначения записей
Origin	адрес источника записей
lif	входной интерфейс записей
Wrong	пакеты, полученные от неправильного интерфейса
Oif	выходной интерфейс записей
TTL	значение TTL

10.2.3. Удаление IGMP-групп (clear ip igmp group)

Синтаксис	clear ip igmp group [A.B.C.D IFNAME] Удаление групповой записи конкретной группы или интерфейса	
Параметр	A.B.C.D	адрес указанной группы
	IFNAME	указанный интерфейс
По умолчанию		
Режим	Привилегированный режим	



Руководство по использованию	Используйте команду с "show" в начале для контроля удаления записи о группе
Пример	Switch#clear ip igmp group

10.2.4. Включить режим отладки (debug igmp event)

Синтаксис	debug igmp event no debug igmp event Запустить отслеживание событий IGMP; Команда " no debug igmp event " отключает отслеживание
Параметр	
По умолчанию	Отключено
Режим	Привилегированный режим
Руководство по использованию	Команда запускает отладочный режим при запросе информации о событиях IGMP
Пример	Switch# debug igmp event igmp event debug is on Switch# 01: 04: 30: 56: IGMP: Group 224.1.1.1 on interface vlan1 timed out

10.2.5. Отладка IGMP пакетов (debug igmp packet)

Синтаксис	debug igmp packet no debug igmp packet Запустить отслеживание информации о сообщениях IGMP; команда «no debug igmp packet» отключает переключатель отладки
Параметр	
По умолчанию	Отключено
Режим	Привилегированный режим
Руководство по использованию	Подключает переключатель отладки при запросе информации о сообщениях IGMP



Пример	<pre>Switch# debug igmp packet igmp packet debug is on Switch #02: 17: 38: 58: IGMP: Send membership query on dvmrp2 for 0.0.0.0 02: 17: 38: 58: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0.0.0 02: 17: 39: 26: IGMP: IGMP: Send membership query on vlan1 for 0.0.0.0 02: 17: 39: 26: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0.0.0</pre>

10.2.6. Список доступа к интерфейсу IGMP (ip igmp access-group)

Синтаксис	ip igmp access-group {<acl_num acl_name>} no ip igmp access-group Настроить интерфейс на фильтрацию группы IGMP. Команда “no ip igmp access-group” отменяет условия фильтрации	
Параметр	{<acl_num acl_name>}	последовательный номер или имя списка доступа, диапазон значений acl_num от 1 до 99
По умолчанию	По умолчанию нет условия фильтрации	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Настраивает интерфейс для фильтрации групп, разрешает или запрещает присоединение некоторых групп	
Пример	<pre>Настроить на интерфейсе vlan1 разрешение группы 224.1.1.1, запрет группы 224.1.1.2. Switch (config)#access-list 1 permit 224.1.1.1 0.0.0.0 Switch (config)#access-list 1 deny 224.1.1.2 0.0.0.0 Switch (config)#interface vlan 1 Switch(Config-If-Vlan1)#ip igmp access-group 1</pre>	

10.2.7. Группы, поддерживающие немедленный выход на интерфейсе (ip igmp immediate-leave)

Синтаксис	<pre>ip igmp immediate-leave group-list {<number> <name>} no ip igmp immediate-leave</pre> Настраивает работу IGMP в режиме immediate-leave, то есть, когда хост передает отчет об идентификации члена группы, эквивалентный выходу из группы, маршрутизатор не передает запрос, а напрямую подтверждает, что в подсети нет члена этой группы; Команда “no ip igmp immediate-leave” отменяет режим немедленного выхода



Параметр	<number>	порядковый номер перечня доступа, в диапазоне от 1 до 99
	<name>	имя списка доступа
По умолчанию	Нет выхода из конфигурации сразу после предварительной настройки интерфейса и готового продукта	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Команда может применяться только к одному состоянию хоста в подсети	
Пример	Настроить режим немедленного выхода для списка группы доступа 1 Switch (Config-if-Vlan1)#ip igmp immediate-leave group-list 1 Switch (Config-if-Vlan1)#	

10.2.8. Подключение интерфейса к группе (ip igmp join-group)

Синтаксис	ip igmp join-group <A.B.C.D > no ip igmp join-group <A.B.C.D > Настроить присоединение интерфейса к некоторой группе IGMP. Команда "no ip igmp join-group" отменяет это присоединение	
Параметр	<A.B.C.D >	адрес группы
По умолчанию	Присоединение не выполнено	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Когда коммутатор является хостом, эта команда позволяет присоединить хост к группе; то есть, если настроить подключение интерфейса к группе 224.1.1.1, когда коммутатор получит запрос группы IGMP от другого коммутатора, он будет отправлять отчет члена IGMP, включая группу 224.1.1.1. Обратите внимание на разницу между этой командой и командой "ip igmp static-group"	
Пример	Настроить подключение к группе join-group 224.1.1.1 на интерфейсе vlan1. Switch (config)#interface vlan 1 Switch(Config-If-Vlan1)#ip igmp join-group 224.1.1.1 Switch(Config-If-Vlan1)#ip igmp join-group 224.1.1.1	



10.2.9. Значение интервала запросов последнего участника (ip igmp last-member-query-interval)

Синтаксис	ip igmp last-member-query-interval <interval> no ip igmp last-member-query-interval Установить значение интервала передачи запросов указанной группы на интерфейсе. Команда «no ip igmp last-member-query-interval» отменяет значение, заданное пользователем, и восстанавливает значение по умолчанию	
Параметр	<interval>	интервал заданного группового запроса, диапазон от 1000 мс до 25500 мс; значение является целым кратным 1000 мс, то есть если вводимое значение не целое кратное 1000 мс, система автоматически переходит на целое число кратное 1000 мс
По умолчанию	1000 мс	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Команда разрешает настраивать интерфейс на фильтрацию групп: разрешать или запрещать доступ определенным группам	
Пример	Установить интервал IGMP last-member-query-interval для интерфейса vlan1 на 2000. Switch (config)#int vlan 1 Switch (Config-if-vlan1)#ip igmp last-member-query-interval 2000	

10.2.10. Максимальное количество разрешённых состояний IGMP (ip igmp limit)

Синтаксис	ip igmp limit <state-count> no ip igmp limit Установка ограничения количества состояний IGMP на интерфейсе; Команда “no ip igmp limit” отменяет установленное вручную значение и восстанавливает значение по умолчанию	
Параметр	<state-count>	максимальное состояние IGMP, зарезервированное интерфейсом, диапазон от 1 до 65000
По умолчанию	0, ограничения отсутствуют	
Режим	Режим конфигурации интерфейса	



Руководство по использованию	После настройки максимального количества состояний интерфейс сохраняет только те состояния, которые не превышают количество групп и источников. Если предел количества состояний достигнут, интерфейс не обрабатывает связанные отчеты о новом членстве в группе при их получении. Если интерфейс сохранил некоторые состояния групп IGMP до установки этой команды, интерфейс удаляет все состояния и немедленно отправляет общий запрос IGMP для сбора отчетов о нахождении в группе, которая не превышает количество состояний группы. Статические состояние и статические источники не входят в ограничение
Пример	Установить предел IGMP в 4000 на vlan1. Switch (config)#int vlan 1 Switch (Config-if-vlan1)#ip igmp limit 4000

10.2.11. Интервал запросов IGMP (ip igmp query-interval)

Синтаксис	ip igmp query-interval <time_val> no ip igmp query-interval Настройка интервала передачи информации о запросах IGMP. Команда "no ip igmp query-interval" восстанавливает значение по умолчанию	
Параметр	<time_val>	интервал периодической передачи информации о запросах IGMP диапазон значений от 1 с до 65535 с
По умолчанию	125 секунд	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Когда на некоторых интерфейсах включены определенные протоколы групповой многоадресной рассылки, на интерфейс периодически отправляется информация о запросах IGMP. Команда применяется для настройки времени периода запроса	
Пример	Настроить интервал периодически передаваемого сообщения запроса IGMP на 10 секунд Switch (config)#interface vlan 1 Switch(Config-If-Vlan1)#ip igmp query-interval 10	



10.2.12. Максимальное время отклика на запрос IGMP (ip igmp query-max-response-time)

Синтаксис	ip igmp query-max-response-time <time_val> no ip igmp query-max-response-time Установка на интерфейсе максимального времени отклика на запрос IGMP. Команда “no ip igmp query-max-response-time” восстанавливает значение по умолчанию	
По умолчанию	10 секунд	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Когда коммутатор получает сообщение о запросе, хост устанавливает таймер для каждой многоадресной группы, к которой он принадлежит. Значение таймера выбирается случайным образом от 0 до максимального времени ответа, хост передает сообщение об участии этой многоадресной группы. Соответствующая настройка максимального времени ответа позволяет хосту быстро реагировать на сообщения-запросы. Маршрутизатор также может быстро отслеживать состояние членов многоадресной группы	
Пример	Установить максимальный период ответа на сообщения IGMP-запроса на 20 секунд Switch (config)#interface vlan 1 Switch(Config-If-Vlan1)#ip igmp query-max-response-time 20	

10.2.13. Тайм-аут запроса IGMP (ip igmp query-timeout)

Синтаксис	ip igmp query-timeout <time_val> no ip igmp query-timeout Команда задает таймаут запроса IGMP для интерфейса. Команда “no ip igmp query-timeout” восстанавливает значение по умолчанию	
Параметр	<time_val>	таймаут запроса IGMP, диапазон значений от 60 до 300 секунд
По умолчанию	255 секунд	
Режим	Режим конфигурации интерфейса	



Руководство по использованию	Если в общей сети несколько коммутаторов работают по протоколу IGMP, один коммутатор будет избран в качестве процессора запросов в общей сети, а другие коммутаторы будут следить за состоянием процессора запросов по таймеру; если по истечении таймаута от процессора запросов не будет получено ни одного сообщения, другой коммутатор будет переизбран в качестве нового процессора запросов
Пример	Установить таймаут сообщения IGMP-запроса на интерфейсе на 100 секунд. Switch (config)#interface vlan 1 Switch(Config-If-Vlan1)#ip igmp query-timeout 100

10.2.14. Значение устойчивости IGMP-запроса (ip igmp robust-variable)

Синтаксис	ip igmp robust-variable <value> no ip igmp robust-variable Команда используется для установки значения переменной устойчивости, команда "no ip igmp robust-variable" возвращает настройки по умолчанию	
Параметр	value	в диапазоне от 2 до 7
По умолчанию	задано значение 2	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Рекомендуется использовать значение по умолчанию. Переменная надежности: позволяют регулировать значение в зависимости от ожидаемой потери пакетов на канале. Если ситуация с ожидаемой потерей сообщений ухудшается, то значение переменной надежности также может увеличиться. IGMP/MLD допускает потерю не более 1 пакета без ущерба для переменной надежности. Значение переменной устойчивости не может быть 0 и не должно быть 1. Значение по умолчанию равно 2	
Пример	Switch (config-if-vlan1)#ip igmp robust-variable 3	

10.2.15. Статическая принадлежность интерфейса группе (ip igmp static-group)

Синтаксис	ip igmp static-group <A.B.C.D > [source <A.B.C.D >] no ip igmp static -group <A.B.C.D > [source <A.B.C.D >] Настраивает интерфейс на присоединение к некоторой статической группе IGMP; Команда «no ip igmp static-group» отменяет это присоединение



Параметр	<A.B.C.D >	адрес группы;
	source <A.B.C.D >	выражает адрес источника SSM конфигурации
По умолчанию	Статическая группа не присоединена	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Если интерфейс настроен на присоединение к статической группе, он будет получать многоадресные пакеты из статической группы независимо от того, есть ли у интерфейса реальный получатель; то есть, если интерфейс настроен на присоединение к статической группе 224.1.1.1, он будет получать многоадресные пакеты из группы 224.1.1.1 независимо от того, есть ли у интерфейса получатель. Обратите внимание, что в этом заключается разница между данной командой и командой ip igmp join-group	
Пример	Настроить статическую группу static-group 224.1.1.1 на интерфейсе vlan1. Switch (config)#interface vlan 1 Switch(Config-If-Vlan1)#ip igmp static-group 224.1.1.1	

10.2.16. Установка версии IGMP на интерфейсе (ip igmp version)

Синтаксис	ip igmp version <version> no ip igmp version Команда устанавливает версию IGMP на интерфейсе. Команда "no ip igmp version" восстанавливает значение по умолчанию	
Параметр	<version>	версия конфигурации IGMP, в настоящее время поддерживаются версии 1, 2 и 3
По умолчанию	версия 2	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Эта команда используется в основном для обеспечения восходящей совместимости между версиями; команда не передается между версиями 1 и 2 нет связи, поэтому они должны быть настроены на одну и ту же версию IGMP в одной сети. Когда другие маршрутизаторы, не обновленным до IGMPv3, в подключенной к интерфейсу подсети, необходимо присоединить к идентификаторам членов IGMP подсети, интерфейс настраивается на соответствующую версию	



Пример	Установить версию 3 IGMP на интерфейсе. Switch (config)#interface vlan 1 Switch(Config-If-Vlan1)#ip igmp version 1

10.2.17. Вывод информации о IGMP-группах (show ip igmp groups)

Синтаксис	show ip igmp groups [<A.B.C.D>] [detail] Используется для отображения информации о IGMP-группах				
Параметр	< A.B.C.D >	это адрес группы, а именно запрос информации об указанной группе;			
	detail	вывести подробную информацию о группе			
По умолчанию	Не выводится на экран				
Режим	В привилегированном режиме				
Руководство по использованию					
Пример	Switch (config)#show ip igmp groups				
	IGMP Connected Group Membership (2 group(s) joined) Group				
	Address	Interface	Uptime	Expires	Last Reporter
	226.0.0.1	Vlan1	00:00:01	00:04:19	1.1.1.1
	239.255.255.250	Vlan1	00:00:10	00:04:10	10.1.1.1
			0		
	Информация, отображаемая на экране	Пояснения			
	Group Address	IP-адрес группы многоадресной рассылки			
	Interface	Интерфейс, связанный с многоадресной группой			
	Uptime	Время доступности группы многоадресной рассылки			
Expires	Окончание функционирования группы многоадресной рассылки				
Last Reporter	Последний отправитель отчетов на хост группы многоадресной рассылки				



```
Switch (config)#show ip igmp groups 234.1.1.1 detail
IGMP Connect Group Membership (2 group(s) joined)
Flags: SG - Static Group, SS - Static Source, SSM - SSM Group, V1 -
V1 Host Present, V2 - V2 Host Present
Interface:      Vlan1
Group:          234.1.1.1
Flags:
Uptime:         00: 00: 19
Group Mode: INCLUDE
Last Reporter: 10.1.1.1
Exptime:        stopped
Source list: (2 members S - Static)
```

Source Address	Uptime	v3 Exp	Fwd Flags
1.1.1.1	00: 00: 19	00: 04: 01	Yes
2.2.2.2	00: 00: 19	00: 04: 01	Yes

Информация, отображаемая на экране	Пояснения
Group	IP адрес группы многоадресной рассылки
Interface	Интерфейс, связанный с группой многоадресной рассылки
Flags	Флаг свойства группы
Uptime	Время доступности группы многоадресной рассылки
Group Mode	Режим работы группы, включая INCLUDE и EXCLUDE. Группа V3 будет доступна, группа V1 и группа V2 относятся к режиму EXCLUDE
Exptime	Окончание функционирования группы многоадресной рассылки
Last Reporter	Последний отправитель отчетов на хост группы многоадресной рассылки
Source Address	Адрес источника данной группы



	V3 Exp	Время истечения срока действия источника
	Fwd	Указывает перенаправляется источник или нет
	Flags	Флаг свойства источника

10.2.18. Вывод информации о IGMP на интерфейсе (show ip igmp interface)

Синтаксис	show ip igmp interface {vlan <vlan_id> <ifname>} Команда используется для отображения информации о IGMP на интерфейсе	
Параметр	<ifname>	имя интерфейса, а именно отображение информации IGMP указанного интерфейса
По умолчанию	Не выводится на экран	
Режим	В привилегированном режиме	
Руководство по использованию		
Пример	Вывести на экран сообщения IGMP интерфейса vlan1 на Ethernet. Switch (config)#show ip igmp interface Vlan1 Interface Vlan1(2005) Index 2005 Internet address is 10.1.1.2 IGMP querier IGMP current version is V3, 2 group(s) joined IGMP query interval is 125 seconds IGMP querier timeout is 255 seconds IGMP max query response time is 10 seconds Last member query response interval is 1000 ms Group Membership interval is 260 seconds IGMP is enabled on interface	

10.3. Настройка протокола PIM-DM

10.3.1. Отладка таймера активности источника PIM (debug pim timer sat)

Синтаксис	debug pim timer sat no debug pim timer sat Активирует переключатель отладки сообщений таймера активности источника PIM-DM; команда "no debug pim timer sat" отключает отладку



Параметр	
По умолчанию	Отсутствует
Режим	Привилегированный режим
Руководство по использованию	Команда позволяет подключить отладку и отслеживать подробную информацию о таймере активности источника
Пример	Switch # debug pim timer sat Остальные команды запуска отладки в PIM-DM являются общими и для PIM-SM, включая debug pim event, debug pim packet, debug pim nexthop, debug pim nsm, debug pim mfc, debug pim mib, debug pim timer, debug pim state

10.3.2. Отладка таймера обновления состояний (debug pim timer srt)

Синтаксис	debug pim timer srt no debug pim timer srt Запускает отладку для получения информации о таймере обновления состояния PIM-DM; Команда "no debug pim timer srt" отключает отладку
Параметр	
По умолчанию	Функция GVRP выключена
Режим	Привилегированный режим
Руководство по использованию	Команда позволяет подключить отладку и отслеживать подробную информацию о таймере обновления состояния PIM-DM
Пример	Switch # debug pim timer srt Остальные команды запуска отладки в PIM-DM являются общими и для PIM-SM, включая debug pim event, debug pim packet, debug pim nexthop, debug pim nsm, debug pim mfc, debug pim mib, debug pim timer, debug pim state

10.3.3. Создание статического multicast-маршрута (ip mroute)

Синтаксис	ip mroute <A.B.C.D> <A.B.C.D> <ifname> <.ifname> no ip mroute <A.B.C.D> <A.B.C.D> [<ifname> <.ifname>] Данная команда используется для создания статического multicast-маршрута. "no" в начале команды удалит определенные статические



	записи многоадресной рассылки или определенные интерфейсы выхода	
Параметр	<A.B.C.D> <A.B.C.D>	адрес источника и адрес группы многоадресной рассылки
	<ifname> <.ifname>	первый это интерфейс входа, а второй это интерфейс выхода
По умолчанию	Если команда не содержит параметров интерфейса, запись статической многоадресной рассылки удаляется	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Имена <ifname> должны быть действительными интерфейсами VLAN. Поток многоадресных данных не будет пересылаться, если на интерфейсе выхода не настроен PIM и интерфейс не находится в состоянии UP. Если состояние интерфейса не UP, или PIM не настроен, или RPF не действует, поток многоадресных данных не будет пересылаться. Удаление указанной записи многоадресной маршрутизации. Если указаны все интерфейсы выхода или не указано ни одного интерфейса, указанная запись многоадресной маршрутизации будет удалена. В ином случае будет удалена запись многоадресной маршрутизации для указанного интерфейса	
Пример	Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30	

10.3.4. Настройка границ BSR (ip pim bsr-border)

Синтаксис	ip pim bsr-border no ip pim bsr-border Настраивает или отменяет настройку граничного BSR для PIM
Параметр	
По умолчанию	BSR-BORDER отсутствуют
Режим	Режим конфигурации интерфейса
Руководство по использованию	Команда настраивает интерфейс в качестве пограничного интерфейса BSR-BORDER. После настройки этой команды сообщения, относящиеся к BSR, не будут получаться с указанного интерфейса и не будут пересылаться. Все сети, подключенные к интерфейсу, будут считаться подключенными напрямую
Пример	Switch(Config-if-Vlan1)#no ip pim bsr-border



10.3.5. Уплотнённый режим (ip pim dense-mode)

Синтаксис	ip pim dense-mode no ip pim dense-mode Включает протокол PIM-DM на интерфейсе; Команда “no ip pim dense-mode” отключает протокол PIM-DM на интерфейсе
Параметр	
По умолчанию	Протокол PIM-DM отключен. Протокол PIM-DM отключен
Режим	Режим конфигурации интерфейса
Руководство по использованию	Команда вступит в силу при выполнении ip multicast-routing в глобальном режиме. Не поддерживает взаимную работу протоколов многоадресной рассылки, то есть нельзя одновременно на одном коммутаторе включить уплотненный режим и разреженный режим
Пример	Включить протокол PIM-DM на интерфейсе vlan1. Switch(config)#ip pim multicast-routing Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip pim dense-mode

10.3.6. Настройка приоритета выбора назначенного маршрутизатора (ip pim dr-priority)

Синтаксис	ip pim dr-priority <priority> no ip pim dr-priority Данная команда используется для изменения значения приоритета назначенного маршрутизатора (DR). Соседние узлы в одном сегменте сети выбирают DR в своем сегменте в соответствии с пакетами "hello". Команда “no ip pim dr-priority” восстанавливает значение по умолчанию	
Параметр	<priority>	это приоритет
По умолчанию	1	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Укажите значение приоритета в диапазоне от 0 до 4294967295, чем больше значение, тем выше приоритет	



Пример	Установить приоритет DR на VLAN равным 100. Switch(config)# interface vlan 1 Switch(Config-if-Vlan1)#ip pim dr-priority 100 Switch (Config-if-Vlan1)#

10.3.7. Исключение опции GenId (ip pim exclude-genid)

Синтаксис	ip pim exclude-genid no ip pim exclude-genid Эта команда исключает опцию GenId из пакетов Hello, отправляемых PIM SM. Команда “no ip pim exclude-genid” восстанавливает значение по умолчанию
Параметр	
По умолчанию	Пакеты Hello включают опцию GenId
Режим	Режим конфигурации интерфейса
Руководство по использованию	Эта команда используется для взаимодействия с более ранними версиями Cisco IOS
Пример	Задать, чтобы пакеты Hello, отправляемые коммутатором, не включали опцию GenId. Switch (Config-if-Vlan1)#ip pim exclude-genid Switch (Config-if-Vlan1)#

10.3.8. Время сохранения информации о сообщениях Hello (ip pim hello-holdtime)

Синтаксис	ip pim hello-holdtime <value> no ip pim hello-holdtime Настраивает или отключает значение Holdtime (время сохранения информации) в пакетах Hello, которое описывает время сохранения информации о соседях, и отключает соседей, от которых в течение заданного времени holdtime на коммутатор не поступало пакетов Hello. Команда “no ip pim hello-holdtime” отменяет настроенное значение времени сохранения и восстанавливает значение по умолчанию	
Параметр	<vaule>	значение времени сохранения информации в диапазоне <1-65535>



По умолчанию	Значение Holdtime по умолчанию равно $3,5 \times \text{Hello\_interval}$, значение Hello_interval по умолчанию равно 30 секунд, поэтому значение Holdtime по умолчанию равно 105 с
Режим	Режим конфигурации интерфейса
Руководство по использованию	Если это значение не задано, по умолчанию hellotime будет равен $3,5 \times \text{Hello\_interval}$. Если задаваемое время сохранения информации меньше, чем текущий интервал hello_interval, эта конфигурация будет отклонена. Каждый раз, когда hello_interval обновляется, hello_holdtime обновляется по следующим правилам: если hello_holdtime не задано, или если hello_holdtime задано, но меньше текущего hello_interval, hello_holdtime будет изменено на $3,5 \times \text{hello\_interval}$. В остальных случаях сохраняется заданное значение
Пример	Настроить Hello Holdtime на vlan1 <pre>Switch (config)# interface vlan1 Switch (Config -if-Vlan1)#ip pim hello-holdtime 10 Switch (Config -if-Vlan1)#</pre>

10.3.9. Интервал отправки hello-пакетов (ip pim hello-interval)

Синтаксис	ip pim hello-interval < interval> no ip pim hello-interval Задаёт интервал отправки сообщений "hello" с интерфейса PIM-DM; Команда "no ip pim hello-interval" восстанавливает значение по умолчанию	
Параметр	< interval>	время, через которое отправляются hello-пакеты PIM-DM в диапазоне от 1 до 18724 секунд
По умолчанию	Интервал периодической передачи сообщения PIM-DM hello по умолчанию равен 30 секундам	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Сообщения Hello позволяют коммутаторам PIM-DM определять взаимное расположение и устанавливать соседство. Коммутатор PIM-DM объявляет о своем присутствии, регулярно отправляя соседям сообщения Hello. Соседи, от которых в течение определенного времени не поступало сообщений Hello, считаются отключившимися. Заданное время не должно превышать время работы соседей	
Пример	Настроить интервал отправки hello PIM-DM на интерфейсе vlan1. <pre>Switch(config)#interface vlan1 Switch(Config-if-Vlan1)#ip pim hello-interval 20</pre>	



10.3.10. Многоадресная маршрутизация для протокола PIM (ip pim multicast-routing)

Синтаксис	ip pim multicast-routing no ip pim multicast-routing Включает протокол PIM-DM в глобальном режиме; Команда "no ip pim multicast-routing" отключает протокол PIM-DM
Параметр	
По умолчанию	Протокол PIM-SM отключен
Режим	Режим конфигурации интерфейса
Руководство по использованию	Подключает протокол PIM-SM в глобальном режиме. Чтобы PIM-SM функционировал, он должен быть включен на интерфейсе
Пример	Подключить протокол PIM-SM в глобальном режиме. Switch (config)#ip pim multicast-routing Switch (config)#

10.3.11. Настройка фильтрации соседей PIM (ip pim neighbor-filter)

Синтаксис	ip pim neighbor-filter <list-number> no ip pim neighbor-filter <list-number> Настраивает диапазон адресов соседних устройств. Если соединение с соседом установлено, но условия фильтрации не выполнены, соединение немедленно обрывается. Если соединение не создано, это соединение не может быть установлено	
Параметр	<list-number>	номер списка доступа, в диапазоне 1 до 99
По умолчанию	Фильтрация соседей не сконфигурирована	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	По умолчанию ACL имеет значение DENY (отклонить). При настройке "access-list 1" его значение по умолчанию будет "deny". В примере ниже, если параметр "permit any-source" не задан, deny 10.1.4.10 255.255.255.0 - это то же самое, что deny any-source	
Пример	Настроить правила фильтрации соседей pim в VLAN. Switch #show ip pim neighbor Neighbor Neighbor Interface Uptime/Expires Ver DR Address Priority/Mode	



10.1.4.10	Vlan1	02: 30: 30/00: 01: 41 v2	4294967294 / DR
Switch (Config-if-Vlan1)#ip pim neighbor-filter 2			
Switch (config)#access-list 2 deny 10.1.4.10 255.255.255.0			
Switch (config)#access-list 2 permit any-source			
Switch (config)#show ip pim neighbor			

10.3.12. Границы управления и ACL для протокола PIM (ip pim scope-border)

Синтаксис	ip pim scope-border [<1-99 > <acl_name>] no ip pim scope-border Устанавливает или удаляет границу управления протокола PIM	
Параметр	<1-99 >	номер ACL для границы управления
	<acl_name>	имя ACL для границы управления
По умолчанию	Границы управления отсутствуют. Если ACL (список контроля доступа) не указан, будет использоваться граница управления по умолчанию	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Команда определяет границы управления и список контроля доступа для протокола PIM. Поток многоадресных данных не будет перенаправляться на SCOPE-BORDER	
Пример	Switch(Config-if-Vlan2)#ip pim scope-border 3	

10.3.13. Установка интервала сообщений SRM (ip pim state-refresh origination-interval)

Синтаксис	ip pim state-refresh origination-interval <interval> no ip pim state-refresh origination-interval Задаёт интервал передачи сообщения об обновлении состояния. Команда "no ip pim state-refresh origination-interval" восстанавливает значение по умолчанию	
Параметр	<interval>	Значение интервала передачи пакетов - от 4 до 100 с
По умолчанию	60 секунд	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Маршрутизатор первого узла периодически отправляет сообщения обновления состояния "stat-refresh" для поддержания записей списка PIM-DM всех последующих маршрутизаторов. Команда может изменять интервал отправления сообщений обновления состояния. Изменять соответствующий интервал таймера обычно не нужно
Пример	Установить интервал передачи сообщения об обновлении состояния на 90 секунд. Switch (config)#ip pim state-refresh origination-interval 90

10.3.14. Вывод информации PIM для интерфейса (show ip pim interface)

Синтаксис	show ip pim interface	
Параметр	выводит информацию о PIM для интерфейса	
По умолчанию	Отсутствует	
Режим	В привилегированном режиме	
Руководство по использованию	Команда выводит на экран информацию о PIM для интерфейса	
Пример	Switch (config)#show ip pim interface	
	Address Interface VIF index Ver/ Nbr DR DR Mode Count Prior	
	10.1.4.3 Vlan1 0 v2/S 1 10.1.4.3	
	1	
	10.1.7.1 Vlan2 2 v2/S 1 10.1.7.1	
	0	
	Информация, отображаемая на экране	Пояснения
	Address	адрес интерфейса
	Interface	имя интерфейса
	VIF index	индекс интерфейса
	Ver/Mode	версия и режим Pim, обычно v2, для разреженного режима отображается S, для уплотненного режима отображается D



	Nbr Count	число соседей интерфейса
	DR Prior	приоритет назначенного маршрутизатора (DR)
	DR	адрес DR интерфейса

10.3.15. Вывод уплотненного режима многоадресной маршрутизации (show ip pim mroute dense-mode)

Синтаксис	show ip pim mroute dense-mode [group <A.B.C.D>] [source <A.B.C.D>] Отображение элементов пересылки сообщений PIM-DM	
Параметр	group <A.B.C.D>	отображает элементы пересылки, относящиеся к данному групповому адресу
	source <A.B.C.D>	отображает элементы пересылки, относящиеся к данному источнику
По умолчанию	Не выводить на экран	
Режим	В привилегированном режиме	
Руководство по использованию	Команда показывает элементы пересылки многоадресной рассылки PIM-DM, а именно элементы пересылки многоадресных пакетов в системной таблице FIB	
Пример	Вывести все элементы пересылки сообщений PIM-DM. <pre>Switch(config)#show ip pim mroute dense-mode IP Multicast Routing Table (*,G) Entries: 1 (S,G) Entries: 1 (*, 226.0.0.1) Local ..l..... (192.168.1.12, 226.0.0.1) RPF nbr: 0.0.0.0 RPF idx: Vlan2 Upstream State: FORWARDING Origin State: ORIGINATOR Local Pruned Asserted Outgoing ..o.....</pre>	



Информация, отображаемая на экране	Пояснения
(* ,226.0.0.1)	(* ,G) Направляемые элементы
(192.168.1.12, 226.0.0.1)	(S,G) Направляемые элементы
RPF nbr	соседнее устройство в нисходящем направлении, соседнее устройство в восходящем направлении в направлении источника в DM, 0.0.0.0 означает коммутатор в первом хопе
RPF idx	интерфейс, находящийся в RPF-соседе
Upstream State	Восходящее направление, включая FORWARDING (пересылка данных), PRUNED (прекращение пересылки данных), ACKPENDING (ожидание ответа от вышестоящего, пересылка данных)
Origin State	Два состояния: ORIGINATOR (в состоянии transmit state-refresh), NON_ORIGINATOR (в состоянии non_transmit state-refresh)
Local	Подсоединение локального члена к интерфейсу, интерфейс получает сообщение IGMP Join
Pruned	PIM помечает интерфейс как pruned (усеченный), интерфейс получает сообщение Prune
Asserted	Состояние подтверждено
Outgoing	Многоадресные данные, окончательно переданные из интерфейса, имеют индексный номер, в данном случае индекс равен 2. Просмотреть детальную информацию об интерфейсе можно с помощью команды show ip pim interface
Origin State	Два состояния: ORIGINATOR (в состоянии transmit state-refresh), NON_ORIGINATOR (в состоянии non_transmit state-refresh)
Local	Подсоединение локального члена к интерфейсу, интерфейс получает сообщение IGMP Join



	Pruned	PIM помечает интерфейс как pruned (усеченный), интерфейс получает сообщение Prune
	Asserted	Состояние подтверждено
	Outgoing	Многоадресные данные, окончательно переданные из интерфейса, имеют индексный номер, в данном случае индекс равен 2. Просмотреть детальную информацию об интерфейсе можно с помощью команды show ip pim interface

10.3.16. Вывод информации о соседних устройствах PIM (show ip pim neighbor)

Синтаксис	show ip pim neighbor Отображение информации о соседних устройствах				
Параметр					
По умолчанию					
Режим	В привилегированном режиме				
Руководство по использованию	Данная команда используется для отображения информации о том, какие многоадресные маршрутизаторы настроены для PIM				
Пример	Switch (config)#show ip pim neighbor				
	Neighbor	Interface	Uptime/Expires	Ver	DR
	Address Priority/Mode				
	10.1.6.1	Vlan1	00: 00: 10/00: 01: 35 v2	1 /	
	10.1.6.2	Vlan1	00: 00: 13/00: 01: 32 v2	1 /	
	10.1.4.2	Vlan3	00: 00: 18/00: 01: 30 v2	1 /	
	10.1.4.3	Vlan3	00: 00: 17/00: 01: 29 v2	1 /	
	Информация, отображаемая на экране		Пояснения		
	Neighbor Address		Адрес соседнего устройства		
	Interface		Интерфейс соседнего устройства		
Uptime/Expires		Время работы/истечения срока			
Ver		Версия Pim, обычно v2			



	DR Priority/Mode	Приоритет DR в сообщениях hello от соседа и является ли сосед DP интерфейса

10.3.17. Вывод информации о следующих хопах multicast-групп (show ip pim nexthop)

Синтаксис	show ip pim nexthop Отображение буферизованного маршрутизатора следующего узла PIM в таблице маршрутов одноадресной рассылки	
Параметр		
По умолчанию	Не задано	
Режим	В привилегированном режиме	
Руководство по использованию	Команда выводит информацию о буферизованном маршрутизаторе PIM nexthop	
Пример	Switch(config)#show ip pim nexthop Flags: N = New, R = RP, S = Source, U = Unreachable Destination Type Nexthop Nexthop Nexthop Nexthop Metric Pref Refcnt Num Addr Ifindex Name 192.168.1.1 N... 1 0.0.0.0 2006 0 0 1 192.168.1.9 ..S. 1 0.0.0.0 2006 0 0 1	
	Информация, отображаемая на экране	Пояснения
	Destination	Назначение следующей записи
	Type	N: создан следующий узел (nexthop), направление RP и направление S не определены. R: направление точки встречи RP S: направление источника U: нет доступа
	Nexthop Num	Номер следующего узла
	Nexthop Addr	Адрес следующего узла
	Nexthop Ifindex	Индекс интерфейса следующего узла
	Nexthop Name	Имя следующего узла
	Metric	Метрика следующего узла



	Pref	Предпочтительный маршрутизатор	выбор
	Refcnt	Счетчик ссылок	

10.4. Настройка протокола PIM-SM

10.4.1. Удаление информации о точках встречи (clear ip pim bsr rp-set)

Синтаксис	clear ip pim bsr rp-set * Удаляет информацию о всех точках встречи (RP)
Параметр	
По умолчанию	
Режим	Привилегированный режим
Руководство по использованию	Команда быстро удаляет все RP
Пример	Switch# clear ip pim bsr rp-set * Switch# clear ip pim bsr rp-set *

10.4.2. Отладка событий PIM (debug pim event)

Синтаксис	debug pim event no debug pim event Включение или отключение функции отладки событий pim
Параметр	
По умолчанию	Отключено
Режим	Привилегированный режим
Руководство по использованию	Команда подключает функцию отладки событий pim и выводит информацию о событиях, связанных с работой pim
Пример	Switch# debug pim event

10.4.3. Отладка кеша PMI (debug pim mfc)

Синтаксис	
Параметр	



По умолчанию	Отключено
Режим	Привилегированный режим
Руководство по использованию	Команда подключает функцию отладки <code>pim mfc</code> и выводит информацию о сгенерированных и переданных идентификаторах многоадресной рассылки
Пример	Switch# debug pim mfc

10.4.4. Отладка базы информации управления PIM (debug pim mib)

Синтаксис	debug pim mib no debug pim mib Включение и отключение отладки PIM MIB
Параметр	
По умолчанию	Отключено
Режим	Привилегированный режим
Руководство по использованию	Команда позволяет просмотреть информацию о PIM MIB с помощью функции отладки PIM MIB. Сейчас эта функция недоступна, она будет добавлена в будущем
Пример	Switch# debug pim mib Switch#

10.4.5. Отладка nexthop в PIM (debug pim nexthop)

Синтаксис	debug pim nexthop no debug pim nexthop Подключить или отключить функцию отладки для pim nexthop
Параметр	
По умолчанию	Отключено
Режим	Привилегированный режим
Руководство по использованию	Команда позволяет проверить информацию об изменении PIM NEXTHop
Пример	Switch# debug pim nexthop



10.4.6. Отладка менеджера сетевых служб PIM (debug pim nsm)

Синтаксис	debug pim nsm no debug pim nsm Включение или отключение функции отладки на PIM, взаимодействующего с сетевыми службами
Параметр	
По умолчанию	Отключено
Режим	Привилегированный режим
Руководство по использованию	Команда позволяет проверить информацию, передаваемую между PIM и сетевыми службами
Пример	Switch# debug pim nsm

10.4.7. Отладка пакета PIM (debug pim packet)

Синтаксис	debug pim packet debug pim packet in debug pim packet out no debug pim packet no debug pim packet in no debug pim packet out Включает или отключает отладку pim	
Параметр	in	показывать только принятые пакеты pim
	out	показывать только переданные пакеты pim
	без параметра	показывать и принятые и переданные пакеты pim
По умолчанию	Отключено	
Режим	Привилегированный режим	
Руководство по использованию	Команда позволяет проверить полученные и переданные этим коммутатором пакеты pim	
Пример	Switch# debug pim packet in	



10.4.8. Просмотр информации о статусе PIM (debug pim state)

Синтаксис	debug pim state no debug pim state Включение и отключение отладки PIM
Параметр	
По умолчанию	Отключено
Режим	Привилегированный режим
Руководство по использованию	Просмотр информации об изменении статуса pim на этом коммутаторе
Пример	Switch# debug pim state

10.4.9. Информация об отладке пакета PIM (debug pim packet)

Синтаксис	debug pim timer debug pim timer assert debug pim timer assert at debug pim timer bsr bst debug pim timer bsr crp debug pim timer bsr debug pim timer hello ht debug pim timer hello nlt debug pim timer hello tht debug pim timer hello debug pim timer joinprune et debug pim timer joinprune jt debug pim timer joinprune kat debug pim timer joinprune ot debug pim timer joinprune plt debug pim timer joinprune ppt debug pim timer joinprune pt debug pim timer joinprune debug pim timer register rst debug pim timer register no debug pim timer no debug pim timer assert no debug pim timer assert at no debug pim timer bsr bst no debug pim timer bsr crp no debug pim timer bsr no debug pim timer hello ht no debug pim timer hello nlt no debug pim timer hello tht no debug pim timer hello no debug pim timer joinprune et no debug pim timer joinprune jt no debug pim timer joinprune kat no debug pim timer joinprune ot no debug pim timer joinprune plt no debug pim timer joinprune ppt no debug pim timer joinprune pt no debug pim timer joinprune no debug pim timer register rst no debug pim timer register Включение или отключение каждого таймера pim
Параметр	
По умолчанию	Отключено
Режим	Привилегированный режим



Руководство по использованию	Включение отладочной информации для указанного таймера
Пример	Switch# debug pim timer assert

10.4.10. Статический многоадресный трафик (ip mroute)

Синтаксис	ip mroute <A.B.C.D> <A.B.C.D> <ifname> <.ifname> no ip mroute <A.B.C.D> <A.B.C.D> [<ifname> <.ifname>] Данная команда используется для создания статического multicast-маршрута. "no" в начале команды удалит определенные статические записи многоадресной рассылки или определенные интерфейсы выхода	
Параметр	<A.B.C.D> <A.B.C.D>	адрес источника и адрес группы многоадресной рассылки
	<ifname> <.ifname>	первый это интерфейс входа, а второй это интерфейс выхода
По умолчанию	Если команда не содержит параметров интерфейса, запись статической многоадресной рассылки удаляется	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Имена <ifname> должны быть действительными интерфейсами VLAN. Поток многоадресных данных не будет пересылаться, если на интерфейсе выхода не настроен PIM и интерфейс не находится в состоянии UP. Если состояние интерфейса не UP, или PIM не настроен, или RPF не действует, поток многоадресных данных не будет пересылаться. Удаление указанной записи многоадресной маршрутизации. Если указаны все интерфейсы выхода или не указано ни одного интерфейса, указанная запись многоадресной маршрутизации будет удалена. В ином случае будет удалена запись многоадресной маршрутизации для указанного интерфейса	
Пример	Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30	



10.4.11. Кеширование многоадресного маршрута (ip multicast unresolved-cache aging-time)

Синтаксис	ip multicast unresolved-cache aging-time <value> no ip multicast unresolved-cache aging-time Устанавливает время кеширования для основной многоадресной маршрутизации. "no" в начале команды восстанавливает значение по умолчанию	
Параметр	< value>	задаваемое время кеширования, в диапазоне от 1 до 20 секунд
По умолчанию	10 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда задает время кеширования записи многоадресного маршрута в ядре	
Пример	Switch(config)# ip multicast unresolved-cache aging-time 18	

10.4.12. Фильтрация пакетов Register (ip pim accept-register)

Синтаксис	Диапазон источника зарегистрированных адресов (ip pim accept-register list <list-number> no ip pim accept-register) Выполнение фильтрации указанной многоадресной группы и многоадресного адреса	
Параметр	<list-number>	номер в списке доступа, в диапазоне от 100 до 199
По умолчанию	Разрешены многоадресные регистры из любых источников в любые группы	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда используется для установки списка доступа для фильтрации пакетов PIM REGISTER. Адреса списка доступа соответственно указывают на отфильтрованные источники многоадресной рассылки и информацию о многоадресных группах. Для комбинаций источник-группа, соответствующих DENY (запрет), PIM немедленно отправляет REGISTER-STOP и не создает групповые записи при получении пакетов REGISTER. В отличие от других списков доступа, при настройке списка доступа по умолчанию используется значение PERMIT (разрешено)	
Пример	Настроить правило фильтра сообщений регистра на myfilter.	



	<pre>Switch(config)#ip pim accept-register list 120 Switch (config)#access-list 120 deny ip 10.1.0.2 0.0.0.255 239.192.1.10 0.0.0.255 Switch (config)#</pre>

10.4.13. Настройка границ BSR (ip pim bsr-border)

Синтаксис	<pre>ip pim bsr-border no ip pim bsr-border</pre> Настраивает или отменяет настройку граничного BSR для PIM
Параметр	
По умолчанию	BSR-BORDER отсутствуют
Режим	Режим конфигурации интерфейса
Руководство по использованию	Команда настраивает интерфейс в качестве пограничного интерфейса BSR-BORDER. После настройки этой команды сообщения, относящиеся к BSR, не будут получаться с указанного интерфейса и не будут пересылаться. Все сети, подключенные к интерфейсу, будут считаться подключенными напрямую
Пример	Switch(Config-if-Vlan1)#no ip pim bsr-border

10.4.14. Назначения роли Candidate BSR маршрутизатору (ip pim bsr-candidate)

Синтаксис	<pre>ip pim bsr-candidate {vlan <vlan-id> <ifname>} [hash-mask-length] [priority] no ip pim bsr-candidate</pre> Данная команда используется для назначения роли Candidate BSR в режиме глобальной конфигурации и указания в PIM-SM информации о кандидате BSR для выполнения сравнений с другими кандидатами на маршрутизатор BSR. Команда "no ip pim bsr-candidate" отменяет назначение роли Candidate BSR	
Параметр	vlan-id	идентификатор VLAN
	ifname	имя указанного интерфейса
	[hash-mask-length]	длина указанной хеш-маски. Используется для выбора RP Диапазон значений от 0 до 32



	[priority]	приоритет для Candidate BSR. Диапазон значений: от 0 до 255. Если значение не указано, приоритет по умолчанию – 64
По умолчанию	Маршрутизатор не назначен в качестве Candidate BSR	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Данная команда используется для назначения роли Candidate BSR в режиме глобальной конфигурации и указания в PIM-SM информации о кандидате BSR для выполнения сравнений с другими кандидатами на маршрутизатор BSR. Только после введения данной команды маршрутизатор становится маршрутизатором-кандидатом BSR	
Пример	Настроить интерфейс vlan1 в режиме глобальной конфигурации в качестве интерфейса-кандидата на передачу BSR-сообщений. Switch (config)# ip pim bsr-candidate vlan1 30 10 Switch (config)#	

10.4.15. Подсчет контрольной суммы пакета Register (ip pim cisco-register-checksum)

Синтаксис	ip pim cisco-register-checksum [group-list <simple-acl>] no ip pim cisco-register-checksum [group-list <simple-acl>] Устанавливает для контрольной суммы пакета регистрационного сообщения группы, указанной фильтром myfilter, использование всей длины пакета	
Параметр	<simple-acl>	<1-99> Простой список доступа
По умолчанию	Вычисление контрольной суммы в соответствии с длиной заголовка регистрационного пакета, по умолчанию: 8	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда используется для взаимодействия с более ранними версиями Cisco IOS	
Пример	Задать для контрольной суммы пакета регистрационного сообщения группы, указанной фильтром myfilter, использование всей длины пакета. Switch (config)# ip pim cisco-register-checksum group-list 23 Switch (config)#	



10.4.16. Настройка приоритета для выбора назначенного маршрутизатора (ip pim dr-priority)

Синтаксис	ip pim dr-priority <priority> no ip pim dr-priority Данная команда используется для изменения значения приоритета назначенного маршрутизатора (DR) Соседние узлы в одном сегменте сети выбирают DR в своем сегменте в соответствии с пакетами "hello". Команда "no ip pim dr-priority" восстанавливает значение по умолчанию	
Параметр	<priority>	это приоритет
По умолчанию	1	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Укажите значение приоритета в диапазоне от 0 до 4294967295, чем больше значение, тем выше приоритет	
Пример	Задать приоритет DR VLAN равный 100 Switch (config)# interface vlan 1 Switch (Config-if-Vlan1)ip pim dr-priority 100 Switch (Config -if-Vlan1)#	

10.4.17. Исключение опции GenId (ip pim exclude-genid)

Синтаксис	ip pim exclude-genid no ip pim exclude-genid Эта команда исключает опцию GenId из пакетов Hello, отправляемых PIM SM. Команда "no ipv6 pim exclude-genid" восстанавливает значение по умолчанию	
Параметр		
По умолчанию	Пакеты Hello включают опцию GenId	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Эта команда используется для взаимодействия с более ранними версиями Cisco IOS	



Пример	Задать, чтобы пакеты Hello, отправляемые коммутатором, не включали опцию GenId. <pre>Switch (Config-if-Vlan1)#ip pim exclude-genid</pre> <pre>Switch (Config-if-Vlan1)#</pre>

10.4.18. Время сохранения информации о сообщениях Hello (ip pim hello-holdtime)

Синтаксис	ip pim hello-holdtime <value> no ip pim hello-holdtime Настраивает или отключает значение Holdtime (время сохранения информации) в пакетах Hello, которое описывает время сохранения информации о соседях, и отключает соседей, от которых в течение заданного времени holdtime на коммутатор не поступало пакетов Hello. Команда "no ip pim hello-holdtime" отменяет настроенное значение времени сохранения и восстанавливает значение по умолчанию	
Параметр	<vaule>	значение времени сохранения информации в диапазоне <1-65535>
По умолчанию	Значение Holdtime по умолчанию равно 3,5*Hello_interval, значение Hello_interval по умолчанию равно 30 секундам, поэтому значение Hold time по умолчанию равно 105 секундам	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Если это значение не задано, по умолчанию hellotime будет равен 3,5*Hello_interval. Если задаваемое время сохранения информации меньше, чем текущий интервал hello_interval, эта конфигурация будет отклонена. Каждый раз, когда hello_interval обновляется, hello_holdtime обновляется по следующим правилам: если hello_holdtime не задано, или если hello_holdtime задано, но меньше текущего hello_interval, hello_holdtime будет изменено на 3,5* hello_interval. В остальных случаях сохраняется заданное значение	
Пример	Настроить Hello Holdtime на vlan1 <pre>Switch (config)# interface vlan1</pre> <pre>Switch (Config -if-Vlan1)#ip pim hello-holdtime 10</pre> <pre>Switch (Config -if-Vlan1)#</pre>	



10.4.19. Интервал отправки hello-пакетов (ip pim hello-interval)

Синтаксис	ip pim hello-interval <interval> no ip pim hello-interval Задает на интерфейсе интервал отправки hello-пакетов pim. Команда "no ip pim hello-interval" восстанавливает значение по умолчанию	
Параметр	<interval>	интервал периодичности отправки pim hello-пакетов, в диапазоне от 1 до 18724 секунды
По умолчанию	Интервал передачи hello_interval пакетов pim составляет 30 секунд	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Сообщения Hello позволяют коммутаторам PIM определять взаимное расположение и устанавливать соседство. Коммутатор PIM объявляет о своем присутствии, регулярно отправляя соседям сообщения Hello. Соседи, от которых в течение определенного времени не поступало hello-сообщений, считаются отключившимися. Это значение не должно быть больше, чем время работы соседей	
Пример	Настроить интервал hello для pim-sm VLAN Switch (config)#interface vlan 1 Switch (Config-If-Vlan1)#ip pim hello-interval 20 Switch (Config-If-Vlan1)#ip pim hello-interval 20 Switch (Config-If-Vlan1)#	

10.4.20. Игнорирование приоритета RP в RP-Set (ip pim ignore-rp-set-priority)

Синтаксис	ip pim ignore-rp-set-priority no ip pim ignore-rp-set-priority При выборе точки встречи (RP) эта команда настраивает коммутатор на включение регулирования хеширования и игнорирование приоритета RP. Команда используется для взаимодействия с более ранними версиями Cisco IOS	
Параметр		
По умолчанию	Отключено	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Когда выбрана RP, Pim обычно выбирает на основе приоритета RP. Когда задана эта команда, pim будет игнорировать приоритет RP. При отсутствии в сети более старого маршрутизатора применять данную команду не рекомендуется
Пример	Switch (config)#ip pim ignore-rp-set-priority

10.4.21. Интервал между сообщениями join/prune (ip pim jp-timer)

Синтаксис	ip pim jp-timer <value> no ip pim jp-timer Задаёт добавление таймера JP. Команда “no ip pim jp-timer” восстанавливает значение по умолчанию	
Параметр	<value>	в диапазоне от 10 до 65535 секунд
По умолчанию	60 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда устанавливает интервал между периодическими передачами пакетов JOIN-PRUNE в PIM, значение по умолчанию - 60 секунд. Если нет особых причин, рекомендуется использовать значение по умолчанию	
Пример	Настроить интервал таймера Switch (config)#ip pim jp-timer 59	

10.4.22. Многоадресная маршрутизация для протокола PIM (ip pim multicast-routing)

Синтаксис	ip pim multicast-routing no ip pim multicast-routing Подключает протокол PIM-SM в глобальном режиме. Команда “no ip pim multicast-routing” отключает протокол PIM-SM в глобальном режиме	
Параметр		
По умолчанию	Протокол PIM-SM отключен	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Подключает протокол PIM-SM в глобальном режиме. Чтобы PIM-SM функционировал, он должен быть включен на интерфейсе	



Пример	Включить протокол PIM-SM в глобальном режиме. Switch (config)#ip pim multicast-routing

10.4.23. Настройка фильтрации соседей PIM (ip pim neighbor-filter)

Синтаксис	ip pim neighbor-filter <list-number> no ip pim neighbor-filter <list-number> Задаёт список доступа, содержащий соседние устройства. Если соединение с соседом установлено, но условия фильтрации не выполнены, соединение немедленно обрывается. Если соединение не создано, это соединение не может быть установлено	
Параметр	<list-number>	номер списка доступа, в диапазоне 1 до 99
По умолчанию	Фильтрация соседей не сконфигурирована	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	По умолчанию ACL имеет значение DENY (отклонить). При настройке "access-list 1" по умолчанию для списка задается значение "deny". В примере ниже, если параметр "permit any" не задан, deny 10.1.4.10 255.255.255.0 - это то же самое, что deny any (отклонить все)	
Пример	Настроить правила фильтрации соседей pim в VLAN. Switch #show ip pim neighbor Neighbor Interface Uptime/Expires Ver DR Address Priority/Mode 10.1.4.10 Vlan1 02: 30: 30/00: 01: 41 v2 4294967294 / DR Switch (Config-if-Vlan1)#ip pim neighbor-filter 2 Switch (config)#access-list 2 deny 10.1.4.10 255.255.255.0 Switch (config)#access-list 2 permit any-source Switch (config)#show ip pim neighbor	

10.4.24. Ограничение скорости отправки пакета Register (ip pim register-rate-limit)

Синтаксис	ip pim register-rate-limit <limit> no ip pim register-rate-limit Команда используется для настройки скорости отправки пакетов регистрации выделенного маршрутизатора (DR); единица измерения - пакетов/секунду. Команда "no ip pim Register-rate-limit" восстанавливает значение по умолчанию. Эта команда действует только для пакета Register каждого (S, G) пакета, но не для всех пакетов Register во всей системе	
Параметр	<limit>	в диапазоне от 1 до 65535



По умолчанию	Скорость отправки не ограничена
Режим	Режим глобальной конфигурации
Руководство по использованию	Эта настройка ограничивает передачу пакетов REGISTER для предотвращения атак на DR
Пример	Настроить скорость отправки пакетов регистрации DR на 59 пакетов/секунду. Switch (config)#ip pim register-rate-limit 59

10.4.25. Обнаружение доступности пакета Register (ip pim register-rp-reachability)

Синтаксис	ip pim register-rp-reachability no ip pim register-rp-reachability Эта команда позволяет DR проверять доступность RP в процессе регистрации	
Параметр		
По умолчанию	Не проверяется	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда задает для DR выполнение проверки доступности RP	
Пример	Задать для DR выполнение проверки доступности RP. Switch (config)#ip pim register-rp-reachability	

10.4.26. Настройка адреса источника пакета Register (ip pim register-source)

Синтаксис	ip pim register-source {<A.B.C.D> <ifname> vlan <vlan-id>} no ip pim register-source Эта команда используется для установки адреса источника пакетов регистрации register, передаваемых DR, вместо адреса источника по умолчанию. Адресом источника по умолчанию обычно является RPF-сосед направления хоста-источника	
Параметр	<ifname>	имя интерфейса
	<vlan-id>	идентификатор VLAN



	<A.B.C.D>	сконфигурированный IP-адрес источников
По умолчанию	Не проверяется	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда «no ip pim register-source» восстанавливает значение по умолчанию без дополнительных параметров. Настроенный адрес должен быть доступен для сообщений Register-Stop, отправляемых RP. Обычно это loopback-адрес, но могут быть и другие физические адреса. Адрес должен быть объявлен по протоколу одноадресного маршрутизатора DR	
Пример	Настроить адреса источника, отправляемого DR. Switch (config)#ip pim register-source 10.1.1.1	

10.4.27. Настройка времени подавления пакета Register (ip pim register-suppression)

Синтаксис	ip pim register-suppression <value> no ip pim register-suppression Команда устанавливает значение времени подавления регистрационных (register) сообщений, единицей измерения является секунда. Команда “no ip pim register-suppression” восстанавливает значение по умолчанию	
Параметр	<value>	значение таймера, в диапазоне от 10 до 65535 секунд
По умолчанию	60 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Если это значение задано на DR, то это значение таймера подавления регистрационных (register) сообщений. Берется большее значение из стандартного времени поддержания регистра в рабочем состоянии на RP (210 с) и суммы утроенного времени подавления регистрационных сообщений и 5. Если задать это значение на RP не устанавливая команду «ip pim rp-register-kat», данная команда может изменить время поддержания активности соединения регистрационных сообщений RP	
Пример	Настройте значение таймера подавления регистра на 10 секунд. Switch (config)#ip pim register-suppression 10	



10.4.28. Настройка статических адресов RP (ip pim rp-address)

Синтаксис	ip pim rp- address <A.B.C.D> <A.B.C.D/M> no ip pim rp-address <A.B.C.D> [<A.B.C.D/M> <all>] Эта команда предназначена для настройки статического RP глобально или в диапазоне адресов многоадресной рассылки. Команда “no ip pim rp-address <A.B.C.D> [<A.B.C.D/M> <all>]” отменяет статические RP	
Параметр	<A.B.C.D>	адрес RP (точки встречи)
	<A.B.C.D/M>	объем указанного адреса RP
	<all>	весь диапазон
По умолчанию	Этот коммутатор не является статическим маршрутизатором RP	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда используется для установки статического RP глобально или для диапазона многоадресных адресов, а также для установки информации о статическом RP для PIM-SM. Обратите внимание, что при вычислении RP сначала выбирается BSR RP, в случае неудачи выбирается статический RP	
Пример	Глобально настроить vlan1 в качестве RP-кандидата, объявляющего интерфейс отправки. Switch (config)# ip pim rp-address 10.1.1.1 238.0.0.0/8	

10.4.29. Назначение роли RP Candidate (ip pim rp-candidate)

Синтаксис	ip pim rp-candidate {vlan<vlan-id> loopback<index> <ifname>} [<A.B.C.D/M>] [<priority>] no ip pim rp-candidate Данная команда используется для назначения роли Candidate RP в режиме глобальной конфигурации и указания в PIM-SM информации о кандидате для выполнения сравнений с другими кандидатами RP. Команда “no ip pim rp-candidate” отменяет назначение candidate RP	
Параметр	vlan-id	идентификатор vlan
	<index>	индексация интерфейса Loopback
	ifname	имя указанного интерфейса



	A.B.C.D/M	префикс и маска ip-адреса
	<priority>	это приоритет выбора RP, он варьируется от 0 до 255, по умолчанию значение 192, меньшее значение имеет больший приоритет
По умолчанию	Этот коммутатор не является статическим маршрутизатором RP	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Данная команда используется для назначения роли Candidate RP в режиме глобальной конфигурации и указания в PIM-SM информации о кандидате для выполнения сравнений с другими кандидатами RP. Коммутатор может стать RP candidate только после ввода данной команды	
Пример	Настроить vlan1 в качестве интерфейса отправки сообщений кандидата RP, объявляющего об отправке сообщений Switch (config)# ip pim rp-candidate vlan1 100	

10.4.30. Настройка времени keep-alive для регистрационных сообщений (ip pim rp-register-kat)

Синтаксис	ip pim rp-register-kat <vaule> no ip pim rp-register-kat Команда настраивает значение таймера KAT (KeepAlive Timer) для записей (S, G) точки встречи RP, в секундах. Команда "no ip pim rp-register-kat" восстанавливает значение по умолчанию	
Параметр	<value>	значение таймера, в диапазоне от 1 до 65535 секунд
По умолчанию	185 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда используется для установки времени время поддержания RP в активном состоянии, в течение которого записи (S, G) RP не удаляются из-за неполучения пакета REGISTER. Если по истечении времени поддержания в активном состоянии не будет получен новый пакет REGISTER, запись будет недействительной	
Пример	Задать значение kat для записей (S, G) на RP равное 180 секундам Switch (config)#ip pim rp-register-kat 180	



10.4.31. Границы управления и ACL для протокола PIM (ip pim scope-border)

Синтаксис	ip pim scope-border [<1-99 > <acl_name>] no ip pim scope-border Устанавливает или удаляет границу управления протокола PIM	
Параметр	<1-99 >	номер ACL для границы управления
	<acl_name>	имя ACL для границы управления
По умолчанию	Границы управления отсутствуют. Если ACL (список контроля доступа) не указан, будет использоваться граница управления по умолчанию	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Команда определяет границы управления и список контроля доступа для протокола PIM. Поток многоадресных данных не будет перенаправляться на SCOPE-BORDER	
Пример	Switch(Config-if-Vlan2)#ip pim scope-border 3	

10.4.32. Включение PIM для работы в разреженном режиме (ip pim sparse-mode)

Синтаксис	ip pim sparse-mode [passive] no ip pim sparse-mode [passive] Включает PIM-SM на интерфейсе; Команда “no ip pim sparse-mode [passive]” отключает PIM-SM	
Параметр	[passive]	означает отключить PIM-SM (то есть PIM-SM не получает никаких пакетов) и включить только IGMP (получать и передавать IGMP-пакеты)
По умолчанию	Режим PIM-SM отключен	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Команда используется для включения PIM-SM на интерфейсе	
Пример	Включить PIM-SM на интерфейсе vlan1. Switch(config)#interface vlan 1 Switch(Config-If-Vlan1)#ip pim sparse-mode	



	Switch(Config-If-Vlan1)#exit

10.4.33. Вывод информации о BSR (show ip pim bsr-router)

Синтаксис	show ip pim bsr-router Отображает адрес BSR												
Параметр													
По умолчанию	Отсутствует												
Режим	В привилегированном режиме												
Руководство по использованию	Команда выводит информацию о BSR, который поддерживается PIM												
Пример	show ip pim bsr-router PIMv2 Bootstrap information This system is the Bootstrap Router (BSR) BSR address: 10.1.4.3 (?) Uptime: 00: 06: 07, BSR Priority: 0, Hash mask length: 10 Next bootstrap message in 00: 00: 00 Role: Candidate BSR State: Elected BSR Next Cand_RP_advertisement in 00: 00: 58 RP: 10.1.4.3(Vlan1) <table> <tr> <th>Информация, отображаемая на экране</th><th>Пояснения</th></tr> <tr> <td>BSR address</td><td>Адрес Bsr-маршрутизатора</td></tr> <tr> <td>Priority</td><td>Приоритет Bsr-маршрутизатора</td></tr> <tr> <td>Hash mask length</td><td>Длина хеш-маски Bsr-маршрутизатора</td></tr> <tr> <td>State</td><td>Текущий статус этого кандидата BSR</td></tr> <tr> <td>Elected BSR</td><td>это выбранный BSR Elected BSR это выбранный BSR</td></tr> </table>	Информация, отображаемая на экране	Пояснения	BSR address	Адрес Bsr-маршрутизатора	Priority	Приоритет Bsr-маршрутизатора	Hash mask length	Длина хеш-маски Bsr-маршрутизатора	State	Текущий статус этого кандидата BSR	Elected BSR	это выбранный BSR Elected BSR это выбранный BSR
Информация, отображаемая на экране	Пояснения												
BSR address	Адрес Bsr-маршрутизатора												
Priority	Приоритет Bsr-маршрутизатора												
Hash mask length	Длина хеш-маски Bsr-маршрутизатора												
State	Текущий статус этого кандидата BSR												
Elected BSR	это выбранный BSR Elected BSR это выбранный BSR												



10.4.34. Вывод информации о конфигурации для PIM на интерфейсе (show ip pim interface)

Синтаксис	show ip pim interface	
Параметр	Отображение информации о конфигурации для PIM на интерфейсе	
По умолчанию	Отсутствует	
Режим	Привилегированный режим и глобальной конфигурации	
Руководство по использованию	Команда выводит информацию о конфигурации для PIM на интерфейсе	
Пример	testS2(config)#show ip pim interface	
	<pre>Address Interface VIFindex Ver/ Nbr DR DR Mode Count Prior 10.1.4.3 Vlan1 0 v2/S 1 1 10.1.4.3 10.1.7.1 Vlan2 2 v2/S 0 1 10.1.7.1</pre>	
	Информация, отображаемая на экране	Пояснения
	Address	адрес интерфейса
	Interface	имя интерфейса
	VIF index	индекс интерфейса
	Ver/Mode	версия и режим Pim, обычно v2, для разреженного режима отображается S, для уплотненного режима отображается D
	Nbr Count	число соседей интерфейса
	DR Prior	приоритет назначенного маршрутизатора (DR)
	DR	адрес DR интерфейса

10.4.35. Вывод таблицы маршрутизации PIM-SM (show ip pim mroute sparse-mode)

Синтаксис	show ip pim mroute sparse-mode [group <A.B.C.D>] [source <A.B.C.D>] Отображение таблицы маршрутов многоадресной рассылки PIM-SM	
Параметр	group <A.B.C.D>	Отображение перераспределенных записей, связанных с этой многоадресной рассылкой адрес интерфейса



	source <A.B.C.D>	Отображение перераспределенных записей, относящихся к этому источнику											
По умолчанию	Отсутствует												
Режим	Привилегированный режим и глобальной конфигурации												
Руководство по использованию	Команда выводит маршрутизаторы BSP в сети, обслуживаемой PIM-SM												
Пример	Switch#show ip pim mroute sparse-mode												
	IP Multicast Routing Table												
	(*,*,RP) Entries: 0												
	(*,G) Entries: 1												
	(S,G) Entries: 0												
	(S,G,rpt) Entries: 0												
	(*, 239.192.1.10)												
	RP: 10.1.6.1												
RPF nbr: 10.1.4.10													
RPF idx: Vlan1 Upstream State: JOINED													
Local ..l.....													
Joined													
Asserted													
Outgoing ..o.....													
<table><tr><td>Информация, отображаемая на экране</td><td>Пояснения</td></tr><tr><td>Entries</td><td>Количество каждой записи</td></tr><tr><td>RP</td><td>RP-адрес общего дерева</td></tr><tr><td>RPF nbr</td><td>Направление RP или направление восходящего соседа источника.</td></tr><tr><td>RPF idx</td><td>Интерфейс RPF nbr</td></tr><tr><td>Upstream State Upstream State</td><td>Статус Upstream. Существует два состояния Joined (присоединен к дереву, ожидается получение данных от вышестоящего маршрутизатора) и Not Joined (вышел из дерева, не ожидается получение данных от вышестоящего маршрутизатора), а также дополнительные опции,</td></tr></table>		Информация, отображаемая на экране	Пояснения	Entries	Количество каждой записи	RP	RP-адрес общего дерева	RPF nbr	Направление RP или направление восходящего соседа источника.	RPF idx	Интерфейс RPF nbr	Upstream State Upstream State	Статус Upstream. Существует два состояния Joined (присоединен к дереву, ожидается получение данных от вышестоящего маршрутизатора) и Not Joined (вышел из дерева, не ожидается получение данных от вышестоящего маршрутизатора), а также дополнительные опции,
Информация, отображаемая на экране	Пояснения												
Entries	Количество каждой записи												
RP	RP-адрес общего дерева												
RPF nbr	Направление RP или направление восходящего соседа источника.												
RPF idx	Интерфейс RPF nbr												
Upstream State Upstream State	Статус Upstream. Существует два состояния Joined (присоединен к дереву, ожидается получение данных от вышестоящего маршрутизатора) и Not Joined (вышел из дерева, не ожидается получение данных от вышестоящего маршрутизатора), а также дополнительные опции,												



		например, RPT Not Joined, Pruned, Not Pruned доступны для (S,G,rpt.)
	Local	Локальный интерфейс присоединения, этот интерфейс получает IGMPJoin
	Joined	Интерфейс присоединения к PIM, этот интерфейс получает сообщения J/P
	Asserted	Состояние подтверждено
	Outgoing	Финальное устройство выхода многоадресных данных, в данном примере, индекс выходного интерфейса равен 2. Команда "show ip pim interface" позволяет запросить информацию об интерфейсе

10.4.36. Вывод информации о соседних устройствах PIM (show ip pim neighbor)

Синтаксис	show ip pim neighbor								
Параметр	Вывод информации о соседних устройствах маршрутизатора								
По умолчанию	Отсутствует								
Режим	Привилегированный режим и глобальной конфигурации								
Руководство по использованию	Данная команда используется для отображения информации о том, какие многоадресные маршрутизаторы настроены для PIM								
Пример	Switch(config)#show ip pim neighbor Neighbor Interface Uptime/Expires Ver DR Address Priority/Mode 10.1.6.1 Vlan1 00: 00: 10/00: 01: 35 v2 1 / 10.1.6.2 Vlan1 00: 00: 13/00: 01: 32 v2 1 / 10.1.4.2 Vlan3 00: 00: 18/00: 01: 30 v2 1 / 10.1.4.3 Vlan3 00: 00: 17/00: 01: 29 v2 1 / <table> <tr> <td>Информация, отображаемая на экране</td><td>Пояснения</td></tr> <tr> <td>Neighbor Address</td><td>адрес соседнего устройства</td></tr> <tr> <td>Interface</td><td>интерфейс соседнего устройства</td></tr> <tr> <td>Uptime/Expires</td><td>Время работы/истечения срока</td></tr> </table>	Информация, отображаемая на экране	Пояснения	Neighbor Address	адрес соседнего устройства	Interface	интерфейс соседнего устройства	Uptime/Expires	Время работы/истечения срока
Информация, отображаемая на экране	Пояснения								
Neighbor Address	адрес соседнего устройства								
Interface	интерфейс соседнего устройства								
Uptime/Expires	Время работы/истечения срока								



	Ver	Версия Pim, обычно v2
	DR Priority/Mode	Приоритет DR в сообщениях hello от соседа и является ли сосед выделенным маршрутизатором (DP) интерфейса

10.4.37. Вывод информации о следующих хопх PIM (show ip pim nexthop)

Синтаксис	show ip pim nexthop Отображение буферизованного маршрутизатора следующего узла PIM в таблице маршрутов одноадресной рассылки	
Параметр		
По умолчанию	Отсутствует	
Режим	Привилегированный режим и глобальной конфигурации	
Руководство по использованию	Команда выводит информацию о буферизованном маршрутизаторе PIM nexthop	
Пример	Switch(config)#show ip pim nexthop Flags: N = New, R = RP, S = Source, U = Unreachable Destination Type Nexthop Nexthop Nexthop Nexthop Metric Pref Refcnt Num Addr Ifindex Name 192.168.1.1 N... 1 0.0.0.0 2006 0 0 1 192.168.1.9 ..S. 1 0.0.0.0 2006 0 0 1	
	Информация, отображаемая на экране	Пояснения
	Destination	Назначение следующей записи
	Type	N: создан следующий узел (nexthop), направление RP и направление S не определены. R: направление точки встречи RP S: направление источника U: нет доступа
	Nexthop Num	номер следующего узла
	Nexthop Addr	адрес следующего узла
	Nexthop Ifindex	индекс интерфейса следующего узла



NextHop Name	имя следующего узла
Metric	метрика следующего узла
Pref	предпочтительный выбор маршрутизатора
Refcnt	Счетчик ссылок

10.4.38. Вывод адреса RP для указанной группы (show ip pim rp-hash)

Синтаксис	show ip pim rp-hash <A.B.C.D> Выводит на экран адреса RP для точки слияния A.B.C.D	
Параметр	<A.B.C.D>	адрес группы
По умолчанию	Отсутствует	
Режим	Привилегированный режим и глобальной конфигурации	
Руководство по использованию	Данная команда применяется для отображения адреса RP, соответствующего указанному адресу группы	
Пример	<pre>Switch(Config-if-Vlan1)#show ip pim rp-hash 239.192.1.10 RP: 10.1.6.1 Info source: 10.1.6.1, via bootstrap</pre> Информация, отображаемая на экране RP Info source Пояснения RP запрашиваемой группы Источник информации Bootstrap	

10.4.39. Вывод точек встреч и привязок групп к RP (show ip pim rp mapping)

Синтаксис	show ip pim rp mapping Отображение привязок (mapping) групп к точкам встреч (RP) и точек встреч (RP)
Параметр	
По умолчанию	Отсутствует
Режим	Привилегированный режим и глобальной конфигурации
Руководство по использованию	Используйте команду, чтобы отобразить активные точки встречи и информации о привязках



Пример	Switch(Config-if-Vlan1)#show ip pim rp mapping PIM Group-to-RP Mappings Group(s): 224.0.0.0/4 RP: 224.0.0.0/4 RP: 10.1.6.1 Info source: 10.1.6.1, via bootstrap, priority 6 Uptime: 00: 11: 04 Информация, отображаемая на экране	
	Group(s)	Пояснения Диапазон адресов групп для RP
	Info source	источник сообщений Bootstrap
	Priority	приоритет сообщений Bootstrap

10.5. Настройка протокола PIM-SSM

10.5.1. Диапазон многоадресной рассылки PIM-SSM (ip multicast ssm)

Синтаксис	ip multicast ssm {default range <access-list-number >} no ip multicast ssm Настраивает диапазон адресов многоадресной рассылки pim ssm. Команда "no ip multicast ssm" удаляет настроенную группу многоадресной рассылки pim ssm	
Параметр	default	диапазон адресов SSM-группы по умолчанию, 232/8
	<access-list-number >	применяемый номер списка доступа, в диапазоне от 1 до 99
По умолчанию	Диапазон адресов многоадресной рассылки pim ssm не задан	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Pim ssm можно использовать, только если задана эта команда. Перед тем как задать команду убедитесь, что "ip pim multicasting" успешно работает. Эта команда не может работать с DVMRP. Access-list не может использовать список, созданный ip access-list, а только список, указанный в access-list. Пользователи могут сначала выполнить данную команду, а потом настроить соответствующий список ACL, или удалить соответствующий ACL в привязке. Удалить привязку после ее выполнения можно только по команде "no ip pim ssm". Если ssm необходим, эта команда должна быть настроена на соответствующем пограничном маршрутизаторе. Например, на локальном коммутаторе с IGMP (обязательно) и источником многоадресной рассылки DR или RP (хотя бы один из двух) задается эта команда, на среднем коммутаторе нужно только включить PIM-SSM	



Пример	Настроить на коммутаторе включение PIM-SSM, диапазон группы задается списком доступа access-list 23. Switch (config)#ip multicast ssm range 23

10.6. PIM-IM6

10.6.1. Отладка сообщений таймера активности источника IPv6 PIM (debug ipv6 pim timer sat)

Синтаксис	debug ipv6 pim timer sat no debug ipv6 pim timer sat Активирует переключатель отладки сообщений таймера активности источника PIM-DM; Команда “ no debug ipv6 pim timer sat ” отключает отладку
Параметр	Отсутствует
По умолчанию	Отключено
Режим	Привилегированный режим
Руководство по использованию	Включает переключатель для отображения подробной информации о таймере активности источника
Пример	Switch # debug ipv6 pim timer sat

10.6.2. Отладка для получения информации о таймере обновления ipv6 pim (debug ipv6 pim timer srt)

Синтаксис	debug ipv6 pim timer srt no debug ipv6 pim timer srt Запускает отладку для получения информации о таймере обновления состояния PIM-DM. Команда “ no debug ipv6 pim timer srt ” отключает переключатель отладки
Параметр	
По умолчанию	Функция GVRP выключена
Режим	Привилегированный режим
Руководство по использованию	Включите переключатель и выведите на экран подробную информацию о таймере обновления состояния PIM-DM
Пример	Switch # debug ipv6 pim timer srt



10.6.3. Создание статического многоадресного маршрута IPv6 (ipv6 mroute)

Синтаксис	ipv6 mroute <X: X: : X: X> <X: X: : X: X> <ifname> <.ifname> no ipv6 mroute <X: X: : X: X> <X: X: : X: X> [<ifname> <.ifname>] Данная команда используется для создания статического multicast-маршрута. "no" в начале команды удалит определенные статические записи многоадресной рассылки или определенные интерфейсы выхода	
Параметр	<X: X: : X: X> <X: X: : X: X>	адрес источника и адрес группы многоадресной рассылки
	<ifname> <.ifname>	первый это интерфейс входа, а второй это интерфейс выхода
По умолчанию	Отсутствует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Имена <ifname> должны быть действительными интерфейсами VLAN. Поток многоадресных данных не будет пересылаться, если на интерфейсе выхода не настроен PIM и интерфейс не находится в состоянии UP. Если состояние интерфейса не UP, или PIM не настроен, или RPF не действует, поток многоадресных данных не будет пересылаться. Удаление указанной записи многоадресной маршрутизации. Если указаны все интерфейсы выхода или не указано ни одного интерфейса, указанная запись многоадресной маршрутизации будет удалена. В ином случае будет удалена запись многоадресной маршрутизации для указанного интерфейса	
Пример	Switch(config)#ipv6 mroute 10.1.1.1 225.1.1.1 v10 v20 v30	

10.6.4. Настройка границ PIM6 BSR (ipv6 pim bsr-border)

Синтаксис	ipv6 pim bsr-border no ipv6 pim bsr-border Настраивает или удаляет интерфейс PIM6 BSR-BORDER
Параметр	Отсутствует
По умолчанию	BSR-BORDER отсутствуют
Режим	Режим конфигурации интерфейса
Руководство по использованию	Команда настраивает интерфейс в качестве пограничного интерфейса BSR-BORDER. После настройки этой команды сообщения,



	относящиеся к BSR, не будут получаться с указанного интерфейса и не будут пересылаться. Все сети, подключенные к интерфейсу, будут считаться подключенными напрямую
Пример	Switch(Config-if-Vlan1)#ipv6 pim bsr-border

10.6.5. Функция многоадресной маршрутизации IPv6 в уплотненном режиме (ipv6 pim dense-mode)

Синтаксис	ipv6 pim dense-mode no ipv6 pim dense-mode Включает протокол PIM-DM на интерфейсе; Команда “ no ipv6 pim dense-mode ” отключает протокол PIM-DM на интерфейсе
Параметр	
По умолчанию	Протокол PIM-DM отключен
Режим	Режим конфигурации интерфейса
Руководство по использованию	Команда вступит в силу при выполнении ipv6 multicast-routing в глобальном режиме. Не поддерживает взаимную работу протоколов многоадресной рассылки, то есть нельзя одновременно включить уплотненный режим и разреженный режим на одном коммутаторе. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Включить протокол PIM-DM на интерфейсе vlan1. Switch(config)#ipv6 pim multicast-routing Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 pim dense-mode

10.6.6. Значения приоритета назначенного маршрутизатора на интерфейсе (ipv6 pim dr-priority)

Синтаксис	ipv6 pim dr-priority <priority> no ipv6 pim dr-priority Данная команда используется для изменения значения приоритета назначенного маршрутизатора (DR) Соседние узлы в одном сегменте выбирают DR в своем сегменте на основе пакета hello. Команда «no ipv6 pim dr-priority» восстанавливает значение по умолчанию	
Параметр	<priority>	приоритет в диапазоне от 0 до 4294967294
По умолчанию	1	



Режим	Режим конфигурации интерфейса
Руководство по использованию	Значения варьируются от 0 до 4294967294, чем больше значение, тем выше приоритет. Эта команда может быть настроена в туннельном интерфейсе IPv6, но для успешной конфигурации необходимо тщательно настроить туннель
Пример	Switch (config)# interface vlan 1 Switch(Config-if-Vlan1)ipv6 pim dr-priority 100

10.6.7. Исключить опцию GenId на интерфейсе (ipv6 pim exclude-genid)

Синтаксис	ipv6 pim exclude-genid no ipv6 pim exclude-genid Эта команда исключает опцию GenId из пакетов Hello, отправляемых PIM SM. Команда “ no ipv6 pim exclude-genid ” восстанавливает значение по умолчанию
Параметр	Отсутствует
По умолчанию	Сообщение Hello содержит опцию Genid
Режим	Режим конфигурации интерфейса
Руководство по использованию	Эта команда используется для взаимодействия с более ранними версиями Cisco IOS. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет рабочей только в том случае, если туннель тщательно настроен
Пример	Эта команда исключает опцию GenId из пакетов Hello, отправляемых коммутатором. Switch(Config-if-Vlan1)#ipv6 pim exclude-genid

10.6.8. Время сохранения информации о сообщениях Hello для IPv6 PIM (ipv6 pim hello-holdtime)

Синтаксис	ipv6 pim hello-holdtime <value> no ipv6 pim hello-holdtime Настраивает или отключает значение Holdtime (время сохранения информации) в пакетах Hello, которое описывает время сохранения информации о соседях, и отключает соседей, от которых в течение заданного времени holdtime на коммутатор не поступало пакетов Hello. Команда “no ip pim hello-holdtime” отменяет заданное время удержания в достижимом состоянии и восстанавливает значение по умолчанию



Параметр	<vaule>	задаваемое значение удержания
По умолчанию	Значение Holdtime по умолчанию равно $3,5 \times \text{Hello\_interval}$, значение Hello_interval по умолчанию равно 30 секунд, поэтому значение Holdtime по умолчанию равно 105 с	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Если не задано, время отправки hello по умолчанию будет установлено в 3,5 раза больше текущего интервала hello_interval. Если задаваемое время отправки hello меньше текущего интервала hello_interval, настройка будет отклонена. При каждом обновлении интервала hello_interval время hello_holdtime также будет обновляться по следующему правилу: если hello_holdtime не задано, или если hello_holdtime задано, но оно меньше текущего hello_interval, значение hello_holdtime будет увеличено в 3,5 раза от hello_interval. В остальных случаях сохраняется заданное значение. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен	
Пример	Задать на интерфейсе vlan1 время удержания для hello-сообщений равным 10. Switch (config)# interface vlan1 Switch (Config-if-Vlan1)#ipv6 pim hello-holdtime 10	

10.6.9. Интервал отправки hello-сообщений для PIM IPv6 (ipv6 pim hello-interval)

Синтаксис	ipv6 pim hello-interval < interval> no ipv6 pim hello-interval Задаёт интервал отправки сообщений "hello" с интерфейса PIM-DM; Команда "no ipv6 pim hello-interval" восстанавливает значение по умолчанию	
Параметр	< interval>	время, через которое отправляются hello-пакеты PIM-DM в диапазоне от 1 до 18724 секунд
По умолчанию	Интервал периодической передачи сообщения PIM-DM hello по умолчанию равен 30 секундам	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Сообщения Hello позволяют коммутаторам PIM-DM определять взаимное расположение и устанавливать соседство. Коммутатор PIM-DM объявляет о своем присутствии, регулярно отправляя соседям сообщения Hello. Соседи, от которых в течение определенного времени не поступало сообщений Hello, считаются отключившимися.	



	Заданное время не должно превышать время работы соседей. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Настроить интервал hello-сообщений PIM-DM на интерфейсе vlan1 Switch (config)#interface vlan1 Switch(Config-if-Vlan1)#ipv6 pim hello-interval 20

10.6.10. Многоадресная маршрутизация для IPv6, протокол PIM (ipv6 pim multicast-routing)

Синтаксис	ipv6 pim multicast-routing no ipv6 pim multicast-routing Включает протокол PIM-DM в глобальном режиме; Команда “ no ipv6 pim multicast-routing ” отключает протокол PIM-DM
Параметр	
По умолчанию	Протокол PIM-SM отключен
Режим	Режим конфигурации интерфейса
Руководство по использованию	Протокол многоадресной рассылки IPv6 PIM может включаться только после выполнения данной команды
Пример	Включить протокол PIM-DM в глобальном режиме Switch (config)#ipv6 pim multicast-routing

10.6.11. Настройка фильтрации соседей для PIM IPv6 (ipv6 pim neighbor-filter)

Синтаксис	ipv6 pim neighbor-filter <access-list-name> no ipv6 pim neighbor-filter <access-list-name> Задаёт список доступа, содержащий соседние устройства. Если отфильтровать по списку и подключить соседа, то соединение сразу же будет разорвано. Если соединение не создано, это соединение не может быть установлено	
Параметр	<access-list-name>	применяемое имя из списка доступа
По умолчанию	Фильтрация соседей не сконфигурирована	
Режим	Режим конфигурации интерфейса	



Руководство по использованию	Команда фильтрует pim-сообщения соседнего устройства, если не требуется установление соседства. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Настроить список доступа pim neighbor на интерфейсе vlan1 Switch (Config-if-Vlan1)#ipv6 pim neighbor-filter myfilter Switch(config)#ipv6 access-list standard myfilter Switch(config_IPv6_Std-Nacl-myfilter)#deny fe80:20e:cff:fe01:facc Switch(config)#ipv6 access-list standard myfilter Switch(config_IPv6_Std-Nacl-myfilter)#permit any

10.6.12. Границы управления и ACL для протокола PIM IPv6 (ipv6 pim scope-border)

Синтаксис	ipv6 pim scope-border [<500-599> <acl_name>] no ipv6 pim scope-border Настроить или удалить границу управления PIM6	
Параметр	<500-599>	номер ACL для границы управления
	<acl_name>	имя ACL для границы управления
По умолчанию	Границы управления отсутствуют. Если ACL (список контроля доступа) не указан, будет использоваться граница управления по умолчанию	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Команда определяет границы управления и список контроля доступа для протокола PIM IPv6. Поток многоадресных данных не будет перенаправляться на SCOPE-BORDER	
Пример	Switch(Config-if-Vlan2)#ipv6 pim scope-border 503	

10.6.13. Установка интервала SRM в PIM IPv6 (ipv6 pim state-refresh origination-interval)

Синтаксис	ipv6 pim state-refresh origination-interval <interval> no ipv6 pim state-refresh origination-interval Настройка интервала передачи сообщения об обновлении состояния. Команда "no ipv6 pim state-refresh origination-interval" восстанавливает значение по умолчанию	
Параметр	<interval>	Значение интервала передачи пакетов - от 4 до 100 с



По умолчанию	60 секунд
Режим	Режим глобальной конфигурации
Руководство по использованию	Маршрутизатор первого хопа периодически отправляет сообщения stat-refresh, чтобы поддерживать записи списка PIM-DM для всех последующих маршрутизаторов. Команда может изменять интервал отправления сообщений обновления состояния. Обычно не следует изменять соответствующий интервал таймера. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Задать интервал передачи сообщения об обновлении состояния на интерфейсе vlan1 на 90 секунд. Switch (Config-if-Vlan1)#ipv6 pim state-refresh origination-interval 90

10.6.14. Вывод конфигурации PIM на интерфейсе (show ipv6 pim interface)

Синтаксис	show ipv6 pim interface [detail] Отображение конфигурации для PIM на интерфейсе	
Параметр		
По умолчанию	Отсутствует	
Режим	Любой режим	
Руководство по использованию	Данная команда используется для отображения конфигурации PIM на интерфейсе	
Пример	Switch#show ipv6 pim interface Interface VIFindex Ver/ Nbr DR Mode Count Prior Vlan2 0 v2/S 0 1 Адрес: fe80: : 203: fff: fee3: 1244 Global Address: 2000: 1: 111: : 100 DR : this system Vlan3 2 v2/S 0 1 Address : fe80: : 203: fff: fee3: 1244 Global Address: 2000: 10: 1: 13: : 1 DR : this system	
	Информация, отображаемая на экране	Пояснения
	Address	Адрес интерфейса



	Interface	Имя интерфейса
	VIF index	Индекс интерфейса
	Ver/Mode	Версия и режим Pim, обычно v2, для разреженного режима отображается S, для уплотненного режима отображается D
	Nbr Count	Число соседей интерфейса
	DR Prior	Приоритет назначенного маршрутизатора (DR)
	DR	Адрес DR интерфейса

10.6.15. Вывод уплотненного режима многоадресной маршрутизации PIM IPv6 (show ipv6 pim mroute dense-mode)

Синтаксис	show ip pim mroute dense-mode [group <X: X: : X: X>] [source <X: X: : X: X>] Отображение элементов пересылки сообщений PIM-DM	
Параметр	group <X: X: : X: X>	отображает элементы пересылки, относящиеся к данному групповому адресу
	source <X: X: : X: X>	отображает элементы пересылки, относящиеся к данному источнику
По умолчанию	Информация не выводится	
Режим	Привилегированный режим	
Руководство по использованию	Команда показывает элементы пересылки многоадресной рассылки PIM-DM, а именно элементы пересылки многоадресных пакетов в системной таблице FIB	
Пример	Вывести все элементы пересылки сообщений PIM-DM. Switch(config)#show ipv6 pim mroute dense-mode IP Multicast Routing Table (*,G) Entries: 1 (S,G) Entries: 1 (*, ff1e: : 15) Local ..l..... (2000: 10: 1: 12: : 11, ff1e: : 15) RPF nbr: : :	



RPF idx: Vlan12 Upstream State: FORWARDING Origin State: ORIGINATOR Local Pruned Asserted Outgoing ..o	
Информация, отображаемая на экране	Пояснения
(*, ff1e: : 15)	(* ,G) Направляемые элементы
(2000: 10: 1: 12: : 11, ff1e: : 15)	(S,G) Направляемые элементы
RPF nbr	соседнее устройство в нисходящем направлении, соседнее устройство в восходящем направлении для источника в DM, 0.0.0.0 означает, что коммутатор является первым хопом.
RPF idx	интерфейс, находящийся в RPF-соседе
Upstream State	Восходящее направление, включая FORWARDING (пересылка данных), PRUNED (прекращение пересылки данных), ACKPENDING (ожидание ответа от вышестоящего, пересылка данных)
Origin State	Два состояния: ORIGINATOR (в состоянии transmit state-refresh), NON_ORIGINATOR (в состоянии non_transmit state-refresh state)
Local	Подсоединение локального члена к интерфейсу, интерфейс получает сообщение IGMP Join
Pruned	PIM помечает интерфейс как pruned (усеченный), интерфейс получает сообщение Prune
Asserted	Состояние подтверждено
Outgoing Outgoing	Многоадресные данные, окончательно переданные из интерфейса, имеют индексный номер, в данном случае индекс равен 2. Просмотреть детальную информацию об интерфейсе можно с помощью команды show ip pim interface



10.6.16. Вывод информации о соседних устройствах PIM для PIMv6 (show ipv6 pim neighbor)

Синтаксис	show ipv6 pim neighbor Отображение информации о соседних устройствах												
Параметр													
По умолчанию													
Режим	В привилегированном режиме и конфигурирования												
Руководство по использованию	Данная команда используется для отображения информации о том, какие многоадресные маршрутизаторы настроены для PIM												
Пример	Switch(config)#show ipv6 pim neighbor Neighbor Interface Uptime/Expires Ver DR Address Priority/Mode Fe80: : 203: fff: fee3: 1244 Vlan1 00: 00: 10/00: 01: 35 v2 1 /DR fe80: : 20e: cff: fe01: facc Vlan1 00: 00: 13/00: 01: 32 v2 1 / <table border="1"> <tr> <th>Информация, отображаемая на экране</th><th>Пояснения</th></tr> <tr> <td>Neighbor Address</td><td>адрес соседнего устройства</td></tr> <tr> <td>Interface</td><td>интерфейс соседнего устройства</td></tr> <tr> <td>Uptime/Expires</td><td>Время работы/истечения срока</td></tr> <tr> <td>Ver</td><td>Версия Pim, обычно v2</td></tr> <tr> <td>DR Priority/Mode</td><td>Приоритет DR в сообщениях hello от соседа и является ли сосед DP интерфейса.</td></tr> </table>	Информация, отображаемая на экране	Пояснения	Neighbor Address	адрес соседнего устройства	Interface	интерфейс соседнего устройства	Uptime/Expires	Время работы/истечения срока	Ver	Версия Pim, обычно v2	DR Priority/Mode	Приоритет DR в сообщениях hello от соседа и является ли сосед DP интерфейса.
Информация, отображаемая на экране	Пояснения												
Neighbor Address	адрес соседнего устройства												
Interface	интерфейс соседнего устройства												
Uptime/Expires	Время работы/истечения срока												
Ver	Версия Pim, обычно v2												
DR Priority/Mode	Приоритет DR в сообщениях hello от соседа и является ли сосед DP интерфейса.												

10.6.17. Вывод информации о следующих хопх multicast-групп для PIMv6 (show ipv6 pim nexthop)

Синтаксис	show ip pim nexthop Отображение буферизованного маршрутизатора следующего узла PIM в таблице маршрутов одноадресной рассылки
Параметр	



По умолчанию	Отсутствует																		
Режим	В привилегированном режиме и конфигурирования																		
Руководство по использованию	Команда выводит информацию о буферизованном маршрутизаторе PIM nexthop																		
Пример	Switch#show ipv6 pim nexthop Flags: N = New, R = RP, S = Source, U = Unreachable Destination Type Nexthop Nexthop Nexthop Nexthop Metric Pref Refcnt Num Addr lindex Name 2000: 1: 111: : 11 ..S. 1 2004 0 0 2 2000: 1: 111: : 100 .RS. 1 2004 0 0 2 <table border="1"> <tr> <td>Информация, отображаемая на экране</td><td>Пояснения</td></tr> <tr> <td>Место назначения</td><td>Назначение следующей записи</td></tr> <tr> <td>Тип</td><td>N: создан следующий узел (nexthop), направление RP и направление S не определены. R: направление точки встречи RP S: направление источника U: нет доступа</td></tr> <tr> <td>Nexthop Num</td><td>номер следующего узла</td></tr> <tr> <td>Nexthop Addr</td><td>адрес следующего узла</td></tr> <tr> <td>Nexthop lindex</td><td>индекс интерфейса следующего узла</td></tr> <tr> <td>Nexthop Name</td><td>имя следующего узла</td></tr> <tr> <td>Metric</td><td>метрика следующего узла</td></tr> <tr> <td>Pref</td><td>предпочтительный выбор маршрутизатора</td></tr> </table>	Информация, отображаемая на экране	Пояснения	Место назначения	Назначение следующей записи	Тип	N: создан следующий узел (nexthop), направление RP и направление S не определены. R: направление точки встречи RP S: направление источника U: нет доступа	Nexthop Num	номер следующего узла	Nexthop Addr	адрес следующего узла	Nexthop lindex	индекс интерфейса следующего узла	Nexthop Name	имя следующего узла	Metric	метрика следующего узла	Pref	предпочтительный выбор маршрутизатора
Информация, отображаемая на экране	Пояснения																		
Место назначения	Назначение следующей записи																		
Тип	N: создан следующий узел (nexthop), направление RP и направление S не определены. R: направление точки встречи RP S: направление источника U: нет доступа																		
Nexthop Num	номер следующего узла																		
Nexthop Addr	адрес следующего узла																		
Nexthop lindex	индекс интерфейса следующего узла																		
Nexthop Name	имя следующего узла																		
Metric	метрика следующего узла																		
Pref	предпочтительный выбор маршрутизатора																		

10.7. PIM-SM6

10.7.1. Удалить информацию о точках встречи для PIMv6 (clear ipv6 pim bsr rp-set)

Синтаксис	clear ipv6 pim bsr rp-set * Удалить информацию о всех (RP) точках встречи
Параметр	
По умолчанию	



Режим	Привилегированный режим
Руководство по использованию	Команда быстро удаляет все RP
Пример	Switch# clear ipv6 pim bsr rp-set *

10.7.2. Отладка событий PIM для PIMv6 (debug ipv6 pim event)

Синтаксис	debug ipv6 pim event no debug ipv6 pim event Включение или отключение функции отладки событий pim
Параметр	
По умолчанию	Отключено
Режим	Привилегированный режим
Руководство по использованию	Команда подключает функцию отладки событий pim и выводит информацию о событиях, связанных с работой pim
Пример	Switch# debug ipv6 pim event

10.7.3. Отладка pim mfc (debug ipv6 pim mfc)

Синтаксис	debug ipv6 pim mfc (in out) no debug ipv6 pim mfc (in out) Включение и отключение отладки pim mfc (кеш многоадресной пересылки)
Параметр	
По умолчанию	Отключено
Режим	Привилегированный режим
Руководство по использованию	Команда подключает функцию отладки pim mfc и выводит информацию о сгенерированных и переданных идентификаторах многоадресной рассылки
Пример	Switch# debug ipv6 pim mfc



10.7.4. Отладка базы информации управления PIM для PIMv6 (debug ipv6 pim mib)

Синтаксис	debug ipv6 pim mib no debug ipv6 pim mib Включение и отключение отладки PIM MIB
Параметр	
По умолчанию	Отключено
Режим	Привилегированный режим
Руководство по использованию	Команда позволяет просмотреть информацию о PIM MIB с помощью функции отладки PIM MIB. Сейчас эта функция недоступна, она будет добавлена в будущем
Пример	Switch# debug ipv6 pim mib

10.7.5. Отладка для pim nexthop (debug ipv6 pim nexthop)

Синтаксис	debug ipv6 pim nexthop no debug ipv6 pim nexthop Включение или отключение функции отладки для pim nexthop
Параметр	
По умолчанию	Отключено
Режим	Привилегированный режим
Руководство по использованию	Команда позволяет проверить информацию об изменении PIM NEXTHOP
Пример	Switch# debug ipv6 pim nexthop

10.7.6. Отладка менеджера сетевых служб PIM для IPv6 PIM (debug ipv6 pim nsm)

Синтаксис	debug ipv6 pim nsm no debug ipv6 pim nsm Включение или отключение функции отладки на PIM, взаимодействующего с сетевыми службами
Параметр	
По умолчанию	Отключено



Режим	Привилегированный режим
Руководство по использованию	Команда позволяет проверить информацию, передаваемую между PIM и сетевыми службами
Пример	Switch# debug ipv6 pim nsm

10.7.7. Отладка пакета pim (debug ipv6 pim packet)

Синтаксис	debug ipv6 pim packet [in out] no debug ipv6 pim packet [in out] Включить или отключить отладку pim	
Параметр	In	показывать только принятые пакеты pim
	out	показывать только переданные пакеты pim
	без параметра	показывать и принятые и переданные пакеты pim
По умолчанию	Отключено	
Режим	Привилегированный режим	
Руководство по использованию	Команда позволяет проверить полученные и переданные этим коммутатором пакеты pim	
Пример	Switch# debug ipv6 pim packet in	

10.7.8. Просмотр информации о статусе PIM для PIMv6 (debug ipv6 pim state)

Синтаксис	debug ipv6 pim state no debug ipv6 pim state Включение и отключение отладки PIM	
Параметр		
По умолчанию	Отключено	
Режим	Привилегированный режим	
Руководство по использованию	Просмотр информации об изменении статуса pim на этом коммутаторе	
Пример	Switch# debug ipv6 pim state	



10.7.9. Отладка пакетов pim (debug ipv6 pim packet)

Синтаксис	debug ipv6 pim timer debug ipv6 pim timer assert debug ipv6 pim timer assert at debug ipv6 pim timer bsr bst debug ipv6 pim timer bsr crp debug ipv6 pim timer bsr debug ipv6 pim timer hello ht debug ipv6 pim timer hello nlt debug ipv6 pim timer hello tht debug ipv6 pim timer hello debug ipv6 pim timer joinprune et debug ipv6 pim timer joinprune grt debug ipv6 pim timer joinprune jt debug ipv6 pim timer joinprune kat debug ipv6 pim timer joinprune ot debug ipv6 pim timer joinprune plt debug ipv6 pim timer joinprune ppt debug ipv6 pim timer joinprune pt debug ipv6 pim timer joinprune debug ipv6 pim timer register rst debug ipv6 pim timer register no debug ipv6 pim timer no debug ipv6 pim timer assert no debug ipv6 pim timer assert at no debug ipv6 pim timer bsr bst no debug ipv6 pim timer bsr crp no debug ipv6 pim timer bsr no debug ipv6 pim timer hello ht no debug ipv6 pim timer hello nlt no debug ipv6 pim timer hello tht no debug ipv6 pim timer hello
	no debug ipv6 pim timer joinprune et no debug ipv6 pim timer joinprune grt no debug ipv6 pim timer joinprune jt no debug ipv6 pim timer joinprune kat no debug ipv6 pim timer joinprune ot no debug ipv6 pim timer joinprune plt no debug ipv6 pim timer joinprune ppt no debug ipv6 pim timer joinprune pt no debug ipv6 pim timer joinprune no debug ipv6 pim timer register rst no debug ipv6 pim timer register no debug ipv6 pim timer Включение или отключение каждого таймера pim
Параметр	
По умолчанию	Отключено
Режим	Привилегированный режим
Руководство по использованию	Включение отладочной информации для указанного таймера
Пример	Switch# debug ipv6 pim timer assert



10.7.10. Статический многоадресный маршрут для PIMv6 (ipv6 mroute)

Синтаксис	ipv6 mroute <X: X: : X: X> <X: X: : X: X> <ifname> <.ifname> no ipv6 mroute <X: X: : X: X> <X: X: : X: X> [<ifname> <.ifname>] Данная команда используется для создания статического multicast-маршрута. "no" в начале команды удалит определенные статические записи многоадресной рассылки или определенные интерфейсы выхода	
Параметр	<X: X: : X: X> <X: X: : X: X>	адрес источника и адрес группы многоадресной рассылки
	<ifname> <.ifname>	первый это интерфейс входа, а второй это интерфейс выхода
По умолчанию	Если команда не содержит параметров интерфейса, запись статической многоадресной рассылки удаляется	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Имена <ifname> должны быть действительными интерфейсами VLAN. Поток многоадресных данных не будет пересылаться, если на интерфейсе выхода не настроен PIM и интерфейс не находится в состоянии UP. Если состояние интерфейса не UP, или PIM не настроен, или RPF не действует, поток многоадресных данных не будет пересылаться. Удаление указанной записи многоадресной маршрутизации. Если указаны все интерфейсы выхода или не указано ни одного интерфейса, указанная запись многоадресной маршрутизации будет удалена. В ином случае будет удалена запись многоадресной маршрутизации для указанного интерфейса	
Пример	Switch(config)#ipv6 mroute 10.1.1.1 225.1.1.1 v10 v20 v30	

10.7.11. Кеширование многоадресного маршрута для PIMv6 (ipv6 multicast unresolved-cache aging-time)

Синтаксис	ipv6 multicast unresolved-cache aging-time <value> no ipv6 multicast unresolved-cache aging-time Устанавливает время кеширования для основной многоадресной маршрутизации. "no" в начале команды восстанавливает значение по умолчанию	
Параметр	< value>	задаваемое время кеширования, в диапазоне от 1 до 20 секунд
По умолчанию	20 секунд	



Режим	Режим глобальной конфигурации
Руководство по использованию	Команда задает время кеширования записи многоадресного маршрута в ядре
Пример	Switch(config)# ipv6 multicast unresolved-cache aging-time 18

10.7.12. Фильтрация пакетов Register для IPv6 PIM (ipv6 pim accept-register)

Синтаксис	ipv6 pim accept-register list <access-list-name> no ipv6 pim accept-register Выполнение фильтрации указанной многоадресной группы и многоадресного адреса	
Параметр	<access-list-name>	номер в списке доступа, в диапазоне от 100 до 199
По умолчанию	Разрешены многоадресные регистры из любых источников в любые группы	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда используется для установки списка доступа для фильтрации пакетов PIM REGISTER. Адреса списка доступа соответственно указывают на отфильтрованные источники многоадресной рассылки и информацию о многоадресных группах. Для комбинаций источник-группа, соответствующих DENY (запрет), PIM немедленно отправляет REGISTER-STOP и не создает групповые записи при получении пакетов REGISTER. В отличие от других списков доступа, при настройке списка доступа по умолчанию используется значение PERMIT (разрешено)	
Пример	Настроить правило фильтра сообщений регистра на myfilter. Switch(config)#ipv6 pim accept-register list myfilter Switch(config)#ipv6 access-list standard myfilter Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::10/128	

10.7.13. Настройка пограничного BSR для IPv6 PIM (ipv6 pim bsr-border)

Синтаксис	ipv6 pim bsr-border no ipv6 pim bsr-border Настраивает или отменяет настройку граничного BSR для PIM	
Параметр		
По умолчанию	BSR-BORDER отсутствуют	



Режим	Режим конфигурации интерфейса
Руководство по использованию	Команда настраивает интерфейс в качестве пограничного интерфейса BSR-BORDER. После настройки этой команды сообщения, относящиеся к BSR, не будут получаться с указанного интерфейса и не будут пересылаться. Все сети, подключенные к интерфейсу, будут считаться подключенными напрямую
Пример	Switch(Config-if-Vlan1)#ipv6 pim bsr-border

10.7.14. Назначение роли Candidate BSR маршрутизатору для PIMv6 (ipv6 pim bsr-candidate)

Синтаксис	ipv6 pim bsr-candidate {vlan <vlan-id> <ifname>} [hash-mask-length] [priority] no ipv6 pim bsr-candidate Данная команда используется для назначения роли Candidate BSR в режиме глобальной конфигурации и указания в PIM-SM информации о кандидате BSR для выполнения сравнений с другими кандидатами BSR. Команда " no ipv6 pim bsr-candidate {vlan <vlan_id> tunnel <tunnel-id> <ifname>} [<hash-mask-length>] [<priority>] " отменяет назначение роли Candidate BSR	
Параметр	vlan-id	идентификатор VLAN, в диапазоне от 1 до 4094;
	ifname	имя указанного интерфейса
	[hash-mask-length]	длина указанной хеш-маски. Используется для выбора RP Диапазон значений от 0 до 32
	[priority]	приоритет для Candidate BSR. Диапазон значений: от 0 до 255. Если параметр не задан, приоритет по умолчанию – 64
По умолчанию	Маршрутизатор не назначен в качестве Candidate BSR	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Данная команда используется для назначения роли Candidate BSR в режиме глобальной конфигурации и указания в PIM-SM информации о кандидате BSR для выполнения сравнений с другими кандидатами на маршрутизатор BSR. Только после введения данной команды маршрутизатор становится маршрутизатором-кандидатом BSR	
Пример	Настроить интерфейс vlan1 в режиме глобальной конфигурации в качестве интерфейса-кандидата на передачу BSR-сообщений.	



	Switch (config)# ipv6 pim bsr-candidate vlan1 30 10

10.7.15. Подсчет контрольной суммы пакета Register в IPv6 PIM (ipv6 pim cisco-register-checksum)

Синтаксис	ipv6 pim cisco-register-checksum [group-list <access-list name>] no ipv6 pim cisco-register-checksum [group-list <access-list name>] Устанавливает для контрольной суммы пакета регистрационного сообщения группы, указанной фильтром myfilter, использование всей длины пакета	
Параметр	<access-list name>	применяемый простой список доступа
По умолчанию	Вычисление контрольной суммы в соответствии с длиной заголовка регистрационного пакета, по умолчанию: 8	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда используется для взаимодействия с более ранними версиями Cisco IOS	
Пример	Установить контрольную сумму пакета регистрационного сообщения группы, указанной фильтром myfilter, на использование всей длины пакета. Switch(config)#ipv6 pim cisco-register-checksum group-list myfilter Switch(config)#ipv6 access-list standard myfilter Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::10/128	

10.7.16. Настройка приоритета для выбора назначенного маршрутизатора в IPv6 PIM (ipv6 pim dr-priority)

Синтаксис	ipv6 pim dr-priority <priority> no ipv6 pim dr-priority Данная команда используется для изменения значения приоритета назначенного маршрутизатора (DR). Соседние узлы в одном сегменте сети выбирают DR в своем сегменте в соответствии с пакетами "hello". Команда "no ipv6 pim dr-priority" восстанавливает значение по умолчанию	
Параметр	<priority>	приоритет, в диапазоне от 0 до 4294967294
По умолчанию	1	
Режим	Режим конфигурации интерфейса	



Руководство по использованию	Укажите значение приоритета в диапазоне от 0 до 4294967295, чем больше значение, тем выше приоритет. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Switch (config)# interface vlan 1 Switch(Config-if-Vlan1)ipv6 pim dr-priority 100

10.7.17. Исключение опции GenId в IPv6 PIM (ipv6 pim exclude-genid)

Синтаксис	ipv6 pim exclude-genid no ipv6 pim exclude-genid Эта команда исключает опцию GenId из пакетов Hello, отправляемых PIM SM. Команда "no ipv6 pim exclude-genid" восстанавливает значение по умолчанию
Параметр	
По умолчанию	Пакеты Hello включают опцию GenId
Режим	Режим конфигурации интерфейса
Руководство по использованию	Эта команда используется для взаимодействия с более ранними версиями Cisco IOS. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Задать, чтобы пакеты Hello, отправляемые коммутатором, не включали опцию GenId. Switch(Config-if-Vlan1)#ipv6 pim exclude-genid

10.7.18. Время сохранения информации о сообщениях Hello для IPv6 PIM (ipv6 pim hello-holdtime)

Синтаксис	ipv6 pim hello-holdtime <value> no ipv6 pim hello-holdtime Настраивает или отключает значение Holdtime (время сохранения информации) в пакетах Hello, которое описывает время сохранения информации о соседях, и отключает соседей, от которых в течение заданного времени holdtime на коммутатор не поступало пакетов Hello. Команда "no ipv6 pim hello-holdtime" отменяет установленное значение "holdtime" и восстанавливает значение по умолчанию	
Параметр	<vaule>	значение времени сохранения информации в диапазоне <1-65535>



По умолчанию	Значение Holdtime по умолчанию равно $3,5 \times \text{Hello\_interval}$, значение Hello_interval по умолчанию равно 30 секундам, поэтому значение Hold time по умолчанию равно 105 секундам
Режим	Режим конфигурации интерфейса
Руководство по использованию	Если это значение не задано, по умолчанию hellotime будет равен $3,5 \times \text{Hello\_interval}$. Если задаваемое время сохранения информации меньше, чем текущий интервал hello_interval, эта конфигурация будет отклонена. Каждый раз, когда hello_interval обновляется, hello_holdtime обновляется по следующим правилам: если hello_holdtime не задано, или если hello_holdtime задано, но меньше текущего hello_interval, hello_holdtime будет изменено на $3,5 \times \text{hello\_interval}$. В остальных случаях сохраняется заданное значение. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Настроить Hello Holdtime на vlan1 Switch (config)# interface vlan1 Switch (Config -if-Vlan1)#ipv6 pim hello-holdtime 10

10.7.19. Интервал отправки hello-пакетов для PIMv6 (ipv6 pim hello-interval)

Синтаксис	ipv6 pim hello-interval <interval> no ipv6 pim hello-interval Задать на интерфейсе интервал отправки hello-пакетов pim. Команда "no ipv6 pim hello-interval" восстанавливает значение по умолчанию	
Параметр	<interval>	интервал периодичности отправки pim hello-пакетов, в диапазоне от 1 до 18724 секунды
По умолчанию	Интервал передачи hello_interval пакетов pim составляет 30 секунд	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Сообщения Hello позволяют коммутаторам PIM определять взаимное расположение и устанавливать соседство. Коммутатор PIM объявляет о своем присутствии, регулярно отправляя соседям сообщения Hello. Соседи, от которых в течение определенного времени не поступало hello-сообщений, считаются отключившимися. Это значение не должно быть больше, чем время работы соседей. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен	



Пример	Настроить интервал hello для pim-sm VLAN Switch (config)#interface vlan 1 Switch (Config-If-Vlan1)#ipv6 pim hello-interval 20 Switch (Config-If-Vlan1)#

10.7.20. Игнорирование приоритета RP в RP-Set для IPv6 PIM (ipv6 pim ignore-rp-set-priority)

Синтаксис	ipv6 pim ignore-rp-set-priority no ipv6 pim ignore-rp-set-priority При выборе точки встречи (RP) эта команда настраивает коммутатор на включение регулирования хеширования и игнорирование приоритета RP. Эта команда используется для взаимодействия с более ранними версиями Cisco IOS
Параметр	
По умолчанию	Отключено
Режим	Режим глобальной конфигурации
Руководство по использованию	При выборе точки встречи (RP) PIM делает выбор на основании присвоенного приоритета RP. Когда задана эта команда, pim будет игнорировать приоритет RP. При отсутствии в сети более старого маршрутизатора применять данную команду не рекомендуется
Пример	Switch (config)#ipv6 pim ignore-rp-set-priority Switch (config)#

10.7.21. Интервал между сообщениями join/prune PIMv6 (ipv6 pim jp-timer)

Синтаксис	ipv6 pim jp-timer <value> no ipv6 pim jp-timer Задает добавление таймера JP. Команда "no ipv6 pim jp-timer" восстанавливает значение по умолчанию	
Параметр	<value>	в диапазоне от 10 до 65535 секунд
По умолчанию	60 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда задает интервал передачи сообщений J/P в 59 секунд	



Пример	Switch (config)#ip pim ip-timer 59 Switch (config)#

10.7.22. Многоадресная маршрутизация для IPv6 PIM (ipv6 pim multicast-routing)

Синтаксис	ipv6 pim multicast-routing no ipv6 pim multicast-routing Подключает протокол PIM-SM в глобальном режиме. Команда " no ipv6 pim multicast-routing " отключает протокол PIM-SM в глобальном режиме
Параметр	
По умолчанию	Протокол PIM-SM отключен
Режим	Режим глобальной конфигурации
Руководство по использованию	Подключает протокол PIM-SM в глобальном режиме. Чтобы PIM-SM функционировал, он должен быть включен на интерфейсе
Пример	Включить PIM-SM в глобальном режиме. Switch (config)#ipv6 pim multicast-routing

10.7.23. Настройка фильтрации соседей в IPv6 PIM (ipv6 pim neighbor-filter)

Синтаксис	ipv6 pim neighbor-filter <access-list-name> no ipv6 pim neighbor-filter <access-list-name> Задаёт список доступа, содержащий соседние устройства. Если соединение с соседом установлено, но условия фильтрации не выполнены, соединение немедленно обрывается. Если соединение не создано, это соединение не может быть установлено	
Параметр	<access-list-name>	имя применяемого списка доступа
По умолчанию	Фильтрация соседей не сконфигурирована	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	По умолчанию ACL имеет значение DENY (отклонить). При настройке "access-list 1" по умолчанию для списка задается значение "deny". В примере ниже, если параметр "permit any" не задан, deny fe80: 20e: cff: fe01: facc это то же самое, что deny any (отклонить все). Эту команду	



	можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Настроить список доступа, содержащий соседние устройства, pim VLAN. <pre>Switch(config)#interface vlan 1 Switch (Config-if-Vlan1)#ipv6 pim neighbor-filter myfilter Switch(config)#ipv6 access-list standard myfilter Switch(config_IPv6_Std-Nacl-myfilter)#deny fe80:20e:cff:fe01:facc Switch(config)#ipv6 access-list standard myfilter Switch(config_IPv6_Std-Nacl-myfilter)#permit any</pre>

10.7.24. Ограничение скорости отправки пакета Register для IPv6 PIM (ipv6 pim register-rate-limit)

Синтаксис	ipv6 pim register-rate-limit <limit> no ipv6 pim register-rate-limit Команда используется для настройки скорости отправки пакетов регистрации выделенного маршрутизатора (DR); единица измерения - пакетов/секунду. Команда "no ipv6 pim Register-rate-limit" восстанавливает значение по умолчанию. Эта команда действует только для пакета Register каждой записи (S, G) пакета, но не для всех пакетов Register во всей системе	
Параметр	<limit>	в диапазоне от 1 до 65535
По умолчанию	Скорость отправки не ограничена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта настройка ограничивает передачу пакетов REGISTER для предотвращения атак на DR	
Пример	Настроить скорость отправки пакетов регистрации DR на 59 пакетов/секунду. <pre>Switch (config)#ipv6 pim register-rate-limit 59</pre>	



10.7.25. Обнаружение доступности пакета Register для IPv6 PIM (ipv6 pim register-rp-reachability)

Синтаксис	ipv6 pim register-rp-reachability no ipv6 pim register-rp-reachability Эта команда позволяет DR проверять доступность RP в процессе регистрации
Параметр	
По умолчанию	Не проверяется
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда задает для DR выполнение проверки доступности RP
Пример	Настроить маршрутизатор на проверку доступности RP перед отправкой пакетов register. Switch(config)# ipv6 pim Register-rp-reachability

10.7.26. Настройка адреса источника пакета Register в PIMv6 (ipv6 pim register-source)

Синтаксис	ipv6 pim register-source {<source-address> <ifname> vlan <vlan-id>} no ipv6 pim register-source Эта команда используется для установки адреса источника пакетов регистрации register, передаваемых DR, вместо адреса источника по умолчанию. Адресом источника по умолчанию обычно является RPF-сосед направления хоста-источника	
Параметр	<ifname>	имя интерфейса, который будет являться источником пакетов регистрационных сообщений
	<vlan-id>	идентификатор VLAN
	<source-address>	адрес интерфейса, который будет являться источником регистрационного пакета. В шестнадцатеричном формате без префикса
По умолчанию	Не проверяется	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда "no ipv6 pim register-source" восстанавливает значение по умолчанию без дополнительных параметров. Настроенный адрес должен быть доступен для сообщений Register-Stop, отправляемых RP. Обычно это loopback-адрес, но могут быть и другие физические адреса. Адрес должен быть объявлен по протоколу одноадресного маршрутизатора DR
Пример	Настроить адрес источника отправляемых пакетов регистра на адрес vlan1 Switch (config)#ipv6 pim register-source vlan 1

10.7.27. Настройка времени подавления пакета Register IPv6 PIM (ipv6 pim register-suppression)

Синтаксис	ipv6 pim register-suppression <value> no ipv6 pim register-suppression Команда устанавливает значение времени подавления регистрационных (register) сообщений, единицей измерения является секунда. Команда "no ipv6 pim register-suppression" восстанавливает значение по умолчанию	
Параметр	<value>	значение таймера, в диапазоне от 10 до 65535 секунд
По умолчанию	60 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Если это значение задано на DR, то это значение таймера подавления регистрационных (register) сообщений. Если это значение задано на RP без команды "ipv6 pim rp-register-kat", данная команда меняет время поддержания активности "Keepalive-period". Команда "no ipv6 pim register-suppression" восстанавливает значение по умолчанию	
Пример	Установить таймер подавления Register на 30 секунд. Switch (config)#ipv6 pim register-suppression 30	

10.7.28. Настройка статических адресов RP для IPv6 PIM (ipv6 pim rp-address)

Синтаксис	ipv6 pim rp-address <rp-address> [<group-range>] no ipv6 pim rp-address <rp-address> [all <group-range>] Эта команда предназначена для настройки статической RP глобально или в диапазоне адресов многоадресной рассылки. Команда "no ipv6 pim rp-address" отменяет статические RP	
Параметр	<rp-address>	адрес RP в формате X: X: : X: X , ipv6 адрес



	<group-range>	планируемая RP в формате X: X: : X: X/M, ipv6 адрес и длина префикса всех диапазонов
	<all>	весь диапазон
По умолчанию	Этот коммутатор не является статическим маршрутизатором RP	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда предназначена для настройки статической RP глобально или в диапазоне адресов многоадресной рассылки	
Пример	Задать 2000:112::8 как адрес RP в режиме глобальной конфигурации. Switch (config)# ipv6 pim rp-address 2000:112::8 ff1e::/64	

10.7.29. Назначение роли RP Candidate маршрутизатору в IPv6 PIM (ipv6 pim rp-candidate)

Синтаксис	<pre>ipv6 pim rp-candidate{vlan<vlan-id> loopback<index> <ifname>}<group range> [<priority>]</pre> <pre>no ipv6 pim rp-candidate</pre> Данная команда используется для назначения роли Candidate RP в режиме глобальной конфигурации и указания в PIM-SM информации о кандидате для выполнения сравнений с другими кандидатами RP. Команда “no ipv6 pim rp-candidate” удаляет candidate RP	
Параметр	vlan-id	идентификатор vlan
	<index>	индексация интерфейса Loopback
	ifname	имя указанного интерфейса
	<group range>	диапазон групп candidate RP, в формате X: X: : X: X/M, ipv6 адрес и длина префикса;
	<priority>	это приоритет выбора RP, он варьируется от 0 до 255, по умолчанию значение 192, меньшее значение имеет больший приоритет
По умолчанию	Этот коммутатор не является статическим маршрутизатором RP	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Данная команда используется для назначения роли Candidate RP в режиме глобальной конфигурации и указания в PIM-SM информации	



	о кандидате для выполнения сравнений с другими кандидатами RP. Коммутатор может стать RP candidate только после ввода данной команды
Пример	Настроить vlan1 в качестве интерфейса отправки сообщений кандидата RP, объявляющего об отправке сообщений Switch (config)# ipv6 pim rp-candidate vlan1 100

10.7.30. Настройка времени keep-alive для регистрационных сообщений в PIMv6 (ipv6 pim rp-register-kat)

Синтаксис	ipv6 pim rp-register-kat <vaule> no ipv6 pim rp-register-kat Команда настраивает значение таймера KAT (KeepAlive Timer) для записей (S, G) точки встречи RP, в секундах. Команда “no ipv6 pim rp-register-kat” восстанавливает значение по умолчанию	
Параметр	<value>	значение таймера в диапазоне от 1 до 65535 секунд
По умолчанию	185 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Задать интервал rp-register-kat равный 30 секундам	
Пример	Switch(config)# ipv6 pim rp-register-kat 30	

10.7.31. Границы управления и ACL для IPv6 PIM (ipv6 pim scope-border)

Синтаксис	ipv6 pim scope-border [<500-599> <acl_name>] no ipv6 pim scope-border Устанавливает или удаляет границу управления протокола PIM	
Параметр	<500-599>	номер ACL для границы управления
	<acl_name>	имя ACL для границы управления
По умолчанию	Границы управления отсутствуют. Если ACL (список контроля доступа) не указан, будет использоваться граница управления по умолчанию	
Режим	Режим конфигурации интерфейса	



Руководство по использованию	Команда определяет границы управления и список контроля доступа для PIM IPv6. Поток многоадресных данных не будет перенаправляться на SCOPE-BORDER
Пример	Switch(Config-if-Vlan2)#ipv6 pim scope-border 503

10.7.32. Включение PIM-SM на интерфейсе (ipv6 pim sparse-mode)

Синтаксис	ipv6 pim sparse-mode [passive] no ipv6 pim sparse-mode [passive] Включает PIM-SM на интерфейсе; команда “no ipv6 pim sparse-mode [passive]” отключает PIM-SM	
Параметр	[passive]	означает отключить PIM-SM (то есть PIM-SM не получает никаких пакетов) и включить только MLD (получать и передавать MLD- пакеты)
По умолчанию	Режим PIM-SM отключен	
Режим	Режим конфигурации интерфейса	
Руководство по использованию	Команда используется для включения PIM-SM на интерфейсе. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен	
Пример	Включить PIM-SM на интерфейсе vlan1. Switch(config)#interface vlan 1 Switch(Config-If-Vlan1)#ipv6 pim sparse-mode	

10.7.33. Вывод информации о BSR для IPv6 PIM (show ipv6 pim bsr-router)

Синтаксис	show ipv6 pim bsr-router Отображает адрес BSR	
Параметр		
По умолчанию	Отсутствует	
Режим	Привилегированный режим и глобальной конфигурации	
Руководство по использованию	Отображение информации о BSR, поддерживаемой PIM	
Пример	Switch#show ipv6 pim bsr-router PIMv2 Bootstrap information	



	This system is the Bootstrap Router (BSR) BSR address: 2000: 1: 111: : 100 (?) Uptime: 00: 16: 00, BSR Priority: 0, Hash mask length: 126 Next bootstrap message in 00: 00: 10 Role: Candidate BSR State: Elected BSR Next Cand_RP_advertisement in 00: 00: 10 RP: 2000: 1: 111: : 100(Vlan2)	
	Информация, отображаемая на экране	Пояснения
	BSR address	Адрес Bsr-маршрутизатора
	Priority	Приоритет Bsr-маршрутизатора
	Hash mask length	Длина хеш-маски Bsr-маршрутизатора
	State	Текущий статус этого кандидата BSR, Elected BSR это выбранный BSR

10.7.34. Вывод информации PIM для IPv6 PIM (show ipv6 pim interface)

Синтаксис	show ipv6 pim interface Отображение конфигурации для PIM на интерфейсе
Параметр	
По умолчанию	Отсутствует
Режим	В любом режиме
Руководство по использованию	Данная команда используется для отображения конфигурации для PIM на интерфейсе
Пример	Switch#show ipv6 pim interface Interface VIFindex Ver/ Nbr DR Mode Count Prior Vlan2 0 v2/S 0 1 Адрес: fe80: : 203: fff: fee3: 1244 Global Address: 2000: 1: 111: : 100 DR : this system Vlan3 2 v2/S 0 1



Address : fe80: : 203: fff: fee3: 1244 Global Address: 2000: 10: 1: 13: : 1 DR : this system	
Информация, отображаемая на экране	Пояснения
Address	адрес интерфейса
Interface	имя интерфейса
VIF index	индекс интерфейса
Ver/Mode	версия и режим Pim, обычно v2, для разреженного режима отображается S, для уплотненного режима отображается D
Nbr Count	число соседей интерфейса
DR Prior	приоритет назначенного маршрутизатора (DR)
DR	адрес DR интерфейса

10.7.35. Вывод таблицы маршрутизации IPv6 PIM-SM multicast (show ipv6 pim mroute sparse-mode)

Синтаксис	show ipv6 pim mroute sparse-mode Вывод на экран таблицы маршрутизации IPv6 PIM-SM multicast
Параметр	
По умолчанию	Отсутствует
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Данная команда используется для отображения маршрутизаторов BSP в сети, обслуживаемой PIM-SM
Пример	Switch#show ipv6 pim mroute sparse-mode IPv6 Multicast Routing Table (* ,*,RP) Entries: 0 (* ,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 (*, ff1e: : 15) RP: 2000: 1: 111: : 100 RPF nbr: : :



RPF idx: Отсутствуют
 Upstream State: JOINED Local ..l.....
 Joined
 Asserted
 FCR:
 (2000: 1: 111: : 11, ff1e: : 15)
 RPF nbr: : :
 RPF idx: None SPT bit: 1
 Upstream State: JOINED Local
 Joined
 Asserted
 Outgoing ..o.....
 (2000: 1: 111: : 11, ff1e: : 15, rpt) 15, rpt)
 RP: 2000: 1: 111: : 100
 RPF nbr: : :
 RPF idx: None
 Upstream State: NOT PRUNED Pruned
 Outgoing ..o.....

Информация, отображаемая на экране	Пояснения
Entries	количество каждой записи
RP	RP-адрес общего дерева
RPF nbr	Направление RP или направление верхнего соседа в направлении источника.
RPF idx	интерфейс RPF nbr
Upstream State	статус Upstream. Существует два состояния Joined (присоединен к дереву, ожидается получение данных от вышестоящего маршрутизатора) и Not Joined (вышел из дерева, не ожидается получение данных от вышестоящего маршрутизатора), а также дополнительные опции, например, RPT Not Joined, Pruned, Not Pruned доступны для (S,G,rpt.)



	Local	Локальный интерфейс присоединения, этот интерфейс получает IGMPJoin
	Joined	Интерфейс присоединения к PIM, этот интерфейс получает сообщения J/P
	Asserted	Состояние подтверждено
	Outgoing	Финальное устройство выхода многоадресных данных

10.7.36. Вывод информации о соседних устройствах IPv6 PIM (show ipv6 pim neighbor)

Синтаксис	show ipv6 pim neighbor [detail] Выводит информацию о соседних устройствах маршрутизатора	
Параметр		
По умолчанию	Отсутствует	
Режим	В любом режиме	
Руководство по использованию	Данная команда используется для отображения информации о том, какие многоадресные маршрутизаторы настроены для PIM	
Пример	Switch(config)#show ipv6 pim neighbor Neighbor Interface Uptime/Expires Ver DR Address Priority/Mode Fe80: : 203: fff: fee3: 1244 Vlan1 00: 00: 10/00: 01: 35 v2 1 /DR fe80: : 20e: cff: fe01: facc Vlan1 00: 00: 13/00: 01: 32 v2 1 /	
	Информация, отображаемая на экране	Пояснения
	Neighbor Address	адрес соседнего устройства
	Interface	интерфейс соседнего устройства
	Uptime/Expires	Время работы/истечения срока
	Ver	Версия Pim, обычно v2
	DR Priority/Mode	Приоритет DR в сообщениях hello от соседа и является ли сосед DP интерфейса.



10.7.37. Вывод информации о следующих хопах IPv6 PIM (show ipv6 pim nexthop)

Синтаксис	show ipv6 pim nexthop Отображение буферизованного маршрутизатора следующего узла PIM в таблице маршрутов одноадресной рассылки	
Параметр		
По умолчанию	Отсутствует	
Режим	В любом режиме	
Руководство по использованию	Команда выводит информацию о буферизованном маршрутизаторе PIM nexthop	
Пример	Switch#show ipv6 pim nexthop Flags: N = New, R = RP, S = Source, U = Unreachable Destination Type Nexthop Nexthop ..Nexthop Nexthop Metric Pref Refcnt Num Addr Ifindex Name 2000: 1: 111: : 11 ..S. 1 2004 0 0 2 2000: 1: 111: : 100 .RS. 1 2004 0 0 2	
	Информация, отображаемая на экране	Пояснения
	Место назначения	Назначение следующей записи
	Тип	N: создан следующий узел (nexthop), направление RP и направление S не определены. R: направление точки встречи RP S: направление источника U: нет доступа
	Nexthop Num	номер следующего узла
	Nexthop Addr	адрес следующего узла
	Nexthop Ifindex	индекс интерфейса следующего узла
	Nexthop Name	имя следующего узла
	Metric	метрика следующего узла
	Pref	предпочтительный выбор маршрутизатора
	Refcnt	Счетчик ссылок



10.7.38. Вывод адреса RP для указанной группы PIMv6 (show ipv6 pim rp-hash)

Синтаксис	show ip pim rp-hash X: X: : X: X Отображение адреса RP для точки слияния группы X: X: : X: X	
Параметр	X: X: : X: X	адрес группы
По умолчанию	Отсутствует	
Режим	В любом режиме	
Руководство по использованию	Данная команда применяется для отображения адреса RP, соответствующего указанному адресу группы	
Пример	Switch#show ipv6 pim rp-hash ff1e: : 15 RP: 2000: 1: 111: : 100 Info source: 2000: 1: 111: : 100, via bootstrap	
	Информация, отображаемая на экране	Пояснения
	RP	RP запрашиваемой группы
	Info source	Источник информации Bootstrap

10.7.39. Вывод точек встреч и привязок групп к RP IPv6 PIM (show ipv6 pim rp mapping)

Синтаксис	show ipv6 pim rp mapping Отображение привязок (mapping) групп к точкам встреч (RP) и точек встреч (RP)
Параметр	
По умолчанию	Отсутствует
Режим	В любом режиме
Руководство по использованию	Команда позволяет вывести на экран активные точки встречи и информацию о привязках
Пример	Switch#show ipv6 pim rp mapping PIM Group-to-RP Mappings This system is the Bootstrap Router (v2) Group(s): ff00: : /8 RP: 2000: 1: 111: : 100



Info source: 2000: 1: 111: : 100, via bootstrap, priority 192 Uptime: 00: 10: 24, expires: 00: 02: 06 Group(s): ff00: : /8, Static RP: 2000: 1: 111: : 100 Uptime: 00: 11: 01	
Информация, отображаемая на экране	Пояснения
Group(s)	Диапазон адресов групп для RP
Info source	источник сообщений Bootstrap
Priority	приоритет сообщений Bootstrap

10.8. Настройка протокола PIM-SSM6

10.8.1. Настройка диапазона адресов многоадресной SSM-группы (ipv6 pim ssm)

Синтаксис	ipv6 pim ssm {default range <access-list-number >} no ipv6 pim ssm Настраивает диапазон адресов многоадресной рассылки pim ssm. Команда "no ipv6 pim ssm" отменяет сконфигурированную группу многоадресной рассылки pim ssm	
Параметр	default	диапазон адресов SSM-группы по умолчанию, равный ff3х: : /32
	<access-list-number >	применяемый список доступа
По умолчанию	Диапазон адресов многоадресной рассылки pim ssm не задан	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Pim ssm можно использовать, только если задана эта команда. Прежде чем задать эту команду, убедитесь, что ipv6 pim multicast успешно работает. Access-list может использовать только списки, созданные с помощью ipv6 access-list. Пользователи могут сначала выполнить данную команду, а потом настроить соответствующий список ACL, или удалить соответствующий ACL в привязке. Удалить привязку после ее выполнения можно только по команде "no ipv6 pim ssm". Если требуется ssm, эта команда должна быть настроена в соответствующем пограничном маршруте. Например, на локальном	



	коммутаторе с igmp (обязательно) и источником многоадресной рассылки DR или RP (хотя бы один из двух) задается эта команда, на среднем коммутаторе нужно только включить PIM-SM
Пример	Настроить на коммутаторе включение PIM-SSM, диапазон группы задается списком доступа access-list 23. Switch (config)#ipv6 pim ssm range 23 Switch(config)#ipv6 access-list standard myfilter Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e: : /48

10.9. Anycast RP V4

10.9.1. Отладка адресации Anycast RP в PIM (debug pim anycast-rp)

Синтаксис	debug pim anycast-rp no debug pim anycast-rp Включение отладки функции ANYCAST RP; "no" в начале команды отключает функцию отладки
Параметр	
По умолчанию	По умолчанию переключатель отладки ANYCAST RP отключен
Режим	Привилегированный режим
Руководство по использованию	Эта команда используется для включения переключателя отладки ANYCAST RP маршрутизатора, по команде выводится информация об обработке пакета регистрационных сообщений PIM коммутатора — packet, и информации о событиях — event
Пример	Switch#debug pim anycast-rp

10.9.2. Подключение адресации Anycast RP в PIM (ip pim anycast-rp)

Синтаксис	ip pim anycast-rp no ip pim anycast-rp Включить ANYCAST RP на коммутаторе; "no" в начале команды отключает функцию ANYCAST RP
Параметр	
По умолчанию	По умолчанию на коммутаторе не включена ANYCAST RP
Режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда включит протокол ANYCAST RP в глобальном режиме конфигурации, но для того, чтобы ANYCAST RP работал, необходимо настроить "self-rp-address" и "other-rp-address"



Пример	Включить ANYCAST RP в глобальном режиме конфигурации. Switch(config)#ip pim anycast-rp

10.9.3. Настройка адресов точек встречи Anycast RP в PIM (ip pim anycast-rp)

Синтаксис	ip pim anycast-rp <anycast-rp-addr> <other-rp-addr> no ip pim anycast-rp <anycast-rp-addr> <other-rp-addr> Задаёт ANYCAST RP-адрес (ARA) и одноадресные маршруты (в качестве RP) других RP, взаимодействующих с этим маршрутизатором. "no" в начале команды отменяет одноадресные маршруты остальных RP в соответствии с настроенным адресом RP
Параметр	anycast-rp-addr : адрес точки встречи RP, допускается отсутствие интерфейса-кандидата в соответствии с адресом. other-rp-addr : Одноадресный адрес другой RP, взаимодействующей с этим маршрутизатором (в качестве RP)
По умолчанию	Конфигурация отсутствует
Режим	Режим глобальной конфигурации
Руководство по использованию	Адресация "anycast-rp-addr" (в качестве RP), настроенная на этом маршрутизаторе, на самом деле является адресом RP, заданным на нескольких RP в сети в соответствии с адресом интерфейса-кандидата RP (или интерфейса Loopback). При конфигурировании допускается текущее отсутствие интерфейса-кандидата, соответствующего адресу. Установить адрес "other-rp-address" других RP, которые взаимодействуют с этим маршрутизатором (в качестве RP). Одноадресный маршрут идентифицирует другую RP и использует для связи с локальным маршрутизатором. Как только этот маршрутизатор (в качестве RP) получает register-сообщение от одноадресного DR, он должен переслать его другим RP в сети, чтобы уведомить все RP в сети о состоянии источника (S.G). При пересылке маршрутизатор изменит адрес назначения в register-сообщения на "other-rp-address". Можно настроить несколько "other-rp-addresses" на основе одного "anycast-rp-addr". После получения регистрационного сообщения от DR оно должно быть направлено на все эти прочие RP по очереди
Пример	Задать "other-rp-address" в режиме глобальной конфигурации. Switch(config)#ip pim anycast-rp 1.1.1.1 192.168.3.2



10.9.4. Личный адрес маршрутизатора для Anycast адресации в PIM (ip pim anycast-rp self-rp-address)

Синтаксис	ip pim anycast-rp self-rp-address <self-rp-addr> no ip pim anycast-rp self-rp-address Задаёт уникальный адрес "self-rp-address" этого маршрутизатора (в качестве RP). Этот адрес будет использоваться исключительно для идентификации этого маршрутизатора среди других RP, а также для связи с другими RP. "no" в начале команды отменяет заданный индивидуальный адрес, используемый данным маршрутизатором (в качестве RP) для коммуникации с другими RP	
Параметр	self-rp-addr	индивидуальный адрес, используемый данным маршрутизатором (в качестве RP) для коммуникации с другими RP
По умолчанию	Адрес self-rp-address не задан	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Как только этот маршрутизатор (в качестве RP) получит регистрационное сообщение от одноадресного DR, ему необходимо переслать регистрационное сообщение всем остальным RP в сети, чтобы проинформировать их о статусе источника (S,G). При пересылке регистрационного сообщения этот маршрутизатор изменит адрес источника на "self-rp-address". Как только этот маршрутизатор (в качестве RP) получает регистрационное сообщение от другого одноадресного DR, например, регистрационное (register) сообщение, адресом назначения которого является self-rp-address этого маршрутизатора, он устанавливает состояние (S,G) и отправляет обратно сообщение register-stop, адресом назначения которого является адрес источника register-сообщения. "self-rp-address" должен быть адресом интерфейса уровня 3 на этом маршрутизаторе, но допускается конфигурирование без интерфейса	
Пример	Задать "self-rp-address" этого маршрутизатора в режиме глобальной конфигурации. <pre>Switch(config)#ip pim anycast-rp self-rp-address 1.1.1.1</pre>	



10.9.5. Назначение роли RP Candidate в PIM (ip pim rp-candidate)

Синтаксис	<pre>ip pim rp-candidate {vlan<vlan-id> loopback<index> <ifname>} [<A.B.C.D>] [<priority>] no ip pim rp-candidate</pre> Добавляет интерфейс Loopback в качестве интерфейса-кандидата RP на основе исходной команды PIM-SM; "no" в начале команды отменяет использование интерфейса Loopback в качестве интерфейса-кандидата RP
Параметр	index : индекс интерфейса Loopback, в диапазоне <1-1024>. vlan-id: идентификатор VLAN. ifname: заданное имя интерфейса. A.B.C.D/M: префикс и маска ip. <priority>: приоритет выбора RP, в диапазоне от 0 до 255, значение по умолчанию - 192, чем меньше значение, тем выше приоритет
По умолчанию	По умолчанию интерфейс RP не настроен
Режим	Режим глобальной конфигурации
Руководство по использованию	Для поддержки функции ANYCAST RP новое правило позволяет настроить интерфейс Loopback в качестве интерфейса-кандидата RP. Интерфейс-кандидат RP должен быть уникальным на данный момент, и его адрес должен быть добавлен в маршрутизатор, чтобы гарантировать, что PIM-маршрутизатор сможет найти ближайший RP. Команда "no ip pim rp-candidate" отменяет выбор кандидата RP
Пример	Настроить интерфейс Loopback1 в качестве интерфейса-кандидата RP в режиме глобальной конфигурации. <pre>Switch(config)#ip pim rp-candidate loopback1</pre>

10.9.6. Вывод отладочных сообщений PIM (show debugging pim)

Синтаксис	show debugging pim
Параметр	
По умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	Текущее состояние переключателя отладки ANYCAST RP



Пример	Switch(config)#show debugging pim Debugging status: PIM anycast-rp debugging is on

10.9.7. Вывод первого хопа Anycast RP в PIM (show ip pim anycast-rp first-hop)

Синтаксис	show ip pim anycast-rp first-hop	
Параметр	-	
По умолчанию	-	
Режим	Привилегированный режим и режим конфигурации	
Руководство по использованию	Команда применяется для вывода информации о состоянии ANYCAST RP и показывает информацию об узле mrt, сгенерированную в RP первого хопа, поддерживаемого протоколом	
Пример	Switch(config)#show ip pim anycast-rp first-hop IP Multicast Routing Table (* ,G) Entries: 0 (S,G) Entries: 1 (E,G) Entries: 0 INCLUDE (192.168.1.136, 224.1.1.1) Local .l.....	
	Информация, отображаемая на экране	Пояснение
	Entries	Количество всех типов записей
	INCLUDE	Информация о mrt, сгенерированная в первом хопе RP.

10.9.8. Вывод не первого хопа Anycast RP в PIM (show ip pim anycast-rp non-first-hop)

Синтаксис	show ip pim anycast-rp non-first-hop	
Параметр	-	
По умолчанию	-	
Режим	Привилегированный режим и режим конфигурации	



Руководство по использованию	Команда позволяет просмотреть информацию о состоянии ANYCAST RP, а также выводит информацию об узле mrt, созданном в RP не первого хопа, который в настоящее время поддерживается протоколом, то есть информации об узле mrt, которая создается после того, как RP первого хопа передает полученное им register-сообщение в этот RP
Пример	<pre>Switch(config)#show ip pim anycast-rp non-first-hop IP Multicast Routing Table</pre> (*,G) Entries: 0 (S,G) Entries: 1 (E,G) Entries: 0 INCLUDE (192.168.10.120, 225.1.1.1) Local .l..... Информация, отображаемая на экране Пояснение Entries Количество всех типов записей. INCLUDE Информация о mrt, сгенерированная в первом хопе RP

10.9.9. Вывод статуса Anycast RP (show ip pim anycast-rp status)

Синтаксис	show ip pim anycast-rp status	
Параметр	-	
По умолчанию	-	
Режим	Привилегированный режим и режим конфигурации	
Руководство по использованию	Команда выводит информацию о конфигурации ANYCAST RP: включен ли ANYCAST RP глобально, настроен ли "self-rp-address" и список текущих настроенных ANYCAST RP	
Пример	Switch(config)#show ip pim anycast-rp status Anycast RP status: anycast-rp: Enabled! self-rp-address: 192.168.3.2 anycast-rp address: 1.1.1.1 other rp unicast rp address: 192.168.2.1 other rp unicast rp address: 192.168.5.1 anycast-rp address: 192.168.1.4 other rp unicast rp address: 192.168.2.1	
	Информация, отображаемая на экране	Пояснение



	anycast-rp:	Подключен или нет коммутатор с ANYCAST RP в глобальном режиме
	self-rp-address:	заданный "self-rp-address"
	anycast-rp address:	заданный "anycast-rp-address"
	other rp unicast rp address:	Другие адреса связи RP, заданные в соответствии с вышеуказанным anycast-rp-address
	other rp unicast rp address:	Другие адреса связи RP, заданные в соответствии с вышеуказанным anycast-rp-address
	anycast-rp address:	заданный anycast-rp-address*
	other rp unicast rp address:	Другие адреса связи RP, заданные в соответствии с вышеуказанным anycast-rp-address

10.10. Anycast RP V6

10.10.1. Отладка адресации Anycast RP в IPv6 PIM (debug ipv6 pim anycast-rp)

Синтаксис	debug ipv6 pim anycast-rp no debug ipv6 pim anycast-rp Включение отладки функции ANYCAST RP; "no" в начале команды отключает функцию отладки
Параметр	
По умолчанию	По умолчанию переключатель отладки ANYCAST RP отключен
Режим	Привилегированный режим
Руководство по использованию	Эта команда используется для включения переключателя отладки ANYCAST RP маршрутизатора, по команде выводится информация об обработке пакета регистрационных сообщений PIM коммутатора — packet и информации о событиях — event
Пример	Switch# debug ipv6 pim anycast-rp



10.10.2. Подключение адресации Anycast RP в IPv6 PIM (ipv6 pim anycast-rp)

Синтаксис	ipv6 pim anycast-rp no ipv6 pim anycast-rp Включает ANYCAST RP на коммутаторе; "no" в начале команды отключает функцию ANYCAST RP
Параметр	
По умолчанию	По умолчанию на коммутаторе не включена ANYCAST RP
Режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда включит протокол ANYCAST RP в глобальном режиме конфигурации, но для того, чтобы ANYCAST RP работал, необходимо настроить "self-rp-address" и "other-rp-address"
Пример	Включить ANYCAST RP в глобальном режиме конфигурации. Switch(config)#ipv6 pim anycast-rp

10.10.3. Настройка адресов точек встречи Anycast RP в IPv6 PIM (ipv6 pim anycast-rp)

Синтаксис	ipv6 pim anycast-rp <anycast-rp-addr> <other-rp-addr> no ipv6 pim anycast-rp <anycast-rp-addr> <other-rp-addr> Устанавливает ANYCAST RP-адрес (ARA) и одноадресные маршруты других RP, взаимодействующих с этим маршрутизатором (в качестве RP). "no" в начале команды отменяет одноадресные маршруты остальных RP в соответствии с настроенным адресом RP
Параметр	anycast-rp-addr : адрес точки встречи RP, допускается отсутствие интерфейса-кандидата в соответствии с адресом. other-rp-addr : одноадресный адрес другой RP, взаимодействующей с этим маршрутизатором (в качестве RP)
По умолчанию	Конфигурация отсутствует
Режим	Режим глобальной конфигурации
Руководство по использованию	Адресация "anycast-rp-addr" (в качестве RP), настроенная на этом маршрутизаторе, на самом деле является адресом RP, заданным на нескольких RP в сети в соответствии с адресом интерфейса-кандидата RP (или интерфейса Loopback). При конфигурировании допускается текущее отсутствие интерфейса-кандидата, соответствующего адресу. Установить адрес "other-rp-address" других RP, которые взаимодействуют с этим маршрутизатором (в качестве RP).



	Одноадресный маршрут идентифицирует другую RP и использует для связи с локальным маршрутизатором. Как только этот маршрутизатор (в качестве RP) получает register-сообщение от одноадресного DR, он должен переслать его другим RP в сети, чтобы уведомить все RP в сети о состоянии источника (S.G). При пересылке маршрутизатор изменит адрес назначения в register-сообщения на "other-rp-address". Можно настроить несколько "other-rp-addresses" на основе одного "anycast-rp-addr". После получения регистрационного сообщения от DR оно должно быть направлено на все эти прочие RP по очереди
Пример	Задать "other-rp-address" в режиме глобальной конфигурации. <pre>Switch(config)#ipv6 pim anycast-rp 2000: : 1 2004: : 2</pre>

10.10.4. Личный адрес маршрутизатора для Anycast адресации в IPv6 PIM (ipv6 pim anycast-rp self-rp-address)

Синтаксис	IPv6 PIM Задаёт уникальный адрес "self-rp-address" этого маршрутизатора (в качестве RP). Этот адрес будет использоваться исключительно для идентификации этого маршрутизатора среди других RP, а также для связи с другими RP. "no" в начале команды отменяет заданный индивидуальный адрес, используемый данным роутером (в качестве RP) для коммуникации с другими RP	
Параметр	self-rp-addr	индивидуальный адрес, используемый данным маршрутизатором (в качестве RP) для коммуникации с другими RP
По умолчанию	Адрес "self-rp-address" не задан	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Как только этот маршрутизатор (в качестве RP) получит регистрационное сообщение от одноадресного DR, ему необходимо переслать регистрационное сообщение всем остальным RP в сети, чтобы проинформировать их о статусе источника (S.G). При пересылке регистрационного сообщения этот маршрутизатор изменит адрес источника на "self-rp-address". Как только этот маршрутизатор (в качестве RP) получает регистрационное сообщение от другого одноадресного DR, например, регистрационное (register) сообщение, адресом назначения которого является self-rp-address этого маршрутизатора, он устанавливает состояние (S,G) и отправляет обратно сообщение register-stop, адресом назначения которого является адрес источника register-сообщения.	



	"self-rp-address" должен быть адресом интерфейса уровня 3 на этом маршрутизаторе, но допускается конфигурирование без интерфейса
Пример	Задать "self-rp-address" этого маршрутизатора в режиме глобальной конфигурации <pre>Switch(config)#ipv6 pim anycast-rp self-rp-address 2000: : 1</pre>

10.10.5. Назначение роли RP Candidate в IPv6 PIM (ipv6 pim rp-candidate)

Синтаксис	<pre>ipv6 pim rp-candidate {vlan<vlan-id> loopback<index> [<ifname>]} [<A: B: : C: D>] [<priority>]</pre> <pre>no ip pim rp-candidate</pre> Добавляет интерфейс Loopback в качестве интерфейса-кандидата RP на основе исходной команды PIM6-SM; "no" в начале команды отменяет использование интерфейса Loopback в качестве интерфейса-кандидата RP
Параметр	index : индекс интерфейса Loopback, в диапазоне <1-1024>. vlan-id: идентификатор VLAN. ifname: заданное имя интерфейса. A: B: : C: D/M: префикс и маска ip. <priority>: приоритет выбора RP, в диапазоне от 0 до 255, значение по умолчанию - 192, чем меньше значение, тем выше приоритет
По умолчанию	По умолчанию интерфейс RP не настроен
Режим	Режим глобальной конфигурации
Руководство по использованию	Для поддержки функции ANYCAST RP новое правило позволяет настроить интерфейс Loopback в качестве интерфейса-кандидата RP. интерфейс-кандидат RP должен быть уникальным на данный момент, и его адрес должен быть добавлен в маршрутизатор, чтобы гарантировать, что PIM-маршрутизатор сможет найти ближайший RP. Команда "no ipv6 pim rp-candidate" отменяет кандидата RP
Пример	Настроить интерфейс Loopback1 в качестве интерфейса-кандидата RP в режиме глобальной конфигурации. <pre>Switch(config)#ipv6 pim rp-candidate loopback1</pre>



10.10.6. Вывод отладочных сообщений IPv6 PIM (show debugging ipv6 pim)

Синтаксис	show debugging ipv6 pim
Параметр	
По умолчанию	-
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Текущее состояние отладочного переключателя ANYCAST RP
Пример	Switch(config)#show debugging ipv6 pim Debugging status: PIM anycast-rp debugging is on

10.10.7. Вывод первого хопа Anycast RP в IPv6 PIM (show ipv6 pim anycast-rp first-hop)

Синтаксис	show ipv6 pim anycast-rp first-hop		
Параметр	-		
По умолчанию	-		
Режим	Привилегированный режим и режим конфигурации		
Руководство по использованию	Команда применяется для вывода информации о состоянии ANYCAST RP и показывает информацию об узле mrt, сгенерированную в RP первого хопа, поддерживаемого протоколом		
Пример	Switch(config)#show ipv6 pim anycast-rp first-hop IP Multicast Routing Table (*G) Entries: 0 (S,G) Entries: 1 (E,G) Entries: 0 INCLUDE (2000: 1: 111: : 2, ff1e: : 1) Local .l.....		
	Информация, отображаемая на экране	Пояснение	
	Entries	Количество записей.	всех типов



	INCLUDE	Информация о mrt, сгенерированная в первом хопе RP.

10.10.8. Вывод не первого хопа Anycast RP в IPv6 PIM (show ipv6 pim anycast-rp non-first-hop)

Синтаксис	show ipv6 pim anycast-rp non-first-hop						
Параметр	-						
По умолчанию	-						
Режим	Привилегированный режим и режим конфигурации						
Руководство по использованию	Команда позволяет просмотреть информацию о состоянии ANYCAST RP, а также выводит информацию об узле mrt, созданном в RP не первого хопа, который в настоящее время поддерживается протоколом, то есть информации об узле mrt, которая создается после того, как RP первого хопа передает полученное им register-сообщение в этот RP						
Пример	Switch(config)#show ip pim anycast-rp non-first-hop IP Multicast Routing Table (*G) Entries: 0 (S,G) Entries: 1 (E,G) Entries: 0 INCLUDE (2002: 1: 111: : 2, ff1e: : 2) Local .l..... <table> <tr> <th>Информация, отображаемая на экране</th><th>Пояснение</th></tr> <tr> <td>Entries</td><td>Количество всех типов записей</td></tr> <tr> <td>INCLUDE</td><td>Информация о mrt, сгенерированная в первом хопе RP</td></tr> </table>	Информация, отображаемая на экране	Пояснение	Entries	Количество всех типов записей	INCLUDE	Информация о mrt, сгенерированная в первом хопе RP
Информация, отображаемая на экране	Пояснение						
Entries	Количество всех типов записей						
INCLUDE	Информация о mrt, сгенерированная в первом хопе RP						

10.10.9. Вывод статуса Anycast RP в IPv6 PIM (show ipv6 pim anycast-rp status)

Синтаксис	show ipv6 pim anycast-rp status
Параметр	-
По умолчанию	-



Режим	Привилегированный режим и режим конфигурации																
Руководство по использованию	Команда выводит информацию о конфигурации ANYCAST RP: включен ли ANYCAST RP глобально, настроен ли "self-rp-address" и список текущих настроенных ANYCAST RP																
Пример	Switch(config)#show ipv6 pim anycast-rp status Anycast RP status: anycast-rp: Enabled! self-rp-address: 2004: : 2 anycast-rp address: 2000: 1: 111: : 2 other rp unicast rp address: 2002: : 1 other rp unicast rp address: 2005: : 1 anycast-rp address: 2003: : 1 other rp unicast rp address: 2002: : 2 <table> <tr> <th>Информация, отображаемая на экране</th><th>Пояснение</th></tr> <tr> <td>anycast-rp:</td><td>Подключен или нет коммутатор с ANYCAST RP в глобальном режиме</td></tr> <tr> <td>self-rp-address:</td><td>заданный "self-rp-address"</td></tr> <tr> <td>anycast-rp address:</td><td>заданный "anycast-rp-address"</td></tr> <tr> <td>other rp unicast rp address:</td><td>Другие адреса связи RP, заданные в соответствии с вышеуказанным anycast-rp-address</td></tr> <tr> <td>other rp unicast rp address:</td><td>Другие адреса связи RP, заданные в соответствии с вышеуказанным anycast-rp-address</td></tr> <tr> <td>anycast-rp address:</td><td>заданный anycast-rp-address*</td></tr> <tr> <td>other rp unicast rp address:</td><td>Другие адреса связи RP, заданные в соответствии с вышеуказанным anycast-rp-address</td></tr> </table>	Информация, отображаемая на экране	Пояснение	anycast-rp:	Подключен или нет коммутатор с ANYCAST RP в глобальном режиме	self-rp-address:	заданный "self-rp-address"	anycast-rp address:	заданный "anycast-rp-address"	other rp unicast rp address:	Другие адреса связи RP, заданные в соответствии с вышеуказанным anycast-rp-address	other rp unicast rp address:	Другие адреса связи RP, заданные в соответствии с вышеуказанным anycast-rp-address	anycast-rp address:	заданный anycast-rp-address*	other rp unicast rp address:	Другие адреса связи RP, заданные в соответствии с вышеуказанным anycast-rp-address
Информация, отображаемая на экране	Пояснение																
anycast-rp:	Подключен или нет коммутатор с ANYCAST RP в глобальном режиме																
self-rp-address:	заданный "self-rp-address"																
anycast-rp address:	заданный "anycast-rp-address"																
other rp unicast rp address:	Другие адреса связи RP, заданные в соответствии с вышеуказанным anycast-rp-address																
other rp unicast rp address:	Другие адреса связи RP, заданные в соответствии с вышеуказанным anycast-rp-address																
anycast-rp address:	заданный anycast-rp-address*																
other rp unicast rp address:	Другие адреса связи RP, заданные в соответствии с вышеуказанным anycast-rp-address																



11. КОМАНДЫ ДЛЯ НАСТРОЙКИ ФУНКЦИИ БЕЗОПАСНОСТИ

11.1. Команды для настройки списков доступа (ACL)

11.1.1. Настройка временного диапазона (absolute-periodic/periodic)

Команда	[no] absolute-periodic {Monday Tuesday Wednesday Thursday Friday Saturday Sunday}<start_time>to{Monday Tuesday Wednesday Thursday Friday Sa turday Sunday}<end_time> [no]periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+ Sunday} daily weekdays weekend} <start_time> to <end_time>	
Параметр	Monday	Понедельник
	Tuesday	Вторник
	Wednesday	Среда
	Thursday	Четверг
	Friday	Пятница
	Saturday	Суббота
	Sunday	Воскресенье
	daily	Ежедневно
	weekdays	С понедельника по пятницу
	weekend	В субботу и воскресенье
	<start_time>	время начала, ЧЧ: ММ: СС (часы: минуты: секунды)
	<end_time>	время окончания, ЧЧ: ММ: СС (часы: минуты: секунды)
По умолчанию	Временной диапазон не задан	



Режим	режим настройки временного диапазона
Руководство по использованию	Позволяет задать на коммутаторе временной диапазон действия различных команд. Создав временной период и сославшись на него в команде, пользователь может задать определенный период выполнения команды. Если, например, правило ACL должно действовать только в определенный период времени, его можно сначала настроить, а затем сослаться на него при настройке правила ACL, чтобы оно выполнялось только в рамках определенного для этого временного периода. Временной диапазон может быть определен двумя способами: Абсолютный период, который действует в течение определенного временного диапазона, например, со вторника 8: 00 до субботы 8: 00. Циклический период: цикл времени, который действует в течение определенного периода (например, с 14:00 до 16: 00 за неделю). "no" в начале команды удаляет настройки временного диапазона
Пример	Обеспечить действие настроек в период с 9: 15: 30 до 12: 30: 00 со вторника по субботу. <pre>Switch(config)#time-range admin_timer</pre> <pre>Switch(config-time-range-admin_timer)#absolute-periodic Tuesday 9:15:30 to Saturday 12: 30: 00</pre> Обеспечить действие настроек в период с 14:30:00 до 16:45:00 в понедельник, среду, пятницу и воскресенье. <pre>Switch(config-time-range-admin_timer)#periodic Monday Wednesday Friday Sunday 14:30:00 to 16:45:00</pre>

11.1.2. Абсолютный временной диапазон (absolute start)

Команда	[no] absolute start <start_time> <start_data> [end <end_time> <end_data>]	
Параметр	<start_time>	Время начала, ЧЧ: ММ: СС (часы: минуты: секунды)
	<start_data>	Дата начала, формат: ГГГГ.ММ.ДД (год.месяц.день)
	<end_time>	Время окончания, ЧЧ: ММ: СС (часы: минуты: секунды)
	<end_data>	Дата окончания, формат: ГГГГ.ММ.ДД (год.месяц.день)



По умолчанию	Временной диапазон не задан
Режим	Режим настройки временного диапазона
Руководство по использованию	Позволяет задать абсолютный временной диапазон по часам, встроенным в оборудование. Если команда вводится несколько раз, абсолютное время и дата, соответствующие определенному году, месяцу, дню, часу и минуте начала временного диапазона не должны совпадать с ранее введенными датами и временем, в противном случае выполнены настройки, введенные последними, сотрут предыдущие. "no" в начале команды удаляет настройки
Пример	Задать действие настроек с 6:00:00 до 13:30:00 с 1 октября 2004 по 26 января 2005. <pre>Switch(config)#time-range admin_timer Switch(config-time-range-admin_timer)#absolute start 6:00:00 2004.10.1 end 13:30:00 2005.1.26</pre>

11.1.3. Нумерованное расширенное правило доступа (access-list (ip extended))

Команда	<pre>access-list <num> {deny permit} icmp {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}} {{<dIpAddr> <dMask>} any-destination {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>] [time-range<time-range-name>]</pre>
	<pre>access-list <num> {deny permit} igmp {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}} {{<dIpAddr> <dMask>} any-destination {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>][time-range <time-range-name>]</pre>
	<pre>access-list <num> {deny permit} tcp {{ <slpAddr> <sMask> } any-source {host-source <slpAddr> } } [s-port { <sPort> range <sPortMin> <sPortMax> }] {{ <dIpAddr> <dMask> } any-destination {host-destination <dIpAddr> } } [d-port { <dPort> range <dPortMin> <dPortMax> }] [ack+ fin+ psh+ rst+ urg+ syn] [precedence <prec>] [tos <tos>][time-range <time-range-name>]</pre>
	<pre>access-list <num> {deny permit} udp {{ <slpAddr> <sMask> } any-source {host-source <slpAddr> } } [s-port { <sPort> range <sPortMin> <sPortMax> }] {{ <dIpAddr> <dMask> } any-destination {host-destination <dIpAddr> } } [d-port</pre>



```
{ <dPort> | range <dPortMin> <dPortMax> } ] [precedence <prec> ] [tos <tos> ] [time-range <time-range-name> ]
```

```
access-list <num> {deny | permit} {eigrp | gre | igmp | ipinip | ip | ospf
```

```
<protocol-num> } { <slpAddr> <sMask> } | any-source | {host-source <slpAddr> } }
```

```
{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> } } [precedence <prec> ] [tos <tos> ] [time-range <time-range-name> ]
```

```
no access-list <num>
```

Параметр	<num>	номер списка доступа, 100-299;
	deny	отклонять пакеты
	permit	принимать пакеты
	<slpAddr>	IP-адрес источника; в десятично-точечной записи
	<sMask>	обратная маска IP-адреса источника; в десятично-точечной записи
	<sPort>	номер порта источника, 0-65535
	<sPortMin>	нижняя граница порта источника
	<sPortMax>	верхняя граница порта источника
	<protocol>	номер протокола верхнего уровня ip, 0-255
	<dIpAddr>	IP-адрес назначения; в десятично-точечной записи
	<dMask>	обратная маска IP-адреса назначения; в десятично-точечной записи
	<dPort>	номер порта назначения, 0-65535
	<dPortMin>	нижняя граница порта назначения
	<dPortMax>	верхняя граница порта назначения
	<igmp-type>	тип igmp, 0-15



	<icmp-type>	тип icmp, 0-255
	<icmp-code>	номер протокола icmp, 0-255
	<prec>	приоритет IP, 0-7
	<tos>	номер типа обслуживания, 0-15
	<time-range-name>	имя временного диапазона
По умолчанию	Списки доступа не настроены	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет создать нумерованное расширенное (extended) правило доступа для согласования с конкретным IP-протоколом, либо со всеми IP-протоколами. Если списка доступа "access-list" с таким номером не существует, то он будет создан. Когда пользователь в первый раз присваивает конкретный номер <num>, создается порядковый номер списка, затем правила добавляются в этот ACL. Для списков доступа с номерами 200-299 могут быть заданы обратные маски IP-адресов, не являющиеся постоянными. <igmp-type> указывает тип пакета IGMP со следующими параметрами: 17(0x11): IGMP QUERY packet 18(0x12): IGMP V1 REPORT packet 22(0x16): IGMP V2 REPORT packet 23(0x17): IGMP V2 LEAVE packet 34(0x22): IGMP V3 REPORT packet 19(0x13): DVMR packet 20(0x14): PIM V1 packet Важное замечание: указанные типы пакетов могут содержать поля IP OPTION. Обычно IGMP-пакет содержит поля OPTION, однако в описываемой настройке эти поля использовать нельзя. Если необходимо настроить пакеты, содержащие поля OPTION, используйте те из них, для которых задана опция OFFSET. "no" в начале команды удаляет настройки	
Пример	Создать нумерованный расширенный список доступа с порядковым номером 110. Запретить прохождение пакетов icmp и разрешить прохождение пакетов udp с адресом назначения 192. 168. 0. 1 и портом назначения 32. <pre>Switch(config)#access-list 110 deny icmp any any-destination</pre>	



	Switch(config)#access-list 110 deny icmp any any-destination Switch(config)#access-list 110 permit udp any host-destination 192.168.0.1 d-port 32

11.1.4. Нумерованный список доступа для IP-адресов (access-list (ip standard))

Команда	access-list <num> {deny permit} {{<slpAddr> <sMask >} any-source}{host-source <slpAddr>}} no access-list <num>	
Параметр	<num>	номер списка доступа, 100-199
	deny	отклонять пакеты
	permit	принимать пакеты
	<slpAddr>	IP-адрес источника; в десятично-точечной записи
	<sMask>	обратная маска IP-адреса источника; в десятичной системе
По умолчанию	Списки доступа не настроены	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет создать стандартный нумерованный список доступа для IP-адресов. Если список доступа существует, к нему будет добавлен список правил. Когда пользователь в первый раз присваивает конкретный номер <num> создается порядковый номер списка, затем правила добавляются в эт от ACL. Команда “no access-list <num>” удаляет стандартный нумерованный список доступа для IP-адресов	
Пример	Создать стандартный нумерованный список доступа для IP-адресов с порядковым номером 20, разрешить прохождение пакетов данных с адресом источника 10.1.1.0/24, запретить прохождение пакетов с адресом источника 10.1.1.0/16. Switch(config)#access-list 20 permit 10.1.1.0 0.0.0.255 Switch(config)#access-list 20 deny 10.1.1.0 0.0.255.255	



11.1.5. Расширенный нумерованный ACL для MAC-адресов (access-list (mac extended))

Команда	access-list <num> {deny permit} {any-source-mac {host-source-mac <slpAddr>}} <host_smac> {<smac> <smac-mask>}} {any-destination-mac {host-destination-mac <host_dmac> {<dmac> <dmac-mask>}} [untagged-eth2 tagged-eth2 untagged-802-3 tagged-802-3] no access-list <num>	
Параметр	<num>	номер списка доступа, десятичное число 100-199
	deny	отклонять пакеты
	permit	принимать пакеты
	any-source-mac	для любого адреса источника
	host-source-mac	MAC-адрес источника
	<slpAddr>	IP-адрес источника; в десятично-точечной записи
	<host_smac>	MAC-адрес источника
	<smac>	MAC-адрес источника
	<smac-mask>	маска (обратная маска) MAC-адреса источника
	any-destination-mac	для любого адреса назначения
	host-destination-mac	MAC-адрес назначения
	<host_dmac>	MAC-адрес назначения
	<dmac>	MAC-адрес назначения
	<dmac-mask>	маска (обратная маска) MAC-адреса назначения
	untagged-eth2	формат нетегированных пакетов Ethernet II



	tagged-eth2	формат тегированных пакетов Ethernet II
	untagged-802-3	формат нетегированных пакетов 802.3
	tagged-802-3	формат тегированных пакетов 802.300
По умолчанию	Списки доступа не настроены	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать расширенное нумерованное правило ACL для MAC-адресов. Когда пользователь в первый раз присваивает конкретный номер <num> создается порядковый номер списка, затем правила добавляются в этот ACL. Команда "no access-list <num>" удаляет расширенное нумерованное правило ACL для MAC-адресов	
Пример	Разрешить прохождение tagged-eth2 с любыми MAC-адресами источника и любыми MAC-адресами назначения и пакетов Switch(config)#access-list 1100 permit any-source-mac any-destination-mac tagged-eth2	

11.1.6. Нумерованное расширенное правило списка доступа MAC-IP ACL (access-list(mac-ip extended))

Команда	<pre> access-list<num>{deny permit}{any-source-mac {host-source-mac<host_smac>}} {<smac><smac-mask>}} {any-destination-mac {host-destination-mac <host_dmac>}} {<dmac><dmac-mask>}}icmp {{<source><source-wildcard>}}any-source {host-source<source-host-ip>}} {{<destination><destination-wildcard>}} any-destination {host-destination<destination-host-ip>}}[<icmp-type> [<icmp-code>]] [precedence <precedence>] [tos <tos>][time-range<time-range-name>] access-list<num>{deny permit}{any-source-mac {host-source-mac<host_smac>}} {<smac><smac-mask>}} {any-destination-mac {host-destination-mac <host_dmac>}} {<dmac><dmac-mask>}}igmp {{<source><source-wildcard>}}any-source {host-source<source-host-ip>}} {{<destination><destination-wildcard>}} any-destination {host-destination<destination-host-ip>}} [<igmp-type>] [precedence <precedence>] [tos <tos>][time-range<time-range-name>] access-list <num> {deny permit}{any-source-mac {host-source-mac<host_smac> }} { <smac> <smac-mask> }}{any-destination-mac {host-destination-mac <host_dmac> }} { <dmac> <dmac-mask> }}tcp {{ <source> <source-wildcard> }}any-source {host-source <source-host-ip> }}[s-port{ </pre>



<pre> <port1> range <sPortMin> <sPortMax>]] {{ <destination> <destination-wildcard> } any-destination {host-destination <destination-host-ip> }} [d-port { <port3> range <dPortMin> <dPortMax> }} [ack+fin+psh+rst+urg+syn] [precedence<precedence>] [tos <tos>] [time-range <time-range-name>] access-list <num> {deny permit}{any-source-mac {host-source-mac<host_smac> }} { <smac> <smac-mask> }}{any-destination-mac {host-destination-mac <host_dmac> }} { <dmac> <dmac-mask> }}udp {{ <source> <source-wildcard> }}any-source {host-source <source-host-ip> }}[s-port{ <port1> range <sPortMin> <sPortMax> }} </pre>		
<pre> {{ <destination> <destination-wildcard> }}any-destination {host-destination <destination-host-ip> }}[d-port{ <port3> range <dPortMin> <dPortMax> }} [precedence <precedence>] [tos <tos>][time-range <time-range-name>] access-list <num> {deny permit}{any-source-mac {host-source-mac <host_smac> }} { <smac> <smac-mask> }} {any-destination-mac {host-destination-mac <host_dmac> }} { <dmac> <dmac-mask> }} {eigrp gre igrp ip ipinip ospf { <protocol-num> }} {{ <source><source-wildcard> }}any-source {host-source <source-host-ip> }} {{ <destination><destination-wildcard> }}any-destination {host-destination <destination-host-ip> }}[precedence <precedence>] [tos <tos>][time-range <time-range-name>] no access-list <num> </pre>		
Параметр	<num>	порядковый номер списка доступа, десятичное число от 3100-3299
	deny	отклонять пакеты
	permit	принимать пакеты
	any-source-mac	любой MAC-адрес источника
	any-destination-mac	любой MAC-адрес назначения
	host_smac , smac	MAC-адрес источника
	smac-mask	(обратная маска) MAC-адреса источника
	host_dmac , dmas	MAC-адрес назначения
	dmac-mask	(обратная маска) MAC-адреса назначения



	protocol	номер имени или IP-протокол. Может быть одним из ключевых слов: eigrp, gre, icmp, igmp, igmp, ip, ipinip, ospf, tcp или udp, или целым числом от 0 до 255, которое является номером списка IP-адресов. Используйте ключевое слово 'ip' для согласования со всеми Интернет протоколами (включая ICMP, TCP и UDP)
	source-host-ip	номер сети-источника или хоста-источника доставляемого пакета. 32-битные числа, представленные в десятично-точечной записи
	source-wildcard	IP-адрес источника в обратном порядке. 32-битные числа, представленные в десятичном формате с 4 точками-разделителями, обратная маска
	destination-host-ip	номер сети-назначения или хоста-назначения доставляемого пакета. 32-битные числа, представленные в десятично-точечной записи
	destination-wildcard	маска назначения. 32-битные числа, представленные в десятичном формате с 4 точками-разделителями, обратная маска
	s-port	означает необходимость согласования с портом источником при TCP/UDP
	port1	номер интерфейса источника при TCP/UDP, целое число в пределах 0-65535
	d-port	необходимость согласования с интерфейсом назначения при TCP/UDP
	sPortMin	нижняя граница порта источника
	sPortMax	верхняя граница порта источника
	port3	номер интерфейса назначения при TCP/UDP, целое число в пределах 0-65535
	dPortMin	нижняя граница порта назначения
	dPortMax	верхняя граница порта назначения



	[ack] [fin] [psh]	только для протокола TCP, порядок следования тегов
	[rst] [urg] [syn]	не важен. Когда данные TCP сообщают о соответствующем порядке в конфигурации, включает инициализация отчета данных TCP для формирования совпадений в момент соединения
	precedence	пакеты могут фильтроваться по приоритетам, под номерами от 0 до 7
	tos	пакеты могут фильтроваться по типу обслуживания, под номерами от 0-15
	icmp-type	ICMP-пакеты могут фильтроваться по типу пакета, под номерами от 0 до 255
	icmp-code	ICMP-пакеты могут фильтроваться по коду пакета под номерами от 0 до 255
	igmp-type	IGMP-пакеты могут фильтроваться по имени IGMP-пакета или по типу пакета под номерами от 0 до 255
	time-range-name	имя временного диапазона
По умолчанию	Списки доступа не настроены	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать нумерованное расширенное правило списка доступа MAC-IP ACL. Когда пользователь в первый раз присваивает конкретный номер <num>, создается порядковый номер списка, затем правила добавляются в этот ACL. Для списков доступа с номерами 3200-3299 могут быть заданы обратные маски IP-адресов, не являющиеся постоянными. "no" в начале команды удаляет расширенное нумерованное правило доступа MAC-IP ACL	
Пример	Permit the passage of TCP packet with source MAC 00-12-34-45-XX-XX, any destination MAC address, source IP address 100.1.1.0 0.255.255.255, and source port 100. Switch(config)#access-list 3199 permit 00-12-34-45-67-00 00-00-00-00-FF-FF any-destination-mac tcp 100.1.1.0 0.255.255.255 s-port 100 any-destination	



11.1.7. Стандартное нумерованное правило ACL для MAC-адресов (access-list (mac standard))

Команда	access-list <num> {deny permit} {any-source-mac {host-source-mac <host_smac> } {<smac> <smac-mask> } } no access-list <num>	
Параметр	<num>	номер списка доступа, десятичное число от 700-799
	deny	отклонять пакеты
	permit	принимать пакеты
	host_smac, smac	MAC-адрес источника
	smac-mask	(обратная маска) MAC-адреса источника
По умолчанию	Списки доступа не настроены	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать стандартное нумерованное правило ACL для MAC-адресов. Когда пользователь в первый раз присваивает конкретный номер <num> создается порядковый номер списка, затем правила добавляются в этот ACL. "no" в начале команды удаляет стандартное нумерованное правило ACL для MAC-адресов	
Пример	Разрешить прохождение с MAC-адресом источника 00-00-XX-XX-00-01, запретить прохождение пакетов с MAC-адресом источника 00-00-00-XX-00-ab. Switch(config)# access-list 700 permit 00-00-00-00-00-01 00-00-FF-FF-00-00 Switch(config)# access-list 700 deny 00-00-00-00-00-ab 00-00-00-FF-00-00	

11.1.8. Очистить статистику пакетов (clear access-group statistic)

Команда	clear access-group statistic [ethernet <interface-name>]	
Параметр	interface-name	имя интерфейса
По умолчанию	Не задано	



Режим	Привилегированный режим
Руководство по использованию	Очищает статистику пакетов на указанном интерфейсе
Пример	Очистить статистику пакетов на интерфейсе. Switch#clear access-group statistic

11.1.9. Межсетевой экран (firewall)

Команда	firewall {enable disable}	
Параметр	{enable disable}	включить или отключить межсетевой экран
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает или выключает межсетевой экран. Правила доступа могут быть заданы как при включенном, так и при выключенном межсетевом экране. Однако только когда межсетевой экран включен, правила могут быть использованы для конкретного порта и направления передачи в нем. Когда межсетевой экран выключен, все списки доступа ACL, привязанные к портам, удаляются	
Пример	Включить межсетевой экран. Switch(config)#firewall enable	

11.1.10. Расширенный список доступа для IP-адресов (ip access extended)

Команда	[no] ip access extended <name>	
Параметр	name	имя списка доступа. Имя может быть задано в буквенно-числовом формате длиной от 1 до 32 символов
По умолчанию	Списки доступа не настроены	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Позволяет создать расширенный список доступа для IP-адресов и присвоить ему имя. Когда эта команда вводится впервые, создается пустой список доступа. Добавление "no" в начале команды удаляет расширенный список доступа вместе со всем его содержимым
Пример	Создать расширенный список доступа для IP-адресов с именем tcpFlow. Switch(config)#ip access-list extended tcpFlow

11.1.11. Стандартный список доступа для IP-адресов (ip access standard)

Команда	[no] ip access standard<name>	
Параметр	name	имя списка доступа. Имя может быть задано в буквенно-числовом формате длиной от 1 до 32 символов
По умолчанию	Списки доступа не настроены	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет создать стандартный список доступа для IP-адресов и присвоить ему имя. Когда эта команда вводится впервые, создается пустой список доступа. "no" в начале команды удаляет список доступа вместе со всем его содержимым	
Пример	Создать стандартный список доступа для IP-адресов с именем ipFlow Switch(config)#ip access-list standard ipFlow	

11.1.12. Стандартный нумерованный список доступа для IP-адресов (ipv6 access-list)

Команда	ipv6 access-list <num-std> {deny permit} {<slPv6Prefix/sPrefixlen> any-source {host-source <slPv6Addr>}} no ipv6 access-list <num-std>	
Параметр	num-std	номер списка доступа, в диапазоне от 500 до 599
	deny	отклонять пакеты
	permit	принимать пакеты



	sIPv6Prefix	префикс ipv6-адреса источника
	sPrefixlen	длина префикса ipv6-адреса источника, в пределах от 1 до 128
	sIPv6Addr	ipv6-адрес источника
По умолчанию	Списки доступа не настроены	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет создать стандартный нумерованный список доступа для IP-адресов. Если список доступа уже существует, в него будет добавлено правило. "no" в начале команды удаляет стандартный нумерованный список доступа для IP-адресов	
Пример	Создать нумерованный стандартный список доступа 520, разрешающий пакетам от назначения 2003: 1: 2: 3: : 1/64 проходить через сеть и запрещающий проходить через нее пакетам от источника с адресом 2003: 1: 2: : 1/48 . Switch (config)#ipv6 access-list 520 permit 2003: 1:2:3::1/64 Switch (config)#ipv6 access-list 520 deny 2003:1:2:::1/48	

11.1.13. Стандартный список доступа для IPv6-адресов (ipv6 access standard)

Команда	ipv6 access-list standard <name> no ipv6 access-list standard <name>	
Параметр	name	имя списка доступа, символьная строка длиной от 1 до 32 символов
По умолчанию	Списки доступа не настроены	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет создать стандартный список доступа для IPv6-адресов на основе имен. Когда эта команда вводится впервые, создается пустой список доступа. "no" в начале команды удаляет стандартный список доступа для IPv6-адресов на основе имен (удаляет все его элементы)	



Пример	Создать стандартный список доступа для IPv6-адресов с именем "ip6Flow". Switch(config)#ipv6 access-list standard ip6Flow

11.1.14. Расширенный список доступа для IPv6-адресов (ipv6 access extended)

Команда	ipv6 access-list extended <name> no ipv6 access-list extended <name>	
Параметр	name	имя списка доступа, символьная строка длиной от 1 до 32 символов
По умолчанию	Списки доступа не настроены	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет создать расширенный список доступа для IPv6-адресов на основе имен. Когда эта команда вводится впервые, создается пустой список доступа. "no" в начале команды удаляет расширенный список доступа для IPv6-адресов на основе имен	
Пример	Создать расширенный список доступа для IPv6-адресов с именем "tcpFlow". Switch(config)#ipv6 access-list extended tcpFlow	

11.1.15. Список доступа, привязанный к порту ({ip|ipv6|mac|mac-ip} access-group)

Команда	{ip ipv6 mac mac-ip} access-group <name> {in} [traffic-statistic] no {ip ipv6 mac mac-ip} access-group <name> {in}	
Параметр	name	имя списка доступа, символьная строка длиной от 1 до 32 символов
	traffic-statistic	статистика потоков
По умолчанию	К входу порта списки доступа ACL не привязаны	
Режим	Режим конфигурации порта	



Руководство по использованию	Позволяет применить список доступа для направления передачи порта, имеет опцию, по которой в правило ACL может быть добавлен счетчик статистики. Примечание: когда список доступа содержит несколько правил, статистику трафика задать невозможно. Всего имеется четыре вида полей заголовка пакетов: MAC ACL, IP ACL, MAC-IP ACL и IPv6 ACL; в некоторых случаях ACL-фильтрация (permit, deny) приводит к конфликтам, когда пакеты могут согласовываться с несколькими типами данных в четырех ACL. В каждом списке ACL точные приоритеты задаются на основе результирующей достоверности. Когда фильтрация приводит к конфликту, можно задать финальный режим работы фильтра на основе приоритетов. При привязке ACL к порту имеются некоторые ограничения: К каждому порту может быть привязан MAC-IP ACL, IP ACL, MAC ACL и IPv6 ACL. При привязке к порту четырех ACL, когда пакетные данные согласуются с несколькими ACL одновременно, приоритеты списков идут от высшего приоритета к низшему: IPv6 ACL, MAC-IP ACL, MAC ACL, IP ACL все для входящего трафика. "no" в начале команды удаляет список доступа, привязанный к порту
Пример	Привязать список доступа AAA к входящему направлению порта. <pre>Switch(config)#interface ethernet 1/0/5 Switch(config-if-Ethernet1/0/5)#ip access-group aaa in</pre>

11.1.16. Список доступа ACL с именем для MAC-адресов и его настройка (mac access extended)

Команда	mac-access-list extended <name> no mac-access-list extended <name>	
Параметр	name	имя списка доступа, не должно содержать пробелов и кавычек, должно начинаться с буквы, длина имени не должна превышать 32 символов (примечание: учитываются различия строчных и прописных букв)
По умолчанию	Списки доступа не сконфигурированы	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Позволяет создать список доступа MAC ACL с именем, либо войти в режим настройки списков доступа. После первого выполнения этой команды создается список доступа с пустым именем, элементы списка отсутствуют. "no" в начале команды удаляет данный ACL
Пример	Создать MAC ACL с именем mac_acl. <pre>Switch(config)# mac-access-list extended mac_acl Switch(config-mac-ext-nacl-mac_acl)#</pre>

11.1.17. Список доступа ACL с именем для MAC-IP-адресов и его настройка (mac-ip access extended)

Команда	<pre>mac-ip-access-list extended <name> no mac-ip-access-list extended <name></pre>	
Параметр	name	имя списка доступа, не должно содержать пробелов и кавычек, должно начинаться с буквы, длина не должна превышать 32 символов (примечание: учитываются различия строчных и прописных букв)
По умолчанию	Именованные списки доступа для MAC-IP-адресов отсутствуют	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет создать список доступа MAC-IP ACL с именем, либо войти в режим настройки списков доступа. После первого выполнения этой команды создается список доступа с пустым именем, элементы списка отсутствуют. "no" в начале команды удаляет данный ACL	
Пример	Создать MAC-IP ACL с именем mac_ac. <pre>Switch(config)# mac-ip-access-list extended macip_acl Switch(config-macip-ext-nacl-macip_acl)#</pre>	



11.1.18. Правило управления доступом для расширенного списка IP-адресов (permit | deny (ip extended))

Команда	<pre>[no] {deny permit} icmp {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}} {{<dIpAddr> <dMask>} any-destination {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>][tos <tos>] [time-range<time-range-name>]</pre>	
	<pre>[no] {deny permit} igmp {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}} {{<dIpAddr> <dMask>} any-destination {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>] [time-range<time-range-name>]</pre>	
	<pre>[no] {deny permit} tcp {{ <slpAddr> <sMask> } any-source {host-source <slpAddr> } } [s-port { <sPort> range <sPortMin> <sPortMax> }] {{ <dIpAddr> <dMask> } any-destination {host-destination <dIpAddr> } } [d-port { <dPort> range <dPortMin> <dPortMax> }] [ack+fin+psh+rst+urg+syn] [precedence <prec>] [tos <tos>] [time- range <time-range-name>]</pre>	
	<pre>[no] {deny permit} udp {{ <slpAddr> <sMask> } any-source {host-source <slpAddr> } } [s-port { <sPort> range <sPortMin> <sPortMax> }] {{ <dIpAddr> <dMask> } any-destination {host-destination <dIpAddr> } } [d-port { <dPort> range <dPortMin> <dPortMax> }] [precedence <prec>] [tos <tos>] [time-range<time-range-name>]</pre>	
	<pre>[no] {deny permit} {eigrp gre igmp ipinip ip ospf <protocol-num>} {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}} {{<dIpAddr> <dMask>} any-destination {host-destination <dIpAddr>}} [precedence <prec>] [tos <tos>][time-range<time-range-name>]</pre>	
Параметр	deny	отклонять пакеты
	permit	принимать пакеты
	<slpAddr>	IP-адрес источника; в десятично-точечной записи
	<sMask>	обратная маска IP-адреса источника; в десятично-точечной записи
	<sPort>	номер порта источника, 0-65535
	<sPortMin>	нижняя граница порта источника



	<sPortMax>	верхняя граница порта источника
	<dIpAddr>	IP-адрес назначения; в десятично-точечной записи
	<dMask>	обратная маска IP-адреса назначения; в десятично-точечной записи, положение принимать во внимание 0, положение игнорирования 1
	<dPort>	номер порта назначения, 0-65535
	<dPortMin>	нижняя граница порта назначения
	<dPortMax>	верхняя граница порта назначения
	<icmp-type>	тип icmp, 0-255
	<icmp-code>	номер протокола icmp, 0-255
	<prec>	приоритет IP, 0-7
	<tos>	номер типа обслуживания, 0-15
	<time-range-name>	имя временного диапазона
По умолчанию	Список доступа не задан	
Режим	Режим настройки доступа для именованного расширенного списка IP-адресов	
Руководство по использованию	Позволяет создать расширенное правило доступа для IP-адресов для согласования с конкретным IP-протоколом или со всеми IP-протоколами. "no" в начале команды удаляет данный список доступа	
Пример	Создать расширенный список доступа, запретить прохождение пакетов icmp, разрешить прохождение пакетов udp с адресом назначения 192. 168. 0. 1 и портом назначения 32. <pre>Switch(config)# ip access-list extended udpFlow Switch(config-ip-ext-nacl-udpFlow)#deny icmp any any-destination Switch(config-ip-ext-nacl-udpFlow)#permit udp any host-destination 192.168.0.1 d-port 32</pre>	



11.1.19. Правило управления доступом для стандартных IP-адресов (permit | deny(ip standard))

Команда	{deny permit} {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}} no {deny permit} {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}}	
Параметр	deny	отклонять пакеты
	permit	принимать пакеты
	<slpAddr>	IP-адрес источника; в десятично-точечной записи
	<sMask>	обратная маска IP-адреса источника; в десятично-точечной системе
По умолчанию	Список доступа не задан	
Режим	Режим настройки списка доступа для стандартных IP-адресов	
Руководство по использованию	Позволяет создать правило доступа для стандартного списка IP-адресов. "no" в начале команды удаляет соответствующее правило доступа	
Пример	Разрешить прохождение пакетов от источника с адресом 10.1.1.0/24, запретить остальные пакеты от источника с адресом 10.1.1.0/16. Switch(config)# ip access-list standard ipFlow Switch(config-std-nacl-ipFlow)# permit 10.1.1.0 0.0.0.255 Switch(config-std-nacl-ipFlow)# deny 10.1.1.0 0.0.255.255	

11.1.20. Правило управления доступом для расширенного списка IPv6-адресов (permit | deny (ipv6 extended))

Команда	[no] {deny permit} icmp {{<slIPv6Prefix/sPrefixlen>} any-source {host-source <slIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> any-destination {host-destination <dIPv6Addr>}} [<icmp-type> [<icmp-code>]] [dscp <dscp>] [flow-label <fl>]
[time-range <time-range-name>]	
[no] {deny permit} tcp { <slIPv6Prefix/sPrefixlen> any-source {host-source <slIPv6Addr> }} [s-port { <sPort> range <sPortMin> <sPortMax> }]	



```
{ <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }}
[d-port { <dPort> | range <dPortMin> <dPortMax> }] [syn | ack | urg | rst | fin | psh] [dscp <dscp>
] [flow-label <fl> ][time-range <time-range-name> ]
```

```
[no] {deny | permit} udp { <sIPv6Prefix/sPrefixlen> | any-source | {host-source
<sIPv6Addr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }]
{ <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }} [d-port { <dPort>
| range <dPortMin> <dPortMax> }] [dscp <dscp> ] [flow-label
<fl> ][time-range <time-range-name> ]
```

```
[no] {deny | permit} <next-header> {<sIPv6Prefix/sPrefixlen> | any-source |
{host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination |
{host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <fl>][time-range
<time-range-name>]
```

```
[no] {deny | permit} {<sIPv6Prefix/sPrefixlen> | any-source | {host-source
<sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination
<dIPv6Addr>}} [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]
```

Параметр	deny	отклонять пакеты
	permit	принимать пакеты
	<sIPv6Addr>	ipv6-адрес источника
	<sPrefixlen>	длина префикса IPv6-адреса, в диапазоне от 1 до 128
	<sPort>	номер порта источника, в диапазоне от 0 до 65535
	<sPortMin>	нижняя граница порта источника
	<sPortMax>	верхняя граница порта источника
	<dIPv6Addr>	ipv6-адрес назначения
	<dPrefixlen>	длина префикса IPv6-адреса, в диапазоне от 1 до 128
	<dPort>	номер порта назначения, в диапазоне от 0 до 65535



	<dPortMin>	нижняя граница порта назначения
	<dPortMax>	верхняя граница порта назначения
	<igmp-type>	тип IGMP
	<icmp-type>	тип icmp
	<icmp-code>	номер протокола icmp
	<dscp>	приоритет IPv6, в диапазоне от 0 до 63
	<flowlabel>	метка потока, в диапазоне от 0 до 1048575
	syn,ack,urg,rst,fin, psh,tcp	положение метки
	<next-header>	следующий заголовок IPv6
	<time-range-name>	имя временного диапазона
По умолчанию	Список управления доступом не настроен	
Режим	Режим расширенного списка управления доступом для IPv6-адресов	
Руководство по использованию	Позволяет создать расширенный список управления доступом для IPv6-адресов для согласования с конкретным IPv6-протоколом. "no" в начале команды удаляет данный список доступа	
Пример	Создать расширенный список доступа с именем "udpFlow", запретить прохождение пакетов igmp и разрешить прохождение пакетов udp с адресом назначения 2001: 1: 2: 3: : 1 и портом назначения 32. Switch(config)#ipv6 access-list extended udpFlow Switch(config-ipv6-ext-nacl-udpFlow)#deny igmp any any-destination Switch(config-ipv6-ext-nacl-udpFlow)#permit udp any-source host-destination 2001: 1: 2: 3: : 1 dPort 32	

11.1.21. Правило управления доступом для стандартных IPv6-адресов (permit | deny (ipv6 standard))

Команда	[no] {deny permit} {{<sIPv6Prefix/sPrefixlen>} any-source {host-source <sIPv6Addr>}}	
Параметр	deny	отклонять пакеты



	permit	принимать пакеты
	<sPrefixlen>	длина префикса IPv6-адреса, в диапазоне от 1 до 128
	<sIPv6Addr>	ipv6-адрес источника
По умолчанию	Список доступа не задан	
Режим	Режим настройки стандартных IPv6-списков доступа	
Руководство по использованию	Позволяет создать правило управления доступом для стандартных IPv6-адресов. "no" в начале команды удаляет правило доступа	
Пример	Разрешить прохождение пакетов от источника с адресом 2001: 1: 2: 3: : 1/64 , запретить прохождение пакетов от источника с адресом 2001: 1: 2: 3: : 1/48. <pre>Switch(config)#ipv6 access-list standard ipv6Flow Switch(config-ipv6-std-nacl-ipv6Flow)# permit 2001: 1: 2: 3: : 1/64 Switch(config-ipv6-std-nacl-ipv6Flow)# deny 2001: 1: 2: 3: : 1/48</pre>	

11.1.22. Правило управления доступом для расширенного списка MAC-адресов (permit | deny (mac extended))

Команда	<pre>[no]{deny permit} {any-source-mac}{host-source-mac <host_smac> }{<smac> <smac-mask> }} {any-destination-mac}{host-destination-mac <host_dmac> }{<dmac> <dmac-mask> }} [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]] [ethertype <protocol> [<protocol-mask>]]</pre> <pre>[no]{deny permit} {any-source-mac}{host-source-mac <host_smac> }{<smac> <smac-mask> }} {any-destination-mac}{host-destination-mac <host_dmac> }{<dmac> <dmac-mask> }} [untagged-eth2 [ethertype <protocol>[protocol-mask]]]</pre> <pre>[no]{deny permit}{any-source-mac}{host-source-mac <host_smac> }{<smac> <smac-mask> }} {any-destination-mac}{host-destination-mac <host_dmac> }{<dmac> <dmac-mask> }} [untagged-802-3]</pre> <pre>[no]{deny permit} {any-source-mac}{host-source-mac <host_smac> }{<smac></pre>



```
<smac-mask> }} {any-destination-mac}{host-destination-mac <host_dmac> }}{ <dmac>
<dmac-mask> }} [tagged-eth2 [cos <cos-val>[ <cos-bitmask> ]] [vlanId <vid-value> [ <vid-
mask> ]] [ethertype <protocol>[ <protocol-mask> ]]]
```

```
[no]{deny|permit}{any-source-mac}{host-source-mac <host_smac> }}{ <smac>
<smac-mask> }} {any-destination-mac}{host-destination-mac <host_dmac> }}{ <dmac>
<dmac-mask> }} [tagged-802-3 [cos <cos-val>[ <cos-bitmask> ]] [vlanId <vid-value> [ <vid-
mask> ]]]
```

Параметр	deny	отклонять пакеты
	permit	принимать пакеты
	any-source-mac	любой источник MAC-адреса
	any-destination-mac	любое назначение MAC-адреса
	host_smac, smac	MAC-адрес источника
	smac-mask	маска (обратная маска) MAC-адреса источника
	host_dmac, dmas	MAC-адрес назначения
	dmac-mask	(обратная маска) MAC-адреса назначения
	untagged-eth2	формат нетегированных пакетов Ethernet II
	tagged-eth2	формат тегированных пакетов Ethernet II
	untagged-802-3	формат нетегированных пакетов 802.3
	tagged-802-3	формат тегированных пакетов 802.300
	cos-val	значение cos, 0-7
	cos-bitmask	маска протокола, 0-7; обратная маска, биты маски берутся последовательно
	vid-value	номер VLAN, 1-4094



	vid-bitmask	маска VLAN, 0-4095, обратная маска, биты маски берутся последовательно
	protocol	номер конкретного Ethernet-протокола, 1536-65535
	protocol-bitmask	маска протокола, 0-65535; обратная маска, биты маски берутся последовательно
По умолчанию	Список доступа не задан	
Режим	Режим настройки именованного расширенного списка доступа для MAC-адресов	
Руководство по использованию	Позволяет задать правило для именованного расширенного MAC ACL. ПРИМЕЧАНИЕ: "биты маски берутся последовательно" означает – биты, имеющие значения, начинаются слева, к ним не могут быть добавлены недопустимые биты Например: формат одного байта обратной маски: 00001111b; формат маски 11110000; недопустимая комбинация: 00010011. "no" в начале команды удаляет данное правило для именованного расширенного списка	
Пример	Запретить передачу пакетных данных 802.3 от источника с MAC-адресом 00-12-11-23-XX-XX. <pre>Switch(config)# mac-access-list extended macExt Switch(config-mac-ext-nacl-macExt)#deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac untagged-802-3 Switch(config-mac-ext-nacl-macExt)#deny 00-12-11-23-00-00 00-00-00-00-ff-ff any tagged-802</pre>	

11.1.23. Правило управления доступом для стандартных MAC-адресов (permit | deny (mac-ip extended))

Команда	<pre>[no]{deny permit} {any-source-mac}{host-source-mac<host_smac>} {<smac><smac-mask>}} {any-destination-mac}{host-destination- mac<host_dmac>}} {<dmac><dmac-mask>}} icmp{{<source><source-wildcard>}}any-source {host-source<source-host-ip>}} {{<destination><destination-wildcard>}} any-destination {host-destination <destination-host-ip>}} [<icmp-type> [<icmp-code>]] [precedence <precedence>] [tos <tos>][time-range<time- range-name>]</pre> <pre>[no]{deny permit} {any-source-mac}{host-source-mac<host_smac>}</pre>



<pre>{<smac><smac-mask>}} {any-destination-mac{{host-destination- mac<host_dmac>}} {<dmac><dmac-mask>}} igmp{{<source><source-wildcard>}}any-source {host-source<source-host-ip>}} {{<destination><destination-wildcard>}} any- destination {{host-destination <destination-host-ip>}} [<igmp-type>] [precedence <precedence>] [tos <tos>][time-range<time-range-name>] [no]{{deny permit}}{any-source-mac{{host-source-mac <host_smac> }} { <smac> <smac-mask> }}{any-destination-mac{{host-destination-mac<host_dmac> }} { <dmac> <dmac-mask> }}tcp{{ <source><source- wildcard> }}any-source {host-source <source-host-ip> }}[s-port { <port1> range <sPortMin> <sPortMax> }} {{ <destination> <destination-wildcard> } any-destination {host-destination <destination-host-ip> }} [d-port { <port3> range<dPortMin> <dPortMax> }} [ack + fin + psh + rst + urg + syn] [precedence <precedence>] [tos <tos>] [time-range <time-range-name>] [no]{{deny permit}}{any-source-mac{{host-source-mac <host_smac> }}{ <smac> <smac-mask> }}{any-destination-mac{{host-destination-mac <host_dmac> }} { <dmac> <dmac-mask> }}udp{{ <source> <source-wildcard> }}any-source {host-source <source-host-ip> }}[s-port{ <port1> range <sPortMin> <sPortMax> }} {{ <destination> <destination-wildcard> }}any-destination {host-destination <destination-host-ip> }} [d-port { <port3> range <dPortMin> <dPortMax> }} [precedence <precedence>] [tos <tos>][time-range <time-range-name>]</pre>		
<pre>[no]{{deny permit}}{any-source-mac{{host-source-mac<host_smac>}}{<smac> <smac-mask>}}{any-destination-mac{{host-destination-mac<host_dmac>}} {<dmac><dmac-mask>}}{eigrp gre igrp ip ipinip ospf{{<protocol-num>}} {{<source><source-wildcard>}}any-source {{host-source<source-host-ip>}} {{<destination><destination-wildcard>}}any-destination {{host-destination <destination-host-ip>}} [precedence <precedence>] [tos <tos>] [time-range<time-range- name>]</pre>		
Параметр	num	порядковый номер списка доступа, десятичное число от 3100 до 3199
	deny	отклонять пакеты



permit	принимать пакеты
any-source-mac	любой MAC-адрес источника
any-destination-mac	любой MAC-адрес назначения
host_smac, smac	MAC-адрес источника
smac-mask	(обратная маска) MAC-адреса источника
host_dmac, dmas	MAC-адрес назначения
dmac-mask	(обратная маска) MAC-адреса назначения
protocol	номер имени или IP-протокол. Может быть одним из ключевых слов: eigrp, gre, icmp, igmp, igmp, ip, ipinip, ospf, tcp или udp или целым числом от 0 до 255, которое является номером IP-адреса. Используйте ключевое слово 'ip' для согласования со всеми Интернет протоколами (включая ICMP, TCP и UDP)
source-host-ip, source	номер сети-источника или хоста-источника доставляемого пакета. 32-битные числа, представленные в десятично-точечной записи
source-wildcard	IP-адрес источника в обратном порядке. 32-битные числа, представленные в десятичном формате с 4 точками-разделителями, обратная маска
destination-host-ip, destination	номер сети назначения или хост доставки пакетов. 32-битные числа, представленные в десятично-точечной записи
destination-wildcard	маска назначения. 32-битные числа, представленные в десятичном формате с 4 точками-разделителями, обратная маска
s-port	означает необходимость согласования с портом источником при TCP/UDP
port1	номер интерфейса источника при TCP/UDP, целое число в пределах 0-65535



	<sPortMin>	нижняя граница порта источника
	<sPortMax>	верхняя граница порта источника
	d-port	необходимость согласования с интерфейсом назначения при TCP/UDP
	port3	номер интерфейса назначения при TCP/UDP, целое число в пределах 0-65535
	<dPortMin>	нижняя граница порта назначения
	<dPortMax>	верхняя граница порта назначения
	[ack] [fin] [psh] [rst] [urg] [syn]	(опции): только для протокола TCP, порядок следования тегов не важен. Когда данные TCP сообщают о соответствующем порядке в конфигурации, включает инициализация отчета данных TCP для формирования совпадений в момент соединения
	precedence	пакеты могут фильтроваться по приоритетам, под номерами от 0 до 7
	tos	пакеты могут фильтроваться по типу обслуживания, под номерами от 0-15
	icmp-type	ICMP-пакеты могут фильтроваться по типу пакета, под номерами от 0 до 255
	icmp-code	ICMP-пакеты могут фильтроваться по коду пакета под номерами от 0 до 255
	igmp-type	ICMP-пакеты могут фильтроваться по имени или типу пакета (целое число в пределах 0-255)
	time-range-name	имя временного диапазона
По умолчанию	Список доступа не задан	
Режим	Режим настройки расширенного списка доступа для MAC-IP-адресов	
Руководство по использованию	Позволяет задать именованное расширенное MAC-IP ACL правило. Команда с "No" в начале команды удаляет одно правило расширенного нумерованного MAC-IP ACL списка доступа	



Пример	Запретить прохождение пакетов UDP с любыми MAC-адресами источника и назначения, любыми IP-адресами источника и назначения и портом источника 100. <pre>Switch(config)# mac-ip-access-list extended macIpExt Switch(config-macip-ext-nacl-macIpExt)# deny any-source-mac any-destination-mac udp any-source s-port 100 any-destination</pre>

11.1.24. Просмотр созданных списков доступа (show access-lists)

Команда	show access-lists [<num> <acl-name>]	
Параметр	<num> <acl-name>	номер конкретного списка доступа ACL символьная строка имени конкретного списка доступа ACL
По умолчанию	Нет	
Режим	Привилегированный режим	
Руководство по использованию	Выводит информации о созданных списках доступа. Если спискам доступа ACL имена не присвоены, на дисплей будет выведена информация обо всех ACL. Для каждого списка будет выведено число раз его использования	
Пример	Показать информацию о созданных списках доступа. <pre>Switch#show access-lists access-list 10(used 0 time(s)) access-list 10 deny any-source access-list 100(used 1 time(s)) access-list 100 deny ip any any-destination access-list 100 deny tcp any any-destination access-list 1100(used 0 time(s)) access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800</pre>	

11.1.25. Просмотр привязки списков доступа ACL к портам (show access-group)

Команда	show access-group in (interface {Ethernet Ethernet IFNAME})	
Параметр	IFNAME	имя порта
По умолчанию	Не задано	
Режим	Привилегированный/режим глобальной конфигурации	



Руководство по использованию	Выводит на экран привязки списков доступа ACL к портам. Если имена интерфейсу не заданы, будут показаны все списки ACL, привязанные к порту
Пример	Показать все привязки списков доступа ACL к порту. Switch#show access-group interface name: Ethernet 1/0/1 IP Ingress access-list used is 100, traffic-statistics Disable. interface name: Ethernet1/0/2 IP Ingress access-list used is 1, packet(s) number is 11110

11.1.26. Просмотр межсетевого экрана (show firewall)

Команда	show firewall	
Параметр	none	отсутствует
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, Привилегированный режим	
Руководство по использованию	Применяется для раскрытия информации о конфигурации функций фильтрации пакетов	
Пример	Показать статус межсетевого экрана. Switch#show firewall Firewall status: Enable	

11.1.27. Просмотр настроек списка доступа ACL IPv6 (show ipv6 access-lists)

Команда	show ipv6 access-lists [<num> <acl-name>]	
Параметр	<num>	номер конкретного списка доступа, в пределах от 500 до 699; номера с 500 до 599 закреплены за стандартными списками доступа IPv6 ACL, номера с 600 по 699 закреплены за расширенными списками доступа IPv6 ACL
	<acl-name>	имя конкретного списка доступа, символьная строка длиной от 1 до 32 символов
По умолчанию	Не задано	



Режим	Режим глобальной конфигурации, Привилегированный режим
Руководство по использованию	Позволяет просмотреть настроенный список управления доступом IPv6. Если спискам доступа ACL имена не присвоены, будет выведена информация обо всех ACL. Для каждого списка будет выведено число раз его использования
Пример	Показать настроенный список управления доступом IPv6. <pre>Switch#show ipv6 access-lists</pre> <pre>ipv6 access-list 500(used 1 time(s)) ipv6 access-list 500 deny any-source</pre> <pre>ipv6 access-list 510(used 1 time(s))</pre> <pre>ipv6 access-list 510 deny ip any-source any-destination ipv6 access-list 510</pre> <pre>deny tcp any-source any-destination ipv6 access-list 520(used 1 time(s))</pre> <pre>ipv6 access-list 520 permit ip any-source any-destination</pre>

11.1.28. Просмотр информации о временных диапазонах (show time-range)

Команда	show time-range <word>	
Параметр	<word>	имя, присвоенное временному диапазону, информация о котором должна быть показана
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, Привилегированный режим	
Руководство по использованию	Выводит информацию о настройках функции временного диапазона. Если имя временного диапазона не задано, выводится информация о всех временных диапазонах. В "used x time (s) " будет выведено число раз отсылок к ACL	
Пример	Показать информацию о настройках функции временного диапазона. <pre>Switch#show time-range</pre> <pre>time-range timer1 (inactive, used 0 times)</pre> <pre>absolute-periodic Saturday 0: 0: 0 to Sunday 23: 59: 59 time-range timer2</pre> <pre>(inactive, used 0 times)</pre> <pre>absolute-periodic Monday 0: 0: 0 to Friday</pre>	



11.1.29. Работа с временными диапазонами (time-range)

Команда	[no] time-range <time_range_name>	
Параметр	<time_range_name>	имя временного диапазона должно начинаться с буквы, длина не более 32 символов
По умолчанию	Временной диапазон не задан	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет присвоить имя временному диапазону и перейти в режим работы с временными диапазонами "no" в начале команды удалит данный временной диапазон	
Пример	Создать именованный временной диапазон с именем admin_timer. Switch(config)#Time-range admin_timer	

11.2. Конфигурация правила Self-Defined ACL (определяемый список ACL)

11.2.1. Создание окна смещения для правила (userdefined-access-list standard offset)

Команда	userdefined-access-list standard offset [window1 { l3start l4start } <offset> [window2 { l3start l4start } <offset>] [window3 { l3start l4start } <offset> [window4 { l3start l4start } <offset>] [window5 { l3start l4start } <offset> [window6 { l3start l4start } <offset>] [window7 { l3start l4start } <offset> [window8 { l3start l4start } <offset>] [window9 { l3start l4start } <offset> [window10 { l3start l4start } <offset>] [window11 { l3start l4start } <offset> [window12 { l3start l4start } <offset> no userdefined-access-list standard offset [window1] [window2] [window3] [window4] [window5] [window6] [window7] [window8] [window9] [window10] [window11] [window12]	
Параметр	window1-window12	задаваемые пользователем окна от 1 до 12
	l3start	начальное положение для смещения — это начало уровня3 (будет работать только если уровень3 существует)
	l4start	начальное положение для смещения — это начало уровня4 (будет работать только если уровень4 существует)



	offset	задаваемая величина смещения, от 0 до 178 (шаг 2 байта)
По умолчанию	Шаблон не сконфигурирован	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Создает шаблон стандартного автоматически определяемого списка ACL. Если шаблон существует, можно редактировать соответствующее окно. Параметры {l2endoftag l3start l4start}: задают начальное положение смещения для окна, <offset>: значение смещения, в диапазоне <0-178>, с шагом 2 байта, т.е. 0 означает смещение 0 байт, а 1 смещение 2 байта. Стандартный шаблон self-defined ACL позволяет задать начальную позицию и величину смещения для 12 окон. Шаблон является общим и действует в глобальном режиме. Изменить окно, если для него создано правило self-defined ACL, нельзя. Но если правило стандартного ACL не задано, с помощью этой команды окно можно изменить. Команда с "no" в начале может удалить одну или несколько конфигураций смещения окна в шаблоне или удалить весь шаблон. Окно в шаблоне не может быть удалено, если оно используется правилом self-defined ACL. Для ipv6 поддерживаются только окна с номерами 1 по 6. Наибольшее смещение l3start включает в себя заголовок L2, а наибольшее смещение l4start включает в себя заголовок L2 и L3. "no" в начале команды удаляет окна шаблона стандартного определяемого списка ACL. Если окно не указано, удаляется весь шаблон стандартного определяемого списка ACL	
Пример	Создать глобальный шаблон с 7 окнами (3-9) для настройки начальной позиции смещения и самого смещения: <pre>Switch(config)#userdefined-access-list standard offset window3 l2 0 window4 l2 2 window5 l3 0 window6 l3 1 window7 l3 2 window8 l4 1 window9 l4 2</pre>	



11.2.2. Создание правила для self-defined ACL (userdefined-access-list standard)

Команда	<pre> userdefined-access-list standard <1200-1299> {permit deny} {window1 window2 window3 window4 window5 window6 window7 window8 window9 window10 window11 window12} no userdefined-access-list standard <1200-1299> {permit deny} {window1 window2 window3 window4 window5 window6 window7 window8 window9 window10 window11 window12} </pre>	
Параметр	<1200-1299>	номер списка доступа от 1200 до 1299, десятичная запись
	permit	разрешить доступ
	deny	запретить доступ
	window1-window12	пользовательские окна от 1 до 12
По умолчанию	Списки доступа не созданы	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет создать нумерованный стандартный определяемый self-defined ACL. Если такой список уже создан, правило будет добавлено в него. Когда пользователь в первый раз присваивает конкретный номер <num>, создается порядковый номер списка, затем правила добавляются в этот ACL. "no" в начале команды удаляет стандартный self-defined ACL	
Пример	Разрешить пакеты, в которых второй байт начала I3 равен 0x4501. Разрешить пакеты, в которых четвертый байт начала I4 равен 0xFF. Настроить правило в том же списке, чтобы запретить пакеты, в которых пятый и шестой байты начала I3 равны 0xFFAA. <pre> Switch(config)#userdefined-access-list standard offset window1 I3 0 window2 I4 1 Switch(config)#userdefined-access-list standard 1200 permit window1 4501 FFFF window2 00FF 00FF Switch(config)#userdefined-access-list standard offset window3 I3 2 Switch(config)#userdefined-access-list standard 1200 deny any-source-mac any-destination-mac untagged-eth2 window3 FFAA FFFF </pre>	



11.2.3. Настройка определяемого списка ACL в порту (userdefined access-group)

Команда	userdefined access-group <name> {in} [traffic-statistic] no userdefined access-group <name> {in}	
Параметр	<name>	имя списка доступа, от 1200 до 1399, десятичная запись
По умолчанию	Определяемый список ACL не привязан к порту	
Режим	Режим конфигурации физического порта	
Руководство по использованию	Применяет определяемый список доступа на одном направлении порта. В зависимости от существующих опций принимает решение о том, следует ли добавлять в список ACL статистический счетчик. Определяемый список доступа можно привязать ко входу порта и настроить на входе того же порта одновременно с другими списками доступа. Правило запрета применяется, когда различные списки доступа совпадают, то есть, если список доступа подпадает под правило запрета, запрет должен быть выполнен, в ином случае действует правило разрешения. Команда, начинающаяся со слова «но», удаляет привязку к порту	
Пример	Настроенный self-defined access-list показан ниже: <pre>Switch(config)#userdefined-access-list standard offset window1 I3 0 window2 I4 1 window3 I3 1</pre> <pre>Switch(config)#userdefined-access-list standard 1300 permit window1 4501 FFFF window2 00FF 00FF</pre> <pre>Switch(config)#userdefined-access-list standard 1300 deny window1 FFAA0000 FFFF0000</pre> Привязать self-defined access-list к Ethernet1/1: <pre>Switch(config)#interface ethernet1/1</pre> <pre>Switch(config-if-ethernet1/1)#userdefined access-group 1300 in</pre>	

11.2.4. Назначение ACL на VLAN (vACL userdefined access-group)

Команда	vACL userdefined access-group <name> {in} vLAN <vLANId> [traffic-statistic] no vACL userdefined access-group <name> {in} vLAN <vLANId>	
Параметр	<name>	имя списка доступа, от 1200 до 1399, десятичная запись
	vLANId	привязанная VLAN, диапазон 1-4094



По умолчанию	Список доступа "userdefined-access-list" не привязан никакой VLAN
Режим	Режим глобальной конфигурации
Руководство по использованию	Применяет определяемый список доступа на одном направлении указанной сети VLAN. В зависимости от существующих вариантов принимает решение о том, следует ли добавлять в список ACL статистический счетчик. Определяемый список доступа можно привязать ко входу VLAN и настроить на входе той же VLAN одновременно с другими списками доступа. Правило запрета применяется, когда различные списки доступа совпадают, то есть, если список доступа подпадает под правило запрета, это правило должно быть выполнено, в ином случае действует правило разрешения. Команда, начинающаяся со слова «по», удаляет связанные с VLAN настройки
Пример	Настроенный "self-defined access-list" показан ниже: <pre>Switch(config)#userdefined-access-list standard offset window1 I3 0 window2 I4 1 window3 I3 1</pre> <pre>Switch(config)#userdefined-access-list standard 1300 permit window1 4501 FFFF window2 00FF 00FF</pre> <pre>Switch(config)#userdefined-access-list standard 1300 deny window1 FFAA0000 FFFF0000</pre> Привязать "self-defined access-list" к VLAN1: <pre>Switch(config)#vACL userdefined access-group 1300 in vlan 1</pre>

11.3. Команды для настройки протокола 802.1X

11.3.1. Добавление MAC-адреса в таблицу фильтруемых адресов dot1x (dot1x accept-mac)

Команда	[no] dot1x accept-mac <mac-address> [interface <interface-name>]	
Параметр	mac-address	MAC-адрес
	interface-name	имя интерфейса и номер порта
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Добавляет MAC-адрес в таблицу фильтруемых адресов dot1x. Если порт указан, адрес добавляется только для указанного порта. Если порт не указан, запись применяется ко всем портам. Функция фильтрации адресов dot1x работает с таблицей фильтруемых MAC-адресов, которая позволяет пользователю вручную добавлять фильтрующие dot1x-адреса в таблицу или удалять их из нее. Если порт указан в команде, то добавление адреса в таблицу выполняется только для этого порта. Если порт не указан, адрес добавляется для всех портов коммутатора. Когда функция фильтруемых dot1x адресов включена, коммутатор будет фильтровать проходящих аутентификацию пользователей, используя MAC-адреса. Будут приниматься только запросы аутентификации, инициированные пользователями, включенными в таблицу фильтруемых dot1x-адресов, остальные запросы будут отклоняться. "no" в начале команды удаляет адрес из таблицы фильтруемых адресов dot1x
Пример	Добавить MAC-адрес 00-01-34-34-2e-0a в таблицу фильтруемых адресов порта Ethernet 1/0/5. <pre>Switch(config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 1/0/5</pre>

11.3.2. Передача аутентификационных данных протокола EAP (dot1x eap enable)

Команда	[no] dot1x eap enable	
Параметр	none	Отсутствует
По умолчанию	Передача аутентификационных данных протокола EAP включена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает функцию передачи аутентификационных данных протокола EAP на коммутаторе. Коммутатор может быть соединен с RADIUS-сервером по протоколам Ethernet или PPP. Если между RADIUS-сервером и коммутатором существует Ethernet-соединение, коммутатору потребуется передача аутентификационной информации пользователя по протоколу EAP (аутентификация EAPoR). Если коммутатор подключен к RADIUS-серверу по PPP, коммутатор будет использовать локальное окончание аутентификации EAP (аутентификацию CHAP). В зависимости от соединения коммутатора с сервером аутентификации коммутатор использовать различные методы аутентификации. "no" в начале команды задает локальное окончание аутентификации	



Пример	Включить на коммутаторе локальное окончание аутентификации EAP. Switch(config)#no dot1x eap or enable

11.3.3. Включение функции 802.1x (dot1x enable)

Команда	[no] dot1x enable	
Параметр	none	Отсутствуют
По умолчанию	Функция 802.1x не включена в глобальном режиме конфигурации. Если функция 802.1x в глобальном режиме конфигурации включена, по умолчанию она не будет включена для портов	
Режим	Режим глобальной конфигурации, режим настройки портов	
Руководство по использованию	Включает функцию 802.1x на коммутаторе и портах. Для того, чтобы аутентификация 802.1x работала на соответствующих портах, она сначала должна быть включена для коммутатора. Если на порту подключено Spanning Tree или привязка MAC-адресов порт является магистральным портом или членом группы агрегации портов, функция 802.1x не может быть включена для этого порта, пока эти условия не будут устранены. "no" в начале команды выключает функцию 802.1x	
Пример	Включить функцию 802.1x на коммутаторе, затем включить 802.1x для порта 1/0/12. <pre>Switch(config)#dot1x enable Switch(config)#interface ethernet 1/0/12 Switch(config-if-ethernet1/0/12)#dot1x enable</pre>	

11.3.4. Функция транзитной пересылки на порту (dot1x ipv6 passthrough)

Команда	[no] dot1x ipv6 passthrough	
Параметр	none	Отсутствуют
По умолчанию	По умолчанию функция IPv6 passthrough (транзитной пересылки) на коммутаторе отключена	
Режим	Режим конфигурации порта	



Руководство по использованию	Включение функции IPv6 passthrough на порту коммутатора применимо только в режиме контроля доступа на основе пользователей. Эта функция может быть включена только в том случае, если функция 802.1x включена и глобально, и на порту, с режимом контролируемого доступа на основе пользователей. После ее включения пользователи могут отправлять сообщения IPv6 без прохождения проверки. "no" в начале команды отключает эту функцию
Пример	Включить функцию IPv6 passthrough на порту Ethernet1/0/12. <pre>Switch(config)#dot1x enable Switch(config)#interface ethernet 1/0/12 Switch(config-if-ethernet1/0/12)#dot1x enable Switch(config-if-ethernet1/0/12)#dot1x ipv6 passthrough</pre>

11.3.5. Гостевой VLAN на порту (dot1x guest-vlan)

Команда	dot1x guest-vlan <vlanid> no dot1x guest-vlan		
Параметр	vlanid	идентификатор заданного VLAN, диапазон значений от 1 до 4094	
По умолчанию	Функция 802.1x guest-vlan не включена на порту		
Режим	Режим конфигурации порта		
Руководство по использованию	Устанавливает для заданного порта гостевой vlan. Устройство доступа будет добавлять порт в гостевой VLAN, если нет клиентского устройства, успешно прошедшего аутентификацию в течение некоторого достаточно короткого времени из-за несовершенства собственной системы аутентификации этого клиентского устройства или слишком старой версии клиентского устройства. В гостевом VLAN пользователи могут получить программное обеспечение стандарта 802.1x для клиентского устройства, обновить систему клиентского устройства, либо обновить некоторые другие приложения (например, обновить антивирусное программное обеспечение, установить пакеты исправлений для операционной системы). Когда пользователь порта гостевого VLAN начинает аутентификацию, и она оканчивается неуспешно, порт будет оставаться в гостевом VLAN. Если аутентификация прошла успешно, возможны два результата: 1. Сервер аутентификации присваивает значение Auto VLAN, в результате порт покидает гостевой VLAN, чтобы войти в состав Auto VLAN. После того, как пользователь перейдет в автономный режим (offline), порт будет возвращен обратно заданному гостевому VLAN.		



	2. Сервер аутентификации назначает Auto VLAN, порт покидает гостевой VLAN, чтобы войти в состав Auto VLAN. После того, как пользователь перейдет в автономный режим (offline), порт будет снова закреплен за заданным гостевым VLAN. Внимание: На разных портах могут быть установлены различные гостевые VLAN, однако на одном порту допускается только один гостевой VLAN. Гостевой VLAN может работать только в том случае, если режим управления доступом основан на портах. Если режим управления доступом к порту основан на MAC-адресах или на пользователях, гостевой VLAN может быть успешно установлен, но будет неработоспособен. "no" в начале команды удаляет guest-vlan
Пример	Установить VLAN 10 в качестве гостевого для порта Ethernet1/0/3 <pre>Switch(config)#dot1x enable Switch(config)#interface ethernet 1/0/3 Switch(config-if-ethernet1/0/3)#dot1x guest-vlan 10</pre>

11.3.6. Функция фильтрации dot1x адресов (dot1x macfilter enable)

Команда	[no] dot1x macfilter enable	
Параметр	none	Отсутствуют
По умолчанию	Функция фильтрации dot1x адресов не включена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает функцию dot1x фильтрации адресов на коммутаторе. Когда функция фильтруемых dot1x адресов включена, коммутатор будет фильтровать проходящих аутентификацию пользователей, используя MAC-адреса. Будут приниматься только запросы аутентификации, инициированные пользователями, включенными в таблицу фильтруемых dot1x-адресов. "no" в начале команды выключает функцию фильтрации dot1x адресов	
Пример	Включить на коммутаторе функцию фильтрации dot1x адресов <pre>Switch(config)#dot1x macfilter enable</pre>	



11.3.7. Гостевой VLAN на основе MAC-аутентификации (dot1x macbased guest-vlan)

Команда	dot1x macbased guest-vlan <vlanid> no dot1x macbased guest-vlan	
Параметр	vlanid	идентификатор заданного VLAN, диапазон значений от 1 до 4094
По умолчанию	Функция 802.1x guest-vlan на основе MAC не включена на порту	
Режим	Режим конфигурации порта	
Руководство по использованию	Устанавливает для заданного порта гостевой vlan на основе MAC-аутентификации Если нет выделенного клиента аутентификации или версия клиента слишком старая и ни один клиент не прошел успешную аутентификацию на порту в течение определенного периода времени, устройство доступа подключит этого пользователя к гостевой VLAN. В гостевом VLAN пользователи могут получить программное обеспечение 802.1x, обновить систему клиентского устройства, либо обновить некоторые другие приложения (например, обновить антивирусное программное обеспечение, установить пакеты исправлений для операционной системы). Когда пользователь порта гостевого VLAN начинает аутентификацию, и она оканчивается неуспешно, порт будет оставаться в гостевом VLAN; если аутентификация прошла успешно, возможны два результата: 1. Сервер аутентификации присваивает значение Auto VLAN, в результате пользователь покидает гостевой VLAN и присоединяется к Auto VLAN. После того как пользователь перейдет в автономный режим, он снова будет возвращен в настроенную гостевую VLAN. 2. Сервер аутентификации не назначает VLAN, пользователь покидает гостевой VLAN и подключается к заданной изначальной VLAN. После того как пользователь перейдет в автономный режим, он снова будет возвращен в настроенную гостевую VLAN. Внимание: 1. dot1x macbased guest-vlan может быть настроен только на порту, работающем на mac-аутентификации, и в режиме HYBRID. 2. На разных портах могут быть установлены различные гостевые VLAN на основе MAC-аутентификации, однако на одном порту допускается только один такой гостевой VLAN. "no" в начале команды удаляет данный гостевой vlan	
Пример	Установить VLAN 10 в качестве гостевого для порта Ethernet1/0/3 <pre>Switch(config-if-ethernet1/0/3)#dot1x macbased guest-vlan 10</pre>	



11.3.8. Удаление пользователя, прошедшего сертификацию, если dot1x не работает (dot1x macbased port-down-flush)

Команда	[no] dot1x macbased port-down-flush	
Параметр	none	Отсутствуют
По умолчанию	По умолчанию команда не включена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет удалять аутентифицированных на порту пользователей, прошедших сертификацию, когда сертификация dot1x согласно MAC-адресу, не работает. Если пользователь, прошедший аутентификацию по MAC, переходит с одного порта на другой, его необходимо удалить для новой аутентификации. Для этого применяется данная команда. Команда, начинающаяся со слова «no», не выполняет операцию	
Пример	Удалить пользователя, прошедшего сертификацию dot1x , согласно MAC-адресу, если dot1x не работает. Switch(config)#dot1x macbased port-down-flush	

11.3.9. Число запросов EAP/кадров MD5 до повторной аутентификации (dot1x max-req)

Команда	dot1x max-req <count> no dot1x max-req	
Параметр	count	число раз повторных передач запроса EAP/ кадров MD5, в диапазоне от 1 до 10
По умолчанию	Задано максимальное число повторных передач, равное 2	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать число запросов/кадров MD5, посылаемых перед тем, как коммутатор повторно инициирует аутентификацию при получении ответа от клиентской системы. Рекомендуется использовать число повторных передач запроса EAP/кадров MD5, заданное по умолчанию. "no" в начале команды восстанавливает значение по умолчанию	
Пример	Изменить максимальное число повторных передач запроса EAP/кадров MD5, установить его равным 5. Switch(config)#dot1x max-req 5	



11.3.10. Разрешенное перемещение пользователя (dot1x user allow-movement)

Команда	[no] dot1x user allow-movement	
Параметр	none	Отсутствуют
По умолчанию	Отключение функции аутентификации после смены пользователем порта	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает функцию аутентификации, чтобы коммутатор позволил пользователю выполнить процесс аутентификации, когда пользователь меняет порт. Если коммутатор подключен к хабу, команда "dot1x user allow-movement" должна быть активирована, когда пользователь переключается на другой порт. "no" в начале команды отключает эту функцию	
Пример	Включить функцию аутентификации после выхода пользователя из порта. Switch(config)#dot1x user allow-movement	

11.3.11. Настройка общедоступного ресурса 802.1x (dot1x user free-resource)

Команда	dot1x user free-resource <prefix> <mask> no dot1x user free-resource	
Параметр	prefix	сегмент, в котором находится ограниченный ресурс
	mask	маска ограниченного ресурса, в десятично-точечном формате
По умолчанию	Общедоступный ресурс не задан	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать общедоступный ресурс 802.1x. Команда доступна только в том случае, если используется управление доступом на основе пользователей. Если используется такое управление доступом команда позволяет установить ограниченный ресурс, к которому могут иметь доступ не аутентифицированные пользователи. При управлении доступом на основе портов и MAC-адресов пользователи до окончания аутентификации не имеют доступа к ресурсам сети.	



	Если доступна система управления TrustView, свободный ресурс можно настроить на сервере TrustView, а сервер TrustView распространит конфигурацию на коммутаторы. Следует отметить, что для всей сети может быть настроен только один свободный ресурс. "no" в начале команды закрывает данную функцию
Пример	Задать сегмент с общедоступным ресурсом 1.1.1.0, маска 255.255.255.0. Switch(config)#dot1x user free-resource 1.1.1.0 255.255.255.0

11.3.12. Максимальное число пользователей с доступом к порту при управлении на основе MAC-адреса (dot1x max-user macbased)

Команда	dot1x max-user macbased <number> no dot1x max-user macbased	
Параметр	number	максимальное число пользователей, которым разрешено подключаться, в пределах от 1 до 256
По умолчанию	Задано максимальное число пользователей, равное 1	
Режим	Режим конфигурации порта	
Руководство по использованию	Позволяет задать максимальное число пользователей, которым разрешено подключаться к порту. Эта команда доступна для портов, на которых используется управление доступом на основе MAC-адресов. Если номер аутентифицированного MAC-адреса больше числа адресов, разрешенных пользователей, то пользователь с этим номером отвергается; остальные пользователи также не получают доступа к сети. "no" в начале команды восстанавливает значение по умолчанию	
Пример	Установить для порта 1/0/3 число разрешенных пользователей, равное 5. Switch(config-if-ethernet1/0/3)#dot1x max-user macbased 5	

11.3.13. Максимальное число пользователей с доступом к порту при управлении на основе пользователей (dot1x max-user userbased)

Команда	dot1x max-user userbased <number> no dot1x max-user userbased	
Параметр	number	максимальное число пользователей, которым разрешено подключаться, в пределах от 1 до 256
По умолчанию	Максимальное число пользователей, которым разрешен доступ, в каждом порту равно 10	



Режим	Режим конфигурации порта
Руководство по использованию	Позволяет задать максимальное число пользователей, которым разрешен доступ к указанному порту, когда используется режим управления доступом на основе пользователей Эта команда будет работать только тогда, когда на порту включен режим пользовательского управления доступом. Если число аутентифицированных пользователей превышает максимальное число пользователей, которым может быть разрешен доступ к сети, то эти дополнительные пользователи не будут иметь доступа к сети. "no" в начале команды восстанавливает значение по умолчанию
Пример	Установить для порта 1/0/3 число разрешенных пользователей, равное 5. <pre>Switch(config-if-ethernet1/0/3)#dot1x max-user userbased 5</pre>

11.3.14. Включение режима аутентификации единственного пользователя на порту (dot1x portbased mode single-mode)

Команда	[no] dot1x portbased mode single-mode	
Параметр	none	Отсутствуют
По умолчанию	Режим аутентификации единственного пользователя на порту выключен	
Режим	Режим конфигурации порта	
Руководство по использованию	Устанавливает режим "portbase" аутентификации единственного пользователя. Эта команда работает, когда режим доступа порта установлен как "portbase only". Перед настройкой аутентификации единственного пользователя, если на порту включена команда "dot1x port-method portbased" и есть подключённые пользователи, коммутатор принудительно отключит этих пользователей. После этого данный порт только одному пользователю разрешается аутентифицироваться на этом порту, этот пользователь получит доступ к указанным сетевым ресурсам, а другим аутентифицированным пользователям на этом порту доступ к сети будет запрещен. После отключения режима "single-mode", коммутатор также принудительно отключит аутентифицированного пользователя от сети. "no" перед началом команды отключает эту функцию	
Пример	Установить для порта 1/0/1, основанного на режиме аутентификации порта, режим аутентификации единственного пользователя. <pre>Switch(config-if-ethernet1/0/1)#dot1x portbased mode single-mode</pre>	



11.3.15. Задать состояние аутентификации 802.1x (dot1x port-control)

Команда	dot1x port-control {auto force-authorized force-unauthorized} no dot1x port-control	
Параметр	auto	включает аутентификацию 802.1x, состояние авторизации порта определяется информацией аутентификации, обмен которой идет между коммутатором и клиентской системой
	force-authorized	устанавливает для порта состояние авторизации, не аутентифицированным пользователям не разрешается проходить через порт
	force-unauthorized	для порта будет задан неавторизованный режим, коммутатор не будет выполнять аутентификацию клиентской системы, прохождение данных через порт запрещено
По умолчанию	Когда функция 802.1x включена для порта, по умолчанию установлен параметр "auto"	
Режим	Режим конфигурации порта	
Руководство по использованию	Позволяет задать состояние аутентификации 802.1x Если порту необходимо обеспечивать аутентификацию 802.1x для пользователя, режим аутентификации порта должен быть установлен на auto. "no" в начале команды восстанавливает значение по умолчанию	
Пример	Установить на порту 1/0/1 запрос режима аутентификации 802.1x Switch(config-if-ethernet1/0/1)#dot1x port-control auto	

11.3.16. Метод управления доступом к указанному интерфейсу (dot1x port-method)

Команда	dot1x port-method {macbased portbased userbased {standard advanced}} no dot1x port-method	
Параметр	macbased	устанавливает метод управления доступом на основе MAC-адресов
	portbased	устанавливает метод управления доступом на основе портов



	userbased	устанавливает метод управления доступом на основе пользователей. Метод имеет два вида - стандартное и расширенное управление доступом
	standard	Стандартный метод контроля доступа на основе пользователя
	advanced	Расширенный контроль доступа на основе пользователей
По умолчанию	Расширенное управление доступом на основе пользователей	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда используется для установки метода аутентификации dot1x для указанного порта. При управлении доступом на основе портов, допускается аутентификация только одного хоста. После аутентификации хосту будут доступны все сетевые ресурсы. При управлении доступом на основе MAC-адресов допускается аутентификация многих хостов, подключенных к одному и тому же порту. Когда применяются методы управления доступом, упомянутые выше, не аутентифицированным хостам недоступны никакие сетевые ресурсы. Если используется метод управления доступом на основе пользователей, пользователям могут быть доступны только ограниченные ресурсы сети. Метод управления доступом на основе пользователей имеет два вида – стандартное управление доступом и расширенное управление доступом. При стандартном управлении доступом, когда хост еще не аутентифицирован, он имеет неограниченный доступ к ограниченным ресурсам сети. При расширенном управлении доступом, когда хост еще не аутентифицирован, может осуществляться управление доступом к ограниченным ресурсам сети. <u>ПРИМЕЧАНИЕ:</u> Для стандартного управления на основе пользователей сначала должны быть сконфигурированы общедоступные ресурсы 802.1x "no" в начале команды восстанавливает управление доступом по умолчанию	
Пример	Включить метод управления доступом на основе портов на порту Ethernet1/0/4. <pre>Switch(config-if-ethernet1/0/4)#dot1x port-method portbased</pre>	



11.3.17. Принудительная аутентификация с использованием частного протокола аутентификации 802.1x (dot1x privateclient enable)

Команда	[no] dot1x privateclient enable	
Параметр	none	Отсутствуют
По умолчанию	Частный формат пакетов аутентификации 802.1x по умолчанию отключен	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает на коммутаторе режим принудительной аутентификации клиента с использованием частного протокола аутентификации 802.1x. Для реализации интегрированного решения коммутатор должен быть включен для использования частного протокола 802.1x, иначе многие приложения не смогут работать. Дополнительные сведения см. в разделе Интегрированные решения DCBI. Если коммутатор заставляет клиентов аутентификации использовать частный протокол 802.1x, стандартные клиенты работать не будут. "no" в начале команды выключает режим принудительной аутентификации клиента и возобновляет использование стандартного протокола аутентификации 802.1x	
Пример	Включить на коммутаторе режим принудительной аутентификации клиента с использованием частного протокола аутентификации 802.1x, Switch(config)#dot1x privateclient enable	

11.3.18. Включить защиту частного клиента (dot1x privateclient protect enable)

Команда	[no] dot1x privateclient protect enable	
Параметр	none	Отсутствуют
По умолчанию	Функция защиты частного клиента на коммутаторе отключена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает функцию защиты privateclient на коммутаторе. Поддерживает частичное шифрование протокола privateclient для повышения безопасности privateclient. "no" в начале команды отключает функцию защиты	



Пример	Включить функцию защиты privateclient на коммутаторе. Switch(config)#dot1x privateclient protect enable

11.3.19. Повторная аутентификация реального времени (dot1x re-authenticate)

Команда	dot1x re-authenticate [interface <interface-name>]	
Параметр	interface-name	номер порта, если этот параметр отсутствует, то одно и то же значение параметра действует для всех портов
По умолчанию	Отсутствует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает повторную аутентификацию 802.1x реального времени (не требующую ожидания) на всех портах, либо на указанном порту. Команда позволяет коммутатору провести повторную аутентификацию клиента без ожидания истечения времени таймера повторной аутентификации. После выполнения аутентификации эта команда не работает	
Пример	Включить повторную аутентификацию реального времени на порту 1/0/8. Switch(config)#dot1x re-authenticate interface ethernet 1/0/8	

11.3.20. Периодическая аутентификация клиентской системы (dot1x re-authentication)

Команда	[no] dot1x re-authentication	
Параметр	none	Отсутствуют
По умолчанию	Периодическая аутентификация клиентской системы не включена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает периодическую аутентификацию клиентской системы. Когда включена периодическая аутентификация клиентской системы, коммутатор будет через регулярные интервалы времени выполнять повторную аутентификацию клиентской системы. Эта функция не рекомендуется для широкого использования. "no" перед началом команды отключает эту функцию	



Пример	Включить периодическую повторную аутентификацию аутентифицированных пользователей. Switch(config)#dot1x re-authentication

11.3.21. Время бездействия при сбое аутентификации клиентской системы (dot1x timeout quiet-period)

Команда	dot1x timeout quiet-period <seconds> no dot1x timeout quiet-period	
Параметр	seconds	время бездействия на порту в секундах, в пределах от 1 до 65535
По умолчанию	10 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать время бездействия в порту при сбое аутентификации клиентской системы. Рекомендуется использовать значение, заданное по умолчанию. "no" в начале команды восстанавливает значение по умолчанию	
Пример	Установить время бездействия 120 секунд. Switch(config)#dot1x timeout quiet-period 120	

11.3.22. Интервал времени для повторной аутентификации клиентской системы (dot1x timeout re-authperiod)

Команда	dot1x timeout re-authperiod <seconds> no dot1x timeout re-authperiod	
Параметр	seconds	интервал времени повторной аутентификации в секундах, в диапазоне от 1 до 65535
По умолчанию	3600 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать интервал времени, по истечении которого выполняется повторная аутентификация запрашивающего устройства. Для того, чтобы стало возможно изменять интервал времени повторной аутентификации клиентской системы, предварительно должна быть включена повторная аутентификация dot1x. Если аутентификация не включена на коммутаторе, команда изменения интервала времени повторной аутентификации клиентской системы работать не будет. "no" в начале команды восстанавливает значение по умолчанию	



Пример	Задать время повторной аутентификации 1200 секунд. Switch(config)#dot1x timeout re-authperiod 1200

11.3.23. Повторная передача запроса/кадра идентичности EAP (dot1x timeout tx-period)

Команда	dot1x timeout tx-period <seconds> no dot1x timeout tx-period	
Параметр	seconds	интервал времени повторной передачи кадров с запросами EAP в секундах, в диапазоне от 1 до 65535 секунд
По умолчанию	30 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать интервал времени, по истечении которого запрашивающее устройство выполняет повторную передачу запроса/кадра идентичности EAP. Рекомендуется использовать значение, заданное по умолчанию. "no" в начале команды восстанавливает значение по умолчанию. "no" в начале команды восстанавливает значение по умолчанию	
Пример	Установить интервал времени повторной передачи кадров с запросами EAP 1200 секунд. Switch(config)#dot1x timeout tx-period 1200	

11.3.24. Включение функции dot1x (dot1x unicast enable)

Команда	[no] dot1x unicast enable	
Параметр	отсутствуют	Отсутствуют
По умолчанию	Функция 802.1x unicast passthrough не включена в глобальном режиме	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает функцию прозрачной передачи unicast 802.1x коммутатора. Функция прозрачной передачи аутентификации 802.1x должна быть включена прежде, чем будет включена функцию прозрачной передачи unicast 802.1x, а затем выполняется настройка функции 802.1x. "no" в начале команды отключает эту функцию	



Пример	Включить на коммутаторе функцию прозрачной передачи unicast 802.1x и подключить 802.1x для порта 1/0/1. <pre>Switch(config)#dot1x enable Switch(config)# dot1x unicast enable Switch(config)#interface ethernet1/0/1 Switch(Config-If-Ethernet1/0/1)#dot1x enable</pre>

11.3.25. Вывод информации о параметрах dot1x (show dot1x)

Команда	show dot1x [interface <interface-list>]	
Параметр	interface-list	список портов. Если параметры не заданы, отображается информация для всех портов
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, Привилегированный режим	
Руководство по использованию	Выводит на дисплей информацию, связанную с параметрами dot1x, если информация о параметрах добавлена, отображается соответствующий статус dot1x для соответствующего порта	
Пример	Вывести на экран информацию о глобальном параметре dot1x для коммутатора. <pre>Switch#show dot1x Global 802.1x Parameters reauth-enabled no reauth-period 3600 quiet-period 10 tx-period 30 max-req 2 authenticator mode passive</pre> Mac Filter Disable MacAccessList : <pre>dot1x-EAPoR Enable dot1x-privateclient Disable dot1x-unicast Disable 802.1x is enabled on ethernet Ethernet1/0/1 Authentication Method: Port based Max User Number: 1 Status Authorized Port-control Auto SupPLICant 00-03-0F-FE-2E-D3</pre> Authenticator State Machine State Authenticated Backend State Machine	



	State Idle Reauthentication State Machine State Stop

11.4. Команды ограничения количества MAC- и IP-адресов на порту и VLAN

11.4.1. Максимальное количество ARP записей на интерфейсе (ip arp dynamic maximum)

Команда	ip arp dynamic maximum <value> no ip arp dynamic maximum	
Параметр	value	верхний предел количества динамических ARP записей в VLAN, в диапазоне от 1 до 4096
По умолчанию	Функция ограничения количества динамических ARP в VLAN отключена	
Режим	Режим настройки VLAN	
Руководство по использованию	Команда позволяет задать максимальное количество динамических ARP записей, разрешенных в VLAN, и одновременно включить функцию ограничения количества динамических ARP записей в VLAN. При настройке максимального количества динамических ARP записей в VLAN, если количество распознанных интерфейсом динамических ARP записей в VLAN уже превышает установленное максимальное количество, лишние динамические ARP записи будут удалены. Команда с "no" в начале используется для отключения функции ограничения количества динамических ARP записей в VLAN	
Пример	Включить функцию ограничения числа динамических ARP записей в VLAN 1, задать максимальное количество равное 50. <pre>Switch(config)#interface vlan1 Switch(config-if-vlan1)# ip arp dynamic maximum 50</pre>	

11.4.2. Максимальное количество ND записей на интерфейсе (ipv6 nd dynamic maximum)

Команда	ipv6 nd dynamic maximum <value> no ipv6 nd dynamic maximum	
Параметр	value	верхний предел количества динамических NEIGHBOR записей в VLAN, в диапазоне от 1 до 4096
По умолчанию	Функция ограничения количества динамических NEIGHBOR записей в VLAN отключена	



Режим	Режим настройки VLAN
Руководство по использованию	Команда позволяет задать максимальное количество динамических NEIGHBOR записей, разрешенных в VLAN, и одновременно включить функцию ограничения количества динамических NEIGHBOR записей в VLAN. При настройке максимального количества разрешенных динамических NEIGHBOR записей в VLAN, если количество распознанных интерфейсом динамических NEIGHBOR записей в VLAN уже превышает установленное максимальное количество, лишние динамические NEIGHBOR записи будут удалены. Команда с "no" в начале используется для отключения функции ограничения количества динамических NEIGHBOR записей в VLAN
Пример	Включить функцию ограничения числа динамических NEIGHBOR записей в VLAN 1, задать максимальное количество равное 50. <pre>Switch(config)#interface vlan1 Switch(config-if-vlan1)# ipv6 nd dynamic maximum 50</pre>

11.4.3. Просмотр текущего количества ARP записей (show arp-dynamic count)

Команда	show arp-dynamic count {vlan interface ethernet <portName>}										
Параметр	vlan	ID указанной vlan									
	portName	имя порта уровня-2									
По умолчанию	Не задано										
Режим	Режим глобальной конфигурации, привилегированный режим										
Руководство по использованию	Позволяет вывести на экран количество динамических ARP записей соответствующего порта и VLAN										
Пример	Показать количество динамических ARP записей для порта и VLAN, для которых задана функция ограничения количества ARP записей. <pre>Switch(config)# show arp-dynamic count interface ethernet 1/0/3</pre> <table> <tr> <td>Port</td> <td>MaxCount</td> <td>CurrentCount</td> </tr> <tr> <td>Ethernet1/0/3</td> <td>5</td> <td>1</td> </tr> </table> <pre>Switch(config)# show arp-dynamic count vlan 1</pre> <table> <tr> <td>Vlan</td> <td>MaxCount</td> <td>CurrentCount</td> </tr> </table>		Port	MaxCount	CurrentCount	Ethernet1/0/3	5	1	Vlan	MaxCount	CurrentCount
Port	MaxCount	CurrentCount									
Ethernet1/0/3	5	1									
Vlan	MaxCount	CurrentCount									



	1	55	15

11.4.4. Просмотр текущего количества MAC-адресов (show mac-address dynamic count)

Команда	show mac-address dynamic count { vlan interface ethernet <portName> }													
Параметр	vlan	VLAN ID												
	portName	имя порта уровня-2												
По умолчанию	Не задано													
Режим	Режим глобальной конфигурации, привилегированный режим													
Руководство по использованию	Позволяет вывести на экран количество динамических MAC-адресов соответствующего порта и VLAN													
Пример	Показать количество динамических MAC-адресов для порта и VLAN, для которых задана функция ограничения количества MAC-адресов. <pre>Switch(config)# show mac-address dynamic count interface ethernet 1/0/3</pre> <table> <tr> <td>Port</td> <td>MaxCount</td> <td>CurrentCount</td> </tr> <tr> <td>Ethernet1/0/3</td> <td>5</td> <td>1</td> </tr> </table> <pre>Switch(config)# show mac-address dynamic count vlan 1</pre> <table> <tr> <td>Vlan</td> <td>MaxCount</td> <td>CurrentCount</td> </tr> <tr> <td>1</td> <td>55</td> <td>15</td> </tr> </table>		Port	MaxCount	CurrentCount	Ethernet1/0/3	5	1	Vlan	MaxCount	CurrentCount	1	55	15
Port	MaxCount	CurrentCount												
Ethernet1/0/3	5	1												
Vlan	MaxCount	CurrentCount												
1	55	15												

11.4.5. Просмотр текущего количества ND записей (show nd-dynamic count)

Команда	show nd-dynamic count { vlan interface ethernet <portName> }	
Параметр	vlan	VLAN ID
	portName	имя порта уровня-2
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, привилегированный режим	
Руководство по использованию	Позволяет вывести на экран количество динамических ND записей соответствующего порта и VLAN	



Пример	Показать количество динамических ND записей для порта и VLAN, для которых задана функция ограничения количества ND записей.		
	Switch(config)# show nd-dynamic dynamic count interface ethernet 1/0/3		
	Port	MaxCount	CurrentCount
	Ethernet1/0/3	5	1
	Switch(config)# show nd-dynamic dynamic count vlan 1		
	Vlan	MaxCount	CurrentCount
	1	55	15

11.4.6. Включить функцию ограничения количества динамических ARP записей (switchport arp dynamic maximum)

Команда	switchport arp dynamic maximum <value> no switchport arp dynamic maximum	
Параметр	value	верхний предел количества динамических ARP записей на порту, в диапазоне от 1 до 4096
По умолчанию	Функция ограничения количества динамических ARP записей на порту отключена	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда позволяет задать максимальное количество динамических ARP записей, разрешенных в порту, и одновременно включить функцию ограничения количества динамических ARP записей на порту. При настройке максимального количества динамических ARP записей на порту, если количество распознанных интерфейсом динамических ARP записей на порту уже превышает установленное максимальное количество, лишние динамические ARP записи будут удалены. Магистральные порты не поддерживают данную функцию. Команда с "no" в начале используется для отключения функции ограничения количества динамических ARP записей на порту	
Пример	Включить функцию ограничения числа динамических ARP записей в порту 1/0/2, задать максимальное количество равное 20. Switch(config)#interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)# switchport arp dynamic maximum 20	



11.4.7. Включить функцию ограничения количества динамических MAC-адресов (switchport mac-address dynamic maximum)

Команда	switchport mac-address dynamic maximum <value> no switchport mac-address dynamic maximum	
Параметр	value	верхний предел количества динамических MAC-адресов порта, в диапазоне от 1 до 4096
По умолчанию	Функция ограничения количества динамических MAC-адресов на порту отключена	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда позволяет задать максимальное количество динамических MAC-адресов, разрешенных в порту, и одновременно включить функцию ограничения количества динамических MAC-адресов на порту. При настройке максимального количества динамических MAC-адресов на порту, если количество распознанных интерфейсом динамических MAC-адресов на порту уже превышает установленное максимальное количество, лишние динамические MAC-адресов будут удалены. Эта функция является взаимоисключающей с dot1x, MAC bonding и т. д. и не разрешается, если на порту включены dot1x, MAC bonding или TRUNK. Команда с "no" в начале используется для отключения функции ограничения количества динамических MAC-адресов на порту	
Пример	Включить функцию ограничения числа динамических MAC-адресов в порту 1/0/2, задать максимальное количество равное 20. <pre>Switch(config)#interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)# switchport mac-address dynamic maximum 20</pre>	

11.4.8. Задать действие при нарушении безопасности (switchport mac-address violation)

Команда	switchport mac-address violation {protect shutdown} [recovery <5-3600>] no switchport mac-address violation	
Параметр	protect	режим защиты
	shutdown	режим отключения



	recovery	задает автоматическое восстановление первоначального состояния пограничного порта после режима shutdown
	<5-3600>	период, по истечении которого будет восстановлено первоначальное состояние, по умолчанию не восстанавливается
По умолчанию	Порт находится в безопасном режиме	
Режим	Режим конфигурации порта	
Руководство по использованию	Позволяет установить действия при нарушении безопасности. Порт переходит в режим нарушения безопасности только если включена функция ограничения числа MAC-адресов. Если установлен параметр "protect" порт будет отключать изучение динамических MAC-адресов, когда количество MAC-адресов порта превышает верхний предел безопасных MAC-адресов. Если задан параметр действий "shutdown", при превышении предельного количества безопасных MAC-адресов порт будет отключен, и пользователь сможет включить порт, вручную введя команду "no shutdown" или задав таймаут автоматического восстановления. Команда с no в начале восстанавливает действие при нарушении на "protect"	
Пример	Установить для порта 1 действие при нарушении безопасности на shutdown, время восстановления 60 секунд. <pre>Switch(config)#interface ethernet 1/0/1</pre> <pre>Switch(config-if-ethernet1/0/1)# switchport mac-address violation shutdown recovery 60</pre>	

11.4.9. Включить функцию ограничения количества динамических ND-записей (switchport nd dynamic maximum)

Команда	switchport nd dynamic maximum <value> no switchport nd dynamic maximum	
Параметр	value	верхний предел количества динамических NEIGHBOR записей в порту, в диапазоне от 1 до 4096
По умолчанию	Функция ограничения количества динамических ARP записей на порту отключена	
Режим	Режим конфигурации порта	



Руководство по использованию	Команда позволяет задать максимальное количество динамических ARP записей, разрешенных в порту, и одновременно включить функцию ограничения количества динамических NEIGHBOR записей на порту. При настройке максимального количества динамических NEIGHBOR записей на порту, если количество распознанных интерфейсом динамических NEIGHBOR записей на порту уже превышает установленное максимальное количество, лишние динамические NEIGHBOR записи будут удалены. Магистральные порты не поддерживают данную функцию. Команда с "no" в начале используется для отключения функции ограничения количества динамических NEIGHBOR записей на порту
Пример	Включить функцию ограничения числа динамических NEIGHBOR записей в порту 1/0/2, задать максимальное количество равное 20. <pre>Switch(config)#interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)# switchport nd dynamic maximum 20</pre>

11.4.10. Задать максимальное количество MAC-адресов (vlan mac-address dynamic maximum)

Команда	vlan mac-address dynamic maximum <value> no vlan mac-address dynamic maximum	
Параметр	value	верхний предел количества динамических MAC-адресов VLAN, в диапазоне от 1 до 4096
По умолчанию	Функция ограничения количества динамических MAC-адресов в VLAN отключена	
Режим	Режим настройки VLAN	
Руководство по использованию	Команда позволяет задать максимальное количество динамических MAC-адресов, разрешенных в порту, и одновременно включить функцию ограничения количества динамических MAC-адресов в VLAN. При настройке максимального количества динамических MAC-адресов в VLAN, если количество распознанных интерфейсом динамических MAC-адресов в VLAN уже превышает установленное максимальное количество, лишние динамические MAC-адресов будут удалены. После включения функции ограничения количества динамических MAC-адресов в VLAN, ограничение количества MAC-адресов применяется только к общему порту доступа, количество MAC-адресов на портах TURNK и специальных портах, на которых включена функция dot1x, MAC binding, не будет ограничиваться или учитываться. Команда с "no" в начале используется для отключения функции ограничения количества динамических MAC-адресов в VLAN	



Пример	Включить функцию ограничения числа динамических MAC-адресов в в VLAN 1, задать максимальное количество равное 50. <pre>Switch(config)#vlan1 Switch(config-if-vlan1)#vlan mac-address dynamic maximum 50</pre>

11.5. Команды для настройки управления доступом (AM)

11.5.1. Включить функцию AM (am enable)

Команда	[no] am enable	
Параметр	none	отсутствует
По умолчанию	По умолчанию функция AM выключена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает или выключает функцию AM в режиме глобальной конфигурации. Команда с "no" в начале отключает функцию AM	
Пример	Включить функцию AM на коммутаторе. <pre>Switch(config)#am enable</pre>	

11.5.2. Включить функцию AM на порту (am port)

Команда	[no] am port	
Параметр	none	отсутствует
По умолчанию	Функция AM выключена на всех портах	
Режим	Режим конфигурации порта	
Руководство по использованию	Включает или выключает функцию AM для портов. "no" в начале команды отключает функцию AM на порту	
Пример	Включить функцию AM на интерфейсе 1/0/3 коммутатора. <pre>Switch(config-if-ethernet 1/0/3)#am port</pre>	



11.5.3. Настроить записи в IP-таблице (am ip-pool)

Команда	[no] am ip-pool <ip-address> <num>	
Параметр	ip-address	начальный адрес сегмента адресов в пуле IP-адресов
	num	число последовательных адресов, следующих за начальным ip-адресом, меньшее или равное 32
По умолчанию	Пул IP-адресов пуст	
Режим	Режим конфигурации порта	
Руководство по использованию	Позволяет задать сегмент IP-адресов АМ для интерфейса, разрешить или запретить передачу IP- или APR-сообщений от IP-источника в этом сегменте, которые могут передаваться через интерфейс. "no" в начале команды удаляет настройки	
Пример	Настроить интерфейс 1/0/3 таким образом, чтобы передавались все пакеты от 10 источников, IP-адреса которых берутся последовательно, начиная с адреса 10.10.10.1. Switch(config-if-ethernet 1/0/3)#am ip-pool 10.10.10.1 10	

11.5.4. Настроить MAC-IP в таблице разрешения доступа АМ (am mac-ip-pool)

Команда	[no] am mac-ip-pool <mac-address> <ip-address>	
Параметр	mac-address	MAC-адрес источника
	ip-address	IP-адрес источника пакетов, 32-разрядное двоичное число, представленное четырьмя десятичными числами
По умолчанию	Пул MAC-IP-адресов пуст	
Режим	Режим конфигурации порта	
Руководство по использованию	Позволяет задать АМ MAC-IP-адрес для интерфейса, разрешить или запретить передачу IP- или APR-сообщений от IP-источника в этом сегменте, которые могут передаваться через интерфейс. "no" в начале команды удаляет настройки	



Пример	Настроить коммутатор так, чтобы через интерфейс 1/0/3 передавались пакеты от источника с MAC-адресом 11-22-22-11-11-11 и от источника с IP-адресом 10.10.10.1. <pre>Switch(config-if-ethernet 1/0/3)#am mac-ip-pool 11-22-22-11-11-11 10.10.10.1</pre>

11.5.5. Удалить записи таблицы AM (no am all)

Команда	no am all [ip-pool mac-ip-pool]	
Параметр	ip-pool	пул IP-адресов
	mac-ip-pool	пул mac-ip-адресов
По умолчанию	Оба пула адресов изначально пусты	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Удаляет все пользовательские настройки для таблиц MAC-IP-пула и IP-пула	
Пример	Очистить все адреса в IP-пуле. <pre>Switch(config)#no am all ip-pool</pre>	

11.5.6. Просмотр информации о настроенной функции AM (show am)

Команда	show am [interface <interface-name>]	
Параметр	interface-name	имя интерфейса, настройки которого будут выведены на дисплей
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, привилегированный режим	
Руководство по использованию	Вывести на дисплей все настройки адресов AM. Параметр "no" означает отображение информации о конфигурации AM для всех интерфейсов	



Пример	Вывести на дисплей все настройки адресов AM. <pre>Switch#show am interface ethernet 1/0/5</pre> AM is enabled Interface Etherne1/0/5 <pre>am interface am ip-pool 50.10.10.1 30 am mac-ip-pool 00-02-04-06-08-09 20.10.10.5 am ip-pool 50.20.10.1 20</pre>

11.6. Конфигурация функций предотвращения атак

11.6.1. Функция предотвращения атаки IP-spoofing (dosattack-check srcip-equal-dstip enable)

Команда	[no] dosattack-check srcip-equal-dstip enable	
Параметр	none	Отсутствует
По умолчанию	Функция, с помощью которой коммутатор проверяет, равен ли IP-адрес источника IP-адресу назначения отключена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда подключает на коммутаторе функцию проверки совпадения IP-адреса источника и IP-адреса назначения. Если эта функция включена, пакеты, IP-адрес источника которых равен IP-адресу назначения, будут отбрасываться. “no” в начале команды отключает функцию	
Пример	Отбросить пакет данных, IP-адрес источника которого равен адресу назначения. <pre>Switch(config)# dosattack-check srcip-equal-dstip enable</pre>	

11.6.2. Функция предотвращения атаки TCP unauthorized label (dosattack-check tcp-flags enable)

Команда	[no] dosattack-check srcip-equal-dstip enable	
Параметр	none	Отсутствует
По умолчанию	Эта функция на коммутаторе отключена	
Режим	Режим глобальной конфигурации	



Руководство по использованию	При включении этой функции коммутатор будет проверять наличие несанкционированных TCP-меток. Если эта функция включена, коммутатор сможет отбрасывать следующие четыре пакета данных, содержащие несанкционированные TCP-метки: SYN=1, когда порт источника меньше 1024; позиции метки TCP все равны 0, а ее порядковый номер =0; FIN=1, URG=1, PSH=1 и порядковый номер TCP =0; SYN=1 и FIN=1. Эта функция работает в сочетании с командой “dosattack-check ipv4-first-fragment enable”. Команда с “no” в начале отключает данную функцию
Пример	Отбросить один или несколько типов из перечисленных выше четырех типов пакетов. Switch(config)# dosattack-check tcp-flags enable

11.6.3. Функция предотвращения атаки подмены порта (dosattack-check srcport-equal-dstport enable)

Команда	[no] dosattack-check srcport-equal-dstport enable	
Параметр	none	отсутствует
По умолчанию	Функция, при которой коммутатор имеет возможность проверять, равен ли порт источника порту назначения отключена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	При включении этой функции коммутатор будет проверять, равен ли порт источника порту назначения. Если эта функция включена, коммутатор сможет отбрасывать TCP- и UDP-пакеты данных, порт назначения которых равен порту источника. Эта функция может использоваться в сочетании с функцией “dosattack-check ipv4-first-fragment enable” для блокирования TCP- и UDP-пакетов данных IPv4-фрагментов, порт назначения которых равен порту источника. “no” перед началом команды отключает эту функцию	
Пример	Отбрасывать нефрагментированные TCP- и UDP-пакеты данных, порт назначения которых равен порту источника. Switch(config)# dosattack-check srcport-equal-dstport enable	



11.7. Команды для настройки протокола TACACS+

11.7.1. Параметры обращения к серверу TACACS+ (tacacs-server authentication host)

Команда	tacacs-server authentication host <ip-address> [port <port-number>][timeout <seconds>] [key {0 7} <string>] [primary] no tacacs-server authentication host <ip-address>	
Параметр	ip-address	IP-адрес сервера
	port-number	номер порта прослушивания сервера, в пределах от 0 до 65535. 0 означает, что прослушивание на сервере аутентификации не выполняется
	seconds	значение таймера аутентификации TACACS+, в диапазоне от 1 до 60 секунд
	string	строка ключа. Если для параметра key установлен 0, ключ не шифруется и его диапазон не должен превышать 64 символов, если для параметра key установлено 7, ключ шифруется и его диапазон не должен превышать 64 символов
	primary	указывает, что сервер является первичным
По умолчанию	Аутентификация TACACS+ в системе не включена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда используется для указания IP-адреса, номера порта, таймера и строки ключа сервера TACACS+, которые используются при аутентификации на коммутаторе. Параметр port определяет номер порта аутентификации, который должен совпадать с номером порта, указанным для сервера TACACS+ (по умолчанию равен 49). Параметры key и timeout используются для установки собственного ключа и таймера коммутатора. Если эти параметры не заданы, будут использованы таймер и ключ, заданные в режиме глобальной конфигурации для tacacs-сервера: timeout<seconds> и tacacs-server key <string>. С помощью этой команды можно сконфигурировать несколько TACACS+ серверов, связывающихся с коммутатором. Последовательность настройки такая же, как и для сервера аутентификации. Если для TACACS+ сервера задана опция primary, сервер будет первичным "по" в начале команды удаляет сервер аутентификации TACACS+	



Пример	Задать адрес сервера аутентификации TACACS+ равным 192.168.1.2 и использовать ключ, заданный в режиме глобальной конфигурации. Switch(config)#tacacs-server authentication host 192.168.1.2

11.7.2. Задать ключ сервера TACACS+ (tacacs-server key)

Команда	tacacs-server key {0 7} <string> no tacacs-server key	
Параметр	string	символьная строка ключа сервера TACACS+. Если для параметра key установлен 0, ключ не шифруется и его диапазон не должен превышать 64 символов, если для параметра key установлено 7, ключ шифруется и его диапазон не должен превышать 64 символов
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать ключ сервера аутентификации TACACS+. Ключ используется для криптозащиты связи коммутатора с TACACS+ сервером. Заданный ключ должен соответствовать одному из ключей, установленных на TACACS+ сервере, в противном случае аутентификация будет выполняться некорректно. Для гарантии безопасности данных рекомендуется задавать ключ аутентификации сервера. "no" в начале команды удаляет ключ сервера TACACS+	
Пример	Установить в качестве ключа TACACS+-сервера аутентификации слово qtech. Switch(config)#tacacs-server key 0 qtech	

11.7.3. Настроить IP-адрес источника для отправляемых TACACS+ пакетов (tacacs-server nas-ipv4)

Команда	tacacs-server nas-ipv4 <ip-address> no tacacs-server nas-ipv4	
Параметр	ip-address	IP-адрес источника пакетов TACACS+ в десятичном представлении с точками, это должен быть корректный одноадресный IP-адрес
По умолчанию	По умолчанию IP-адрес источника для пакета TACACS+ не задается, в качестве IP-адреса источника пакета TACACS+ используется IP-адрес интерфейса, с которого отправляются пакеты TACACS+	



Режим	Режим глобальной конфигурации
Руководство по использованию	Позволяет задать IP-адрес источника для TACACS+ пакетов, отправляемых коммутатором. IP-адрес источника должен принадлежать одному из IP-интерфейсов коммутатора, в противном случае при отправке коммутатором пакета TACACS+ придет сообщение об ошибке привязки IP-адреса. Рекомендуется использовать IP-адрес интерфейса loopback в качестве исходного IP-адреса, чтобы избежать отбрасывания пакетов сервера TACACS+ при прерывании соединения интерфейса. "no" в начале команды удаляет настройку
Пример	Установить ip-адрес источника пакета TACACS+ как 192.168.2.254. <pre>Switch(config)#tacacs-server nas-ipv4 192.168.2.254</pre>

11.7.4. Время таймера для сервера TACACS+ (tacacs-server timeout)

Команда	tacacs-server timeout <seconds> no tacacs-server timeout	
Параметр	seconds	значение таймера аутентификации TACACS+, в диапазоне от 1 до 60 секунд
По умолчанию	3 секунды	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет настроить для сервера TACACS+ время таймера. Команда позволяет задать время ожидания коммутатором окончания аутентификации на сервере TACACS+. После подключения к TACACS+ и отправки на сервер пакета данных с запросом аутентификации коммутатор ожидает ответа сервера. Если в течение указанного периода времени ответ не принят, аутентификация считается безуспешной. "no" в начале команды восстанавливает настройки по умолчанию	
Пример	Установить таймер для tacacs+ сервера на 30 секунд. <pre>Switch(config)#tacacs-server timeout 30</pre>	



11.8. Команды для настройки протокола RADIUS

11.8.1. Включить функцию AAA (aaa enable)

Команда	[no] aaa enable	
Параметр	none	отсутствует
По умолчанию	AAA аутентификация не включена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает функцию аутентификации AAA на коммутаторе. Для того, чтобы аутентификация AAA работала, надо включить на коммутаторе аутентификацию IEEE 802.1x "no" в начале команды выключает функцию аутентификации AAA	
Пример	Включить функцию AAA коммутатора. Switch(config)#aaa enable	

11.8.2. Включить учет сетевых сервисов (aaa-accounting enable)

Команда	[no] aaa-accounting enable	
Параметр	none	Отсутствует
По умолчанию	Функция "AAA accounting" не включена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает на коммутаторе функцию учета AAA accounting. Когда учет сетевых сервисов включен в коммутаторе, они будут учитываться на основе трафика или времени подключения аутентифицированного пользователя к порту. В момент начала учета сетевых ресурсов коммутатор пошлет на сервер RADIUS, учитывающий сетевые сервисы, сообщение «учет сетевых сервисов начат». Через каждые пять секунд на RADIUS-сервер, учитывающий сетевые сервисы для онлайн-пользователя, будет поступать пакет учета сетевых сервисов. В момент окончания учета сетевых сервисов на RADIUS-сервер, учитывающий сетевые сервисы, будет отправлено сообщение "учет сетевых сервисов прекращен". Примечание: Коммутатор посылает сообщение "пользователь в автономном режиме" на RADIUS-сервер, учитывающий сетевые сервисы, только в том случае, если учет сетевых сервисов включен. Сообщение "пользователь в автономном режиме" не будет послано на RADIUS-сервер аутентификации.	



	"no" в начале команды выключает функцию AAA accounting
Пример	Включить функцию учета AAA accounting на коммутаторе. Switch(config)#aaa-accounting enable

11.8.3. Обновление информации учета сетевых сервисов (aaa-accounting update)

Команда	aaa-accounting update {enable disable}	
Параметр	none	Отсутствует
По умолчанию	Обновление информации учета сетевых сервисов при AAA включено	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает или выключает обновление информации учета сетевых сервисов при AAA. После включения функции учета обновлений коммутатор будет периодически отправлять сообщение об учете каждому пользователю, находящемуся в сети	
Пример	Выключить обновление информации учета сетевых сервисов при AAA на коммутаторе. Switch(config)#aaa-accounting update disable	

11.8.4. Задать IP-адрес источника для отправляемых пакетов RADIUS (radius nas-ipv4)

Команда	radius nas-ipv4 <ip-address> no radius nas-ipv4	
Параметр	ip-address	IP-адрес источника пакетов RADIUS в десятичном представлении с точками, это должен быть корректный одноадресный IP-адрес
По умолчанию	IP-адрес источника пакетов RADIUS не задан. В качестве IP-адреса источника пакетов RADIUS используется IP-адрес интерфейса, с которого посылаются пакеты RADIUS	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Позволяет задать IP-адрес источника для пакетов RADIUS, посылаемых коммутатором. IP-адрес источника должен принадлежать одному из IP-интерфейсов коммутатора. В противном случае в ответ на пакет RADIUS, посланный коммутатором придет сообщение об ошибке привязки IP-адреса. Рекомендуется использовать в качестве IP-адреса источника IP-адрес интерфейса петли. Это позволяет избежать отбрасывания пакетов на сервере RADIUS, когда интерфейсы выключены. "no" в начале команды удаляет настройку
Пример	Задать IP-адрес источника пакетов RADIUS равным 192.168.2.254. <pre>Switch(config)#radius nas-ipv4 192.168.2.254</pre>

11.8.5. Задать IPv6-адрес источника для отправляемых пакетов RADIUS (radius nas-ipv6)

Команда	radius nas-ipv6 <ipv6-address> no radius nas-ipv6	
Параметр	ipv6-address	IPv6-адрес источника пакетов RADIUS, должен быть корректным unicast-IPv6-адресом
По умолчанию	IPv6-адрес источника пакетов RADIUS не задан. В качестве IPv6-адреса источника пакетов RADIUS используется IPv6-адрес интерфейса, с которого посылаются пакеты RADIUS	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать IPv6-адрес источника для пакетов RADIUS, посылаемых коммутатором. IPv6-адрес источника должен принадлежать одному из IPv6-интерфейсов коммутатора. В противном случае в ответ на пакет RADIUS, посланный коммутатором придет сообщение об ошибке привязки IPv6-адреса. Рекомендуется использовать в качестве IPv6-адреса источника IPv6-адрес интерфейса петли. Это позволяет избежать отбрасывания пакетов на сервере RADIUS, когда интерфейсы выключены. "no" в начале команды удаляет настройку	
Пример	Задать IPv6-адрес источника пакетов RADIUS равным 2001:da8:456::1. <pre>Switch(config)#radius nas-ipv6 2001:da8:456::1</pre>	



11.8.6. Настроить параметры RADIUS-сервера для учета (radius-server accounting host)

Команда	radius-server accounting host {<ipv4-address> <ipv6-address>} [port <port-number>] [key {0 7} <string>] [primary] no radius-server accounting host {<ipv4-address> <ipv6-address>}	
Параметр	ipv4-address	IPv4 -адрес сервера
	ipv6-address	IPv6 -адрес сервера
	port-number	номер порта прослушивания сервера от 0 до 65535
	string	строка ключа. Если для параметра key установлен 0, ключ не шифруется и его диапазон не должен превышать 64 символов, если для параметра key установлено 7, ключ шифруется и его диапазон не должен превышать 64 символов
	primary	первичный сервер. Могут быть настроены и сделаны доступными несколько RADIUS-серверов. Могут быть настроены и сделаны доступными несколько RADIUS-серверов. Если параметр primary не задан, поиск RADIUS-серверов будет выполнен в порядке, заданном настройками. В противном случае первым будет использован указанный RADIUS-сервер
По умолчанию	RADIUS-сервер учета сетевых сервисов не настроен	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать IPv4/IPv6-адрес и номер порта для сервера учета сетевых сервисов RADIUS. Эта команда используется для указания IPv4/IPv6 -адреса и номера порта для указанного RADIUS-сервера учета сетевых сервисов. Может быть введено несколько команд с разными настройками. В параметре <port-number> задается номер порта учета, он должен совпадать с номером порта учета сетевых сервисов RADIUS-сервера, по умолчанию это 1813. Если задан номер порта 0, номер порта учета сетевых сервисов будет сгенерирован случайным образом, что может привести к неправильной настройке. Эту команду можно использовать несколько раз для настройки нескольких RADIUS-серверов, связывающихся с коммутатором. Коммутатор будет посылать пакеты учета на все настроенные серверы учета сетевых сервисов. Все серверы учета сетевых сервисов могут дублировать друг друга. Если задан параметр primary, то первичным RADIUS-сервером будет сервер, указанный в этом параметре. Настраивается только	



	первичный сервер RADIUS, независимо от того, использует ли он IPv4-адрес или IPv6-адрес. "no" в начале команды удаляет сервер учета RADIUS
Пример	Установить RADIUS-сервер учета сетевых сервисов с IPv6-адресом 2004:1:2:3::2, как первичный сервер, с номером порта учета 3000. Switch(config)#radius-server accounting host 2004:1:2:3::2 port 3000 primary

11.8.7. Настроить параметры RADIUS-сервера для аутентификации (radius-server authentication host)

Команда	radius-server authentication host {<ipv4-address> <ipv6-address>}[port <port-number>] [key {0 7} <string>] [primary] [access-mode {dot1x telnet}] no radius-server authentication host {<ipv4-address> <ipv6-address>}	
Параметр	ipv4-address	IPv4 -адрес сервера
	ipv6-address	IPv6 -адрес сервера
	port-number	номер порта прослушивания сервера от 0 до 65535
	string	строка ключа. Если для параметра key установлен 0, ключ не шифруется и его диапазон не должен превышать 64 символов, если для параметра key установлено 7, ключ шифруется и его диапазон не должен превышать 64 символов
	primary	первичный сервер. Могут быть настроены и сделаны доступными несколько RADIUS-серверов. Если параметр primary не задан, поиск RADIUS-серверов будет выполнен в порядке, заданном настройками. В противном случае первым будет использован указанный RADIUS-сервер
	dot1x telnet	текущий RADIUS-сервер будет использовать только для аутентификации 802.1x или telnet, все службы могут по умолчанию использовать текущий RADIUS-сервер
По умолчанию	RADIUS-сервер аутентификации не настроен	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Позволяет задать для RADIUS сервера IPv4- или IPv6 -адрес, номер порта прослушивания, секретный ключ, является ли сервер первичным или нет, режим доступа. Эта команда используется для указания IPv4/IPv6 -адреса и номера порта, ключа шифрования и способа доступа для указанного RADIUS-сервера аутентификации коммутатора. Может быть введено несколько команд с разными настройками. В параметре "port" задается номер порта аутентификации, он должен совпадать с номером порта аутентификации RADIUS-сервера, номер порта по умолчанию: 1812. Если задан номер порта 0, указанный сервер считается не аутентифицирующим. Эта команда может быть введена несколько раз для настройки нескольких RADIUS-серверов, связывающихся с коммутатором. Выбор сервера аутентификации производится в соответствии с приоритетами, заданными при настройке. После ответа первого сервера (не важно при этом была аутентификация успешной или нет), коммутатор не будет посылать на следующий сервер запрос на аутентификацию. Если задан параметр primary, то первичным RADIUS-сервером будет сервер, указанный в этом параметре. Если для текущего RADIUS-сервера строка ключа не задана, будет использоваться ключ шифра, заданный командой radius-server key<string> в режиме глобальной конфигурации. Кроме того, можно задать, чтобы текущий RADIUS-сервер использовался только для аутентификации 802.1x или telnet с опцией режима доступа (access-mode option). Опция access-mode не настроена и по умолчанию все службы могут использовать текущий RADIUS-сервер. "no" в начале команды удаляет RADIUS-сервер аутентификации
Пример	Задать адрес RADIUS-сервера аутентификации 2004:1:2:3::2. Switch(config)#radius-server authentication host 2004:1:2:3::2

11.8.8. Время восстановления RADIUS-сервера после выключения (radius-server dead-time)

Команда	radius-server dead-time <minutes> no radius-server dead-time	
Параметр	minutes	время восстановления RADIUS-сервера в минутах, диапазон значений от 1 до 255
По умолчанию	5 минут	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда позволяет задать время ожидания восстановления RADIUS-сервера из недоступного в доступное состояние. Когда подтверждения, посылаемые сервером, недоступны на коммутаторе, он помечается как неработающий сервер; по истечении периода,	



	установленного в таймере, система переустанавливает состояние сервера на рабочее. "no" в начале команды восстанавливает значение по умолчанию
Пример	Задать время восстановления RADIUS-сервера после выключения и повторного включения 3 минуты. Switch(config)#radius-server dead-time 3

11.8.9. Ключ для RADIUS-сервера (radius-server key)

Команда	radius-server key {0 7} <string> no radius-server key	
Параметр	string	строка ключа RADIUS-сервера. Если для параметра key установлен 0, ключ не шифруется и его диапазон не должен превышать 64 символов, если для параметра key установлено 7, ключ шифруется и его диапазон не должен 64 символов
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать ключ для RADIUS-сервера (для аутентификации и учета сетевых сервисов). Ключ используется для шифрованной связи коммутатора с указанным RADIUS-сервером. Ключ должен совпадать с тем ключом, который задан для RADIUS-сервера, в противном случае RADIUS-аутентификация и учет сетевых сервисов будут работать неправильно. "no" в начале команды удаляет ключ для RADIUS-сервера	
Пример	Задать ключ аутентификации RADIUS "qtech". Switch(config)#radius-server key 0 qtech	

11.8.10. Число попыток повторной передачи пакетов аутентификации (radius-server retransmit)

Команда	radius-server retransmit <retries> no radius-server retransmit	
Параметр	retries	число попыток повторной передачи пакетов аутентификации для RADIUS-сервера, в пределах от 0 до 100
По умолчанию	3 попытки	



Режим	Режим глобальной конфигурации
Руководство по использованию	Команда позволяет задать число попыток повторной передачи пакета, если RADIUS-сервер не ответил после того, как коммутатор послал на него пакет аутентификации. Если информация для аутентификации, поступающая от сервера аутентификации, потеряна, на сервер необходимо повторно передать запрос аутентификации AAA. Если счетчик числа попыток повторной передачи запроса AAA достигает порогового значения, а сервер не отвечает, то сервер будет считаться неработоспособным (на коммутаторе его состояние изменится на invalid). "no" в начале команды восстанавливает значение по умолчанию
Пример	Задать 5 попыток повторной передачи пакета аутентификации RADIUS. Switch(config)#radius-server retransmit 5

11.8.11. Время таймера RADIUS-сервера (radius-server timeout)

Команда	radius-server timeout <seconds> no radius-server timeout	
Параметр	seconds	время таймера RADIUS-сервера в секундах, диапазон значений от 1 до 1000
По умолчанию	3 секунды	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда позволяет задать интервал времени, в течение которого коммутатор будет ожидать ответа RADIUS-сервера. После отправки на RADIUS-сервер пакетов запросов, коммутатор будет ожидать ответных пакетов. Если ответ RADIUS-сервера не получен в течение заданного времени, коммутатор повторно пошлет пакет, либо установит для сервера состояние invalid (в зависимости от текущих условий). "no" в начале команды восстанавливает значение по умолчанию	
Пример	Установить таймер аутентификации RADIUS на 30 секунд. Switch(config)#radius-server timeout 30	



11.8.12. Интервал отправки сообщений обновления информации учета сервисов (radius-server accounting-interim-update timeout)

Команда	radius-server accounting-interim-update timeout <seconds> no radius-server accounting-interim-update timeout													
Параметр	seconds	интервал отправки сообщений обновления учета сервисов, в секундах, в диапазоне от 60 до 3600												
По умолчанию	Задан интервал отправки сообщений обновления учета сервисов 300 секунд													
Режим	Режим глобальной конфигурации													
Руководство по использованию	Эта команда позволяет задать интервал, через который NAS посылает сообщения обновления учета сервисов. Для того, чтобы реализовать учет сервисов для пользователей в реальном времени, с момента подключения пользователя в режиме онлайн, NAS посылает на RADIUS-сервер сообщения обновления учета сервисов для этого пользователя через заданный интервал. Интервал отправки сообщений обновления учета сервисов зависит от максимального числа пользователей, поддерживаемых NAS. Чем меньше интервал, тем меньше максимальное число пользователей, поддерживаемых NAS; чем больше интервал, тем больше максимальное число пользователей, поддерживаемых NAS. В таблице ниже приведены рекомендуемые отношения интервала отправки сообщений обновления учета сервисов к максимальному числу пользователей, поддерживаемых NAS: <table><tr><td>Максимальное число пользователей</td><td>Интервал отправки сообщений обновления учета сервисов (в секундах)</td></tr><tr><td>1-299</td><td>300 (по умолчанию)</td></tr><tr><td>300-599</td><td>600</td></tr><tr><td>600-1199</td><td>1200</td></tr><tr><td>1200-1799</td><td>1800</td></tr><tr><td>≥1800</td><td>3600</td></tr></table> "no" в начале команды возвращает настройки по умолчанию		Максимальное число пользователей	Интервал отправки сообщений обновления учета сервисов (в секундах)	1-299	300 (по умолчанию)	300-599	600	600-1199	1200	1200-1799	1800	≥1800	3600
Максимальное число пользователей	Интервал отправки сообщений обновления учета сервисов (в секундах)													
1-299	300 (по умолчанию)													
300-599	600													
600-1199	1200													
1200-1799	1800													
≥1800	3600													
Пример	Задать максимальное число пользователей, поддерживаемых NAS, равным 700 и интервал отправки сообщений обновления учета сервисов равным 1200 секундам. Switch(config)#radius-server accounting-interim-update timeout 1200													



11.8.13. Просмотр информации об аутентифицированных пользователях (show aaa authenticated-user)

Команда	show aaa authenticated-user	
Параметр	none	отсутствует
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, привилегированный режим	
Руководство по использованию	Выводит на экран информацию о подключенных аутентифицированных пользователях. Администратора обычно интересует информация только об аутентифицированных пользователях, остальная информация используется при устранении неполадок службой технической поддержки	
Пример	Вывести информацию о подключенных аутентифицированных пользователях. <pre>Switch(config)#show aaa authenticated-user authenticated users UserName Retry RadID Port EapID ChapID OnTime UserIP MAC total: 0</pre>	

11.8.14. Просмотр информации о проходящих аутентификацию пользователях (show aaa authenticating-user)

Команда	show aaa authenticating-user	
Параметр	none	отсутствует
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, привилегированный режим	
Руководство по использованию	Выводит на экран информацию об аутентифицируемых пользователях Администратора обычно интересует информация только об аутентифицируемых пользователях, остальная информация используется при устранении неполадок службой технической поддержки	



Пример	Вывести информацию о проходящих аутентификацию пользователях <pre>Switch(config)#show aaa authenticating-user</pre> authenticating users User-name Retry-time Radius-ID Port Eap-ID Chap-ID Mem-Addr State total: 0

11.8.15. Просмотр информации коммутатора как RADIUS-клиента (show aaa config)

Команда	show aaa config	
Параметр	none	отсутствует
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, привилегированный режим	
Руководство по использованию	Выводит на дисплей информацию аутентификации AAA, информацию о включении учета сетевых сервисов, ключе, аутентификации и сервере учета сетевых сервисов	
Пример	Просмотр информации о конфигурации aaa <pre>Switch(config)#show aaa config</pre> AAA config data Is Aaa Enabled = 1 : 1 means AAA authentication is enabled, 0 means is not enabled Is Account Enabled= 1 : 1 means AAA account is enabled, 0 means is not enabled MD5 Server Key = qtech : Authentication key authentication server sum = 2 : Configure the number of authentication server	

11.8.16. Статистика аутентифицированных пользователей RADIUS (show radius authenticated-user count)

Команда	show radius authenticated-user count	
Параметр	none	отсутствует
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, привилегированный режим	



Руководство по использованию	Выводит на экран информации о подключенных пользователях, прошедших аутентификацию
Пример	Показать количество пользователей, которые уже прошли аутентификацию. Switch(config)#show radius authenticated-user count The authenticated online user num is: 105

11.8.17. Статистика аутентифицируемых пользователей RADIUS (show radius authenticating-user count)

Команда	show radius authenticating-user count	
Параметр	none	отсутствует
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, привилегированный режим	
Руководство по использованию	Позволяет просмотреть количество пользователей, проходящих аутентификацию	
Пример	Вывод информации обо всех пользователях, проходящих аутентификацию Switch(config)#show radius authenticating-user count The authenticating user num is: 10	

11.8.18. Статистика пользователей RADIUS-аутентификации (show radius count)

Команда	show radius count {authenticated-user authenticating-user} count	
Параметр	authenticated-user	вывод информации о подключенных аутентифицированных пользователях
	authenticating-user	вывод информации обо всех пользователях, проходящих аутентификацию
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, привилегированный режим	
Руководство по использованию	Выводит на дисплей статистику для пользователей RADIUS-аутентификации	



Пример	Вывести на дисплей статистику пользователей RADIUS-аутентификации. Switch#show radius authenticated-user count The authenticated online user num is: 0

11.9. Команды для настройки SSL

11.9.1. Управление коммутатором через защищенное подключение (ip http secure-server)

Команда	[no] ip http secure-server	
Параметр	none	отсутствует
По умолчанию	Функция отключена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет включать и отключать протокол SSL. После включения функции SSL пользователи могут получить доступ к коммутатору через https-клиентов, а коммутатор и клиенты используют SSL-соединение для формирования защищенного канала SSL-соединения. После этого все данные, передаваемые на уровне, обеспечивающем взаимодействие пользовательских приложений с сетью, будут зашифрованы, что обеспечит конфиденциальность связи. "no" в начале команды выключает функцию SSL	
Пример	Включить функцию SSL. Switch(config)#ip http secure-server	

11.9.2. Порт защищенного подключения (ip http secure-port)

Команда	ip http secure-port <port-number> no ip http secure-port	
Параметр	port-number	номер порта, в диапазоне от 1025 до 65535. По умолчанию - 443
По умолчанию	По умолчанию номер порта SSL не настроен	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда настраивает/удаляет номера порта для используемого SSL. Если эта команда используется для настройки номера порта, то для мониторинга будет использоваться настроенный номер порта. Если номер порта для https изменен, то при попытке пользователей использовать https для подключения, необходимо использовать измененный номер. Например: https: //device: port_number. Функция SSL должна перезагружаться после каждого изменения. "no" в начале команды удаляет заданный номер порта
Пример	Установить для порта номер 1028. Switch(config)#ip http secure-port 1028

11.9.3. Метод шифрования для SSL (ip http secure- ciphersuite)

Команда	ip http secure-ciphersuite {des-cbc3-sha rc4-128-sha des-cbc-sha} no ip http secure-ciphersuite	
Параметр	des-cbc3-sha	алгоритм шифрования DES_CBC3, суммарный алгоритм SHA
	rc4-128-sha	алгоритм шифрования RC4_128, суммарный алгоритм SHA
	des-cbc-sha	алгоритм шифрования DES_CBC, суммарный алгоритм SHA
По умолчанию	По умолчанию набор безопасных паролей SSL не настроен	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет настроить/удалить набор безопасных шифров для используемого SSL. Если с помощью этой команды задать шифр безопасности, будет использоваться указанный метод шифрования. Для того чтобы изменения в конфигурации вступили в силу, необходимо перезапустить SSLn. Для des-cbc-sha требуется IE 7.0 или выше. "No" в начале команды удаляет настроенный набор безопасных паролей	
Пример	Задать безопасный набор шифров rc4-128-sha. Switch(config)#ip http secure- ciphersuite rc4-128-sha	



11.9.4. Просмотр информации о конфигурации SSL (show ip http secure-server status)

Команда	show ip http secure-server status	
Параметр	none	отсутствует
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, привилегированный режим	
Руководство по использованию	Отобразить информацию о конфигурации SSL	
Пример	Показать состояние настроенного SSL. Switch(config)#show ip http secure-server status HTTP secure server status: Enabled HTTP secure server port: 1028 HTTP secure server ciphersuite: rc4-128-sha	

11.10. Конфигурация IPv6 RA Security

11.10.1. Активация функции RA Security (ipv6 security-ra enable)

Команда	[no] ipv6 security-ra enable	
Параметр	none	отсутствует
По умолчанию	Функция IPv6 security RA по умолчанию отключена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	При включении функции IPv6 security RA в глобальном режиме сообщения объявления маршрутизатора RA не будут передаваться через аппаратное обеспечение, а отправляться на обработку в центральный процессор. Включить security RA на порту можно только после включения глобальной функции security RA. Отключение функции security RA в глобальном режиме очистит все сконфигурированные порты security RA. Глобальные функции безопасности RA и IPv6 SAVI являются взаимоисключающими, поэтому они не могут быть включены одновременно. "no" в начале команды глобально отключит функцию IPv6 security RA	
Пример	Включить IPv6 RA Security глобально. Switch(config)#ipv6 security-ra enable	



11.10.2. Включить функцию IPv6 RA Security на порту (ipv6 security-ra enable)

Команда	[no] ipv6 security-ra enable	
Параметр	none	отсутствует
По умолчанию	Функция IPv6 security RA по умолчанию отключена	
Режим	Режим конфигурации порта	
Руководство по использованию	Включает IPv6 secure RA на порту, чтобы этот порт не пересылал входящие RA-сообщения. Функция безопасного RA на порту может быть задана только после глобального включения функции безопасного RA. При отключении функции безопасного RA глобально, она отключается и на порту. Команда "no ipv6 security-ra enable" отключает IPv6 secure RA на порту	
Пример	Включить IPv6 security RA на порту. Switch(config-if-ethernet1/0/2)#ipv6 security-ra enable	

11.10.3. Отобразить информацию о функции IPv6 RA Security на интерфейсе (show ipv6 security-ra)

Команда	show ipv6 security-ra [interface <interface-list>]	
Параметр	interface-list	указывается номер порта. При отсутствии параметра отображаются все недоверенные порты. При вводе параметра отображается соответствующий недоверенный порт
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, привилегированный режим	
Руководство по использованию	Выводит на экран все интерфейсы с включенной функцией IPv6 RA	
Пример	Показать все интерфейсы с включенной функцией IPv6 RA. Switch# show ipv6 security-ra IPv6 security ra config and state information in the switch Global IPv6 Security RA State: Enable Ethernet1/0/1	



	IPv6 Security RA State: Yes Ethernet1/0/3 IPv6 Security RA State: Yes

11.11. Команды для настройки MAB

11.11.1. Методы аутентификации MAB (authentication mab)

Команда	authentication mab {radius local} (none) no authentication mab	
Параметр	radius	RADIUS аутентификация
	local	локальная аутентификация
	none	аутентификация не требуется
По умолчанию	По умолчанию используется режим аутентификации RADIUS	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда задает порядок и приоритет методов аутентификации MAC-адресов. Параметр "none" используется для отмены функции аутентификации MAC-адресов. Если ни один настроенный сервер RADIUS не отвечает, коммутатор перейдет в режим аутентификации "none", который позволяет пользователям, прошедшим аутентификацию по MAC-адресу, получать прямой доступ к сети. Параметр "local" используется для локальной аутентификации MAC-адреса, аутентификация осуществляется с помощью локального имени пользователя и пароля. Если в качестве метода аутентификации задан "mab radius local none" и от Radius-сервера нет ответа, система определяет, заданы ли имя пользователя и пароль для локальной аутентификации mab. Если они заданы, то используется локальная аутентификация, если нет, то используется резервная аутентификация по параметру "none". Команда с "no" в начале восстанавливает режим аутентификации по умолчанию	
Пример	Установить функцию уклонения для локальной аутентификации и аутентификации по MAC-адресу. Switch(config)#authentication mab radius local none	



11.11.2. Удаление информации о привязках MAB (clear mac-authentication-bypass binding)

Команда	clear mac-authentication-bypass binding {mac WORD interface (ethernet IFNAME IFNAME) all}	
Параметр	mac	удаление привязок MAB для указанного MAC-адреса
	IFNAME	удаление привязок MAB для указанного интерфейса
	all	удаление всех привязок
По умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Очищает информацию о привязках MAB	
Пример	Удалить все привязки MAB. Switch#clear mac-authentication-bypass binding all	

11.11.3. Максимальное количество привязок MAB (mac-authentication-bypass binding-limit)

Команда	mac-authentication-bypass binding-limit <1-100> no mac-authentication-bypass binding-limit	
Параметр	1-100	максимальное количество привязок, в диапазоне от 1 до 100
По умолчанию	По умолчанию максимальное число привязок MAB равно 3	
Режим	Режим конфигурации порта	
Руководство по использованию	Устанавливает максимальное количество привязок MAB. Устанавливает максимальное количество привязок MAB. Если количество привязок достигнет максимума, порт перестанет создавать новые привязки. Если устанавливаемое значение меньше, чем текущее количество привязок, оно не будет принято. "no" в начале команды восстановит количество привязок по умолчанию равное 3	



Пример	Установить максимальное количество привязок равное 10. Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mac-authentication-bypass binding-limit 10

11.11.4. Включение функции MAB глобально и на порту (mac-authentication-bypass enable)

Команда	[no] mac-authentication-bypass enable	
Параметр	none	отсутствует
По умолчанию	Отключено глобально и на порту	
Режим	Режим конфигурации порта	
Руководство по использованию	Включает глобально и на порту функцию MAB. Чтобы выполнить MAB-аутентификацию на порту, сначала необходимо включить глобальную функцию MAB, а затем функцию MAB для соответствующего порта. Команда "no" отключает функцию MAB	
Пример	Включить функцию MAB глобально и для порта Eth1/0/1. Switch(config)#mac-authentication-bypass enable Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mac-authentication-bypass enable	

11.11.5. Гостевой vlan для MAB аутентификации (mac-authentication-bypass guest-vlan)

Команда	mac-authentication-bypass guest-vlan <1-4094> no mac-authentication-bypass guest-vlan	
Параметр	1-4094	ID гостевого vlan, в диапазоне от 1 до 4094
По умолчанию	Не задано	
Режим	Режим конфигурации порта	



Руководство по использованию	Устанавливает гостевой vlan для MAB аутентификации. Данную команду можно использовать только на порту типа "hybrid", она не будет работать на порте доступа "access port". Если гостевой vlan сконфигурирован, то после неудачной MAB аутентификации, MAB пользователь может присоединиться к гостевому vlan. Команда "no" удаляет гостевой vlan
Пример	Настроить гостевой vlan аутентификации MAB для порта 1/0/1. <pre>Switch(config)#interface ethernet 1/0/1</pre> <pre>Switch(config-if-ethernet1/0/1)#mac-authentication-bypass guest-vlan 10</pre>

11.11.6. Функция обнаружения атаки GARP-spoofing (mac-authentication-bypass spoofing-garp-check)

Команда	[no] mac-authentication-bypass spoofing-garp-check	
Параметр	none	отсутствует
По умолчанию	Функция "spoofing-garp-check" отключена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда включает функцию обнаружения атак "spoofing-garp-check" и функция MAB больше не будет взаимодействовать с "spoofing-garp". Когда терминал операционной системы Windows обнаруживает конфликт адресов, он отправляет самообращенный запрос "gratuitous ARP" для исправления ошибочных ARP-записей, сгенерированных "gratuitous ARP". Эта команда используется для обнаружения "spoofing-garp" при возникновении конфликта адресов, функция MAB больше не обрабатывает пакеты. Примечание: когда функция проверки включена, все ARP проверяются программным обеспечением, что увеличивает нагрузку на коммутатор. "no" в начале команды отключает эту функцию	
Пример	Включить функцию spoofing-garp-check. <pre>Switch(config)#mac-authentication-bypass spoofing-garp-check enable</pre>	



11.11.7. Время восстановления состояния порта (mac-authentication-bypass timeout linkup-period)

Команда	mac-authentication-bypass timeout linkup-period <0-30> no mac-authentication-bypass timeout linkup-period	
Параметр	0-30	после автоматического отключения порта, интервал до его повторного включения, единица измерения - секунда, 0 означает отсутствие операции отключения/подключения
По умолчанию	Интервал 0	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Устанавливает период между переключениями состояний down и up, когда привязка vlan на порту меняется, чтобы пользователь мог снова получить IP-адрес. В случае успешной MAB аутентификации, принадлежность к vlan определяется на основании настроек auto-vlan, если MAB аутентификация закончилась неуспешно, принадлежность к vlan определяется на основании настроек guest-vlan. Если период установлен, то, когда привязка интерфейса к vlan изменяется, порт будет выключен автоматически, и будет включен снова спустя установленный период, чтобы пользователь мог снова получить IP-адрес. Команда с "no" в начале восстанавливает значение по умолчанию	
Пример	Установить время down/up равным 12 секундам. Switch(config)#mac-authentication-bypass timeout linkup-period 12	

11.11.8. Время обнаружения не подключенных пользователей и удаления записи MAB (mac-authentication-bypass timeout offline-detect)

Команда	mac-authentication-bypass timeout offline-detect (0 <60-7200>) no mac-authentication-bypass timeout offline-detect	
Параметр	0 <60-7200>	время обнаружения отсутствия подключения, в диапазоне от 0 или 60 до 7200 секунд
По умолчанию	180 секунд	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Задаёт время определения состояния не в сети. Если задано значение 0, коммутатор не обнаруживает привязки MAB, если время обнаружения в автономного режиме составляет от 60 до 7200 секунд, коммутатор своевременно обнаруживает поток, соответствующий привязке MAB. Если в течение времени обнаружения автономной работы трафик отсутствует, коммутатор удаляет привязку и отключает трафик. "no" в начале команды восстанавливает значение по умолчанию
Пример	Настроить время обнаружения автономного режима в 200 секунд. Switch(config)#mac-authentication-bypass timeout offline-detect 200

11.11.9. Период тишины MAB привязок (mac-authentication-bypass timeout quiet-period)

Команда	mac-authentication-bypass timeout quiet-period <1-60> no mac-authentication-bypass timeout quiet-period	
Параметр	1-60	период тишины, в диапазоне от 1 до 60 секунд
По умолчанию	период тишины 30 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Устанавливает период тишины (quiet-period) MAB привязок Задать время, в течении которого коммутатор не будет реагировать на запрос аутентификации от MAC после неудачной аутентификации этого MAC. Спустя период тишины, коммутатор снова начнет отвечать на запросы аутентификации с этого MAC-адреса. Команда "no" восстанавливает значение quiet-period по умолчанию	
Пример	Установить quiet-period аутентификации MAB на 60 секунд. Switch(config)#mac-authentication-bypass timeout quiet-period 60	

11.11.10. Интервал повторной аутентификации при неудачной аутентификации (mac-authentication-bypass timeout reauth-period)

Команда	mac-authentication-bypass timeout reauth-period <1-3600> no mac-authentication-bypass timeout reauth-period	
Параметр	1-3600	интервал повторной аутентификации, в диапазоне от 1 до 3600 секунд



По умолчанию	интервал повторной аутентификации 30 секунд
Режим	Режим глобальной конфигурации
Руководство по использованию	Устанавливает интервал повторной аутентификации при неудачной аутентификации. В состоянии неудачной аутентификации, пользователь запрашивает повторную аутентификацию периодически, до тех пор, пока попытка не завершится успешно. при успешной аутентификации пользователь получает доступ к сетевым ресурсам. "no" в начале команды восстанавливает значение по умолчанию
Пример	Установить время повторной аутентификации в 20 секунд. Switch(config)#mac-authentication-bypass timeout reauth-period 20

11.11.11. Период до удаления привязок после отключения МАВ-порта (mac-authentication-bypass timeout stale-period)

Команда	mac-authentication-bypass timeout stale-period <0-60> no mac-authentication-bypass timeout stale-period	
Параметр	0-60	период до удаления, в диапазоне от 0 до 60 секунд
По умолчанию	Время удаления привязок составляет 30 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Устанавливает период, по прошествии которого удаляется привязка, после того, как МАВ-порт перешел в состояние down. Если время удаления привязки равно 0, то все пользовательские привязки этого порта удаляются сразу после отключения МАВ-порта, если время больше 0, то пользовательские привязки удаляются с задержкой после отключения МАВ-порта. "no" в начале команды восстанавливает значение по умолчанию	
Пример	Настроить время удаления 40 секунд. Switch(config)#mac-authentication-bypass timeout stale-period 40	



11.11.12. Метод МАВ-аутентификации (mac-authentication-bypass username-format)

Команда	[no] mac-authentication-bypass username-format {mac-address {fixed username WORD password WORD}}	
Параметр	mac-address	использовать MAC-адрес в качестве имени пользователя и пароля для аутентификации
	fixed username WORD password WORD	использовать указанные имя пользователя и пароль для аутентификации, длина имени пользователя и пароля от 1 до 32 символов
По умолчанию	Использовать MAC-адрес в качестве имени пользователя и пароля	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Устанавливает метод МАВ-аутентификации. Существует два метода аутентификации МАВ: использовать MAC-адрес в качестве имени пользователя и пароля или указанные имя пользователя и пароль. Если имя пользователя и пароль не указаны, устройство по умолчанию использует первый метод аутентификации. Команда с "no" в начале восстанавливает значения по умолчанию	
Пример	Все пользователи МАВ должны применять одно и то же имя пользователя и пароль для аутентификации: имя пользователя - mab-user, пароль - mab-pwd. <pre>Switch(config)#mac-authentication-bypass username-format fixed username mab-user password mab-pwd</pre>	

11.11.13. Просмотр информации о МАВ-аутентификации (show mac-authentication-bypass)

Команда	show mac-authentication-bypass {interface {ethernet IFNAME IFNAME}}}	
Параметр	IFNAME	имя порта
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, привилегированный режим	
Руководство по использованию	Отображает информацию о привязке аутентификации МАВ	



Пример	Вывести информацию о привязке аутентификации MAB. Switch#show mac-authentication-bypass The Number of all binding is 5 <table><tr><th>MAC</th><th>Interface</th><th>Vlan ID</th><th>State</th></tr><tr><td>04-0a-eb-6a-7f-88</td><td>Ethernet1/0/1</td><td>1</td><td>MAB_QUIET</td></tr><tr><td>03-0a-eb-6a-7f-88</td><td>Ethernet1/0/1</td><td>1</td><td>MAB_QUIET</td></tr><tr><td>02-0a-eb-6a-7f-88</td><td>Ethernet1/0/1</td><td>1</td><td>MAB_AUTHENTICATED</td></tr><tr><td>00-0a-eb-6a-7f-8e</td><td>Ethernet1/0/1</td><td>1</td><td>MAB_AUTHENTICATED</td></tr></table> Switch(config)#show mac-authentication-bypass int e1/0/1 Interface Ethernet1/0/1 user config: MAB enable: Enable Binding info: 1 MAB Binding built at SUN JAN 01 01: 14: 48 2006 VID 1, Port: Ethernet1/1 Client MAC: 00-0a-eb-6a-7f-8e Binding State: MAB_AUTHENTICATED Binding State Lease: 164 seconds left	MAC	Interface	Vlan ID	State	04-0a-eb-6a-7f-88	Ethernet1/0/1	1	MAB_QUIET	03-0a-eb-6a-7f-88	Ethernet1/0/1	1	MAB_QUIET	02-0a-eb-6a-7f-88	Ethernet1/0/1	1	MAB_AUTHENTICATED	00-0a-eb-6a-7f-8e	Ethernet1/0/1	1	MAB_AUTHENTICATED
MAC	Interface	Vlan ID	State																		
04-0a-eb-6a-7f-88	Ethernet1/0/1	1	MAB_QUIET																		
03-0a-eb-6a-7f-88	Ethernet1/0/1	1	MAB_QUIET																		
02-0a-eb-6a-7f-88	Ethernet1/0/1	1	MAB_AUTHENTICATED																		
00-0a-eb-6a-7f-8e	Ethernet1/0/1	1	MAB_AUTHENTICATED																		

11.12. Команды для настройки PPPoE Intermediate Agent

11.12.1. Включить PPPoE intermediate agent глобально (pppoe intermediate-agent)

Команда	[no] pppoe intermediate-agent	
Параметр	none	отсутствует
По умолчанию	PPPoE intermediate agent выключен	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Включает функционал PPPoE intermediate agent глобально. После включения, коммутатор начинает обрабатывать пакеты инициализации PPPoE (discovery stage) в соответствии с введенной конфигурацией. Команда с "no" в начале отключает глобально функцию PPPoE intermediate agent	



Пример	Включить функцию PPPoE intermediate agent глобально. Switch(config)#pppoe intermediate agent

11.12.2. Включить PPPoE intermediate agent на порту (pppoe intermediate-agent (Port))

Команда	[no] pppoe intermediate-agent	
Параметр	none	отсутствует
По умолчанию	PPPoE intermediate agent выключен	
Режим	Режим конфигурации порта	
Руководство по использованию	Включает функционал PPPoE intermediate agent на порту. После включения, коммутатор начинает добавлять vendor-тег в пакеты PPPoE на данном порту. <u>ПРИМЕЧАНИЕ:</u> PPPoE intermediate agent должен быть включен глобально Как минимум один порт коммутатора должен быть подключен к PPPoE-серверу и этот порт должен быть в режиме trust. Команда с "no" в начале отключает функцию PPPoE intermediate agent на порту	
Пример	Включить функцию PPPoE intermediate agent для порта ethernet 1/0/2. Switch(config-if-ethernet1/0/2)#pppoe intermediate agent	

11.12.3. Идентификатор узла доступа для порта (pppoe intermediate-agent circuit-id)

Команда	[no] pppoe intermediate-agent circuit-id <string>	
Параметр	string	идентификатор узла доступа circuit-id, максимальное количество символов 63 байта
По умолчанию	По умолчанию эта функция не настроена	
Режим	Режим конфигурации порта	
Руководство по использованию	Задаёт значение "circuit-id" для порта. Команда задаёт значение "circuit-id" для каждого порта. Имеет более высокий приоритет, чем команда "pppoe intermediate-agent identifier-string".	



	Команда с "no" в начале отменяет эту настройку
Пример	Задать идентификатор узла доступа "circuit-id" на порту ethernet1/0/3 vlan3 как abcd/efgh . <pre>Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent circuit-id abcd/efgh</pre>

11.12.4. Разделитель полей в идентификаторе (pppoe intermediate-agent delimiter)

Команда	pppoe intermediate-agent delimiter <WORD> no pppoe intermediate-agent delimiter	
Параметр	WORD	разделитель между полями, возможны варианты (# . , ; : / space)
По умолчанию	По умолчанию для полей задано значение '\0'	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда задает разделитель между полями в "circuit-id" и "remote-id". После настройки для разделения добавленных полей в "circuit-id" и "remote-id" будут использоваться указанный разделитель. Примечание: Функция "pppoe intermediate-agent" должна быть глобально включена. Команда с "no" в начале отменяет настройку	
Пример	Установить в качестве разделителя пробел (space). <pre>Switch(config)#pppoe intermediate-agent delimiter space</pre>	

11.12.5. Задать формат представления (pppoe intermediate-agent format)

Команда	pppoe intermediate-agent format (circuit-id remote-id) (hex ascii) no pppoe intermediate-agent format (circuit-id remote-id)	
Параметр	hex	шестнадцатеричный
	ascii	ASCII код
По умолчанию	По умолчанию эта функция не настроена	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда устанавливает шестнадцатеричный или ASCII-формат представления "circuit-id" и "remote-id". Идентификаторы "circuit-id" и "remote-id" инкапсулируются как метки поставщика в шестнадцатеричном формате ASCII. Примечание: Функция "pppoe intermediate-agent" должна быть глобально включена. Команда с "no" в начале отменяет настройку
Пример	Настроить доверенный порт 1/0/1 для включения функции "vendor-tag strip". <pre>Switch(config)#pppoe intermediate-agent format remote-id ascii</pre>

11.12.6. Задать идентификатор (pppoe intermediate-agent remote-id)

Команда	[no] pppoe intermediate-agent remote-id <string>	
Параметр	string	remote-id, максимальное количество символов - 63 байта
По умолчанию	По умолчанию эта функция не настроена	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда задает идентификатор "remote-id" порта. Необходимо настроить "remote-id" для каждого порта. Если конфигурация отсутствует, в качестве значения "remote-id" используется MAC коммутатора. Команда с "no" в начале отменяет эту настройку	
Пример	Задать remote-id в виде abcd на порту ethernet1/0/2. <pre>Switch(config-if-ethernet1/0/2)# pppoe intermediate-agent remote-id abcd</pre>	

11.12.7. Выбрать порт в качестве доверенного (pppoe intermediate-agent trust)

Команда	[no] pppoe intermediate-agent trust	
Параметр	none	отсутствует
По умолчанию	Порт является не доверенным	
Режим	Режим конфигурации порта	



Руководство по использованию	Настраивает порт в качестве доверенного. Порт, к которому подключен сервер, должен работать в режиме trust. Примечание: минимум один порт, к которому подключен PPPoE-сервер, должен работать в качестве доверенного. Команда с "no" в начале выбирает порт в качестве не доверенного
Пример	Установить порт ethernet1/0/1 в качестве доверенного порта trust. Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust

11.12.8. Задать собственный формат идентификатора узла доступа (pppoe intermediate-agent type self-defined circuit-id)

Команда	pppoe intermediate-agent type self-defined circuit-id {vlan port id (switch-id (mac hostname) remote-mac) string WORD} no pppoe intermediate-agent type self-defined circuit-id	
Параметр	vlan	идентификатор VLAN
	port	номер порта
	id switch-id mac	локальный MAC-адрес
	id switch-id hostname	локальное имя хоста
	remote-mac	удаленный MAC-адрес
	string WORD	заданное ключевое слово
По умолчанию	По умолчанию эта конфигурация равна нулю	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет задать собственный формат "circuit-id". Эта настройка является взаимоисключающей для типа "tr-101 circuit-id" и очищает соответствующую конфигурацию типа "tr-101 circuit-id". Команда с "no" в начале отменяет настройку	
Пример	Задать собственный формат "circuit-id" как "vlan port id switch-id hostname". Switch(config)#pppoe intermediate-agent type self-defined circuit-id vlan port id switch-id hostname	



11.12.9. Задать собственный формат идентификатора удаленного хоста (pppoe intermediate-agent type self-defined remoteid)

Команда	pppoe intermediate-agent type self-defined remoteid {mac vlan-mac hostname string WORD} no pppoe intermediate-agent type self-defined remote-id	
Параметр	mac	MAC-адрес порта Ethernet
	vlan-mac	MAC-адрес IP-интерфейса
	hostname	имя локального хоста
	string WORD	указанное ключевое слово
По умолчанию	По умолчанию эта конфигурация пуста	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Задает собственный формат идентификатора удаленного хоста "remote-id". Порядок конфигурации этой команды соответствует порядку полей в "remote-id". Команда с "no" в начале отменяет настройку	
Пример	Задать собственный формат "remote-id" как "string abcd mac hostname". Switch(config)#pppoe intermediate-agent type self-defined remoteid string abcd mac hostname	

11.12.10. Настроить идентификатор узла доступа (pppoe intermediate-agent type tr-101 circuit-id access-node-id)

Команда	pppoe intermediate-agent type tr-101 circuit-id access-node-id <string> no pppoe intermediate-agent type tr-101 circuit-id access-node-id	
Параметр	string	идентификатор узла доступа access-node-id, максимальное количество символов 47 байт
По умолчанию	В access-node-id заносится MAC-адрес коммутатора	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Задаёт значение поля "access-node-id" в "circuit-id" в добавляемом vendor-теге со стандартом tr-101. Данная конфигурация применяется для создания "access-node-id" идентификатора "circuit ID" в vendor-теге. Значение "circuit-id" это "access-node-id + " eth "+ Slot ID + разделитель + Port Index + разделитель + Vlan ID, идентификатор access-node-id занимает n байт (n<48), " eth " это пробел + e + t + h + пробел, занимает 5 байт. Идентификатор слота Slot ID занимает 2 байта, Port Index занимает 3 байта, Vlan ID занимает 4 байта, разделитель занимает 1 байт. По умолчанию значение "access-node-id" в "circuit-id" это MAC-адрес коммутатора размером 6 байт. Например: MAC-адрес - "0a0b0c0d0e0f", идентификатор слота - 12, индекс порта - 34, идентификатор Vlan - 567, значение circuit-id по умолчанию - "0a0b0c0d0e0f eth 12/034: 0567". Команда с "no" в своем начале снимает конфигурацию
Пример	Указать в качестве "access-node-id" для "circuit ID" abcd в vendor-теге. Switch(config)#pppoe intermediate-agent access-node-id abcd После того как порт ethernet1/0/3 vlan3 получает пакеты PPPoE, значение "circuit-id" добавленного vendor-тега дано как "abcd eth 01/003: 0003"

11.12.11. Разделитель каждого параметра (pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter)

Команда	pppoe intermediate-agent type tr-101 circuit-id identifier-string <string> option {sp sv pv spv} delimiter <WORD> [delimiter <WORD>] no pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter	
Параметр	string	identifier-string, максимальное количество символов - 47 байт
	{sp sv pv spv}	данная опция позволяет выбрать формат комбинации для слота, порта, vlan, Sp означает slot и port, sv означает slot и vlan, pv означает port и vlan, spv означает slot, port и vlan
	WORD	разделитель между полями slot, port и vlan. Возможны варианты (# . , ; : / пробел). Примечание: в комбинированном режиме spv есть два разделителя WORD: первый - между слотом и портом, второй - между портом и vlan
По умолчанию	Значение не задано	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Задаёт значение "circuit-id" добавляемого vendor-тега стандартом tr-101. Команда используется для задания "circuit-id" глобально и имеет более высокий приоритет, чем команда "pppoe intermediate-agent access-node-id". Значение "circuit-id" это "access-node-id + " eth "+ Slot ID + разделитель + Port Index + разделитель + Vlan ID идентификатор "access-node-id" занимает n байт (n<48), " eth " это пробел + e + t + h + пробел, занимает 5 байт. Идентификатор слота Slot ID занимает 2 байта, Port Index занимает 3 байта, Vlan ID занимает 4 байта, разделитель занимает 1 байт. Команда с "no" в начале удаляет данную конфигурацию
Пример	Сконфигурировать "access-node-id" как xyz, используя комбинацию spv и разделитель "#" для Slot ID и Port ID и разделитель "/" для Port ID и Vlan ID. <pre>Switch(config)#pppoe intermediate-agent identifier-string xyz option spv delimiter # delimiter /</pre> <pre>Switch# show pppoe intermediate-agent identifier-string option delimiter config identifier string is : xyz</pre> config option is : slot , port and vlan the first delimiter is : "# " the second delimiter is : "/" " After port ethernet1/0/3 of vlan3 receives PPPoE packets, circuit-id value of the added vendor tag is "xyz eth 01#003/0003"

11.12.12. Удаление vendor-тега из пакета PPPoE (pppoe intermediate-agent vendor-tag strip)

Команда	[no] pppoe intermediate-agent vendor-tag strip	
Параметр	none	отсутствует
По умолчанию	Удаление не производится	
Режим	Режим конфигурации порта	
Руководство по использованию	Включает режим удаление vendor-тега из пакета PPPoE. Если пакет, полученный от PPPoE-сервера, содержит vendor-тег, то этот тег будет удален. ПРИМЕЧАНИЕ: функционал "pppoe intermediate-agent" должен быть включен глобально. Данный порт должен работать в режиме trust. Команда с "no" в начале отменяет эту функцию	



Пример	Доверенный порт ethernet1/0/1 включает функцию разделения vendor-тегов. <pre>Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent vendor-tag strip</pre>

11.12.13. Просмотр идентификатора узла доступа (show pppoe intermediate-agent access-node-id)

Команда	show pppoe intermediate-agent access-node-id	
Параметр	none	отсутствует
По умолчанию	По умолчанию информация о конфигурации не заполнена	
Режим	Привилегированный режим	
Руководство по использованию	Эта команда используется для отображения "access-node-id", настроенного пользователем	
Пример	Показать информацию о конфигурации узла доступа "access-node-id". <pre>Switch#pppoe intermediate-agent access-node-id abcd Switch#show pppoe intermediate-agent access-node-id pppoe intermediate-agent access-node-id is : abcd</pre>	

11.12.14. Просмотр конфигурации разделителя опций (show pppoe intermediate-agent identifier-string option delimiter)

Команда	show pppoe intermediate-agent identifier-string option delimiter	
Параметр	none	отсутствует
По умолчанию	По умолчанию информация о конфигурации не заполнена	
Режим	Привилегированный режим	
Руководство по использованию	Отображает значение "identifier-string" и формат комбинации для слота, порта, vlan	
Пример	Показать информацию о конфигурации pppoe intermediate-agent identifier-string. <pre>Switch#pppoe intermediate-agent identifier-string abcd option spv delimiter # delimiter /</pre>	



	Switch# show pppoe intermediate-agent identifier-string option delimiter config identifier string is : abcd config option is : slot , port and vlan the first delimiter is : "# " the second delimiter is : "/"

11.12.15. Просмотр настроек PPPoE Intermediate Agent (show pppoe intermediate-agent info)

Команда	show pppoe intermediate-agent info [interface ethernet <interface-name>]						
Параметр	interface-name	имя порта					
По умолчанию	По умолчанию информация о конфигурации не заполнена						
Режим	Привилегированный режим						
Руководство по использованию	Отображает настройки "pppoe intermediate-agent" для всех портов или для указанного порта. Позволяет проверить информацию о конфигурации соответствующего порта, показывает, является ли порт доверительным, включена ли функция удаления, подключено ли ограничение скорости, а также отображает настроенные идентификаторы Circuit ID и Remote ID						
Пример	Показать информацию о конфигурации pppoe intermediate-agent порта ethernet1/0/2.						
	Switch# show pppoe intermediate-agent info interface ethernet 1/0/2						
	Interface	IA	Trusted	vendor Strip	Rate limit	circuit id	remote id
	Ethernet1/0/2	yes	no	no	no	test1/port1	host1

11.13. Команды для конфигурации VLAN-ACL

11.13.1. Очистка статистики VLAN-ACL (clear vACL statistic vlan)

Команда	clear vACL [in out] statistic vlan [<1-4094>]					
Параметр	in out	очистить статистику входящего/исходящего трафика				
	1-4094	VLAN, для которой необходимо удалить статистическую информацию VACL. Если не				



		вводить идентификатор VLAN, то очистится вся статистическая информация VLAN
По умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Эта команда позволяет очистить статистическую информацию VACL	
Пример	Удалить статистическую информацию для Vlan1. Switch#clear vACL statistic vlan 1	

11.13.2. Просмотр конфигурации и статистики (show vACL vlan)

Команда	show vACL [in out] vlan [<1-4094>] [begin include exclude <regular-expression>]	
Параметр	in out	показать конфигурацию и статистику входящего/исходящего потока
	1-4094	VLAN, для которой необходимо показать конфигурацию и статистическую информацию VACL. Если идентификатор не указан, будет показана конфигурация и статистическая информация VACL для всех VLAN
	begin [include] exclude <regular-expression>	регулярное выражение . соответствует любому символу, кроме символа смещения строки ^ соответствует началу ряда \$ соответствует концу ряда соответствует строке символов слева или справа от вертикальной строки [0-9] соответствует числу от 0 до 9 [a-z] строчные буквы от a до z [aeiou] любые буквы в «aeiou» \ Escape Character используется для соответствия интервокальному символу, например, \\$ будет соответствовать символу \$, но не будет соответствовать концу строки символов \w буква, цифра или подчеркивание \b начало или конец слов



		\W любые символы, не являющиеся буквами алфавита, цифрами и подчеркиванием \B места, которые не являются началом или концом слова [^x] совпадают с любыми символами, кроме x [^aeiou] совпадают с любыми символами, кроме букв aeiou * повторить ноль раз или много раз + повторить один или много раз (n) повторить n раз (n,) повторять n или более раз (n, m) повторять от n до m раз В настоящее время применяемое регулярное выражение не поддерживает следующий синтаксис: \s соответствует пустому символу \d соответствует числу \S соответствует любым символам, кроме пустого символа \D соответствует нечисловому символу ? повторить ноль раз или один раз
По умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Эта команда показывает конфигурацию и статистическую информацию VACL	
Пример	Показать статистику vlan2 VACL. Switch (config)#show vACL vlan 2 Vlan 2: IP Ingress access-list used is 100, traffic-statistics Disable	



11.13.3. Применить IP-ACL на на входящее направление трафика на VLAN (vacl ip access-group)

Команда	vacl ip access-group {<1-299> WORD} {in out} [traffic-statistic] vlan WORD WORD no vael ip access-group {<1-299> WORD} {in out} vlan WORD	
Параметр	<1-299> WORD	задает числовой IP ACL (в том числе: стандартное правило ACL <1-99>, расширенное правило ACL <100-299>) или именованный ACL
	in out	фильтрация входящего/исходящего трафика
	traffic-statistic	подсчет статистики количества согласованных пакетов
	vlan WORD	VLAN будет привязана к VACL
По умолчанию	Отсутствует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда конфигурирует IP VACL на конкретной VLAN. Для ввода VLAN или нескольких VLAN применяется “; ” или “-”, количество символов не должно превышать 128, а длина CLI не должна превышать 80 символов. Коммутатор не поддерживает фильтрацию исходящего направления. Команда с "no" в своем начале снимает конфигурацию	
Пример	Настроить числовой IP ACL и включить функцию статистики для Vlan 1-5,6,7-9. Switch(config)#vacl ip access-group 1 in traffic-statistic vlan 1-5; 6; 7-9	

11.13.4. Применить IPv6 ACL на на входящее направление трафика на VLAN (vacl ipv6 access-group)

Команда	vacl ipv6 access-group (<500-699> WORD) {in } (traffic-statistic) vlan WORD WORD no ipv6 access-group {<500-699> WORD} {in } vlan WORD	
Параметр	<500-699> WORD	задает правило нумерованного стандартного IPv6 ACL и стандартного списка доступа IPv6 ACL
	in out	фильтрация входящего/исходящего трафика



	traffic-statistic	подсчет статистики количества согласованных пакетов
	vlan WORD	VLAN будет привязана к VACL
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда настраивает применение IPv6 ACL на определенной VLAN. Для ввода VLAN или нескольких VLAN применяется “; ” или “-”, количество символов не должно превышать 128, а длина CLI не должна превышать 80 символов. Коммутатор не поддерживает фильтрацию выходящего направления и расширенный IPv6. Команда с "no" в своем начале снимает конфигурацию	
Пример	Настроить числовой IPv6 ACL для Vlan 5. Switch(config)#vACL ipv6 access-group 600 in traffic-statistic vlan 5	

11.13.5. Применить MAC ACL на на входящее направление трафика на VLAN (vACL mac access-group)

Команда	vACL mac access-group {<700-1199> WORD} {in } [traffic-statistic] vlan WORD no vACL mac access-group {<700-1199> WORD} {in } vlan WORD	
Параметр	<700-1199> WORD	задает числовой IP ACL (в том числе: <700-799> стандартный список доступа MAC, <1100-1199> расширенный список доступа MAC) или именованный ACL
	In	фильтрация входящего трафика
	traffic-statistic	подсчет статистики количества согласованных пакетов
	vlan WORD	VLAN будет привязана к VACL
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда настраивает применение MAC ACL на определенной VLAN. Для ввода VLAN или нескольких VLAN применяется “; ” или “-”, количество символов не должно превышать 128, а длина CLI не должна превышать 80 символов. Коммутатор не поддерживает фильтрацию выходящего направления. Команда с "no" в своем начале снимает конфигурацию
Пример	Настроить числовой MAC ACL для Vlan 5. <pre>Switch(config)#vACL mac access-group 700 in traffic-statistic vlan 1-5</pre>

11.13.6. Применить MAC-IP ACL на на входящее направление трафика на VLAN (vACL mac-ip access-group)

Команда	vACL mac-ip access-group {<3100-3299> WORD} {in } [traffic-statistic] vlan WORD no vACL mac-ip access-group {<3100-3299> WORD} {in } vlan WORD	
Параметр	<3100-3299> WORD	задает числовой MAC-IP ACL или именованный ACL
	in	фильтрация входящего трафика
	traffic-statistic	подсчет статистики количества согласованных пакетов
	vlan WORD	VLAN будет привязана к VACL
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда настраивает MAC-IP VACL для конкретной VLAN. Для ввода VLAN или нескольких VLAN применяется “; ”или “-”, количество символов не должно превышать 128, а длина CLI не должна превышать 80 символов. Коммутатор не поддерживает фильтрацию выходящего направления. Команда с "no" в своем начале снимает конфигурацию	
Пример	Настроить числовой MAC-IP ACL для Vlan 1, 2, 5. <pre>Switch(config)#vACL mac-ip access-group 3100 in traffic-statistic vlan 1; 2; 5</pre>	



11.14. Конфигурация SAVI

11.14.1. Задать префикс вручную (ipv6 cps prefix)

Команда	ipv6 cps prefix <ipv6-address> vlan <vid> no ipv6 cps prefix<ipv6-address>	
Параметр	ipv6-address	префикс адреса ссылки, например 2001: : /64
	vid	идентификатор vlan текущего соединения
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда задает префикс IPv6-адреса соединения вручную. Пользователи должны установить локальный префикс адреса: fe80: : /64 соединения перед включением функции проверки соответствия префикса адреса соединения, которая принимает пакеты, чей адрес источника является локальным адресом соединения. Команда с "no" удаляет запись префикса IPv6 -адреса	
Пример	Настроить для IPv6-адреса следующий префикс вручную - 2001::/64. Switch(config)#ipv6 cps prefix 2001::/64	

11.14.2. Включить функцию проверки префикса (ipv6 cps prefix check enable)

Команда	[no] ipv6 cps prefix check enable	
Параметр	none	Отсутствует
По умолчанию	По умолчанию функция проверки префикса адреса SAVI отключена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Подключает функцию проверки соответствия префикса адреса. После включения функции проверки префикса, если префикс IPv6-адреса пакета не совпадает с префиксом соединения, соответствующее связывание IPv6-адресов не будет установлено. Если пользователь подключает функцию проверки соответствия префикса адреса ссылке, сначала необходимо настроить префикс локального адреса fe80: : /64, чтобы принимать пакеты, в которых адрес источника используется как адрес локальной ссылки. По умолчанию функция проверки префикса адреса отключена. "no" в начале команды отключает данную функцию	



Пример	Подключить функцию проверки соответствия префикса адреса. Switch(config)#ipv6 cps prefix check enable

11.14.3. Назначить доверенный порт DHCPv6 Snooping (ipv6 dhcp snooping trust)

Команда	[no] ipv6 dhcp snooping trust	
Параметр	none	отсутствует
По умолчанию	Функция отключена	
Режим	Режим конфигурации порта	
Руководство по использованию	При установке порта в качестве доверенного порта dhcpv6 не будет создаваться динамическая привязка DHCPv6, и все пакеты протокола DHCPv6 будут проходить через него. Установите для порта атрибута "dhcpv6 trust", включите на порту восходящей линии коммутатора функцию SAVI для подключения к серверу dhcpv6 или ретранслятору dhcpv6. "no" в начале команды назначает порт как недоверенный	
Пример	Задать ethernet1/0/1 как доверенный порт DHCP. Switch(config)#interface ethernet1/0/1 Switch(config-if-ethernet1/0/1)#ipv6 dhcp snooping trust	

11.14.4. Назначить доверенный порт ND Snooping (ipv6 nd snooping trust)

Команда	[no] ipv6 nd snooping trust	
Параметр	none	отсутствует
По умолчанию	Функция отключена	
Режим	Режим конфигурации порта	
Руководство по использованию	Назначает порт в качестве доверенного "slaac trust" и "RA trust port" порта, этот порт не будет устанавливать динамические привязки slaac и пересылать RA-пакеты. Если на порту отключена функция "ipv6 nd snooping trust", он будет считаться недоверенным портом для RA-пакетов и все RA-пакеты отбрасываются. Установка для порта атрибута "trust" обычно позволяет использовать порты на коммутаторах с SAVI или порты между	



	коммутаторами с SAVI. "no" в начале команды назначает порт как недоверенный
Пример	Установить порт ethernet1/0/1 в качестве доверенного порта ND Snooping. <pre>Switch(config)#interface ethernet1/0/1 Switch(config-if-ethernet1/0/1)#ipv6 nd snooping trust</pre>

11.14.5. Метод проверки при обнаружении конфликта записей (savi check binding)

Команда	savi check binding <simple probe> mode no savi check binding mode	
Параметр	simple	проверять только состояние порта на наличие конфликта записей, если порт работает, сохранить конфликтную привязку и не создавать новых. При неработающем состоянии удалить конфликтную привязку, чтобы установить новую
	probe	помимо проверки состояния порта на наличие конфликтующих привязок, если состояние порта рабочее, дополнительно посылать NS-пакет для проверки доступности соответствующего пользователя. При получении от пользователя NA-пакета, текущая конфликтующая привязка сохраняется, новая не будет устанавливаться, в противном случае конфликтующая привязка удаляется и создается новая
По умолчанию	Режим проверки конфликтующих привязок по умолчанию отключен. Принят режим прямого удаления конфликтующих привязок для установки новых	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Задаёт метод проверки при обнаружении конфликта записей. Рекомендуется установить режим обнаружения для предотвращения атак, при которых ложный конфликт записи адресов удаляет легитимную привязку пользователя. "no" в начале команды удаляет режим проверки	
Пример	Установить для проверки конфликта записей режим "probe". <pre>Switch(config)#savi check binding probe mode</pre>	



11.14.6. Включить функцию SAVI (savi enable)

Команда	[no] savi enable	
Параметр	none	отсутствует
По умолчанию	Функция SAVI глобально отключена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Подключает функцию SAVI глобально. После включения функции SAVI глобально можно управлять настройками команд функции SAVI. Поскольку функция SAVI уже содержит функцию безопасности RA, глобальная функция SAVI и функция безопасности RA являются взаимоисключающими в режиме глобальной конфигурации. "no" в начале команды отключает данную функцию	
Пример	Подключить функцию SAVI. Switch(config)#savi enable	

11.14.7. Задать лимит записей SAVI для порта (savi ipv6 binding num)

Команда	savi ipv6 binding num <limit-num> no savi ipv6 binding num	
Параметр	limit-num	установить диапазон от 0 до 65535
По умолчанию	Значение записей по умолчанию - 65535	
Режим	Режим конфигурации порта	
Руководство по использованию	Задаёт лимит записей привязок для порта. В число задаваемых привязок входят только динамические привязки типа slaac, dhcp. Если сумма привязок превышает заданное число, этот порт больше не создает новых динамических привязок, если заданное число равно 0, этот порт не создает никаких динамических привязок. "no" в начале команды восстанавливает значение по умолчанию	
Пример	Задать порта ethernet1/0/1 количество записей равное 100. Switch(config)#interface ethernet1/0/1 Switch(config-if-ethernet1/0/1)# savi ipv6 binding num 100	



11.14.8. Создать запись в таблице SAVI (savi ipv6 check source binding)

Команда	<pre>savi ipv6 check source binding ip <ip-address> mac <mac-address> interface <if-name> {type [slaac dhcp] lifetime <lifetime> type static} no savi ipv6 check source binding ip <ip-address> interface <if-name></pre>	
Параметр	ip-address	адрес одноадресной рассылки IPv6, включая локальный канал и глобальный адрес одноадресной рассылки
	mac-address	mac-адрес Ethernet
	if-name	имя порта, например, интерфейс ethernet 1/0/1
	slaac dhcp	slaac означает создание динамической привязки для типа slaac, dhcp означает создание динамической привязки для типа dhcp
	lifetime	настройка периода времени жизни динамической привязки, единица измерения секунда
	static	создать статическую привязку
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда позволяет ручную настройку функций статической или динамической привязки. Когда срок жизни динамической привязки, сконфигурированной вручную, завершается, соответствующая привязка удаляется, но конфигурация сохраняется, поэтому привязка по-прежнему отображается. Если необходимо снова активировать привязку, ее необходимо сначала удалить, а затем создать новую. Для статической привязки не нужно задавать период времени жизни, он неограничен. "no" в начале команды удалит созданную привязку	
Пример	Настроить динамическую привязку типа slaac для SAVI вручную. <pre>Switch(config)#savi ipv6 check source binding ip 2001::10 mac 00-25-64-BB-8F-04 Interface ethernet1/0/1 type slaac lifetime 2010</pre> Настроить статическую привязку для SAVI вручную. <pre>Switch(config)#savi ipv6 check source binding ip 2001::20 mac 00-25-64-BB-8F-04 Interface ethernet1/0/1 type static</pre>	



11.14.9. Контроль проверки подлинности (savi ipv6 check source ip-address mac-address)

Команда	savi ipv6 check source [ip-address mac-address ip-address mac-address] no savi ipv6 check source	
Параметр	none	отсутствует
По умолчанию	По умолчанию функция фильтрации на порту отключена	
Режим	Режим конфигурации порта	
Руководство по использованию	Включает функцию проверки подлинности пакетов. Перед настройкой этой команды должна быть включена глобальная функция SAVI. "no" перед началом команды отключает эту функцию	
Пример	Включить функцию фильтрации пакетов на порту ethernet1/0/1. Switch(config)#interface ethernet1/0/1 Switch(config-if-ethernet1/0/1)# savi ipv6 check source ip-address mac-address	

11.14.10. Задать метод обнаружения SAVI (savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable)

Команда	[no] savi ipv6 {dhcp-only slaac-only dhcp-slaac} enable	
Параметр	dhcp-only	сценарий применения dhcp-only
	slaac-only	сценарий применения slaac-only
	dhcp-slaac	сценарий применения комбинации dhcp-only и slaac-only
По умолчанию	Сценарий применения SAVI отключен	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Задаёт функцию обнаружения SAVI. Сценарий применения "dhcp-only" задаёт обнаружение только DHCPv6 пакетов и DAD NS пакетов "link-local" адреса с назначенным IPv6 адресом, но не будет обнаруживать DAD NS пакеты адресов "non-link-local". Сценарий "slaac-only" обнаруживает DAD NS пакеты любого типа. Сценарий "dhcp-slaac" обнаруживает все DHCPv6 и DAD NS	



	пакеты. По умолчанию функция обнаружения любых типов для SAVI отключена. "no" в начале команды отключает эту функцию

11.14.11. Максимальное количество записей с одним MAC (savi ipv6 mac-binding-limit)

Команда	savi ipv6 mac-binding-limit <limit-num> no savi ipv6 mac-binding-limit	
Параметр	limit-num	задает диапазон от 1 до 10, по умолчанию количество динамических привязок для одного MAC-адреса равно 32
По умолчанию	Число динамических привязок для одного MAC-адреса по умолчанию равно 32	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда устанавливает количество динамических привязок с одним MAC-адресом. Эта команда используется для предотвращения исчерпания динамической привязки SAVI в результате атаки. "no" в начале команды восстанавливает значение по умолчанию	
Пример	Установить количество динамических привязок для одного и того же MAC-адреса равное 5. Switch(config)#savi ipv6 mac-binding-limit 5	

11.14.12. Время обнаружения записи в таблице SAVI (savi max-dad-dalay)

Команда	savi max-dad-delay <max-dad-delay> no savi max-dad-delay	
Параметр	max-dad-delay	задаваемое значение в диапазоне от 1 до 65535 секунд, значение по умолчанию 1 секунда
По умолчанию	1 секунда	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Задаёт время нахождения динамической записи в состоянии DETECTION и отправки времени жизни для обнаружения пакета DAD NS. Рекомендуется использовать значение по умолчанию. "no" в начале команды восстанавливает значение по умолчанию	



Пример	Задать период обнаружения 2 секунды. Switch(config)#savi max-dad-delay 2

11.14.13. Время повторного обнаружения динамической записи (savi max-dad-prepare-delay)

Команда	savi max-dad-prepare-delay <max-dad-prepare-delay> no savi max-dad-prepare-delay	
Параметр	max-dad-prepare-delay	задаваемое значение в диапазоне от 1 до 65535 секунд, значение по умолчанию 1 секунда
По умолчанию	1 секунда	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Задаёт время повторного обнаружения динамической записи. Рекомендуется использовать значение по умолчанию. "no" в начале команды восстанавливает значение по умолчанию	
Пример	Задать время повторного обнаружения 2 секунды. Switch(config)#savi max-dad-prepare-delay 2	

11.14.14. Время жизни для записи SLAAC (savi max-slaac-life)

Команда	savi max-slaac-life <max-slaac-life> no savi max-slaac-life	
Параметр	max-slaac-life	задаваемый диапазон от 1 до 31536000 секунд, значение по умолчанию 4 часа
По умолчанию	4 часа	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Задаёт период жизни динамической привязки slaac в состоянии BOUND. "no" в начале команды восстанавливает значение по умолчанию	



11.14.15. Время хранения записи в таблице SAVI (savi timeout bind-protect)

Параметр	savi timeout bind-protect <protect-time> no savi timeout bind-protect	
Параметр	protect-time	задаваемый диапазон от 1 до 300 секунд, по умолчанию 30 секунд
По умолчанию	30 секунд	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Задаёт время хранения записи после обнаружения перехода порта в состояние down. Если по истечении заданного периода жизни порт все еще находится в состоянии down, привязка этого порта будет удалена. Если состояние порта изменится с down на up в течение заданного периода времени, привязка порта будет сброшена в состояние BOUND периода времени жизни. Если параметр имеет значение 0 секунд, все привязки порта будут удалены немедленно. "no" в начале команды восстанавливает значение по умолчанию	
Пример	Задать время хранения записи 20 секунд. Switch(config)#savi timeout bind-protect 20	

11.14.16. Просмотр записи в таблице SAVI (show savi ipv6 check source binding)

Команда	show savi ipv6 check source binding [interface<if-name>]	
Параметр	if-name	имя порта, например, interface ethernet 1/0/1
По умолчанию	Не задано	
Режим	Привилегированный режим	
Руководство по использованию	Позволяет просмотреть глобальный список записей привязки SAVI	
Пример	Вывести глобальные записи в таблице SAVI. Switch(config)#show savi ipv6 check source binding Static binding count: 0 Dynamic binding count: 3	



Binding count: 3							
MAC	IP	VLAN	Port	Type	State	Expires	
00-25-64-bb-8f-04	fe80: : 225: 64ff: febb: 8f04	1	Ethernet1/0/5	slaac	BOUND	14370	
00-25-64-bb-8f-04	2001: : 13: 1	1	Ethernet1/0/5	slaac	BOUND	14370	
00-25-64-bb-8f-04	2001: : 10: 1	1	Ethernet1/0/5	slaac	BOUND	14370	



12. КОМАНДЫ ДЛЯ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ

12.1. Команды для настройки MRPP

12.1.1. Задать виртуальный VLAN ID для кольца MRPP (control-vlan)

Команда	control-vlan <vid> no control-vlan	
Параметр	vid	идентификатор VLAN ID для управления, в пределах от 1 до 4094
Состояние по умолчанию	-	
Режим	Режим кольца MRPP	
Руководство по использованию	Команда позволяет задать виртуальный VLAN ID для кольца MRPP, в настоящее время его значение должно быть в пределах 1-4094. Во избежание конфликтов рекомендуется, чтобы этот ID принадлежал VLAN, которая еще не сконфигурирована и совпадал с ID кольца MRPP. При конфигурации кольца MRPP одной и той же петли коммутаторов MRPP, VLAN ID управляющей VLAN на коммутаторах должны быть одинаковыми, в противном случае, все кольцо MRPP может работать неправильно, либо возникнет broadcast-шторм. До применения команды "control-vlan" должна быть введена команда "mrpp enable". Если после ввода команды control-vlan сконфигурированы первичный и вторичный порты, тип узлы и введена команда "enable", будет включена функция "mrpp-ring"	
Пример	Для кольца mrpp 4000 назначить VLAN 4000. <pre>Switch(config)#mrpp ring 4000 Switch(mrpp-ring-4000)#control-vlan 4000</pre>	

12.1.2. Удалить статистику принимаемых и передаваемых пакетов MRPP (clear mrpp statistics)

Команда	clear mrpp statistics [<ring-id>]	
Параметр	ring-id	идентификатор (ID) кольца MRPP, в диапазоне от 1 до 4096. Если ID не указан, будет очищена статистическая информация всех колец MRPP
Состояние по умолчанию	-	
Режим	Привилегированный режим	



Руководство по использованию	Очищает статистику принимаемых и передаваемых пакетов MRPP в кольце MRPP
Пример	Очистить статистическую информацию кольца MRPP 4000 на коммутаторе. Switch#clear mrpp statistics 4000

12.1.3. Включить сконфигурированное кольцо MRPP (enable)

Команда	enable no enable	
Параметр	-	
Состояние по умолчанию	по	Кольцо MRPP выключено
Режим	Режим кольца MRPP	
Руководство по использованию	по	Позволяет включить сконфигурированное кольцо MRPP. Команда "no enable" выключает данное кольцо MRPP
Пример	Сконфигурировать кольцо MRPP 4000 коммутатора в первичном узле и включить его. <pre>Switch(config)#mrpp enable Switch(config)#mrpp ring 4000 Switch(mrpp-ring-4000)#control-vlan 4000 Switch(mrpp-ring-4000)# node-mode master Switch(mrpp-ring-4000)#fail-timer 18 Switch(mrpp-ring-4000)#hello-timer 6 Switch(mrpp-ring-4000)#enable Switch(mrpp-ring-4000)#exit Switch(config)#in ethernet1/0/1 Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port Switch(config)#in ethernet 1/0/3 Switch(config-If-Ethernet1/0/3)#mrpp ring 4000 secondary-port</pre>	

12.1.4. Создать домен ERPP (errp domain)

Команда	errp domain <domain-id> no errp domain <domain-id>	
Параметр	domain-id	идентификатор домена ERPP, диапазон от 1 до 15



Состояние по умолчанию	Идентификатор домена не сконфигурирован
Режим	Режим глобальной конфигурации
Руководство по использованию	Если необходимо настроить идентификатор домена ERRP, сначала следует включить режим совместимости ERRP. При выполнении этой команды необходимо создать новый домен ERRP, если домен ERRP отсутствует. При этом форма команды с "no" в начале применяется для удаления соответствующего ID домена ERRP
Пример	Настроить идентификатор домена для ERRP глобально. Switch(Config)#errp domain 1

12.1.5. Таймер получения пакетов Hello в первичном узле (fail-timer)

Команда	fail-timer <timer> no fail-timer	
Параметр	timer	в диапазоне от 1 до 300 секунд
Состояние по умолчанию	3 секунды	
Режим	Режим кольца MRPP	
Руководство по использованию	Если первичный узел кольца MRPP не получит пакет Hello от первичного порта первичного узла в течение интервала таймера, то кольцо считается неработоспособным. На промежуточных узлах MRPP задавать таймер нет необходимости. Во избежание задержки передачи пакетов Hello промежуточным узлом, значение таймера должно быть втрое больше таймера Hello или равно ему. Из-за задержки в кольце необходимо изменить значение таймера, заданное по умолчанию. Необходимо увеличить его, чтобы не создавалось ситуаций, когда таймер уже истек, а первичный узел еще не принял пакета Hello из-за задержки в кольце	
Пример	Установить fail-timer кольца MRPP 4000 равным 10 секундам. Switch(config)# mrpp ring 4000 Switch(mrpp-ring-4000)#fail-timer 10	

12.1.6. Таймер передачи пакетов Hello из первичного узла (hello-timer)

Команда	hello-timer <timer> no hello-timer	
Параметр	timer	в диапазоне от 1 до 100 секунд



Состояние по умолчанию	по 1 секунда
Режим	Режим кольца MRPP
Руководство по использованию	Первичный узел кольца MRPP регулярно, через заданный в таймере интервал, передает пакеты Hello, если вторичному порту первичного узла удастся принять эти пакеты в течение заданного периода времени, кольцо считается работоспособным. В противном случае – неработоспособным. На промежуточных узлах кольца MRPP задавать этот таймер не требуется
Пример	Установить таймер hello кольца MRPP 4000 равным 3 секундам. Switch(config)# mrpp ring 4000 Switch(mrpp-ring-4000)#hello-timer 3

12.1.7. Включить режим совместимости с EARS (mrpp eaps compatible)

Команда	mrpp eaps compatible no mrpp eaps compatible
Параметр	-
Состояние по умолчанию	Режим совместимости с EARS отключен
Режим	Режим глобальной конфигурации
Руководство по использованию	Если необходимо настроить функцию совместимости EAPS, сначала следует включить протокол MRPP. При выполнении команды "no mrpp eaps compatible" необходимо убедиться, что на коммутаторе включен протокол MRPP
Пример	Включить режим совместимости с EARS глобально. Switch(Config)#mrpp enable Switch(Config)#mrpp eaps compatible

12.1.8. Включить модуль протокола MRPP (mrpp enable)

Команда	mrpp enable no mrpp enable
Параметр	-
Состояние по умолчанию	Модуль протокола MRPP в системе не включен



Режим	Режим глобальной конфигурации
Руководство по использованию	Если необходимо сконфигурировать кольцо MRPP, должен быть включен протокол MRPP. Выполнение команды "no mrpp enable" обеспечивает отключение кольца MRPP на коммутаторе
Пример	Включить MRPP в режиме глобальной конфигурации. Switch(config)#mrpp enable

12.1.9. Включить режим совместимости с ERPP (mrpp errp compatible)

Команда	mrpp errp compatible no mrpp errp compatible	
Параметр	-	
Состояние по умолчанию	Режим совместимости с ERPP отключен	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Если необходимо настроить функцию совместимости ERPP, сначала следует включить протокол MRPP. Кроме того, порт с режимом совместимости с ERPP должен быть настроен как гибридный или магистральный и пропускать пакеты с информацией Control Vlan	
Пример	Включить режим совместимости с ERPP в режиме глобальной конфигурации. Switch(Config)#mrpp enable Switch(Config)#mrpp errp compatible Switch(Config)#mrpp ring 2 Switch(mrpp-ring-2)#control-vlan 4000 Switch(config-if-ethernet1/51)#switchport mode hybrid Switch(config-if-ethernet1/51)#switchport hybrid allowed vlan 4000 tag Switch(config-if-ethernet1/52)#switchport mode hybrid Switch(config-if-ethernet1/52)#switchport hybrid allowed vlan 4000 tag	

12.1.10. Установить интервал опроса MRPP (mrpp poll-time)

Команда	mrpp poll-time <20-2000>	
Параметр	<20-2000>	время запроса, единица измерения: мс



Состояние по умолчанию	Конфигурация по умолчанию 100 мс
Режим	Режим глобальной конфигурации
Руководство по использованию	Позволяет задать интервал опроса для корректировки времени опроса MRPP, по умолчанию 100 мс
Пример	Установить время опроса в 200 мс. Switch(Config)# mrpp poll-time 200

12.1.11. Создать кольцо MRPP и войти в режим настройки (mrpp ring)

Команда	mrpp ring <ring-id> no mrpp ring <ring-id>	
Параметр	ring-id	идентификатор кольца MRPP, в пределах от 1 до 4096
Состояние по умолчанию	Идентификатор кольца настроен	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Если данное кольцо MRPP не существует, будет создано новое кольцо и выполнен вход в режим кольца MRPP. Отключение данного кольца MRPP выполняется по команде "no mrpp ring"	
Пример	Создать кольцо MRPP 100. Switch(config)#mrpp ring 100	

12.1.12. Задать первичный порт кольца MRPP (mrpp ring primary-port)

Команда	mrpp ring <ring-id> primary-port {cos <cos>}] no mrpp ring <ring-id> primary-port	
Параметр	ring-id	идентификатор кольца MRPP; в диапазоне <1-4096>
	cos <cos>	значение присваиваемого приоритета cos в заголовке пакета; в диапазоне <0-7>
Состояние по умолчанию	Конфигурация отсутствует, значение cos по умолчанию равно 0	



Режим	Настройка портов
Руководство по использованию	Команда позволяет задать первичный порт кольца MRPP. Первичный узел отправляет пакеты Hello через первичный порт, вторичный порт принимает пакеты Hello, посылаемые первичным узлом. Первичный и вторичный порты вторичного узла работают одинаково
Пример	Установить порт Ethernet 1/0/1 как первичный порт кольца MRPP 4000. Switch(Config)#interface ethernet 1/0/1 Switch(config-if-Ethernet1/0/1)#mrpp ring 4000 primary-port

12.1.13. Задать вторичный порт кольца MRPP (mrpp ring secondary-port)

Команда	mrpp ring < ring-id > secondary-port {cos <cos>} no mrpp ring < ring-id > secondary-port	
Параметр	ring-id	идентификатор кольца MRPP; в диапазоне <1-4096>
	cos <cos>	значение присваиваемого приоритета cos в заголовке пакета; в диапазоне <0-7>
Состояние по умолчанию	Конфигурация отсутствует, значение cos по умолчанию равно 0	
Режим	Настройка портов	
Руководство по использованию	Команда позволяет задать вторичный порт кольца MRPP. Первичный узел использует вторичный порт для приема пакетов Hello от первичного узла. Первичный и вторичный порты вторичного узла работают одинаково. Команда "mrpp enable" должна быть введена до ввода команды "control-vlan". Если после ввода команды control-vlan сконфигурированы первичный и вторичный порты, тип узлов и введена команда "enable", то тем самым будет включена функция mrpp-ring	
Пример	Установить порт 1/0/3 как вторичный порт кольца MRPP Switch(config)#interface ethernet1/0/3 Switch(Config-If-Ethernet1/0/3)#mrpp ring 4000 secondary-port	

12.1.14. Задать тип узла кольца MRPP (node-mode)

Команда	node-mode {maser transit}
Параметр	-



Состояние по умолчанию	По умолчанию тип узла - вторичный узел
Режим	Режим кольца MRPP
Руководство по использованию	Позволяет задать тип узла как первичный узел или вторичный узел
Пример	Установить коммутатор, как первичный узел кольца MRPP 4000. Switch(config)# mrpp ring 4000 Switch(mrpp-ring-4000)#node-mode master

12.1.15. Просмотр настроек кольца MRPP (show mrpp)

Команда	show mrpp [<ring-id>]	
Параметр	ring-id	идентификатор кольца MRPP, в пределах от 1 до 4096. Если ID не указан, будет выведена информация о настройках всех колец MRPP
Состояние по умолчанию	-	
Режим	Привилегированный режим и режим конфигурации	
Руководство по использованию	Позволяет вывести на экран информацию о настройках кольца MRPP	
Пример	Вывести информацию о настройках кольца MRPP 4000. Switch# show mrpp 4000	

12.1.16. Просмотр статистики кольца MRPP (show mrpp statistics)

Команда	show mrpp statistics [<ring-id>]	
Параметр	ring-id	идентификатор кольца MRPP, в пределах от 1 до 4096. Если ID не задан будут выведена статистическая информация для всех колец MRPP
Состояние по умолчанию	-	
Режим	Привилегированный режим и режим конфигурации	



Руководство по использованию	Позволяет вывести на дисплей информацию о переданных и принятых пакетах кольца MRPP
Пример	Вывести статистическую информацию кольца MRPP 4000 на коммутаторе. Switch# show mrpp statistic 4000

12.2. Команды для настройки ULPP

12.2.1. Очистить счетчики flush-пакетов на интерфейсе (clear ulpp flush counter interface)

Команда	clear ulpp flush counter interface <name>	
Параметр	name	имя порта
Состояние по умолчанию	-	
Режим	Привилегированный режим	
Руководство по использованию	Очищает статистику пакетов	
Пример	Удалить статистическую информацию о пакетах flush для порта 1/0/1 Switch#clear ulpp flush counter interface e1/0/1	

12.2.2. Задать управляющий VLAN (control vlan)

Команда	control vlan <integer> no control vlan	
Параметр	integer	идентификатор управляющей виртуальной локальной сети, которая отправляет flush-пакеты, диапазон от 1 до 4094
Состояние по умолчанию	По умолчанию используется VLAN 1	
Режим	Режим конфигурации группы ULPP	



Руководство по использованию	Позволяет задать идентификатор VLAN ID, управляющей группой ULPP. Эта VLAN должна соответствовать существующей VLAN, после чего эта VLAN не может быть удалена. Она должна принадлежать VLAN, защищенной группой ULPP во избежание возникновения петли flush-пакетов
Пример	Настроить управляющую отправкой VLAN для группы ULPP как 10. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# control vlan 10

12.2.3. Задать описание для ULPP группы (description)

Команда	description <string> no description	
Параметр	string	имя ULPP группы, не более 128 символов
Состояние по умолчанию	Имя ULPP не задано	
Режим	Режим конфигурации группы ULPP	
Руководство по использованию	Задаёт описание для ULPP группы. "no" в начале команды удаляет описание	
Пример	Задать описание для ULPP группы как коммутатора. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# description switch	

12.2.4. Включить/выключить функцию отправки flush пакета для обновления ARP-таблицы (flush {enable |disable} arp)

Команда	flush {enable disable} arp
Параметр	-
Состояние по умолчанию	По умолчанию включена функция отправки flush-пакетов, удаленных ARP
Режим	Режим конфигурации группы ULPP
Руководство по использованию	Данная команда позволяет отключить отправку flush-пакетов, инициализирующих удаление записей ARP, вышестоящему коммутатору, которая производится, если произошло переключение линии



Пример	Отключить отправку flush-пакетов удаления записи ARP. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# flush disable arp

12.2.5. Включить/выключить функцию отправки flush пакета для обновления MAC-таблицы (flush {enable |disable} mac)

Команда	flush {enable disable}mac
Параметр	-
Состояние по умолчанию	Отправка flush пакета для обновления MAC-адреса включена
Режим	Режим конфигурации группы ULPP
Руководство по использованию	Данная команда позволяет отключить отправку flush-пакетов, инициализирующих обновление таблицы MAC-адресов, вышестоящему коммутатору, которое выполняется, если произошло переключение линии
Пример	Отключить отправку flush пакета для обновления MAC-адреса. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# flush disable mac

12.2.6. Включить/выключить функцию отправки flush пакета для удаления MAC из MAC-VLAN (flush {enable |disable} mac-vlan)

Команда	flush {enable disable}mac-vlan
Параметр	-
Состояние по умолчанию	Отключено
Режим	Режим конфигурации группы ULPP
Руководство по использованию	Данная команда позволяет отключить отправку flush-пакетов, инициализирующих удаление динамических одноадресных MAC-адресов, вышестоящему коммутатору, которое выполняется, если произошло переключение линии



Пример	Выключить функцию отправки flush пакета для удаления mac-vlan. Switch(config)#ulpp group 1 Switch(ulpp-group-1)#flush disable mac-vlan

12.2.7. Время задержки приоритетного переключения (preemption delay)

Команда	preemption delay <integer> no preemption delay	
Параметр	integer	задержка, в диапазоне от 1 до 600 секунд
Состояние по умолчанию	30 секунд	
Режим	Режим конфигурации группы ULPP	
Руководство по использованию	Задержка приоритетного переключения - это время задержки до того, как ведущий порт будет переведен в состояние переадресации, что позволяет избежать колебаний соединения в течение короткого времени. Задержка приоритетного переключения выполняется после того, как включен режим приоритетного переключения	
Пример	Установить задержку приоритетного переключения в 50 секунда для группы ULPP. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# preemption delay 50	

12.2.8. Режим приоритетного переключения (preemption mode)

Команда	preemption mode no preemption mode
Параметр	-
Состояние по умолчанию	Переключение не производится
Режим	Режим конфигурации группы ULPP
Руководство по использованию	Если группой ULPP настроен режим переключения приоритета, то, когда slave-порт находится в состоянии передачи (forwarding state), а master-порт в резервном состоянии (standby state), master-порт вернется в состояние передачи, а slave-порт – в резервное состояние, только спустя время, заданное командой "preemption delay"



Пример	Установить режим переключения группы ULPP. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# preemption mode

12.2.9. Обозначить VLAN, защищаемые ULPP группой (protect vlan-reference-instance)

Команда	protect vlan-reference-instance <instance-list> no protect vlan-reference-instance <instance-list>	
Параметр	instance-list	список MSTP экземпляров связующего дерева (instance), например, i; j-k. Количество экземпляров в списке не ограничено
Состояние по умолчанию	Защита VLAN не производится, то есть не выполняется отсылок ни на какой экземпляр	
Режим	Режим конфигурации группы ULPP	
Руководство по использованию	Данная команда задает список MSTP экземпляров для защиты VLAN. VLAN, соответствующие этому экземпляру, передаются через один из портов ULPP группы и заблокированы на другом порту группы. Каждая ULPP группа может ссылаться на все экземпляры связующего дерева MSTP. Она также может ссылаться на несуществующие экземпляры MSTP, что означает, что никакие VLAN не защищены. Различные ULPP группы не могут ссылаться на одни и те же экземпляры связующего дерева	
Пример	Настроить защищаемую VLAN с отсылкой из экземпляра 1 для группы ULPP. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# protect vlan-reference-instance 1	

12.2.10. Просмотр статистики о переданных и полученных flush-пакетах (show ulpp flush counter interface)

Команда	show ulpp flush counter interface {ethernet <IFNAME> <IFNAME>}	
Параметр	IFNAME	имя порта
Состояние по умолчанию	-	
Режим	Привилегированный режим	



Руководство по использованию	Выводит на экран статистику о flush-пакетах, например, сколько пакетов было
Руководство по использованию	получено и время получения пакетов
Пример	Вывести статистическую информацию о flush пакетах для группы ULPP1. Switch# show ulpp flush counter interface e1/0/1 Received flush packets: 10

12.2.11. Просмотр информации о порте, получившем flush-пакет (show ulpp flush-receive-port)

Команда	show ulpp flush-receive-port
Параметр	-
Состояние по умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	Выводит на экран информацию о порте, получившем flush-пакет и тип пакета и управляющей VLAN
Пример	Вывести информацию о порте, получающем flush-пакеты. Switch# show ulpp flush-receive-port ULPP flush-receive portlist: Portname Type Control Vlan Ethernet1/0/1 ARP 1 Ethernet1/0/3 MAC 1; 3; 5-10

12.2.12. Просмотр информации о сконфигурированных ULPP группах (show ulpp group)

Команда	show ulpp group [group-id]	
Параметр	group-id	информация о указанной группе ULPP



Состояние по умолчанию	По умолчанию отображается информация обо всех группах ULPP, которые были настроены														
Режим	Привилегированный режим														
Руководство по использованию	Выводит на экран информацию о сконфигурированных ULPP группах: состояние портов "master" и "slave", режим переключения, задержку переключения и прочее														
Пример	Вывести информацию о настройках ULPP group1. <pre>Switch# show ulpp group 1</pre> ULPP flush-receive portlist: <table><thead><tr><th>Portname</th><th>Type</th><th>Control Vlan</th></tr></thead><tbody><tr><td colspan="3"> </td></tr></tbody></table> Switch#show ulpp group 20 ULPP group 20 information: Description: switch Preemption mode: ON Preemption delay: 50s Control VLAN: 10 Flush packet: NONE Protected VLAN: Reference Instance 1 <table><thead><tr><th>Member</th><th>Role</th><th>State</th><th>Track-cfm-level</th></tr></thead><tbody><tr><td colspan="4"> </td></tr></tbody></table>	Portname	Type	Control Vlan				Member	Role	State	Track-cfm-level				
Portname	Type	Control Vlan													
Member	Role	State	Track-cfm-level												

12.2.13. Задать список управляющих VLAN, принимающих flush-пакеты (ulpp control vlan)

Команда	ulpp control vlan <vlan-list> no ulpp control vlan <vlan-list>	
Параметр	vlan-list	список управляющих VLAN, которые получают flush-пакеты, например, i; j-k. Количество VLAN в каждой строке символов не может превышать. Допускается добавление получающей управляющей VLAN порта
Состояние по умолчанию	VLAN 1	
Режим	Настройка портов	



Руководство по использованию	Задаёт список управляющих VLAN, которые принимают flush-пакеты. Данная команда должна ссылаться на существующие VLAN. После ввода команды эти VLAN не могут быть удалены
Пример	Задать управляющую VLAN, принимающую пакеты как 10. Switch(config)# interface ethernet 1/0/1 Switch(config-If-Ethernet1/0/1)# ulpp control vlan 10

12.2.14. Включить/выключить функцию приема flush-пакета для обновления ARP-таблицы на порту (ulpp flush {enable|disable} arp)

Команда	ulpp flush {enable disable} arp
Параметр	-
Состояние по умолчанию	Функция приема flush-пакета для обновления ARP-таблицы отключена
Режим	Режим конфигурации порта
Руководство по использованию	Если эта команда установлена, flush-пакеты для удаления ARP не будут приниматься
Пример	Отключить прием flush-пакетов удаления ARP. Switch(config)# interface ethernet 1/0/1 Switch(config-If-Ethernet1/0/1)# ulpp flush disable arp

12.2.15. Включить/выключить функцию отправки flush пакета для обновления MAC-таблицы на порту (ulpp flush {enable|disable} mac)

Команда	ulpp flush {enable disable} mac
Параметр	-
Состояние по умолчанию	Функция приема flush-пакета для обновления MAC-адресов отключена
Режим	Режим конфигурации порта
Руководство по использованию	Если эта команда задана, flush-пакеты для обновления MAC-адресов не будут приниматься



Пример	Отключить получение flush-пакетов обновления MAC-адресов. Switch(config)# interface ethernet 1/0/1 Switch(config-if-Ethernet1/0/1)# ulpp flush disable mac

12.2.16. Включить/выключить функцию отправки flush пакета для удаления MAC из MAC-VLAN на порту (ulpp flush {enable|disable} mac-vlan)

Команда	ulpp flush {enable disable} mac-vlan
Параметр	-
Состояние по умолчанию	Отключение
Режим	Режим конфигурации порта
Руководство по использованию	При включении этой функции аппаратное обеспечение будет пересылать полученные в порт пакеты flush с типом mac-vlan. Они не будут анализироваться
Пример	Отключить прием flush-пакетов, удаленных mac-vlan порта. Switch(config)#interface e1/0/2 Switch(config-if-ethernet1/0/2)#ulpp flush disable mac-vlan

12.2.17. Создать ULPP группу (ulpp group)

Команда	ulpp group <integer> no ulpp group <integer>	
Параметр	integer	идентификатор ULPP группы, от 1 до 48
Состояние по умолчанию	Ни одна группа ULPP не создана	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Создает ULPP группу. Если группа существует, команда позволяет войти в режим настройки данной ULPP группы. "no" в начале команды удаляет группу ULPP	
Пример	Создать группу ulpp 20 или зайти в режим конфигурации группы ulpp 20. Switch(config)# ulpp group 20	



	Switch(ulpp-group-20)#

12.2.18. Определение master-порта и slave-порта в группе (ulpp group {master|slave})

Команда	ulpp group <integer> {master slave} no ulpp group <integer> {master slave}	
Параметр	integer	идентификатор ULPP группы, от 1 до 48
Состояние по умолчанию	master-порт не задан	
Режим	Настройка портов	
Руководство по использованию	Последовательность определения master-порта и slave-порта в группе не важна, но защищаемые VLAN должны быть определены до конфигурации портов. В каждой группе может быть только один master-порт, если master-порт существует, то конфигурация не работает	
Пример	Задать master-порт для ULPP группы. Switch(config)# interface ethernet 1/0/2 Switch(config-If-Ethernet1/0/2)# ulpp group 20 slave	

12.3. Команды для настройки ULSM

12.3.1. Просмотр сконфигурированных ULSM групп (show ulsm group)

Команда	show ulsm group [group-id]	
Параметр	group-id	идентификатор группы ULSM
Состояние по умолчанию	Отображается информация о всех сконфигурированных ULSM группах	
Режим	Привилегированный режим	
Руководство по использованию	Команда выводит на экран информацию о сконфигурированных ULSM группах	
Пример	Вывести на дисплей информацию о ULSM group1. Switch# show ulsm group 1	



12.3.2. Создать ULSM группу (ulsm group)

Команда	ulsm group <group-id> no ulsm group <group-id>	
Параметр	group-id	идентификатор ULSM группы, от 1 до 32
Состояние по умолчанию	По умолчанию группы ULSM не существует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда создает ULSM группу. "no" в начале команды удаляет группу ULSM	
Пример	Создать группу 10 ULSM. Switch(config)# ulsm group 10	

12.3.3. Задать порт исходящей/нисходящей связи ULSM-группы (ulsm group {uplink | downlink})

Команда	ulsm group <group-id> {uplink downlink} no ulsm group <group-id>	
Параметр	group-id	идентификатор ULSM группы, от 1 до 32
	uplink	конфигурирует порт как порт исходящей uplink связи
	downlink	конфигурирует порт как порт нисходящей downlink связи
Состояние по умолчанию	Порты не принадлежат ULSM группе	
Режим	Режим конфигурации порта	
Руководство по использованию	Задаёт порт исходящей/нисходящей связи ULSM-группы. В каждой ULSM группе может быть до 8 uplink-портов и до 16 downlink-портов	
Пример	Установит port1/0/3 в качестве uplink-порта группы 10 ULSM. Switch(config)# interface ethernet 1/0/3 Switch(config-if-Ethernet1/0/3)# ulsm group 10 uplink	



13. КОМАНДЫ ДЛЯ НАСТРОЙКИ ЗЕРКАЛИРОВАНИЯ ПОРТОВ

13.1. Команды для настройки зеркалирования портов

13.1.1. Задать интерфейс-источник зеркалирования (monitor session source interface)

Команда	monitor session <session> source {interface <interface-list> cpu} {rx tx both} no monitor session <session> source {interface <interface-list> cpu}	
Параметр	session	номер сессии зеркалирования. В настоящее время поддерживается только 1
	interface-list	список портов-источников зеркального порта, в качестве разделителей можно использовать "-" и " , "
	cpu	обозначает процессор на материнской плате, который будет использоваться в качестве источника зеркалирования для отладки. Датаграммы, полученные или переданные этим процессором
	rx	зеркалирование принимаемого трафика
	tx	зеркалирование передаваемого трафика
	both	зеркалирование принимаемого и передаваемого трафика
Состояние по умолчанию	Порт источник зеркалирования не указан	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда используется для настройки интерфейсов-источников зеркалирования. На порт-источник в коммутаторах не накладывается никаких ограничений. Это может быть один интерфейс, либо множество интерфейсов. Принимаемые и посылаемые данные могут зеркалироваться одновременно и выборочно. Если параметр для направления [rx tx both] не указан, по умолчанию используется значение "both". При зеркалировании нескольких интерфейсов направление может быть разным, но они должны быть настроены по отдельности	



Пример	Настроить зеркалирование потока, посланного интерфейсом 1/0/1-4 и зеркалирование потока, полученного интерфейсом 1/0/5. <pre>Switch(config)#monitor session 1 source interface ethernet 1/0/1-4 tx Switch(config)#monitor session 1 source interface ethernet 1/0/5 rx</pre>

13.1.2. Список доступа для управления источником порта зеркалирования (monitor session source interface access-list)

Команда	<pre>monitor session <session> source {interface <interface-list>} access-list <num> {rx tx both} no monitor session <session> source {interface <interface-list>} access-list <num></pre>	
Параметр	session	номер сессии зеркалирования. В настоящее время поддерживается 1
	interface-list	список интерфейсов источника зеркального порта, в качестве разделителей применяется '-' и ','
	num	номер списка доступа
	rx	зеркалирование принимаемого трафика
	tx	зеркалирование передаваемого трафика
	both	зеркалирование принимаемого и передаваемого трафика
Состояние по умолчанию	Не сконфигурирован	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда используется для настройки интерфейсов-источников зеркалирования. На порт-источник в коммутаторах не накладывается никаких ограничений. Это может быть один интерфейс, либо множество интерфейсов. При зеркалировании потоков могут зеркалироваться только принятые данные. Указываемыми параметрами могут быть rx, tx, both. Список доступа, используемый в команде, должен быть подготовлен до ее ввода. О том, как настроить список доступа, читайте в разделе настройки списка доступа ACL. Зеркальный порт может быть создан только после того, как будут заданы интерфейс назначения и соответствующий сеанс. В данный момент команда включает только IP ACL и MAC ACL	



Пример	Задать на зеркальном интерфейсе 1/0/6 фильтрацию пакетов в соответствии со списком доступа 120 в сеансе 1. Switch(config)#monitor session 1 source interface 1/0/6 access-list 120 rx

13.1.3. Задать интерфейс назначения зеркалирования (monitor session destination interface)

Команда	monitor session <session> destination interface <interface-number> no monitor session <session> destination interface <interface-number>	
Параметр	session	номер сеанса зеркала, в настоящее время поддерживается только 1-4
	interface-number	это интерфейс назначения зеркала
Состояние по умолчанию	По умолчанию не совпадает с портом назначения зеркала	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Коммутатор поддерживает только четыре зеркальных интерфейса назначения. Обратите внимание: интерфейс, заданный в качестве назначения зеркалирования, не должен быть интерфейсом магистрального канала. Кроме того, рекомендуется, чтобы максимальная пропускная способность интерфейса превышала суммарную пропускную способность зеркалируемых интерфейсов. Если назначение удалено, настроенный путь зеркалирования также удаляется. Если интерфейс назначения перенастроен, пути зеркалирования интерфейса и процессора будут восстановлены. Важно отметить, что зеркалирование трафика может быть возобновлено только после изменения конфигурации интерфейса назначения	
Пример	Задать интерфейс 1/0/7 в качестве интерфейса назначения зеркалирования Switch(config)#monitor session 1 destination interface ethernet 1/0/7	

13.1.4. Просмотр информации о сессии зеркалирования (show monitor)

Команда	show monitor
Параметр	-
Состояние по умолчанию	-



Режим	Привилегированный режим
Руководство по использованию	Команда позволяет вывести на экран информацию об источнике и порте назначения для указанной сессии зеркалирования. Для зеркалирования портов, зеркалирования процессора и зеркалирования трафика можно отобразить режим зеркалирования источника
Пример	Просмотр информации о конфигурации для текущего изображения. Switch#show monitor

13.2. Команды для настройки протокола sFlow

13.2.1. Идентификатор агента sFlow (sflow agent-address)

Команда	sflow agent-address <agent-address> no sflow agent-address	
Параметр	agent-address	IP-адрес прокси-сервера, который отображается в десятичной записи с точками
Состояние по умолчанию	Значение по умолчанию отсутствует	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда используется для настройки адреса sFlow-прокси. Адрес прокси используется для маркировки образца прокси, что аналогично OSPF или Router ID в BGP. Однако он не является необходимым для правильной работы прокси-сервера sFlow	
Пример	Выбрать адрес прокси-сервера в глобальном режиме. switch (config)#sflow agent-address 192.168.1.200	

13.2.2. Анализатор sFlow (sflow analyzer)

Команда	sflow analyzer sflowtrend no sflow analyzer sflowtrend	
Параметр	-	
Состояние по умолчанию	Не настроен	
Режим	Режим глобальной конфигурации	



Руководство по использованию	Эта команда используется для настройки анализатора sFlow, команда с "no" в своем начале отключает анализатор. Команда задается при использовании sFlowTrend
Пример	Подключить анализатор sFlow. Switch(config)#sflow analyzer sflowtrend

13.2.3. Интервал сбора статистики sFlow (sflow counter-interval)

Команда	sflow counter-interval <interval-value> no sflow counter-interval	
Параметр	interval-value	значение интервала с допустимым диапазоном 20~120, в секундах
Состояние по умолчанию	Значение по умолчанию отсутствует	
Режим	Режим конфигурации порта	
Руководство по использованию	Если интервал выборки статистики не задан, выборка статистики на интерфейсе производиться не будет	
Пример	Установить интервал выборки статистики на интерфейсе e1/0/1 равный 20 секундам. Switch(Config-If-Ethernet1/0/1)#sflow counter-interval 20	

13.2.4. Настроить максимальную длину группы выборок sFlow (sflow data-len)

Команда	sflow data-len <length-value> no sflow data-len	
Параметр	length-value	значение длины в диапазоне 500-1470
Состояние по умолчанию	1400	
Режим	Режим конфигурации порта	
Руководство по использованию	Команда задает значение длины пакета sFlow. При объединении нескольких выборок в одну группу пакетов sFlow длина группы пакетов без учета MAC-заголовка и части IP-заголовка не должна превышать установленного значения	



Пример	Установить максимальную длину данных пакета sFlow на 1000. switch (Config-If-Ethernet1/0/2)#sflow data-len 1000

13.2.5. Адрес и порт назначения для отправки данных sFlow (sflow destination)

Команда	sflow destination <collector-address> [<collector-port>] no sflow destination	
Параметр	collector-address	IP-адрес анализатора, отображается в десятично-точечной записи
	collector-port	порт назначения отправленных пакетов sFlow
Состояние по умолчанию	Порт назначения пакета sFlow по умолчанию равен 6343, а у анализатора нет адреса по умолчанию	
Режим	В режиме глобальной конфигурации и конфигурации порта	
Руководство по использованию	Если адрес анализатора настроен в режиме порта, то этот IP-адрес и сконфигурированный порт будут применяться при отправке пакетов выборки. В противном случае будут применяться адрес и порт, настроенные в глобальном режиме. Для правильной работы прокси-сервера выборки sFlow необходимо установить адрес анализатора	
Пример	Настроить адрес и порт анализатора в глобальном режиме. switch (config)#sflow destination 192.168.1.200 1025	

13.2.6. Настроить длину заголовка пакета, копируемого в sFlow (sflow header-len)

Команда	sflow header-len <length-value> no sflow header-len	
Параметр	length-value	значение длины в диапазоне 32-256
Состояние по умолчанию	128	
Режим	Режим конфигурации порта	



Руководство по использованию	Команда позволяет задать длину заголовка пакета, копируемого в sFlow. Команда с "no" в начале возвращает значение по умолчанию. Если образец пакета отправляется на CPU без идентификации его как IPv4 или IPv6, определенная длина содержимого группового заголовка должна быть скопирована в пакет sFlow и отправлена. Длина копируемого содержимого задается этой командой
Пример	Установить длину копируемого содержимого заголовка в sFlow равной 50. Switch(Config-If-Ethernet1/0/2)#sflow header-len 50

13.2.7. Задать приоритет sFlow прокси (sflow priority)

Команда	sflow priority <priority-value> no sflow priority	
Параметр	priority-value	значение приоритета в диапазоне 0-3
Состояние по умолчанию	0	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда используется для установки приоритета передачи сообщения выборки. Рекомендуется не назначать высокий приоритет пакетам выборки при их отправке на CPU, чтобы не мешать нормальному приему и передаче других протокольных пакетов. Чем выше установлено значение, тем выше будет приоритет	
Пример	Настроить приоритет при получении пакетов sFlow от оборудования в глобальном режиме. switch (config)#sflow priority 1	

13.2.8. Настроить частоту дискретизации (sflow rate)

Команда	sflow rate { input <input-rate> output <output-rate >} no sflow rate [input output]	
Параметр	input-rate	скорость выборки входящих групп, допустимый диапазон 1000~16383500
	output-rate	скорость выборки исходящих групп, допустимый диапазон 1000~16383500
Состояние по умолчанию	Отсутствует	



Режим	Режим конфигурации порта
Руководство по использованию	Выборка трафика не будет выполняться, если на порту не настроена частота выборки. Если частота выборки входящих групп установлена на 10000, это означает, что на каждые 10000 входящих групп будет выбрана одна группа
Пример	Задать частоту выборки входящих групп на порту e1/0/1 на 10000, а частоту выборки исходящих групп - на 20000. <pre>Switch(Config-If-Ethernet1/0/1)#sflow rate input 10000 Switch(Config-If-Ethernet1/0/1)#sflow rate output 20000</pre>

13.2.9. Просмотр информации о работе sFlow (show sflow)

Команда	show sflow						
Параметр	-						
Состояние по умолчанию	-						
Режим	Все режимы						
Руководство по использованию	Команда используется для отображения информации о работе sFlow						
Пример	Вывести информацию о конфигурации sFlow. <pre>Switch#show sflow Sflow version 1.2 Agent address is 172.16.1.100 Collector address have not configured Collector port is 6343 Sampler priority is 2 Sflow DataSource: type 2, index 194(Ethernet1/0/2) Collector address is 192.168.1.200 Collector port is 6343 Counter interval is 0 Sample rate is input 0, output 0 Sample packet max len is 1400 Sample header max len is 50 Sample version is 4</pre> <table border="1"> <tr> <th>Информация, отображаемая на экране</th><th>Пояснения</th></tr> <tr> <td>Sflow version 1.2</td><td>Версия протокола sFlow 1.2</td></tr> <tr> <td>Agent address is 172.16.1.100</td><td>IP-адрес агента sFlow: 172.16.1.1100</td></tr> </table>	Информация, отображаемая на экране	Пояснения	Sflow version 1.2	Версия протокола sFlow 1.2	Agent address is 172.16.1.100	IP-адрес агента sFlow: 172.16.1.1100
Информация, отображаемая на экране	Пояснения						
Sflow version 1.2	Версия протокола sFlow 1.2						
Agent address is 172.16.1.100	IP-адрес агента sFlow: 172.16.1.1100						



	Collector address have not configured	Глобальный адрес анализатора sFlow не сконфигурирован
	Collector port is 6343	Глобальный порт назначения для отправки данных sFlow установлен по умолчанию - 6343.
	Sampler priority is 2	Приоритет, когда sFlow получает пакеты от аппаратной части 2.
	Sflow DataSource: type 2, index 194(Ethernet1/0/1)	Одним из прокси-источников выборки данных sFlow является интерфейс e1/0/1, тип 2 (Ethernet), индекс интерфейса - 194.
	Collector address is 192.168.1.200	Адрес коллектора данных выборки интерфейса E1/0/1 - 192.168.1.200
	Collector port is 6343	Значение по умолчанию для порта прокси выборки интерфейса E1/0/1 равно 6343.
	Counter interval is 20	Интервал выборки статистики на интерфейсе e1/0/1 составляет 20 секунд.
	Sample rate is input 10000, output 0	Скорость входящего трафика прокси-выборки интерфейса e1/0/1 равна 10000, а выборка исходящего трафика не будет производиться
	Sample packet max len is 1400	Длина данных группы sFlow, отправляемых интерфейсом e1/0/1, не должна превышать 1400 байт.
	Sample header max len is 50	Длина заголовка данных пакета, скопированного в выборку данных интерфейса e1/0/1, составляет 50
	Sample version is 4	Версия дейтаграммы группы sFlow, отправленной прокси-выборкой интерфейса E1/0/1, равна 4



13.3. Команды конфигурирования RSPAN

13.3.1. Настройка RSPAN VLAN (remote-span)

Команда	remote-span no remote-span	
Параметр	-	
Состояние по умолчанию	по	Не сконфигурировано
Режим	Режим настройки VLAN	
Руководство по использованию	Команда позволяет настроить существующую VLAN как RSPAN VLAN. Перед началом работы RSPAN необходимо настроить выделенную сеть RSPAN VLAN. При настройке RSPAN VLAN следует убедиться, что такие виртуальные локальные сети как стандартные, динамические, частные, многоадресные и виртуальные локальные сети с включенными интерфейсами уровня 3, не сконфигурированы как RSPAN VLAN. Если при отключении RSPAN все еще активны существующие сеансы, они останутся активными независимо от изменений конфигурации. Однако если после отключения RSPAN в VLAN будут настроены интерфейсы уровня 3, существующие сеансы RSPAN прекратятся	
Пример	RSPAN VLAN. Сконфигурирована VLAN 5. Switch(Config-Vlan5)#remote-span	

13.3.2. Задать удаленный VLAN для мониторинговой сессии (monitor session remote vlan)

Команда	monitor session <session> remote vlan <vid> no monitor session <session> remote vlan	
Параметр	session	идентификатор сессии, в диапазоне от 1 до 4
	vid	идентификатор RSPAN VLAN
Состояние по умолчанию	по	Не сконфигурировано
Режим	Режим глобальной конфигурации	



Руководство по использованию	Команда применяется для настройки локальной зеркальной сессии RSPAN. Идентификатор VLAN - это VLAN RSPAN. Зеркалируемые дейтаграммы будут снабжены тегами RSPAN
Пример	Настроить удаленный vlan зеркалирования для сессии 1 на 5. Switch(config)#monitor session 1 remote vlan 5

13.3.3. Настройка порта-отражателя (monitor session reflector-port)

Команда	monitor session <session> reflector-port <interface-number> no monitor session <session> reflector-port <interface-number>	
Параметр	session	идентификатор сессии в диапазоне от 1 до 4
	interface-number	номер интерфейса
Состояние по умолчанию	Не сконфигурировано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда устанавливает порт-отражатель в качестве порта назначения для зеркалированных дейтаграмм и отключает обучение MAC-адресов для указанного порта. Конфигурация порта-отражателя заключается в изменении режима локального порта с режима порта назначения на режим рефлектора. Таким образом, конфигурация порта-отражателя и порта назначения являются эксклюзивными. Для восстановления нормального режима работы порта-рефлектора в начало команды ставится "no". Порт источника, работающий как порт доступа или магистральный порт, не должен добавляться в RSPAN VLAN. Если порт-отражатель настроен как отправная точка зеркалирования направления CPU TX, он должен быть настроен как порт TRUNK и позволять передачу данных RSPAN VLAN, Native VLAN не должен быть настроен как RSPAN VLAN. После настройки RSPAN, к пакету зеркала на выходе добавляется тег vlan. Это приведет к ошибке прерывания кадра на порту отражения, поэтому значение MTU коммутатора по умолчанию должно быть изменено	
Пример	Настроить порт 1/0/5 как порт-отражатель. Switch(config)#monitor session 1 reflector-port ethernet1/0/5	



14. КОМАНДЫ ДЛЯ УПРАВЛЕНИЯ СЕТЕВЫМ ВРЕМЕНЕМ

14.1. Команды для настройки SNTP

14.1.1. Задать часовой пояс (clock timezone)

Команда	clock timezone WORD {add subtract} <0-23> [<0-59>] no clock timezone WORD	
Параметр	WORD	название часового пояса, длина не должна превышать 16
	add subtract	смещение времени в часовом поясе
	<0-23>	часы
	<0-59>	минуты
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Эта команда настраивает часовой пояс в глобальном режиме. Имя часового пояса не может быть пустым, значение часа и минуты должно находиться в определенном диапазоне. Команда с "no" в начале удаляет заданный часовой пояс	
Пример	Установить смещение в часовой пояс +3 в глобальном режиме. Switch(config)#clock timezone MSK add 3	

14.1.2. Задать интервал синхронизации SNTP (sntp polltime)

Команда	sntp polltime <interval> no sntp polltime	
Параметр	<interval>	значение интервала, в пределах от 16 до 16284
По умолчанию	64 секунды	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать интервал отправки запросов на NTP/SNTP-сервер. "no" в начале команды отменяет настройки для интервала опроса и восстанавливает значение, заданное по умолчанию	



Пример	Задать отправку клиентом запросов на сервер каждые 128 секунд. Switch(config)#ntp polltime128

14.1.3. Указать сервер времени как источник синхронизации (ntp server)

Команда	ntp server {<ip-address> <ipv6-address>} [source {vlan <vlan no> loopback <loopback no>}] [version <version_no>] no ntp server {<ip-address> <ipv6-address>} [source {vlan <vlan no> loopback <loopback no>}] [version <version_no>]	
Параметр	<ip-address>	IPv4-адрес сервера времени
	<ipv6-address>	IPv6-адрес сервера времени
	<vlan no>	номер виртуальной локальной сети, в диапазоне от 1 до 4094
	<loopback no>	идентификатор интерфейса loopback, в диапазоне от 1 до 1024
	<version_no>	номер версии, от 1 до 4, по умолчанию - 4
По умолчанию	Сервер времени не задан	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет указать сервер времени как источник синхронизации. Команда с "no" в начале удаляет указанный сервер	
Пример	Задать адрес сервера времени как 1.1.1.1, указать интерфейс исходного адреса как vlan1: Switch(config)#ntp server 1.1.1.1 source vlan 1	

14.1.4. Просмотр текущих настроек SNTP (show sntp)

Команда	show sntp	
Параметр	none	отсутствует
По умолчанию	Не задано	



Режим	Привилегированный режим /Режим глобальной конфигурации
Руководство по использованию	Позволяет вывести на экран текущие настройки SNTP-клиента и состояние сервера
Пример	Вывести на экран текущие настройки SNTP. Switch(config)#show sntp

14.2. Команды для настройки NTP

14.2.1. Фильтрация по списку доступа при работе коммутатора в режиме NTP-сервера (ntp access-group)

Команда	ntp access-group server <acl> no ntp access-group server <acl>	
Параметр	<acl>	номер ACL, в пределах от 1 до 99
По умолчанию	Список доступа на NTP-сервере не задан	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет установить или отменить фильтрацию по списку доступа на NTP-сервере. "no" в начале команды удаляет настройки	
Пример	Задать для коммутатора список доступа ACL с номером 2. Switch(config)#ntp access-group server 2	

14.2.2. Включить функцию аутентификации NTP (ntp authenticate)

Команда	ntp authenticate no ntp authenticate	
Параметр	none	отсутствует
По умолчанию	Функция аутентификации NTP отключена	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет включить или отключить функцию аутентификации NTP. "no" в начале команды отменяет аутентификацию	
Пример	Включить функцию аутентификации NTP. Switch(config)#ntp authenticate	



14.2.3. Ключ NTP-аутентификации (ntp authentication-key)

Команда	ntp authentication-key <key-id> md5 <value> no ntp authentication-key <key-id>	
Параметр	<key-id>	идентификатор ключа, в диапазоне от 1 до 4294967295
	<value>	значение ключа, в пределах от 1 до 16 символов ascii
По умолчанию	Ключ NTP-аутентификации не задан	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет включить или отменить функцию аутентификации NTP и задать ключ аутентификации. "no" в начале команды отменяет аутентификацию NTP	
Пример	Задать ключ NTP-аутентификации - идентификатор ключа 20, значение abc (алгоритм md5). Switch(config)#ntp authentication-key 20 md5 abc	

14.2.4. Задать поддерживаемые broadcast и multicast NTP серверы (ntp broadcast server count)

Команда	ntp broadcast server count <number> no ntp broadcast server count	
Параметр	<number>	максимальное число broadcast-серверов, 1-100
По умолчанию	задано 50 broadcast-серверов	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать максимальное число broadcast- или multicast-серверов, поддерживаемых клиентом NTP. Команда с "no" в начале удаляет введенные настройки и восстанавливает настройки по умолчанию	
Пример	Задать на коммутаторе максимальное число broadcast-серверов равным 70. Switch(config)#ntp broadcast server count 70	



14.2.5. Включить функцию NTP в порту (ntp disable)

Команда	ntp disable no ntp disable	
Параметр	none	отсутствует
По умолчанию	Функция NTP включена во всех портах	
Режим	Режим настройки VLAN	
Руководство по использованию	Позволяет включить и отключить функцию NTP в порту. Команда с "no" в начале выключает функцию NTP в порту	
Пример	Выключить функцию NTP в интерфейсе vlan1. Switch(config)# interface vlan 1 Switch(config-if-Vlan1)#ntp disable	

14.2.6. Включить или выключить функцию NTP в глобальном режиме (ntp enable)

Команда	ntp enable ntp disable	
Параметр	none	отсутствует
По умолчанию	Функция выключена в глобальном режиме	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет включить или выключить функцию NTP в режиме глобальной конфигурации. Команда Disable глобально отключает функцию NTP	
Пример	Configure switch global enable NTP function. Switch(config)# ntp enable	

14.2.7. Настроить прием IPv6 multicast NTP пакетов на интерфейсе (ntp ipv6 multicast client)

Команда	ntp ipv6 multicast client no ntp ipv6 multicast client	
Параметр	None отсутствует	



По умолчанию	По умолчанию интерфейс не получает многоадресные пакеты IPv6 NTP
Режим	Режим конфигурации интерфейса VLAN
Руководство по использованию	Позволяет настроить указанный интерфейс для приема IPv6 multicast NTP пакетов. Команда с "no" в начале отменяет получение пакетов на указанном интерфейсе
Пример	Включить функцию приема многоадресных пакетов IPv6 NTP на интерфейсе vlan1. Switch(config)# interface vlan 1 Switch(config-if-Vlan1)#ntp ipv6 multicast client

14.2.8. Настроить интерфейс для приема multicast NTP пакетов (ntp multicast client)

Команда	ntp multicast client no ntp multicast client	
Параметр	none	отсутствует
По умолчанию	По умолчанию интерфейс не получает многоадресные пакеты NTP	
Режим	Режим конфигурации интерфейса VLAN	
Руководство по использованию	Позволяет настроить указанный интерфейс на прием многоадресных пакетов NTP. Команда с "no" отменяет прием указанным интерфейсом многоадресных пакетов NTP	
Пример	Включить функцию приема многоадресных пакетов NTP на интерфейсе vlan1. Switch(config)# interface vlan 1 Switch(config-if-Vlan1)#ntp multicast client	

14.2.9. Указать в NTP-сервер (ntp server)

Команда	ntp server {<ip-address> <ipv6-address>} [version <version_no>] [key <key-id>] no ntp server {<ip-address> <ipv6-address>}
Параметр	<ip-address> IPv4-адрес сервера времени <ipv6-address> IPv6-адрес сервера времени



	<version_no>	Номер версии сервера, диапазон от 1 до 4, по умолчанию 4
	<key-id>	идентификатор ключа
По умолчанию	Отключено	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет включить указанный сервер времени в качестве источника времени. Команда с "no" отменяет указанный сервер времени	
Пример	Настроить на коммутаторе адрес сервера времени 1.1.1.1. Switch(config)# ntp server 1.1.1.1	

14.2.10. Период отправки NTP-клиентом пакетов запроса (ntp syn-interval)

Команда	ntp syn-interval <1-3600> no ntp syn-interval	
Параметр	<1-3600>	интервал отправки пакетов запросов ntp-клиента от 1 до 3600 секунд
По умолчанию	задан интервал в 64 секунды	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Задаёт период отправки NTP-клиентом пакетов запроса Для устранения риска подстройки ntp к системному времени в сети с высокой задержкой, ntp-клиент выберет информацию о времени с наименьшей задержкой для синхронизации системного времени после отправки 8 запросов времени ntp. Поэтому по умолчанию ntp-клиент отправляет пакет запроса каждые 64 секунды, и после 8 раз выполняется корректировка времени. Это означает, что системное время корректируется каждые 8 минут. Если пользователь хочет задать временной интервал, например, один час, то интервал доставки пакетов должен быть настроен на 450(3600/8) секунд. Команда, начинающаяся со слова "no", восстанавливает значение по умолчанию, равное 64 секундам	
Пример	Установить корректировку системного времени один раз в час, и время отправки пакетов на 450 секунд. Switch(config)# ntp syn-interval 450	



14.2.11. Задать безопасный ключ (ntp trusted-key)

Команда	ntp trusted-key <key-id> no ntp trusted-key <key-id>	
Параметр	<key-id>	идентификатор ключа, в диапазоне от 1 до 4294967295
По умолчанию	Безопасный ключ не задан	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать безопасный ключ. Команда с "no" в начале отменяет безопасный ключ	
Пример	Задать ключ 20 как безопасный. Switch(config)# ntp trusted-key 20	

14.2.12. Просмотр информации о статусе и конфигурации NTP (show ntp status)

Команда	show ntp status	
Параметр	none	отсутствует
По умолчанию	Не задано	
Режим	Режим глобальной конфигурации, привилегированный режим	
Руководство по использованию	Позволяет вывести на экран состояние временной синхронизации, в том числе информацию о том, синхронизирован коммутатор или нет, уровни, адрес источника времени и т. д.	
Пример	Вывести на экран состояние синхронизации времени. Switch(config)# show ntp status Clock status: synchronized Clock stratum: 3 Reference clock server: 1.1.1.2 Clock offset: 0.010 s Root delay: 0.012 ms Root dispersion: 0.000 ms Reference time: TUE JAN 03 01: 27: 24 2006	



14.2.13. Просмотр информации о сеансах NTP (show ntp session)

Команда	show ntp session [<ip-address> <ipv6-address>]					
Параметр	<ip-address>	IPv4-адрес определенного настроенного сервера времени				
	<ipv6-address>	IPv6-адрес определенного настроенного сервера времени				
По умолчанию	Не задано					
Режим	Режим глобальной конфигурации, привилегированный режим					
Руководство по использованию	Позволяет вывести на экран информацию о всех сеансах NTP или об одном конкретном сеансе, в том числе, идентификатор сервера, уровень сервера, локальный сдвиг, соответствующий серверу. (Символ * означает, что этот сервер выбран в качестве локального источника времени)					
Пример	Вывести информацию обо всех сеансах NTP.					
	Switch(config)# show ntp session					
	server	stream	type	rootdelay	rootdispersion	trustlevel
	*1.1.1.2	2	unicast	0.010s	0.002s	10
	2.2.2.2	3	unicast	0.005s	0.000s	10



15. ДИАГНОСТИКА И КОНТРОЛЬ СОСТОЯНИЯ УСТРОЙСТВА

15.1. Команды Show

15.1.1. Очистить историю команд пользователей (clear history all-users)

Синтаксис	clear history all-users
Параметр	none
По умолчанию	отсутствует
Режим	Привилегированный режим
Руководство по использованию	Команда позволяет очистить историю команд всех пользователей системы
Пример	Switch#clear history all-users

15.1.2. Очистить системный журнал (clear logging)

Синтаксис	clear logging sdram
Параметр	none
По умолчанию	отсутствует
Режим	Привилегированный режим
Руководство по использованию	Когда информация в буфере устаревает и становится больше не актуальной, данная команда позволяет удалить всю информацию
Пример	Удалить всю информацию из зоны sdram буфера. Switch#clear logging sdram

15.1.3. Максимальное число хранимых в истории команд (history all-users max-length)

Синтаксис	history all-users max-length <count>	
Параметр	<count>	число команд, которое может сохраняться, в диапазоне от 100 до 1000



По умолчанию	По умолчанию система может сохранять историю максимум 100 последних команд всех пользователей
Режим	Режим глобальной конфигурации
Руководство по использованию	С помощью этой команды можно установить максимальное количество хранимых в истории команд
Пример	Switch#config Switch(config)#history all-users max-length 500

15.1.4. Настройка журнала хоста канала вывода (logging)

Синтаксис	logging { <ipv4-addr> <ipv6-addr> } [facility <local-number>] [level <severity>] no logging { <ipv4-addr> <ipv6-addr> } [facility <local-number>]	
Параметр	<ipv4-addr>	IPv4-адрес хоста
	<ipv6-addr>	IPv6-адрес хоста
	<local-number>	записывающее оборудование хоста с допустимым диапазоном local0~ local7, который соответствует объекту, определенному в RFC3164
	<severity>	уровень значимости системных сообщений Правила вывода сообщений журнала описаны ниже: выводятся только сообщения, равные или превышающие порог. Подробные сведения об уровне серьезности см. в руководстве по эксплуатации
По умолчанию	Информация системных сообщений на хост не выводится. По умолчанию регистратором хоста системных сообщений является the local0; уровень серьезности по умолчанию - предупреждения	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Команда используется для настройки канала вывода на хост системных сообщений. Команда с "no" в начале отключает функцию вывода на канал вывода. Эта команда доступна только в том случае, когда хост системных сообщений сконфигурирован командой logging. Можно сконфигурировать несколько хостов системных сообщений с IPv4- и IPv6-адресами	



Пример	Послать информацию системных сообщений с уровнем значимости равным или большим уровня предупреждений (warning) на сервер системных сообщений с IPv4-адресом 100.100.100.5 и сохранить их в записывающем оборудовании с идентификатором local1. <pre>Switch#config Switch(config)#logging 100.100.100.5 facility local1 level warnings</pre>

15.1.5. Запись в журнал вводимых команд (logging executed-commands)

Синтаксис	logging executed-commands {enable disable}
Параметр	отсутствует
По умолчанию	Отключена
Режим	Режим глобальной конфигурации
Руководство по использованию	После выполнения этой команды команды, выполняемые пользователем на консоли, telnet или ssh-терминале, будут записываться в журнал, поэтому ее следует использовать вместе с командой logging LOGHOST
Пример	Применить команду и отправлять команды, выполняемые пользователем, на хост системных записей (10.1.1.1) <pre>Switch#config Switch(config)#logging 10.1.1.1 Switch(config)#logging executed-commands enable</pre>

15.1.6. Задать сообщению порядковый номер (logging loghost sequence-number)

Синтаксис	<pre>logging loghost sequence-number no logging loghost sequence-number</pre>
Параметр	отсутствует
По умолчанию	Сообщение не имеет порядкового номера
Режим	Режим глобальной конфигурации



Руководство по использованию	Команда добавляет порядковый номер к loghost, отправляемых в журнал; при "no" в начале команды порядковый номер не добавляется. Перед применением необходимо задать команду "logging" для установки хоста "loghost"
Пример	Открыть добавление порядкового номера loghost sequence-number Switch#config Switch(config) #logging loghost sequence-number

15.1.7. Задать адрес источника при отправке логов (logging source-ip)

Синтаксис	logging source-ip { <A.B.C.D> <X: X: : X: X> }	
Параметр	<ipv4-addr>	IPv4-адрес хоста
	<ipv6-addr>	IPv6-адрес хоста
По умолчанию	None0000	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Указывает IP-адрес источника пакетов записей, отправляемых на сервер, который может быть установлен в виде ipv4 или ipv6 адреса. После ввода команды системные сообщения, отправляемые на сервер, будут содержать IP-адрес; если эта команда не введена, то сообщения не будут содержать IP-адреса	
Пример	Задать IP-адрес источника пакета сообщений, который отправляется на сервер. Switch#config Switch(config)#logging source-ip 2010::10	

15.1.8. Отправка пакета запроса ICMP устройству и проверка связи на обеих сторонах (ping)

Синтаксис	ping [[src <source-address>] { <destination-address> host <hostname> }]	
Параметр	<source-address>	<source-address> IP-адрес источника, с которого выдана команда ping в десятичном представлении с точками
	<destination-address>	<destination-address> IP-адрес назначения команды ping в десятичном представлении с точками



	<hostname>	<hostname> имя хоста назначения команды ping, длиной не более 64 символов						
По умолчанию	отправка 5 пакетов с запросами ICMP. Размер пакета 56 байт, интервал отправки 2 секунды							
Режим	Привилегированный режим							
Руководство по использованию	Коммутатор посылает пакет запроса ICMP удаленному устройству и проверяет может ли коммутатор подключиться к удаленному устройству. Если команда "ping" введена без параметров, включается интерактивный режим. Внем можно задать параметры команды "ping"							
Пример	Пример 1: Использовать "ping" с параметрами, заданными по умолчанию. Switch#ping 10.1.128.160 Type ^c to abort. Sending 5 56-byte ICMP Echos to 10.1.128.160, timeout is 2 seconds. ...!! Success rate is 40 percent (2/5), round-trip min/avg/max = 0/0/0 ms В этом примере команда "ping" будет выдана из коммутатора в устройство с IPадресом 10.1.128.160. Посколькусоответствующие ответные пакеты ICMP (echo reply) не были получены в течение 2 секунд таймаута по умолчанию. Пинг не удался в первых трех попытках. Однако следующие две попытки были успешными. Поэтому процент успешно полученных ответных пакетов будет 40%. На коммутаторе сбой обозначен точкой "." что означает недоступность соединения, а"! " означает успешную операцию, т.е. доступную связь. Пример2 : Пинг с параметрами, введенными в интерактивном режиме. Switch#ping VRF name : Use IP Address[y]: y Target IP address : 10.1.128.160 Use source address option[n]: y Source IP address: 10.1.128.161 Repeat count [5]: 100 Datagram size in byte [56] : 1000 Timeout in milli-seconds [2000]: 500 Extended commands [n]: n <table><tr><th>Отображаемая информация</th><th>Пояснение</th></tr><tr><td>VRF name</td><td>Имя VRM. Если протокол MPLS не включен, это поле должно оставаться незаполненным.</td></tr><tr><td>Target IP address :</td><td>IP-адрес устройства назначения.</td></tr></table>		Отображаемая информация	Пояснение	VRF name	Имя VRM. Если протокол MPLS не включен, это поле должно оставаться незаполненным.	Target IP address :	IP-адрес устройства назначения.
Отображаемая информация	Пояснение							
VRF name	Имя VRM. Если протокол MPLS не включен, это поле должно оставаться незаполненным.							
Target IP address :	IP-адрес устройства назначения.							



	Use source address option[n]	Необходимость применения опции адреса источника
	Source IP address	Указывает IP-адрес источника, который используется в команде ping.
	Repeat count [5]	Число посылаемых командой ping эхо-пакетов По умолчанию равно 5.
	Datagram size in byte [56]	Размер эхо-пакета команды ping в байтах. По умолчанию равен 56
	Timeout in milli-seconds [2000]:	Временной интервал в миллисекундах. По умолчанию равен 2 секундам.
	Extended commands [n]:	Использовать ли другие расширенные опции.

15.1.9. Проверка связи с сетью назначения (ping6)

Синтаксис	ping6 [<dst-ipv6-address> host <hostname> src <src-ipv6-address> {<dst-ipv6-address> host <hostname>}]	
Параметр	<dst-ipv6-address>	IPv6-адрес назначения команды
	<src-ipv6-address>	IPv6-адрес источника отправки команды
	<hostname>	имя хоста назначения, длиной не более 64 символов
По умолчанию	отправка 5 пакетов с запросами ICMP6; размер пакета 56 байт, с интервалом - 2 секунды	
Режим	Привилегированный режим	
Руководство по использованию	Позволяет проверить связь с сетью назначения Если команда ping6 введена только с IPv6-адресом, остальные параметры будут выбраны по умолчанию. Когда ipv6-адрес является link local адресом, необходимо указать имя VLAN-интерфейса. Когда указан ipv6-адрес источника, командой будут сформированы запросы istrb с этим адресом для приема эхо-пакетов	



Пример

Пример 1: Использовать опции ping6, заданные по умолчанию.

Switch#ping6 2001:1:2::4 Type ^c to abort.

Sending 5 56-byte ICMP Echos to 2001: 1: 2: : 4, timeout is 2 seconds.

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/320/1600 ms

Пример2 : Выдать команду ping6 с параметрами, введенными в интерактивном режиме.

Switch#ping6

Target IPv6 address: fe80::2d0:59ff:feb8:3b27 Output Interface: vlan1

Use source address option[n]: y

Source IPv6 address: fe80::203:fff:fe0b:16e3 Repeat count [5]:

Datagram size in byte [56]:

Timeout in milli-seconds [2000]:

Extended commands [n]:

Type ^c to abort.

Sending 5 56-byte ICMP Echos to fe80: : 2d0: 59ff: feb8: 3b27, using src address fe80: : 203: fff: fe0b: 16e3, timeout is 2 seconds.

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms

Отображаемая информация	Пояснение
ping6	Команда ping6
Target IPv6 address	IPv6-адрес назначения.
Output Interface	Имя интерфейса VLAN, должно быть указано, когда адрес назначения является link local адресом.
Use source IPv6 address [n]:	Использовать или нет IPv6-адрес источника. По умолчанию задано не использовать
Source IPv6 address	IPv6-адрес источника.
Repeat count[5]	Число посылаемых командой ping6 эхо-пакетов.
Datagram size in byte[56]	Размер эхо-пакета команды ping6 в байтах. По умолчанию 56 байт.
Timeout in milli-seconds[2000]	Временной интервал для ответных пакетов



		миллисекундах. По умолчанию 2 секунды.
	Extended commands[n]	Расширенный формат команды. По умолчанию выключен.
	!	Сеть доступна.
	.	Сеть недоступна.
	Success rate is 100 percent(8/8), round-trip min/avg/max = 1/1/1ms	Статистическая информация, 100 % успех.

15.1.10. Просмотр файлов загрузки (show boot-files)

Синтаксис	show boot-files
Параметр	отсутствует
По умолчанию	отсутствуют
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Выводит на экран первый и второй IMG-файлы, а также CFG-файл, подключенный коммутатором. При выполнении этой команды отображается последовательность запуска IMG-файла на соответствующем устройстве хранения, IMG-файл, используемый в данный момент для запуска, информация о настройках CFG-файла на устройстве хранения и CFG-файл, запущенный в данный момент
Пример	Показать стартовый CFG-файл, запущенный коммутатором. <pre>Switch#show boot-files</pre> Booted files on switch The primary img file at the next boot time: flash: /nos.img The backup img file at the next boot time: flash: /nos.img Current booted img file: flash: /nos.img The startup-config file at the next boot time: flash: /startup.cfg Current booted startup-config file: flash: /startup.cfg If the CFG file of the next booting is set as NULL, the CFG part mentioned above will be displayed as follows: The startup-config file at the next boot time: NULL Current booted startup-config file: flash: /startup.cfg



15.1.11. Просмотр информации о файлах, хранящихся во флеш-памяти (show flash)

Синтаксис	Show flash									
Параметр	отсутствуют									
По умолчанию	отсутствуют									
Режим	Привилегированный режим и режим конфигурации									
Руководство по использованию	Команда позволяет просмотреть размер файлов, хранящихся во флеш-памяти системы									
Пример	Вывести перечень файлов в флеш-памяти и их размер. Switch#show flash <table><tr><td>total</td><td>12227K</td><td></td></tr><tr><td>-rw-</td><td>12516553</td><td>nos.img</td></tr><tr><td>-rw-</td><td>3224</td><td>startup.cfg</td></tr></table> Drive : flash: Size: 30.0M Used: 13.0M Available: 17.0M Use: 43%	total	12227K		-rw-	12516553	nos.img	-rw-	3224	startup.cfg
total	12227K									
-rw-	12516553	nos.img								
-rw-	3224	startup.cfg								

15.1.12. Просмотр введенных пользователем команды в хронологическом порядке (show history)

Синтаксис	show history
Параметр	отсутствует
По умолчанию	отсутствует
Режим	Привилегированный режим
Руководство по использованию	Отображает введенные пользователем команды в хронологическом порядке. Система сохраняет в хронологическом порядке до 20 команд, введенных пользователями. Команды из последовательности ввода



	можно выбирать клавишами UP и DOWN, либо комбинациями клавиш (ctrl+p и ctrl+n)
Пример	<pre>Switch# show history enable config interface ethernet 1/0/3 enable dir show ftp</pre>

15.1.13. Просмотр информации о истории действий всех пользователей (show history all-users)

Синтаксис	show history all-users [detail]	
Параметр	detail	показывает имя пользователя, выполняющего команду. IP-адрес пользователя будет показан при входе в систему при выполнении команды через Telnet или SSH
По умолчанию	отсутствует	
Режим	Привилегированный режим и режим глобальной конфигурации	
Руководство по использованию	Эта команда используется для отображения истории последних команд всех пользователей, включая время, тип регистрации, выполняемую команду и т.д. Примечание: Пользователи могут проверять историю команд только тех пользователей, чьи полномочия не выше проверяющего	
Пример	<pre>Switch# show history all-users detail Time Type User Command 0w 0d 0h 2m Telnet/SSH admin show history all-users detail 192.168.1.2: 1419 0w 0d 0h 1m Telnet/SSH admin show history all-users 192.168.1.2: 1419 0w 0d 0h 1m Console Null show history all-users 0w 0d 0h 1m Console Null end 0w 0d 0h 1m Console Null ip address 192.168.1.1 255.255.255.0 0w 0d 0h 0m Console Null in v 1 0w 0d 0h 0m Console Null telnet-server enable</pre>	



15.1.14. Просмотр детальной информации о канале буфера системных сообщений (show logging buffered)

Синтаксис	show logging buffered [level {critical warnings} range <begin-index> <end-index>]	
Параметр	level {critical warnings}	уровень значимости информации
	<begin-index>	начальный номер системного сообщения, в пределах 1-65535
	<end-index>	конечный номер системного сообщения, в пределах 1-65535. Если отображается только информация о буфере журнала для сетевой карты, необходимо добавить параметр диапазона, но для ведущего устройства в этом нет необходимости
По умолчанию	При вводе команды без параметров будут выведены все системные сообщения критического уровня значимости	
Режим	Привилегированный режим и режим глобальной конфигурации	
Руководство по использованию	Выводит на дисплей детальную информацию о канале буфера системных сообщений. Эта команда не поддерживается на коммутаторах низкого класса. В буфере хранятся сообщения критического уровня значимости и предупреждения. При выводе на терминал они имеют следующий формат: идентификационный номер (ID), время, <level> ID модуля [имя задания], информация сообщения	
Пример	Вывести системные сообщения критического уровня значимости, хранящиеся в буфере системных сообщений, идентификаторы с 940 по 946. Switch# show logging buffered level critical range 940 946 Current messages in SDRAM: 0	

15.1.15. Отображение статуса логирования действий пользователя (show logging executed-commands state)

Синтаксис	show logging executed-commands state
Параметр	отсутствует
По умолчанию	отсутствует



Режим	Привилегированный режим
Руководство по использованию	Команда применяется для отображения состояния (включено или выключено)
Пример	Switch#show logging executed-commands state Logging executed command state is enable

15.1.16. Просмотр детальной информации о сообщениях модуля MSTP (show logging source)

Синтаксис	show logging source mstp
Параметр	без параметра
По умолчанию	отсутствует
Режим	Привилегированный режим и режим глобальной конфигурации
Руководство по использованию	Выводит информацию журнала о сообщениях модуля MSTP
Пример	Показать информацию журнала о сообщениях MSTP. Switch#show logging source mstp system module log switch status: Channel Onoff Severity logbuff on warning loghost on warning terminal on warning

15.1.17. Просмотр параметров текущей конфигурации коммутатора (show running-config)

Синтаксис	show running-config
Параметр	без параметра
По умолчанию	Не задано
Режим	Привилегированный режим
Руководство по использованию	Выводит на дисплей параметры текущей конфигурации коммутатора. Команда "show running-config" используется для проверки правильности введенных пользователями конфигураций и отображения текущих параметров



Пример	Switch#show running-config

15.1.18. Просмотр параметров конфигурации при текущем режиме пользователя (show running-config current-mode)

Синтаксис	show running-config current-mode
Параметр	без параметра
По умолчанию	отсутствуют
Режим	Все режимы конфигурации
Руководство по использованию	В любом режиме конфигурации выводит на экран параметры конфигурации при текущем режиме
Пример	Switch(config-if-ethernet1/0/1)#show run c ! Interface Ethernet1/0/1 switchport access vlan 2 !

15.1.19. Отобразить текущую загрузочную конфигурацию (show startup-config)

Синтаксис	show startup-config
Параметр	без параметра
По умолчанию	Если параметры текущей конфигурации те же, что и параметры, считанные из флеш-памяти, то на экран ничего не будет выведено
Режим	Привилегированный режим
Руководство по использованию	Команда "show running-config" отличается от команды "show startup-config". После того, как пользователь завершит конфигурирование, команда "show running-config" отобразит новые заданные опции, а при вводе "show startup-config" никакая конфигурация не отображается. Если была введена команда "write" для сохранения активной конфигурации во флеш-памяти, то результат для "show running-config" и "show startup-config" будет одинаковый
Пример	Switch#show startup-config



15.1.20. Отобразить информацию о VLAN принадлежащих к интерфейсу (show switchport interface)

Синтаксис	show switchport interface [ethernet] <IFNAME>	
Параметр	<IFNAME>	номер порта
По умолчанию	отсутствует	
Режим	Привилегированный режим и режим глобальной конфигурации	
Руководство по использованию	Выводит на экран информацию о режиме работы порта, идентификаторе VLAN и сообщения магистрального порта для режима порта VLAN на коммутаторе	
Пример	Показать сообщения VLAN порта ethernet 1/0/1	
	Switch#show switchport interface ethernet 1/0/1 Ethernet1/0/1	
	Type : Universal Mode : Trunk Port VID : 1	
	Trunk allowed Vlan : 1-4094	
	Информация, отображаемая на экране	Описание
	Ethernet1/0/1	Имя порта Ethernet-интерфейса
	Type	Тип текущего интерфейса
	Mode: Trunk	Режим работы текущего VLAN интерфейса
	Port VID : 1	Идентификатор vlan, которому принадлежит текущий интерфейс
	Trunk allowed Vlan: ALL	Разрешенные VLAN для интерфейса, работающего в режиме trunk.

15.1.21. Отображение информации о текущих TCP-сессиях (show tcp)

Синтаксис	show tcp
Параметр	без параметра
По умолчанию	отсутствует



Режим	Привилегированный режим	
Руководство по использованию	Выводит на экран состояние текущего TCP-соединения, установленного с коммутатором	
Пример	Switch#show tcp LocalAddress LocalPort ForeignAddress ForeignPort State 0.0.0.0 23 0.0.0.0 0 LISTEN 0.0.0.0 80 0.0.0.0 0 LISTEN	
	Информация, отображаемая на экране	Описание
	LocalAddress	Локальный адрес TCP-соединения
	LocalPort	Локальный порт TCP-соединения
	ForeignAddress	Адреса удаленного устройства TCP-соединения
	ForeignPort	Порт удаленного устройства TCP-соединения
	State	Текущее состояние TCP-соединения

15.1.22. Отобразить информацию о текущих TCP сессиях (show tcp ipv6)

Синтаксис	show tcp ipv6					
Параметр	без параметра					
По умолчанию	отсутствует					
Режим	Привилегированный режим и режим глобальной конфигурации					
Руководство по использованию	Выводит на экран информацию о текущих TCP сессиях					
Пример	Switch#show tcp ipv6					
	Local Address	LocalPort	Remote Address	RemotePort	State	IF VRF
	::	0	LISTEN	0	0	80 ::
	::	0	LISTEN	0	0	23 ::



	Информация, отображаемая на экране	Пояснение
	LocalAddress	Локальный IPv6-адрес TCP-соединения
	LocalPort	Локальный порт TCP-соединения
	RemoteAddress	IPv6-адреса удаленного устройства TCP-соединения
	RemotePort	Порт удаленного устройства TCP-соединения
	State	Текущее состояние TCP-соединения
	IF	Индекс локального порта TCP-соединения
	VRF	Экземпляр виртуальной маршрутизации и переадресации

15.1.23. Просмотр текущих telnet-сессий к коммутатору (show telnet login)

Синтаксис	show telnet login
Параметр	без параметра
По умолчанию	отсутствует
Режим	Привилегированный режим и режим глобальной конфигурации
Руководство по использованию	Данная команда используется для отображения информации о пользователях, подключенных к коммутатору по telnet
Пример	Switch#show telnet login Authenticate login by local. Login user: aa

15.1.24. Отобразить информацию о текущих UDP сессиях (show udp)

Синтаксис	show udp
Параметр	без параметра
По умолчанию	отсутствует



Режим	Привилегированный режим				
Руководство по использованию	Выводит на экран состояние текущего UDP-соединения, установленного с коммутатором				
Пример	Switch#show udp				
	LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
	0.0.0.0	32768	0.0.0.0	0	CLOSE
	0.0.0.0	3071	0.0.0.0	0	CLOSE
	Информация, отображаемая на экране		Описание		
	LocalAddress		Локальный адрес UDP-соединения		
	LocalPort		Номер локального порта UDP-соединения		
	ForeignAddress		Адрес удаленного устройства UDP-соединения		
	ForeignPort		Номер порта удаленного устройства UDP-соединения		
	State		Текущее состояние UDP-соединения		

15.1.25. Отобразить информацию о текущих UDP сессиях (show udp ipv6)

Синтаксис	show udp ipv6				
Параметр	без параметра				
По умолчанию	отсутствуют				
Режим	Привилегированный режим и режим глобальной конфигурации				
Руководство по использованию	Выводит на экран информацию о текущих UDP сессиях				
Пример	Switch#show udp ipv6				
	LocalAddress	LocalPort	RemoteAddress	RemotePort	State
	::	3071	::	0	CLOSE



	Информация, отображаемая на экране	Описание
	LocalAddress	Локальный IPv6-адрес UDP-соединения.
	LocalPort	Номер локального порта UDP-соединения.
	RemoteAddress	IPv6-адрес удаленного устройства UDP-соединения
	RemotePort	Номер порта удаленного устройства UDP-соединения
	State	Текущее состояние UDP-соединения

15.1.26. Просмотр версии коммутатора (show version)

Синтаксис	show version	
Параметр	без параметра	
По умолчанию	отсутствуют	
Режим	Привилегированный режим	
Руководство по использованию	Позволяет просмотреть версию коммутатора. Команда применяется для просмотра информации о версии коммутатора, включая версию оборудования и версию программного обеспечения	
Пример	Switch#show version	

15.1.27. Проверка маршрута прохождения пакетов через сеть (traceroute)

Синтаксис	traceroute [source <ipv4-addr>] { <ip-addr> host <hostname> } [hops <hops>] [timeout <timeout>]	
Параметр	<ipv4-addr>	IPv4-адрес хоста назначения в десятичном представлении с точками
	<ip-addr>	IP-адрес хоста



	<hostname>	имя удаленного хоста
	<hops>	максимальное число шлюзов, допускаемое при трассировке
	<timeout>	время таймера для пакетов в миллисекундах, диапазон значений от 100 до 10000
По умолчанию	По умолчанию максимальное число шлюзов равно 30, время таймера: 2000 миллисекунд	
Режим	Привилегированный режим	
Руководство по использованию	Команда используется для проверки маршрута прохождения пакета от отправившего их оборудования до оборудования назначения. Это необходимо для проверки доступности и локализации отказов сети Команда "traceroute" используется для локализации недоступных узлов сети, когда пакеты не достигают оборудования назначения	
Пример	<pre>Switch#traceroute 192.168.2.36 Type ^c to abort. Traceroute to host 192.168.2.36, maxhops is 30, timeout is 2000ms. 1 0ms 192.168.2.36 Traceroute completed</pre>	

15.1.28. Проверка маршрута прохождения пакетов через сеть (traceroute6)

Синтаксис	traceroute6 [source <addr>] {<ipv6-addr> host <hostname>} [hops <hops>] [timeout <timeout>]	
Параметр	<ipv4-addr>	IPv6-адрес хоста источника в шестнадцатеричной записи
	<ip-addr>	IPv6-адрес хоста назначения в шестнадцатеричной записи в десятично-точечной записи
	<hostname>	имя удаленного хоста
	<hops>	максимальное число шлюзов, допускаемое при трассировке с использованием команды traceroute6, в пределах от 1 до 255



	<timeout>	время таймера для пакетов в миллисекундах, в диапазоне от 100 до 10000
По умолчанию	По умолчанию максимальное число шлюзов равно 30, время таймера: 2000 миллисекунд	
Режим	Привилегированный режим	
Руководство по использованию	Команда используется для проверки маршрута прохождения пакета от отправившего их оборудования до оборудования назначения, чтобы проверить доступность сети и локализацию отказов в ней. Команда "Traceroute6" используется для локализации недоступных узлов сети, когда пакеты не достигают оборудования назначения	
Пример	Switch#traceroute6 2004: 1: 2: 3: : 4 Type ^c to abort. Traceroute to IPv6 host 2004: 1: 2: 3: : 4, maxhops is 30, timeout is 2000ms. Traceroute6 error occurred	

15.1.29. Перезагрузка коммутатора (reload after)

Синтаксис	reload after {[<HH: MM: SS>] [days <days>]}	
Параметр	<HH: MM: SS>	заданный период времени, HH (часы) в пределах от 0 до 23, MM (минуты) и SS (секунды) в пределах от 0 до 59
	<days>	заданные дни, единица измерения - день, диапазон от 1 до 30
По умолчанию	отсутствует	
Режим	Привилегированный режим	
Руководство по использованию	Команда позволяет перезагрузить коммутатор через определённое время без отключения питания, обычно во время обновления версии прошивки. Коммутатор может быть перезагружен через какой-либо период времени после успешного обновления версии. Эта команда не сохраняется, используется однократно. После настройки этой команды при входе пользователя в коммутатор по telnet будет запрашиваться информация о перезагрузке	
Пример	Перезагрузить коммутатор по прошествии 2 дней, 10 часов и 1 секунды. Switch#reload after 10: 00: 01 days 2 Process with reboot after? [Y/N] y	



15.1.30. Отмена перезагрузки коммутатора (reload cancel)

Синтаксис	reload cancel
Параметр	без параметра
По умолчанию	отсутствует
Режим	Привилегированный режим
Руководство по использованию	Отменяет перезагрузку коммутатора по истечении заданного периода времени. Команда позволяет отменить перезагрузку коммутатора по истечении заданного периода времени, т.е. отменяет команду "reload after". Эта команда не может быть зарезервирована
Пример	Запретить автоматическую перезагрузку коммутатора по истечении указанного времени. Switch#reload cancel Reload cancel successful

15.1.31. Просмотр времени, на которое назначена перезагрузка (show reload)

Синтаксис	show reload
Параметр	без параметра
По умолчанию	отсутствует
Режим	Привилегированный режим и режим глобальной конфигурации
Руководство по использованию	Выводит на дисплей настройки, введенные пользователем в команде "reload after". Команда позволяет просмотреть настройки, заданные в команде "reload after" и проверить, сколько времени осталось до перезагрузки коммутатора
Пример	Вывести на экран настройки команды "reload after". В примере ниже пользователь задал перезагрузку коммутатора через 10 часов и 1 секунду, до перезагрузки осталось 9 часов 59 минут и 48 секунд. Switch#show reload The original reload after configuration is 10: 00: 01. System will be rebooted after 09: 59: 48 from now



15.1.32. Очистить статистику пакетов, принятых в CPU (clear cpu-rx-stat protocol)

Синтаксис	clear cpu-rx-stat protocol [<protocol-type>]	
Параметр	<protocol-type>	тип протокола пакета, включая dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh
По умолчанию	отсутствуют	
Режим	Привилегированный режим	
Руководство по использованию	Команда очищает статистику пакетов протокола определенного типа, принятых CPU, предназначена для персонала технической поддержки	
Пример	Очистить статистику принятых CPU пакетов протокола ARP. Switch#config Switch(config)#clear cpu-rx-stat protocol arp	

15.1.33. Задать максимальную скорость приема пакетов для указанного типа протокола (cpu-rx-ratelimit protocol)

Синтаксис	cpu-rx-ratelimit protocol <protocol-type> <packets> no cpu-rx-ratelimit protocol <protocol-type>	
Параметр	<protocol-type>	тип протокола, включая dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh
	<packets>	максимальная скорость приема пакетов определенного типа протокола в CPU, в диапазоне от 1 до 2000 пакетов/с
По умолчанию	Для разных типов протоколов заданы разные скорости	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать максимальную скорость приема пакетов для указанного типа протокола, "no" в начале команды возвращает настройки по умолчанию. Команда позволяет установить максимальную скорость приема пакетов определенного типа протокола в CPU, предназначена для персонала технической поддержки	



Пример	Установить скорость приема пакетов ARP равной 500 пакетов/с. Switch#config Switch(config)#cpu-rx-ratelimit protocol arp 500

15.1.34. Задать для CPU максимальную скорость приема пакетов (cpu-rx-ratelimit total)

Синтаксис	cpu-rx-ratelimit total <packets> no cpu-rx-ratelimit total	
Параметр	<packets>	максимальное число пакетов, принимаемых CPU за 1 секунду
По умолчанию	1200 пакетов в секунду	
Режим	Режим глобальной конфигурации	
Руководство по использованию	Позволяет задать для CPU максимальную скорость приема пакетов, "no" в начале команды возвращает настройки по умолчанию. Команда позволяет установить максимальную скорость приема пакетов в CPU, предназначена для персонала технической поддержки	
Пример	Задать максимальную скорость приема пакетов CPU равной 1500 пакетов/с. Switch#config Switch(config)# cpu-rx-ratelimit total 1500	

15.1.35. Просмотр статистики принятых CPU пакетов протокола указанного типа (show cpu-rx protocol)

Синтаксис	show cpu-rx protocol [<protocol-type>]	
Параметр	<protocol-type>	тип протокола пакетов. При отсутствии параметров отображается статистика всех пакетов
По умолчанию	отсутствуют	
Режим	Привилегированный режим и режим глобальной конфигурации	
Руководство по использованию	Выводит на экран статистику принятых CPU пакетов протокола указанного типа. Команда используется для отладки, предназначена только для специалистов службы технической поддержки	



Пример	Показать статистику принятых CPU пакетов протокола ARP. <pre>Switch#show cpu-rx protocol arp Type Rate-limit TotPkts DropPkts DelayCount CurState ARP 300 0 0 0 allowed</pre>



16. КОНФИГУРАЦИЯ ПРОТОКОЛОВ МАРШРУТИЗАЦИИ

16.1. Команды протокола RIP

16.1.1. Время действия ключа аутентификации (accept-lifetime)

Команда	accept-lifetime <start-time> {<end-time> duration<seconds> infinite} no accept-lifetime Команда устанавливает период времени, в течение которого ключ аутентификации в цепочке ключей считается действительным. Команда "no accept-lifetime" удаляет конфигурацию
Параметр	<start-time> начало периода. Допускаются следующие варианты синтаксиса: <start-time>={<hh: mm: ss> <month> <day> <year> <hh: mm: ss> <day> <month> <year>} <hh: mm: ss> конкретное время действия параметра accept-lifetime в часах, минутах и секундах <day> дата действия, в диапазоне от 1 до 31 <month> месяц начала действия, отображается первыми тремя буквами месяца, например, Янв. (Jan) <year> год начала действия, в диапазоне 1993 - 2035 <end-time> окончание периода времени. Допускаются следующие варианты синтаксиса: <end-time>={<hh: mm: ss> <month> <day> <year> <hh: mm: ss> <day> <month> <year>}<hh: mm: ss> конкретное время действия параметра accept-lifetime в часах, минутах и секундах <day> дата действия, в диапазоне от 1 до 31 <month> месяц действия, отображается первыми тремя буквами месяца, например, Янв. (Jan) <year> год начала действия, в диапазоне 1993 - 2035 <seconds> период действия ключа в секундах, в диапазоне 1-2147483646 Infinite ключ действителен до бесконечности
По умолчанию	конфигурация по умолчанию отсутствует
Режим	Режим конфигурации ключа в цепочке ключей



Руководство по использованию	Если задан только режим аутентификации, но не задана цепочка ключей или пароль, используемые интерфейсом, аутентификация не будет работать. Если до ввода команды не сконфигурирован режим, то после ввода команды будет установлен режим аутентификации с открытым текстом. Команда с "no" в начале отменяет аутентификацию, но это не означает, что тип режима будет задан без проверки подлинности, только то, что при отправке или получении пакетов не будет выполняться обработка аутентификации. Ввод "ip rip authentication key-chain my key" указывает, что имя цепочки ключей "my key" длиной всего 6 символов
Пример	В примере ниже показана конфигурация "accept-lifetime" для ключа 1 в цепочке ключей с именем mychain. <pre>Switch# config terminal Switch(config)# key chain mychain Switch(config-keychain)# key 1 Switch(config-keychain-key)# accept-lifetime 03:03:01 Dec 3 2004 04: 04: 02 Oct 6 2006</pre>

16.2. Команды протокола OSPF.

16.2.1. Включить аутентификацию для OSPF области (area authentication)

Команда	area <id> authentication [message-digest] no area <id> authentication Применяется для включения режима аутентификации области OSPF. Команда "no area <id> authentication" восстанавливает значение по умолчанию
Параметр	<id> номер области, задается в формате числа в диапазоне от 0 до 4294967295 или IPv4-адреса message-digest включает аутентификацию MD5 в указанной области, либо простую аутентификацию с помощью обычного текста, если не выбрать этот параметр
По умолчанию	Аутентификация отсутствует
Режим	Режим протокола OSPF
Руководство по использованию	Команда устанавливает аутентификацию с простым текстовым паролем или аутентификацию MD5. Режим аутентификации также может быть установлен в режиме интерфейса, который имеет более высокий приоритет, чем режим области. Необходимо использовать команду "ip ospf authentication-key" для установки пароля, если на интерфейсе и в области не настроен режим аутентификации, а если включена аутентификация MD5 необходимо применить команду "ip ospf message-digest key command" для настройки ключа MD5. Режим



	аутентификации области не может повлиять на режим аутентификации интерфейса в этой области
Пример	Установить режим аутентификации MD5 в области 0. Switch(config-router)#area 0 authentication message-digest

16.2.2. Стоимость для маршрута по умолчанию, отправляемого в стабильную область (area default-cost)

Команда	area <id> default-cost <cost> no area <id> default-cost Предназначена для указания стоимости суммарного маршрута по умолчанию, отправляемого в тупиковую область или область NSSA. Команда “no area <id> default-cost” восстанавливает значение по умолчанию
Параметр	<id> номер области, задается в формате числа в диапазоне от 0 до 4294967295 или IPv4-адреса; <cost> в диапазоне <0-16777215>
По умолчанию	Стоимость OSPF равна 1
Режим	Режим протокола OSPF
Руководство по использованию	Команда применяется на граничном маршрутизаторе ABR, который подключен к NSSA или тупиковой области
Пример	Установить стоимость по умолчанию для области 1 на 10. Switch(config-router)#area 1 default-cost 10

16.2.3. Настройка фильтрации в области (area filter-list)

Команда	[no] area <id> filter-list {access prefix} {in out} Задаёт фильтр широковещательной суммарной маршрутизации на граничном маршрутизаторе области (ABR); команда “no area <id> filter-list {access prefix} {in out}” восстанавливает значение по умолчанию
Параметр	<id>номер области, задается в формате числа в диапазоне от 0 до 4294967295 или IPv4-адреса access-list указывает на применение списка доступа, prefix-list указывает применение списка префиксов; <name> имя фильтра длиной в диапазоне 1-256; “in” означает в указанную область из других областей, “out” - из указанной области в другие области
По умолчанию	Фильтр не настроен



Режим	Режим протокола OSPF
Руководство по использованию	Эта команда используется для ограничения распространения маршрутов из определенной области между этой и другими областями
Пример	Установить фильтр в области 1. <pre>Switch(config)#access-list 1 deny 172.22.0.0 0.0.0.255 Switch(config)#access-list 1 permit any-source Switch(config)#router ospf 100 Switch(config-router)#area 1 filter-list access 1 in</pre>

16.2.4. Определение области как области NSSA (area nssa)

Команда	<pre>area <id> nssa [TRANSLATOR] no-redistribution [DEFAULT-ORIGINATE no-summary] no area <id> nssa[TRANSLATOR] no-redistribution [DEFAULT-ORIGINATE no-summary]</pre> Предназначена для задания «не совсем тупиковой» (NSSA, not so stubby area) области OSPF
Параметр	<id> номер области, задается в формате числа в диапазоне от 0 до 4294967295 или IPv4-адреса TRANSLATOR = роль транслятора {candidate never always}, определяет режим трансляции LSA для маршрутизатора: "candidate" транслирует LSA тип 7 в LSA тип 5 если выбран маршрутизатор является параметром по умолчанию. "never" маршрутизатор не транслирует LSA типа 7 в LSA типа 5. "always" маршрутизатор всегда транслирует LSA типа 7 в LSA типа 5 no-redistribution внешние LSA никогда не транслируются в NSSA. DEFAULT-ORIGINATE=default-information-originate [metric <0-16777214>] [metric-type <1-2>], используется для генерации LSA типа 7. metric <0-16777214> значение метрики маршрута. metric-type <1-2> тип метрики для external-LSA, значение по умолчанию 2. no-summary показывает отсутствие отправки маршрута области в NSSA
По умолчанию	Область NSSA не указана
Режим	Режим протокола OSPF



Руководство по использованию	Одна и та же область не может быть одновременно и тупиковой областью, и областью NSSA
Пример	Установить область 3 как NSSA. <pre>Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#area 0.0.0.51 nssa Switch(config-router)#area 3 nssa default-information-originate metric 34 metric-type 2 translator-role candidate no-redistribution</pre>

16.2.5. Формирование суммарного префикса для области OSPF (area range)

Команда	<pre>area <id> range <address> [advertise not-advertise substitute] no area <id> range <address></pre> Суммирует маршруты OSPF на границе области. Команда “no area <id> range <address>” отменяет данную функцию
Параметр	<id> номер области, задается в формате числа в диапазоне от 0 до 4294967295 или IPv4-адреса <address>=<A.B.C.D/M>, указывает префикс сети и его длину ; advertise : указание распространять данную область, параметр по умолчанию; not-advertise : указание не распространять данную область; substitute= substitute <A.B.C.D/M> : указание распространять данную область как другой префикс; <A.B.C.D/M> : заменить префикс сети, который будет распространяться в данной области
По умолчанию	Не задано
Режим	Режим протокола OSPF
Руководство по использованию	Команда суммирует маршруты внутри области. Если идентификаторы сетей в этой области заданы непоследовательно, можно объявлять суммарный маршрут, задав эту команду на граничном маршрутизаторе ABR. Этот маршрут состоит из всех отдельных сетей, принадлежащих к определенному диапазону
Пример	<pre>Switch # config terminal Switch (config)# router ospf 100 Switch (config-router)# area 1 range 192.16.0.0/24</pre>



16.2.6. Определение области как тупиковой (area stub)

Команда	<code>area <id> stub [no-summary] no area <id> stub [no-summary]</code> Команда используется для определения области как тупиковой. Команда “no area <id> stub [no-summary]” отменяет данную функцию
Параметр	<code><id></code> номер области, задается в формате числа в диапазоне от 0 до 4294967295 или IPv4-адреса <code>no-summary</code> : граничные маршрутизаторы прекращают отправку сводных объявлений о соединениях в тупиковую область
По умолчанию	Не задано
Режим	Режим протокола OSPF
Руководство по использованию	Данную команду необходимо применить на всех маршрутизаторах, имеющих доступ к тупиковой области. Существуют две команды конфигурации маршрутизатора в тупиковой области: “stub” и “default-cost”. Для всех маршрутизаторов, подключенных к тупиковой области, область должна быть настроена с использованием команды “area stub”. На маршрутизаторе граничной области, подключенном к тупиковой области, стоимость отправляемого им маршрута определяется параметром “default-cost”
Пример	<pre>Switch # config terminal Switch (config)# router ospf 100 Switch (config-router)# area 1 stub</pre>

16.2.7. Формирование виртуального соединения для обмена LSA (area virtual-link)

Команда	<code>area <id> virtual-link A.B.C.D {AUTHENTICATION AUTH_KEY INTERVAL}</code> <code>no area <id> virtual-link</code> Позволяет настроить логическую связь между двумя магистральными областями, разделенными не магистральной областью. Команда “no area <id> virtual-link A.B.C.D {AUTHENTICATION AUTH_KEY INTERVAL}” удаляет данное виртуальное соединение
Параметр	<code><id></code> номер области, задается в формате числа в диапазоне от 0 до 4294967295 или IPv4-адреса. <code>AUTHENTICATION</code> = authentication [message-digest[message-digest-key <1-255> md5 <LINE>] [null AUTH_KEY]]. <code>authentication</code> : включение аутентификации на этом виртуальном канале. <code>message-digest</code> : алгоритм аутентификации MD-5.



	null : перезапись пароля или суммарных пакетов с нулевой аутентификацией. AUTH_KEY= authentication-key <key>. <key>: пароль состоит минимум из 8 символов. INTERVAL= [dead-interval hello-interval message-digest-key<1-255>md5<LINE> retransmit-interval transmit-delay] <value>. <value>: >: Задержка или интервал в секундах, в диапазоне 1~65535. <dead-interval>: интервал, в течение которого пакеты сообщений не принимаются, и по истечении которого соседний маршрутизатор считается отключенным от сети. По умолчанию 40 секунд. <hello-interval>: интервал перед отправкой маршрутизатором пакета сообщений hello, по умолчанию 10 секунд. <message-digest-key>: алгоритм аутентификации MD-5. <retransmit-interval>: интервал перед повторной передачей маршрутизатором пакета сообщений, по умолчанию 5 секунд <transmit-delay>: время задержки перед отправкой маршрутизатором сообщения, по умолчанию 1 секунда
По умолчанию	конфигурация по умолчанию отсутствует
Режим	Режим протокола OSPF
Руководство по использованию	В топологии OSPF все области должны граничить с магистральной областью. Если соединение с магистральной областью будет потеряно, виртуальный канал восстановит это соединение. Можно настроить виртуальную связь между любыми двумя маршрутизаторами магистральных областей, соединенными с публичной не магистральной областью. Протокол рассматривает маршрутизаторы, соединенные виртуальными каналами, как сеть в режиме точка-точка (неблокирующий обмен)
Пример	<pre>Switch#config terminal Switch(config) #router ospf 100 Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20</pre>

16.2.8. Параметр для вычисления метрики протокола OSPF (auto-cost reference-bandwidth)

Команда	auto-cost reference-bandwidth <bandwidth> no auto-cost reference-bandwidth Команда задает базовый параметр для вычисления метрики протокола OSPF. Команда "no auto-cost reference-bandwidth" назначает стоимость только на основе типа интерфейса



Параметр	<bandwidth> : значение базовой ширины пропускания в Мбит/с. Диапазон 1-4294967
По умолчанию	Пропускная способность по умолчанию составляет 100 Мбит/с
Режим	Режим протокола OSPF
Руководство по использованию	Значение метрики интерфейса получается путем деления пропускной способности интерфейса на базовую пропускную способность. Эта команда предназначена в основном для дифференциации каналов с высокой пропускной способностью. Если имеется несколько каналов с высокой пропускной способностью, можно разграничить их стоимость, установив большее значение базовой пропускной способности
Пример	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#auto-cost reference-bandwidth 50

16.2.9. Установка выбора расчета цены маршрута согласно RFC1583 (compatible rfc1583)

Команда	compatible rfc1583 no compatible rfc1583 Команда настраивает совместимость с rfc1583. Команда “no compatible rfc1583” закрывает совместимость
Параметр	-
По умолчанию	Совместимость с rfc1583 существует по умолчанию
Режим	Режим протокола OSPF
Руководство по использованию	-
Пример	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#compatible rfc1583



16.2.10. Удаление всех процессов OSPF (clear ip ospf process)

Команда	clear ip ospf [<process-id>] process Команда используется для очистки и перезапуска процессов маршрутизации OSPF. Для удаления только одного процесса OSPF необходимо указать идентификатор. Если ID процесса не указан, все процессы OSPF будут удалены
Параметр	-
По умолчанию	конфигурация по умолчанию отсутствует
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Switch#clear ip ospf process

16.2.11. Генерация внешнего маршрута по умолчанию в область OSPF (default-information originate)

Команда	default-information originate [always METRIC METRICTYPE ROUТЕMAP] no default-information originate Команда создает внешний маршрут по умолчанию в область маршрутизации OSPF. Команда "no default-information originate" отменяет создание маршрута
Параметр	always : всегда объявляет маршрут по умолчанию, независимо от наличия системы маршрута по умолчанию METRIC = metric <value> : Значение метрики для создания маршрута по умолчанию, <value> ranges between 0~16777214, default metric value is 0. METRICTYPE = metric-type {1 2} тип метрики OSPF External Type, связанный с маршрутом по умолчанию. 1 - задаёт метрику OSPF External Type 1. 2 - задаёт метрику OSPF External Type 2 ROUТЕMAP = route-map <WORD> <WORD> имя применяемой карты маршрутов
По умолчанию	Значение метрики по умолчанию 10. Значение метрики OSPF External Type по умолчанию равно 2
Режим	Режим протокола OSPF



Руководство по использованию	Когда данная команда используется для определения маршрутов в область маршрутизации OSPF, система начинает работать как маршрутизатор границы автономной системы (ASBR)
Пример	<pre>Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#default-information originate always metric 23 metric-type 2 route-map myinfo</pre>

16.2.12. Установка значений метрики по умолчанию для OSPF (default-metric)

Команда	<pre>default-metric <value> no default-metric</pre> Команда применяется для установки значений метрики по умолчанию для протокола маршрутизации OSPF. Команда “no default-metric” возвращает состояние по умолчанию
Параметр	<value> значение метрики в диапазоне от 0~16777214
По умолчанию	Встроено, автоматическая трансляция значения метрики
Режим	Режим протокола OSPF
Руководство по использованию	Метрика по умолчанию упрощает обработку несовместимых метрик и обеспечивает маршрутизацию. Если метрику невозможно конвертировать, то эта метрика по умолчанию используется вместо нее. Эта команда обеспечивает применение одного и того же значения метрики всеми входящими маршрутами. Используйте эту команду совместно с командой “redistribute”
Пример	<pre>Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#default-metric 100</pre>

16.2.13. Определение административных расстояний маршрутов в OSPF (distance)

Команда	<pre>distance {<value> ROUTEPARAMETER} no distance ospf</pre> Команда задает административное расстояние OSPF на основе типа маршрута. Команда “no distance ospf” восстанавливает значение по умолчанию
Параметр	<value> административное расстояние маршрутизации OSPF, в диапазоне 1~235



	ROUTEPARAMETER= ospf {ROUTE1 ROUTE2 ROUTE3} ROUTE1= external <external-distance> задает расстояние, полученное от других областей маршрутизации. <external-distance> расстояние, в диапазоне от 1 до 255. ROUTE2= inter-area <inter-distance> задает расстояние от одной области до другой. <inter-distance> значение административного расстояния в диапазоне 1~255. ROUTE3= intra-area <intra-distance> все значения расстояний в одной области. <intra-distance> значение административного расстояния в диапазоне 1~255
По умолчанию	Расстояние по умолчанию 110
Режим	Режим протокола OSPF
Руководство по использованию	Административное расстояние показывает надежность источника маршрутных сообщений. Значение расстояния может находиться в диапазоне 1~255. Чем больше значение административного расстояния, тем ниже надежность источника
Пример	<pre>Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#distance ospf inter-area 20 intra-area 10 external 40</pre>

16.2.14. Фильтрация обновлений маршрута (distribute-list)

Команда	distribute-list <access-list-name> out {kernel connected static rip isis bgp} no distribute-list out {kernel connected static rip isis bgp} Команда позволяет фильтровать обновления маршрута. Команда “no distribute-list out {kernel connected static rip isis bgp}” отключает данную функцию
Параметр	< access-list-name> имя применяемого списка доступа. out: фильтр отправленного обновления маршрута. kernel маршрутизация Kernel. connected прямая маршрутизация ; static статический маршрут ; rip RIP-маршрут; isis маршрут ISIS ; bgp маршрут BGP



По умолчанию	конфигурация по умолчанию отсутствует
Режим	Режим протокола OSPF
Руководство по использованию	Команда применяется при распределении маршрутов из других протоколов маршрутизации в таблицу маршрутизации OSPF
Пример	Ниже приведен пример объявления маршрута BGP на основании списка доступа access-list 1. <pre>Switch#config terminal Switch(config)#access-list 1 permit 172.10.0.0 0.0.255.255 Switch(config)#router ospf 100 Switch(config-router)#redistribute rip Switch(config-router)#distribute-list 1 out rip</pre>

16.2.15. Политика фильтрации (filter-policy)

Команда	filter-policy <access-list-name> no filter-policy Фильтрации обновления маршрутов, полученных OSPF, по списку контроля доступа. Команда с "no" в начале отменяет фильтрацию маршрута
Параметр	<access-list-name> имя списка доступа, для настройки можно использовать числовой стандартный список доступа IP и именованный стандартный список доступа IP
По умолчанию	конфигурация по умолчанию отсутствует
Режим	Режим протокола OSPF
Руководство по использованию	Команда применяется для фильтрации обновления маршрутов, полученных OSPF. Если указанный список доступа не существует, маршруты не фильтруются, фильтруются только маршруты, не удовлетворяющие правилам разрешения списка доступа. Для этой команды может быть задан один список доступа, при настройке нескольких списков доступа в силу вступит только последний
Пример	Применить список доступа 1 для фильтрации маршрутов, не принадлежащих сегменту 172.10.0.0/16. <pre>Switch#config terminal Switch(config)#access-list 1 permit 172.10.0.0 0.0.255.255 Switch(config)#router ospf Switch(config-router)#filter-policy 1</pre>



16.2.16. Принадлежность хоста к области (host area)

Команда	host <host-address> area <area-id> [cost <cost>] no host <host-address> area <area-id> [cost <cost>] Данная команда задает принадлежность всех тупиковых хостов к определенной области. Команда "[no] host <host-address> area <area-id> [cost <cost>]" отменяет данную конфигурацию
Параметр	<host-address> IP-адрес хоста в десятичной системе с точками. <area-id> идентификатор области, отображаемый в десятичной системе с точками или в виде целого числа в диапазоне 0~4294967295. <cost> задает полную стоимость, которая представляет собой целое число в диапазоне 0~65535, по умолчанию 0
По умолчанию	Принадлежность отсутствует
Режим	Режим протокола OSPF
Руководство по использованию	С помощью этой команды можно объявить некоторые определенные маршруты хостов в качестве тупиковых. Поскольку тупиковые хосты относятся к специальным маршрутизаторам, где настройка хоста не важна
Пример	<pre>Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#host 172.16.10.100 area 1 Switch(config-router)#host 172.16.10.101 area 2 cost 10</pre>

16.2.17. Настройка параметров ospf аутентификации на интерфейсе (ip ospf authentication)

Команда	ip ospf [<ip-address>] authentication [message-digest null] no ip ospf [<ip-address>] authentication Команда предназначена для отправки и получения пакетов OSPF с указанным методом аутентификации на текущем интерфейсе. Команда "no ip ospf [<ip-address>] authentication" отменяет аутентификацию
Параметр	<ip-address> IP-адрес интерфейса в десятичном представлении с точками. message-digest : аутентификация с использованием MD5. null : без аутентификации, сбрасывает пароль или MD5-аутентификацию, применяемую на интерфейсе



По умолчанию	При получении пакетов OSPF на интерфейсе не требуется аутентификация
Режим	Режим конфигурации интерфейса
Руководство по использованию	-
Пример	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf authentication message-digest

16.2.18. Задать пароль аутентификации OSPF (ip ospf authentication-key)

Команда	ip ospf [<ip-address>] authentication-key <0 LINE 7 WORD LINE> no ip ospf [<ip-address>] authentication Команда создает ключ аутентификации для отправки и получения пакетов OSPF на интерфейсе. Команда с "no" отменяет ключ аутентификации
Параметр	<ip-address> IP-адрес интерфейса в десятичном представлении с точками; <LINE> задает ключ аутентификации. тип ключа 0 означает незашифрованный криптографический ключ тип ключа 7 означает зашифрованный криптографический ключ. По умолчанию при отсутствии указания на тип применяется незашифрованный криптографический ключ
По умолчанию	При получении пакетов OSPF на интерфейсе не требуется аутентификация
Режим	Режим конфигурации интерфейса
Руководство по использованию	-
Пример	Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip ospf authentication-key 0 password



16.2.19. Стоимость пересылки данных через интерфейс (ip ospf cost)

Команда	ip ospf [<ip-address>] cost <cost> no ip ospf [<ip-address>] cost Команда указывает стоимость отправки для работы протокола OSPF на интерфейсе. Команда “no ip ospf [<ip-address>] cost” возвращает значение по умолчанию
Параметр	<ip-address> IP-адрес интерфейса в десятичном представлении с точками. <cost > значение стоимости протокола OSPF, диапазон от 1 до 65535
По умолчанию	Стоимость OSPF по умолчанию для интерфейса автоматически рассчитывается на основе пропускной способности
Режим	Режим конфигурации интерфейса
Руководство по использованию	-
Пример	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf cost 3

16.2.20. Фильтр базы данных LSA для конкретного интерфейса (ip ospf database-filter)

Команда	ip ospf [<ip-address>] database-filter all out no ip ospf [<ip-address>] database-filter Команда включает фильтр базы данных LSA для конкретного интерфейса. Команда “no ip ospf [<ip-address>] database-filter” закрывает фильтр
Параметр	<ip-address> IP-адрес интерфейса в десятичном представлении с точками; all : все LSA. out : отправленные LSA
По умолчанию	Фильтрация закрыта
Режим	Режим конфигурации интерфейса
Руководство по использованию	-



Пример	<pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf database-filter all out</pre>

16.2.21. Интервал ожидания отклика до объявления соседнего устройства недоступным (ip ospf dead-interval)

Команда	<pre>ip ospf [<ip-address>] dead-interval <time > no ip ospf [<ip-address>] dead-interval</pre> Задаёт продолжительность интервала, по истечении которого соседний маршрутизатор уровня 3 считается выключенным. Команда "no ip ospf [<ip-address>] dead-interval" command restores the default value
Параметр	<ip-address> IP-адрес интерфейса в десятичном представлении с точками; <time > интервал, после которого соседний маршрутизатор уровня 3 считается отключенным, в диапазоне от 1 до 65535 секунд
По умолчанию	Интервал по умолчанию - 40 секунд (4 интервала отправки hello-пакетов)
Режим	Режим конфигурации интерфейса
Руководство по использованию	Если по истечении "dead-interval" не получено ни одного пакета Hello, данный коммутатор 3 уровня считается недоступным и недействительным. Данная команда используется для установки интервала "dead" соседних коммутаторов уровня 3, в соответствии с фактическим состоянием соединения. Задаваемое значение "dead-interval" передается в пакетах Hello. Для обеспечения нормальной работы протокола OSPF "dead-interval" между соседними коммутаторами уровня 3 должен соответствовать значению отправки hello пакетов или быть равным 4-м интервалам отправки hello-пакетов
Пример	<pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf dead-interval 80</pre>

16.2.22. Запрет обработки OSPF пакетов на интерфейсе (ip ospf disable all)

Команда	<pre>ip ospf disable all no ip ospf disable all</pre> Команда останавливает обработку пакетов OSPF на интерфейсе
Параметр	-



По умолчанию	-.
Режим	Режим конфигурации интерфейса
Руководство по использованию	Команда сбрасывает команды сетевой области и останавливает групповые программы на определенном интерфейсе
Пример	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf disable all

16.2.23. Интервал между пакетами hello на интерфейсе (ip ospf hello-interval)

Команда	ip ospf [<ip-address>] hello-interval <time> no ip ospf [<ip-address>] hello-interval Указывает интервал отправки пакетов hello на интерфейсе. Команда "no ip ospf [<ip-address>] hello-interval" восстанавливает значение по умолчанию
Параметр	<ip-address> IP-адрес интерфейса в десятичном представлении с точками; <time> интервал отправки пакетов HELLO, указывается в секундах и находится в диапазоне 1~65535
По умолчанию	Интервал для hello-interval на интерфейсе 10 секунд
Режим	Режим конфигурации интерфейса
Руководство по использованию	Пакет данных HELLO является наиболее распространенным пакетом, который периодически отправляется на соседний коммутатор уровня 3 для обнаружения и поддержания отношений смежности, выбора DR и BDR. Пользовательское значение "hello-interval" передается в пакетах HELLO. Чем меньше интервал hello, тем быстрее будут обнаружены топологические изменения, но это приведет к увеличению трафика маршрутизации. Для обеспечения нормальной работы протокола OSPF параметр "hello-interval" между соседними с интерфейсом коммутаторами уровня 3 должен быть одинаковым
Пример	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf hello-interval 20



16.2.24. Парегистрировать ключ для аутентификации OSPF (ip ospf message-digest-key)

Команда	<pre>ip ospf [<ip-address>] message-digest-key <key_id> MD5 <0 LINE 7 WORD LINE></pre> <pre>no ip ospf [<ip-address>] message-digest-key <key_id></pre> Задаёт идентификатор ключа и значение MD5 аутентификации на интерфейсе. Команда с "no" в начале восстанавливает значение по умолчанию
Параметр	<ip-address> IP-адрес интерфейса в десятичном представлении с точками; <key_id> диапазон от 1 до 255; <LINE> ключ OSPF. тип ключа 0 означает незашифрованный криптографический ключ, тип ключа 7 означает зашифрованный криптографический ключ. По умолчанию при отсутствии указания на тип применяется незашифрованный криптографический ключ
По умолчанию	По умолчанию ключ MD5 для аутентификации OSPF не задан
Режим	Режим конфигурации интерфейса
Руководство по использованию	Аутентификация с использованием ключа MD5 используется для обеспечения безопасности между маршрутизаторами OSPF в сети. При использовании этой команды между соседями должны быть настроены одинаковые идентификатор и ключ, иначе отношения смежности не будут созданы
Пример	<pre>Switch#config terminal</pre> <pre>Switch(config)#interface vlan 1</pre> <pre>Switch(config-if-vlan1)#ip ospf message-digest-key 2 MD5 0 yourpassword</pre>

16.2.25. Размер MTU для OSPF (ip ospf mtu)

Команда	<pre>ip ospf mtu <mtu> no ip ospf mtu</pre> Устанавливает значение MTU (максимальный передаваемый блок данных) интерфейса для создания пакетов OSPF на основе этого значения. Команда "no ip ospf mtu" восстанавливает значение по умолчанию
Параметр	<mtu > значение mtu интерфейса в диапазоне 576~65535
По умолчанию	Применяется mtu интерфейса, полученное из ядра
Режим	Режим конфигурации интерфейса



Руководство по использованию	Значение интерфейса, заданное этой командой, используется только протоколом OSPF, а не обновляется в ядре
Пример	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf mtu 1480

16.2.26. Игнорировать эту проверку MTU (ip ospf mtu-ignore)

Команда	ip ospf <ip-address> mtu-ignore no ip ospf <ip-address> mtu-ignore Использование этой команды заставляет игнорировать проверку размера MTU в ходе обмена описанием базы данных DD. Команда "no ip ospf <ip-address> mtu-ignore" обеспечивает проверку размера mtu при обмене DD
Параметр	<ip-address> IP-адрес интерфейса в десятичном представлении с точками
По умолчанию	Проверка размера mtu при обмене DD выполняется
Режим	Режим конфигурации интерфейса
Руководство по использованию	-
Пример	Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf mtu-ignore

16.2.27. Задать тип сети OSPF (ip ospf network)

Команда	ip ospf network {broadcast non-broadcast point-to-point point-to-multipoint} no ip ospf network Команда указывает тип сети OSPF на интерфейсе. Команда "no ip ospf network" восстанавливает значение по умолчанию
Параметр	broadcast : выбор режима широковещательной сети для интерфейса non-broadcast : выбор режима NBMA сети для интерфейса point-to-point : выбор режима сети "точка-точка" для интерфейса point-to-multipoint : выбор режима сети "один-ко-многим" для интерфейса



По умолчанию	По умолчанию для OSPF используется тип сети "broadcast"(широковещательная сеть)
Режим	Режим конфигурации интерфейса
Руководство по использованию	-
Пример	В приведенной ниже конфигурации тип сети OSPF для интерфейса vlan 1 установлен на "point-to-point". Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf network point-to-point

16.2.28. Задать приоритет маршрутизатора (ip ospf priority)

Команда	ip ospf [<ip-address>] priority <priority> no ip ospf [<ip-address>] priority Команда задает приоритет маршрутизатора для определения "Defined layer 3 switch" назначенного коммутатора уровня 3 на интерфейсе. Команда "no ip ospf [<ip-address>] priority" восстанавливает значение по умолчанию
Параметр	<ip-address> IP-адрес интерфейса в десятичном представлении с точками. <priority> is the priority of which the valid value ranges between 0~255
По умолчанию	Приоритет по умолчанию выборе назначенного маршрутизатора равен 1
Режим	Режим конфигурации интерфейса
Руководство по использованию	Когда два маршрутизатора, подключенные к одному сегменту сети, пытаются стать назначенными маршрутизаторами, предпочтение отдается тому, у которого выше приоритет. Как правило выбирается маршрутизатор с более высоким приоритетом, но, если для двух маршрутизаторов приоритет одинаковый, предпочтение отдается маршрутизатору с более высоким ID маршрутизатора. Маршрутизатор уровня 3 с приоритетом равным 0, не может стать назначенным маршрутизатором "Defined layer 3 switch" или резервным назначенным маршрутизатором "Backup Defined layer 3 switch"
Пример	Настроить приоритет выбора DR. Установить для интерфейса vlan 1 отсутствие права на выбор, а именно установить приоритет 0. Switch#config terminal Switch(config)#interface vlan 1



	Switch(config-if-vlan1)#ip ospf priority 0

16.2.29. Интервал между повторными передачами объявлений о состоянии связи (ip ospf retransmit-interval)

Команда	ip ospf [<ip-address>] retransmit-interval <time> no ip ospf [<ip-address>] retransmit-interval Задаёт интервал повторной передачи объявлений о состоянии соединения между интерфейсом и соседними коммутаторами уровня 3. Команда “no ip ospf [<ip-address>] retransmit-interval” восстанавливает значение по умолчанию
Параметр	<ip-address> IP-адрес интерфейса в десятичном представлении с точками. <time> интервал повторной передачи объявлений о состоянии соединения между интерфейсом и соседними коммутаторами уровня 3, указывается в секундах и находится в диапазоне 1 ~ 65535
По умолчанию	Интервал повторной передачи 5 секунд
Режим	Режим конфигурации интерфейса
Руководство по использованию	Когда коммутатор уровня 3 передает LSA соседу, он сохраняет объявление о состоянии соединения до тех пор, пока не получит подтверждение от адресата. Если в течение этого интервала времени пакет подтверждения не получен, LSA передается повторно. Интервал повторной передачи должен быть больше, чем время, необходимое для одного раунда передачи между двумя коммутаторами уровня 3
Пример	Задать интервал повторной передачи LSA для интерфейса vlan 1 в 10 секунд. <pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf retransmit-interval 10</pre>

16.2.30. Предполагаемое время для отправки пакета LSA (ip ospf transmit-delay)

Команда	ip ospf [<ip-address>] transmit-delay <time> no ip ospf [<ip-address>] transmit-delay Задаёт предполагаемое время, необходимое для отправки пакета обновления состояния канала на интерфейсе. Команда “no ip ospf [<ip-address>] transmit-delay” восстанавливает значение по умолчанию



Параметр	<ip-address>IP-адрес интерфейса в десятичном представлении с точками. <time>время задержки отправки анонсов о состоянии канала на интерфейс, которое указывается в секундах и находится в диапазоне 1 ~65535
По умолчанию	По умолчанию время задержки отправки LSA на интерфейс составляет 1 секунду
Режим	Режим конфигурации интерфейса
Руководство по использованию	В LSA-пакете время жизни пакета должно быть увеличено на значение, указанное в параметрах для коммутатора уровня 3, но до процесса передачи. При добавлении "transit-delay" до отправки LSA, пакет будет отправлен до истечения времени жизни
Пример	Установить задержку отправки LSA интерфейса vlan 1 на 3 секунды. <pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip ospf transmit-delay 3</pre>

16.2.31. Создание ключа в ключевой цепочке (key)

Команда	key <keyid> no key <keyid> Команда используется для создания и добавления ключа в ключевой цепочке. Команда "no key <keyid>" удаляет один ключ
Параметр	<keyid>идентификатор ключа в диапазоне 0-2147483647
По умолчанию	-.
Режим	Режим конфигурации цепочки ключей (keychainMode и keychain-key)
Руководство по использованию	Эта команда позволяет войти в режим цепочки ключей, чтобы установить пароли для соответствующих ключей
Пример	<pre>Switch#config terminal Switch(config)#key chain mychain Switch(config-keychain)#key 1 Switch(config-keychain-key)#</pre>



16.2.32. Цепочка ключей (key chain)

Команда	key chain <name-of-chain> no key chain < name-of-chain > Команда позволяет войти в режим управления цепочкой ключей и выполнить настройки. Команда Команда “no key chain < name-of-chain >” удаляет одну цепочку ключей
Параметр	<name-of-chain>имя цепочки ключей, длина строки не ограничена
По умолчанию	-
Режим	Режим глобальной конфигурации и режим конфигурации цепочки ключей
Руководство по использованию	-
Пример	Switch#config terminal Switch(config)#key chain mychain Switch(config-keychain)#

16.2.33. Отправка сообщений об изменении состояния для протокола OSPF (log-adjacency-changes detail)

Команда	log-adjacency-changes detail no log-adjacency-changes detail Команда настраивает ведение журнала изменений смежности OSPF
Параметр	-
По умолчанию	По умолчанию отправка сообщений об изменении смежности OSPF не ведется
Режим	Режим конфигурации протокола OSPF
Руководство по использованию	После ввода данной команды информация об изменении смежности OSPF записывается в системный журнал
Пример	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)# log-adjacency-changes detail



16.2.34. Максимальное количество одновременно обрабатываемых сообщений обмена базами данных (max-concurrent-dd)

Команда	max-concurrent-dd <value> no max-concurrent-dd Команда устанавливает максимальное количество обрабатываемых сообщений обмена базами данных dd в процессе OSPF. Команда "no max-concurrent-dd" восстанавливает значение по умолчанию
Параметр	<value> в диапазоне <1-65535>, количество одновременно обрабатываемых пакетов данных dd
По умолчанию	Нет ограничений на максимальное количество одновременно обрабатываемых сообщений dd
Режим	Режим протокола OSPF
Руководство по использованию	Команда ограничивает максимальное число обменов dd, находящихся в обработке OSPF
Пример	Ограничить одновременно обрабатываемые dd до 20. Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#max-concurrent-dd 20

16.2.35. Указание соседа по протоколу OSPF (neighbor)

Команда	neighbor A.B.C.D [<cost> priority <value> poll-interval <value>] no neighbor A.B.C.D [<cost> priority <value> poll-interval <value>] Команда применяется для конфигурирования соединения маршрутизатора OSPF с NBMA сетью. Команда "no neighbor A.B.C.D [<cost> priority <value> poll-interval <value>]" удаляет конфигурацию
Параметр	<cost>, стоимость OSPF для соседа в диапазоне 1-65535 ; priority <value>, приоритет соседнего устройства. По умолчанию 0, диапазон настройки 0-255 ; poll-interval <value>, по умолчанию 120 секунд. Интервал опроса до появления отношений смежности, в диапазоне 1-65535
По умолчанию	конфигурация по умолчанию отсутствует
Режим	Режим протокола OSPF



Руководство по использованию	Команда применяется в сети NBMA для явного указания соседнего узла. Для каждого известного соседнего маршрутизатора в не широковещательной сети необходимо сделать запись. Адрес настроенного соседа должен быть первичным адресом интерфейса. Интервал опроса должен быть больше hello-интервала
Пример	<pre>Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#neighbor 1.2.3.4 priority 1 poll-interval 90 Switch(config-router)#neighbor 1.2.3.4 cost 15</pre>

16.2.36. Определение OSPF области (network area)

Команда	<pre>network NETWORKADDRESS area <area-id> no network NETWORKADDRESS area <area-id></pre> Команда включает функцию маршрутизации OSPF для интерфейса с IP-адресом, совпадающим с адресом сети. Команда “no network NETWORKADDRESS area <area-id>” удаляет конфигурацию и останавливает протокол OSPF на соответствующем интерфейсе
Параметр	NETWORKADDRESS = A.B.C.D/M A.B.C.D X.Y.Z.W, сетевой адрес с префиксом или маской. Для адреса с маской должна применяться перевернутая маска wildcast; <area-id>ip-адрес или номер области, указывается в десятичной системе, в диапазоне 0~4294967295
По умолчанию	Конфигурация по умолчанию отсутствует
Режим	Режим протокола OSPF
Руководство по использованию	Когда определенный сегмент принадлежит определенной области, интерфейс, которому принадлежит сегмент, отправляет hello-сообщения и обменивается базой данных с подключенным соседним узлом
Пример	Конфигурация 10.1.1.0/24 находится в области 1. <pre>Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#network 10.1.1.0/24 area 1</pre>



16.2.37. Тип пограничного маршрутизатора (ospf abr-type)

Команда	ospf abr-type {cisco ibm shortcut standard} no ospf abr-type Команда указывает тип пограничного маршрутизатора OSPF. Команда "no ospf abr-type" восстанавливает значение по умолчанию
Параметр	cisco пограничный маршрутизатор cisco; ibm, пограничный маршрутизатор ibm; shortcut, пограничный маршрутизатор с короткими путями; standard, стандартный пограничный маршрутизатор (RFC2328)
По умолчанию	Cisco
Режим	Режим протокола OSPF
Руководство по использованию	Команда указывает тип пограничного маршрутизатора. Эта команда подходит для взаимодействия между различными протоколами OSPF, особенно в среде с несколькими хостами
Пример	Задать пограничный маршрутизатор как "standard". Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#ospf abr-type standard

16.2.38. ID маршрутизатора для процессов OSPF (ospf router-id)

Команда	ospf router-id <address> no ospf router-id Определяет идентификатор маршрутизатора для OSPF. Команда "no ospf router-id" сбрасывает идентификационный номер
Параметр	<address> , идентификатор маршрутизатора в формате IPv4-адреса
По умолчанию	Конфигурация по умолчанию отсутствует
Режим	Режим протокола OSPF
Руководство по использованию	Новый идентификатор начинает действовать сразу же



Пример	Задать router-id для ospf 100 на 2.3.4.5. Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#ospf router-id 2.3.4.5

16.2.39. Ограничить количество LSA, получаемых маршрутизатором (overflow database)

Команда	overflow database <maxdbsize > [{hard soft}] no overflow database Команда ограничивает максимальное число объявлений о состоянии связи LSA. Команда "no overflow database" снимает ограничение
Параметр	< maxdbsize > максимальное количество LSA в диапазоне 0~4294967294. soft : мягкие ограничения, при превышении выдается предупреждение hard : жесткие ограничения, при превышении экземпляр OSPF отключается. Если тип ограничения не задан, устанавливается жесткое ограничение
По умолчанию	Не сконфигурировано
Режим	Режим протокола OSPF
Руководство по использованию	-
Пример	Switch#config terminal Switch(config)#router ospf Switch(config-router)#overflow database 10000 soft



16.2.40. Максимальное количество LSA от внешних автономных систем (overflow database external)

Команда	overflow database external [<maxdbsize> <maxtime>] no overflow database external [<maxdbsize> <maxtime>] Команда позволяет настроить размер внешней базы данных внешних систем и время ожидания маршрутизатора перед выходом из состояния переполнения. Команда “no overflow database external [<maxdbsize> <maxtime>]” восстанавливает значение по умолчанию
Параметр	< maxdbsize > размер базы данных внешних связей, в диапазоне от 0 до 4294967294, по умолчанию 4294967294. < maxtime > время в секундах, которое маршрутизатор ожидает выхода из режима переполнения базы, в диапазоне 0~65535
По умолчанию	-
Режим	Режим протокола OSPF
Руководство по использованию	-
Пример	Switch#config terminal Switch(config)#router ospf Switch(config-router)#overflow database external 5 3

16.2.41. Отключить отправку обновлений маршрутизации (passive-interface)

Команда	passive-interface<ifname> [<ip-address>] no passive-interface<ifname> [<ip-address>] Отключает отправку пакетов hello на определенные интерфейсы. Команда “no passive-interface <ifname> [<ip-address>]” отменяет эту функцию
Параметр	<ifname> имя определенного интерфейса. <ip-address> IP-адрес интерфейса в десятичном представлении с точками
По умолчанию	Не сконфигурировано
Режим	Режим протокола OSPF



Руководство по использованию	-
Пример	<pre>Switch#config terminal Switch(config)#router ospf Switch(config-router)#passive-interface vlan1</pre>

16.2.42. Перераспределение маршрутов (redistribute)

Команда	<pre>redistribute {kernel connected static rip isis bgp} [metric<value>] [metric-type {1 2}][route-map<word>][tag<tag-value>] no redistribute {kernel connected static rip isis bgp} [metric<value>] [metric-type {1 2}][route-map<word>][tag<tag-value>]</pre> Вводит маршруты, полученные от других протоколов маршрутизации
Параметр	kernel задается из маршрута kernel connected задается из прямого маршрута. static задается из статических маршрутов. rip задается из маршрута RIP isis задается из маршрута ISIS. bgp задается из маршрута BGP. metric <value> метрика, которая будет использоваться для перераспределенных маршрутов, в диапазоне 0-16777214. metric-type {1 2} тип метрики задаваемого внешнего маршрута, может быть 1 или 2, значение по умолчанию 2. route-map <word> указывает на карту маршрутов для задаваемых маршрутов tag<tag-value> идентификационный номер внешнего маршрута, в диапазоне 0~4294967295, по умолчанию 0
По умолчанию	-
Режим	Режим протокола OSPF
Руководство по использованию	Получение и внедрение других протоколов маршрутизации в область OSPF для создания маршрутов LSA от внешних источников (AS-external_LSAs.)
Пример	<pre>Switch#config terminal Switch(config)#router ospf Switch(config-router)#redistribute bgp metric 12</pre>



16.2.43. Перераспределение маршрутов OSPF (redistribute ospf)

Команда	<pre>redistribute ospf [<process-id>] [metric<value>] [metric-type {1 2}][route-map<word>]</pre> <pre>no redistribute ospf [<process-id>] [metric<value>] [metric-type {1 2}] [route-map<word>]</pre> Переназначает ID маршрутизации процесса указанному процессу. Команда с "no" в начале удаляет перераспределение. При вводе необязательных параметров metric, metric type и routemap восстанавливается значение по умолчанию
Параметр	process-id идентификатор процесса OSPF, по умолчанию 0. metric <value> метрика для перераспределенной маршрутизации, диапазон от 0 до 16777214 metric-type {1 2} тип метрики для перераспределенной маршрутизации, может быть только 1 или 2, по умолчанию 2. route-map <word> указатель на введенную карту маршрутизации
По умолчанию	По умолчанию маршрутизация OSPF не перераспределяется
Режим	Режим протокола OSPF
Руководство по использованию	Если идентификатор process-id не введен, это означает, что маршрутизация OSPF будет перераспределена по умолчанию (Process-id равен 0)
Пример	Switch(config-router)#redistribute ospf

16.2.44. Включение процесса маршрутизации OSPF (router ospf)

Команда	<pre>router ospf <process_id> no router ospf <process_id></pre> Команда используется для настройки процесса маршрутизации OSPF
Параметр	<process_id> идентификатор создаваемого процесса OSPF, в диапазоне от 1 до 65535
По умолчанию	-
Режим	Режим глобальной конфигурации
Руководство по использованию	-



Пример	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#network 10.1.1.0/24 area 0

16.2.45. Создание суммированных адресов (summary-address)

Команда	summary-address <A.B.C.D/M> [{not-advertise tag<tag-value>}] Команда предназначена для суммирования или подавления внешних маршрутов с указанным диапазоном адресов
Параметр	<A.B.C.D/M> диапазон адресов, IPv4-адрес в десятичной записи с точками плюс длина маски. not-advertised подавлять (не анонсировать) внешние маршруты. tag<tag-value> идентификация тега внешнего маршрута в диапазоне 0~4294967295, по умолчанию равно 0
По умолчанию	-
Режим	Режим протокола OSPF
Руководство по использованию	Для перераспределения маршрутов из других протоколов в OSPF требуется, чтобы маршрутизатор объявлял каждый маршрут отдельно во внешнем LSA. Команда позволяет объявлять один суммарный маршрут для всех перераспределенных маршрутов, охватываемых указанным сетевым адресом и маской. Это минимизирует размер базы данных состояний каналов OSPF
Пример	Switch#config terminal Switch(config)#router ospf Switch(config-router)#summary-address 172.16.0.0/16 tag 3

16.2.46. Время выполнения вычислений кратчайшего пути (timers spf)

Команда	timers spf <spf-delay> <spf-holdtime> no timers spf Регулирует время выполнения алгоритма вычисления кратчайших путей. Команда “no timers spf” возвращает значения по умолчанию
Параметр	<spf-delay> 5 секунд по умолчанию <spf-holdtime> 10 секунд по умолчанию
По умолчанию	-
Режим	Режим протокола OSPF



Руководство по использованию	Эта команда устанавливает время задержки между получением изменения топологии и расчетом SPF, а также устанавливает время удержания между двумя прерванными расчетами SPF
Пример	Switch#config terminal Switch(config)#router ospf Switch(config-router)#timers spf 5 10

16.2.47. Просмотр общей информации о процессах маршрутизации OSPF (show ip ospf)

Команда	show ip ospf [<process-id>] Команда отображает текущее состояние процесса маршрутизации OSPF
Параметр	<process-id> идентификатор процесса в диапазоне 0~65535
По умолчанию	Информация не отображается
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	-
Пример	Switch#show ip ospf Routing Process "ospf 0" with ID 192.168.1.1 Process bound to VRF default Process uptime is 2 days 0 hour 30 minutes Conforms to RFC2328, and RFC1583Compatibility flag is disabled Supports only single TOS(TOS0) routes Supports opaque LSA SPF schedule delay 5 secs, Hold time between two SPFs 10 secs Refresh timer 10 secs Number of external LSA 0. Checksum Sum 0x000000 Number of opaque AS LSA 0. Checksum Sum 0x000000 Number of non-default external LSA 0 External LSA database is unlimited. Number of LSA originated 0 Number of LSA received 0 Number of areas attached to this router: 1 Area 0 (BACKBONE) (Inactive) Number of interfaces in this area is 0(0)



	Number of fully adjacent neighbors in this area is 0 Area has message digest authentication SPF algorithm executed 0 times Number of LSA 0. Checksum Sum 0x000000 Routing Process "ospf 10" with ID 0.0.0.0 Process bound to VRF test Process uptime is 4 days 23 hours 51 minutes Conforms to RFC2328, and RFC1583Compatibility flag is disabled Supports only single TOS(TOS0) routes Supports opaque LSA SPF schedule delay 5 secs, Hold time between two SPFs 10 secs Refresh timer 10 secs Number of external LSA 0. Checksum Sum 0x000000 Number of opaque AS LSA 0. Checksum Sum 0x000000 Number of non-default external LSA 0 External LSA database is unlimited. Number of LSA originated 0 Number of LSA received 0 Number of areas attached to this router: 1 Area 0 (BACKBONE) (Inactive) Number of interfaces in this area is 0(0) Number of fully adjacent neighbors in this area is 0 Area has no authentication SPF algorithm executed 0 times Number of LSA 0. Checksum Sum 0x000000

16.2.48. Просмотр внутренней таблицы маршрутизации OSPF для граничных маршрутизаторов (show ip ospf border-routers)

Команда	show ip ospf [<process-id>] border-routers Выводит на экран записи внутренней таблицы маршрутизации для маршрутизаторов граничных областей (ABR) и граничных маршрутизаторов автономных систем (ASBR) всех экземпляров
Параметр	<process-id> идентификатор процесса, в диапазоне 0~65535
По умолчанию	Информация не отображается



Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	-
Пример	Switch#show ip ospf border-routers OSPF process 0 internal Routing Table Codes: i - Intra-area route, I - Inter-area route i 10.15.0.1 [10] via 10.10.0.1, Vlan1, ASBR, Area 0.0.0.0 i 172.16.10.1 [10] via 10.10.11.50, Vlan2, ABR, ASBR, Area 0.0.0.0

16.2.49. Просмотр информации о базе данных OSPF (show ip ospf database)

Команда	show ip ospf [<process-id>] database[adv-router [{<linkstate_id> self-originate adv-router <advertiser_router>}]asbr-summary[{<linkstate_id> self-originate adv-router <advertiser_router>}] external [{<linkstate_id> self-originate adv-router <advertiser_router>}] network [{<linkstate_id> self-originate adv-router <advertiser_router>}]nssa-external [{<linkstate_id> self-originate adv-router <advertiser_router>}]opaque-area [{<linkstate_id> self-originate adv-router <advertiser_router>}]opaque-as [{<linkstate_id> self-originate adv-router <advertiser_router>}]opaque-link [{<linkstate_id> self-originate adv-router <advertiser_router>}]router [{<linkstate_id> self-originate adv-router <advertiser_router>}]summary [{<linkstate_id> self-originate adv-router <advertiser_router>}]self-originate max-age } Выводит на экран сообщения о базе данных OSPF
Параметр	<process-id> идентификатор процесса маршрутизации, в диапазоне 0~65535 <linkstate_id> идентификатор состояния соединения, в десятичном формате с точками. <advertiser_router> идентификатор анонсирующего маршрутизатора в виде IP-адреса в десятичном формате с точками
По умолчанию	Информация не отображается
Режим	Привилегированный режим и режим конфигурации



Руководство по использованию	В сообщениях, появляющихся после ввода этой команды, можно просмотреть информацию о базе данных состояния соединений OSPF
Пример	<pre>Switch#show ip ospf database Router Link States (Area 0.0.0.2) Link ID ADV Router Age Seq# CkSum Link count 192.168.1.2 192.168.1.2 254 0x800000031 0xec21 1 192.168.1.3 192.168.1.3 236 0x800000033 0x0521 2 Net Link States (Area 0.0.0.2) Link ID ADV Router Age Seq# CkSum 20.1.1.2 192.168.1.2 254 0x80000002b 0xece4 Summary Link States (Area 0.0.0.2) Link ID ADV Router Age Seq# CkSum Route 6.1.0.0 192.168.1.2 68 0x80000002b 0x5757 6.1.0.0/22 6.1.1.0 192.168.1.2 879 0x80000002a 0xf8bc 6.1.1.0/24 22.1.1.0 192.168.1.2 308 0x80000000c 0xc8f0 22.1.1.0/24 ASBR-Summary Link States (Area 0.0.0.2) Link ID ADV Router Age Seq# CkSum 192.168.1.1 192.168.1.2 1702 0x80000002a 0x89c7 AS External Link States Link ID ADV Router Age Seq# CkSum Route 2.2.2.0 192.168.1.1 1499 0x800000056 0x3a63 E2 2.2.2.0/24 [0x0] 2.2.3.0 192.168.1.1 1103 0x80000002b 0x0ec3 E2 2.2.3.0/24 [0x0]</pre>

16.2.50. Просмотр информации об интерфейсе для OSPF (show ip ospf interface)

Команда	<pre>show ip ospf interface <interface></pre> Выводит на экран информацию об интерфейсе для OSPF
Параметр	<interface> имя интерфейса
По умолчанию	Информация не отображается
Режим	Привилегированный режим и режим конфигурации



Руководство по использованию	-
Пример	<pre>Switch#show ip ospf interface Loopback is up, line protocol is up OSPF not enabled on this interface Vlan1 is up, line protocol is up Internet Address 10.10.10.50/24, Area 0.0.0.0 Process ID 0, Router ID 10.10.11.50, Network Type BROADCAST, Cost: 10 Transmit Delay is 5 sec, State Waiting, Priority 1 No designated router on this network No backup designated router on this network Timer intervals configured, Hello 35, Dead 35, Wait 35, Retransmit 5 Hello due in 00: 00: 16 Neighbor Count is 0, Adjacent neighbor count is 0</pre>

16.2.51. Просмотр информации о соседних узлах (show ip ospf neighbor)

Команда	<pre>show ip ospf [<process-id>] neighbor [{<neighbor_id> all detail [all] interface<ifaddress>}]</pre> Выводит на экран сообщения о соседних узлах протокола OSPF
Параметр	<process-id> идентификатор процесса в диапазоне 0~65535 <neighbor_id> идентификатор соседа в десятичной системе с точечной записью all : выводит информацию обо всех соседних устройствах detail : выводит подробную информацию о соседних устройствах <ifaddress> IP-адрес интерфейса
По умолчанию	Информация не отображается
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	Команда позволяет просмотреть состояние соседних устройств протокола OSPF
Пример	<pre>Switch#show ip ospf neighbor OSPF process 0: Neighbor ID Pri State Dead Time Address Interface</pre>



	192.168.1.1 1 Full/Backup 00: 00: 32 6.1.1.1 Vlan1 192.168.1.3 1 Full/DR 00: 00: 36 20.1.1.3 Vlan2 192.168.1.3 1 Full/ - 00: 00: 30 20.1.1.3 VLINK2	
	Информация, отображаемая на экране	Пояснение
	Neighbor ID	Идентификатор соседнего устройства
	Priority	Приоритет
	State	Состояние смежности
	Dead time	Период неактивности
	Address	Адрес интерфейса
	Interface	Имя интерфейса

16.2.52. Просмотр информации о перераспределении в OSPF (show ip ospf redistribute)

Команда	show ip ospf [<process-id>] redistribute Выводит на экран сообщения о маршрутизации, перераспределенной из внешнего процесса OSPF
Параметр	<process-id> идентификатор процесса в диапазоне 0~65535
По умолчанию	-
Режим	Привилегированный режим, режим конфигурации
Руководство по использованию	-
Пример	Switch#show ip ospf redistribute ospf process 1 redistribute information : ospf process 2 ospf process 3 bgp ospf process 2 redistribute information : ospf process 1 bgp ospf process 3 redistribute information :



	<pre>ospf process 1 bgp Switch#show ip ospf 2 redistribute ospf process 2 redistribute information : ospf process 1 bgp</pre>

16.2.53. Просмотр сводной информации о маршрутах в OSPF (show ip ospf route)

Команда	<pre>show ip ospf [<process-id>] route</pre> Выводит на экран таблицу маршрутизации в процессе OSPF
Параметр	<process-id> идентификатор процесса в диапазоне 0~65535
По умолчанию	-
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	-
Пример	<pre>Switch#show ip ospf route O 10.1.1.0/24 [10] is directly connected, Vlan1, Area 0.0.0.0 O 10.1.1.4/32 [10] via 10.1.1.4, Vlan1, Area 0.0.0.0 IA 11.1.1.0/24 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0 IA 11.1.1.2/32 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0 IA 12.1.1.0/24 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0 IA 12.1.1.2/32 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0 O 13.1.1.0/24 [10] is directly connected, Vlan4, Area 0.0.0.3 O 14.1.1.0/24 [10] is directly connected, Vlan5, Area 0.0.0.4 IA 15.1.1.0/24 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3 IA 15.1.1.2/32 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3 E1 100.1.0.0/16 [21] via 10.1.1.1, Vlan1 E1 100.2.0.0/16 [21] via 10.1.1.1, Vlan1</pre>



16.2.54. Просмотр виртуальных соединений с другими маршрутизаторами OSPF (show ip ospf virtual-links)

Команда	show ip ospf [<process-id>] virtual-links Выводит информацию о виртуальных соединениях OSPF
Параметр	<process-id> идентификатор процесса в диапазоне 0~65535
По умолчанию	-
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	-
Пример	Switch#show ip ospf virtual-links Virtual Link VLINK0 to router 10.10.0.9 is up Transit area 0.0.0.1 via interface Vlan1 Transmit Delay is 1 sec, State Point-To-Point, Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00: 00: 02 Adjacency state Full Virtual Link VLINK1 to router 10.10.0.123 is down Transit area 0.0.0.1 via interface Vlan1 Transmit Delay is 1 sec, State Down, Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in inactive Adjacency state Down

16.2.55. Просмотр подробной информации о маршрутизации (show ip route process-detail)

Команда	show ip route [database] process-detail Выводит на экран таблицу IP-маршрутизации с указанным идентификатором процесса или меткой
Параметр	Параметр database выводит все маршрутизаторы, при отсутствии параметра отображаются только работающие маршрутизаторы
По умолчанию	По умолчанию ни для какого маршрутизатора процесса OSPF информация не выводится



Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	-
Пример	Switch#show ip route database process-detail Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area > - selected route, * - FIB route, p - stale info C *> 127.0.0.0/8 is directly connected, Loopback O 192.168.2.0/24 [110/10] is directly connected, Vlan2, 00: 06: 13,process 12 C *> 192.168.2.0/24 is directly connected, Vlan2

16.2.56. Просмотр статуса и параметров протоколов маршрутизации (show ip protocols)

Команда	show ip protocols Выводит на экран информацию о запущенном протоколе маршрутизации
Параметр	
По умолчанию	-
Режим	Привилегированный режим и режим конфигурации
Руководство по использованию	-
Пример	Switch#show ip protocols Команда "show ip protocols" отобразит сообщения протокола маршрутизации, запущенного на текущем коммутаторе уровня 3. Например, на экране появятся следующие сообщения: Routing Protocol is "ospf 0" Invalid after 0 seconds, hold down 0, flushed after 0 Outgoing update filter list for all interfaces is Incoming update filter list for all interfaces is



	Redistributing: Routing for Networks: 10.1.1.0/24 12.1.1.0/24 Routing Information Sources: Gateway Distance Last Update Distance: (default is 110) Address Mask Distance List Routing Protocol is "bgp 0" Outgoing update filter list for all interfaces is Incoming update filter list for all interfaces is IGP synchronization is disabled Automatic route summarization is disabled Neighbor(s): Address FiltIn FiltOut DistIn DistOut Weight RouteMap Incoming Route Filter:

16.2.57. Параметры отладки и устранения неполадок событий OSPF (debug ospf events)

Команда	debug ospf events [abr asbr lsa nssa os router vlink] no debug ospf events [abr asbr lsa nssa os router vlink] Открывает параметры отладки, показывающие различные сообщения о событиях OSPF. Команда "no debug ospf events [abr asbr lsa nssa os router vlink]" закрывает параметры отладки
Параметр	-
По умолчанию	Закреты
Режим	Привилегированный режим и Режим глобальной конфигурации
Руководство по использованию	-
Пример	Switch#debug ospf events router



16.2.58. Параметры отладки состояний IFSM в OSPF (debug ospf ifsm)

Команда	<pre>debug ospf ifsm [status events timers] no debug ospf ifsm [status events timers]</pre> Команда включает параметры отладки полученных сообщений от NSM для RIP. Форма этой команды с "no" отключает отладку полученных сообщений от NSM для RIP
Параметр	-
По умолчанию	Закрыты
Режим	Привилегированный режим и глобальной конфигурации
Руководство по использованию	-
Пример	Switch#debug ospf ifsm events

16.2.59. Параметры отладки объявлений о состоянии канала (debug ospf lsa)

Команда	<pre>debug ospf lsa [generate flooding install maxage refresh] no debug ospf lsa [generate flooding install maxage refresh]</pre> Открывает параметры отладки, показывающие сообщения о состоянии канала. Команда "no debug ospf lsa [generate flooding install maxage refresh]" закрывает параметры отладки
Параметр	-
По умолчанию	Закрыты
Режим	Привилегированный режим и глобальной конфигурации
Руководство по использованию	-
Пример	Switch#debug ospf lsa generate



16.2.60. Параметры отладки состояний NFSM (debug ospf nfsm)

Команда	<code>debug ospf nfsm [status events timers] no debug ospf nfsm [status events timers]</code> Команда открывает опции отладки, показывающие состояние конечного автомата соседей OSPF. Команда “no debug ospf nfsm [status events timers]” закрывает параметры отладки
Параметр	-
По умолчанию	Закреты
Режим	Привилегированный режим и глобальной конфигурации
Руководство по использованию	-
Пример	Switch#debug ospf nfsm events

16.2.61. Параметры отладки, относящиеся к NSM в OSPF (debug ospf nsm)

Команда	<code>debug ospf nsm [interface redistribute] no debug ospf nsm [interface redistribute]</code> Открывает параметры отладки, относящихся к NSM в OSPF. Команда “no debug ospf nsm [interface redistribute]” закрывает параметры отладки
Параметр	-
По умолчанию	Закреты
Режим	Привилегированный режим и глобальной конфигурации
Руководство по использованию	-
Пример	Switch#debug ospf nsm interface



16.2.62. Параметры отладки пакетов OSPF (debug ospf packet)

Команда	debug ospf packet [dd detail hello ls-ack ls-request ls-update rcv detail] no debug ospf packet [dd detail hello ls-ack ls-request ls-update rcv detail] Открывает отладочные сообщения, относящиеся ко пакетам OSPF. Команда “no debug ospf packet [dd detail hello ls-ack ls-request ls-update rcv detail]” закрывает параметры отладки
Параметр	-
По умолчанию	Закреты
Режим	Привилегированный режим и глобальной конфигурации
Руководство по использованию	-
Пример	Switch#debug ospf packet hello

16.2.63. Параметры отладки процесса расчета маршрута (debug ospf route)

Команда	debug ospf route [ase ia install spf] no debug ospf route [ase ia install spf] Открывает процесс отладки, отображающий соответствующие маршруты OSPF. Команда “no debug ospf route [ase ia install spf]” закрывает параметры отладки
Параметр	-
По умолчанию	Закреты
Режим	Привилегированный режим и глобальной конфигурации
Руководство по использованию	-
Пример	Switch#debug ospf route spf



16.2.64. Параметры отладки отправленных сообщений перераспределения (debug ospf redistribute message send)

Команда	debug ospf redistribute message send no debug ospf redistribute message send Команда включает отладку отправки команды из процесса OSPF, перераспределенного в другие процессы маршрутизации OSPF. Форма команды с "no" в начале выключает отладку отправки команды из процесса OSPF, перераспределенного в другие процессы маршрутизации OSPF
Параметр	-
По умолчанию	Функция выключена
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Включить отладку отправки команды из процесса OSPF, перераспределенного в другие процессы маршрутизации OSPF Switch#debug ospf redistribute message send

16.2.65. Параметры отладки полученных сообщений о перераспределении маршрута (debug ospf redistribute route receive)

Команда	debug ospf redistribute route receive no debug ospf redistribute route receive Команда подключает и отключает отладку полученных сообщений маршрутизации от NSM для процесса OSPF
Параметр	-
По умолчанию	Функция выключена
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Подключить отладку полученных сообщений маршрутизации от NSM для процесса OSPF. Switch# debug ospf redistribute route receive



16.2.66. Поддержка мягкого перезапуска соседних маршрутизаторов (capability restart graceful)

Команда	capability restart graceful no capability restart Подключает мягкий перезапуск GR определенных процессов OSPF, форма команды с "no" отключает эту функцию
Параметр	-
По умолчанию	Функция мягкого перезапуска в процессе OSPF подключена
Режим	Режим конфигурации протокола OSPF
Руководство по использованию	Если на коммутаторе включено специальное свойство процесса OSPF "мягкий перезапуск" (GR), то при его отключении коммутатор сразу отзовет разрешение на GR
Пример	Подключить функцию GR для OSPF. Switch(config)#router ospf Switch(config-router)#capability restart graceful

16.2.67. Параметры отладки мягкого перезапуска на OSPF (debug ospf events gr)

Команда	debug ospf events gr no debug ospf events gr Подключает опции отладки для просмотра соответствующих событий GR на OSPF. Команда с "no" на начале отключает опции отладки
Параметр	-
По умолчанию	Функция выключена
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Включить параметры отладки для просмотра соответствующих событий GR на OSPF. Switch#debug ospf events gr



16.2.68. Период отсрочки мягкого перезапуска (ospf graceful-restart grace-period)

Команда	ospf graceful-restart grace-period <integer> no ospf restart grace-period Команда задает период отсрочки для перезапуска маршрутизатора. Команда с "no" на начале восстанавливает период отсрочки до значения по умолчанию
Параметр	<integer>: значение периода отсрочки в секундах, диапазон от 1 до 1800
По умолчанию	60 секунд
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда задает период отсрочки перезапуска GR (коммутатор обрабатывает протокол переключения или перезапуска). Процесс GR должен быть завершен в течение периода отсрочки. Если процесс не завершается вовремя, он завершается принудительно, а OSPF перезапускается в обычном режиме
Пример	Задать период мягкого перезапуска 100 секунд. Switch(config)#ospf graceful-restart grace-period 100

16.2.69. Поведение помощника для мягкого перезапуска (ospf graceful-restart helper max-grace-period)

Команда	ospf graceful-restart helper max-grace-period <integer> no ospf graceful-restart helper Команда задает одну из политик помощника для мягкого перезапуска. Устанавливает максимальный период отсрочки, поддерживаемый помощником. Команда с "no" удаляет все настроенные политики помощника
Параметр	<integer>: значение периода отсрочки в секундах, диапазон от 1 до 1800
По умолчанию	Период, поддерживаемый помощником, не ограничен
Режим	Режим глобальной конфигурации
Руководство по использованию	Помощь только в случае, если период отсрочки, заданный устройством мягкого перезапуска, превышает максимальный период отсрочки, установленный помощником, помощник не будет помогать завершать период GR. Команда с "no" удаляет все политики помощника



Пример	Задать максимальный период отсрочки, разрешенный помощником безопасного перезапуска в 100 секунд. <pre>Switch(config)#ospf graceful-restart helper max-grace-period 100</pre>

16.2.70. Запрет роли помощника для маршрутизатора (ospf graceful-restart helper never)

Команда	<pre>ospf graceful-restart helper never no ospf graceful-restart helper</pre> Команда задает одну из политик помощника для мягкого перезапуска. Команда запрещает коммутатору работать в качестве помощника мягкого перезапуска для определенного соседнего узла в OSPF. Команда с "no" удаляет все настроенные политики помощника
Параметр	-
По умолчанию	Коммутатор может работать в качестве помощника мягкого перезапуска
Режим	Режим глобальной конфигурации
Руководство по использованию	После настройки политики коммутатор может работать только как устройство мягкого перезапуска GR restarter (коммутатор обрабатывает протокол переключения и перезапуска), а не как GR helper (когда коммутатор помогает устройству перезапуска завершить GR)
Пример	Запретить коммутатору работать в качестве помощника OSPF. <pre>Switch(config)#ospf graceful-restart helper never</pre>

16.2.71. Просмотр состояния мягкого перезапуска OSPF протокола (show ip ospf graceful-restart)

Команда	<pre>show ip ospf [<process-id>] graceful-restart</pre> Показывает состояние OSPF GR, в том числе обрабатывается ли GR в режиме помощника и оставшееся время работы GR
Параметр	<process-id>: идентификатор процесса, в диапазоне от 0 до 65535. Это означает, что при отсутствии параметра отображается GR-статус всех процессов
По умолчанию	-
Режим	Привилегированный режим



Руководство по использованию	-														
Пример	Показать GR-состояние всех процессов на устройстве мягкого перезапуска GR. <pre>Switch#show ip ospf graceful-restart</pre> OSPF process 0 graceful-restart information GR status : GR in progress GR remaining time : 50 <table border="1"> <thead> <tr> <th>Информация, отображаемая на экране</th><th>Описание</th></tr> </thead> <tbody> <tr> <td>OSPF process 0 graceful-restart information</td><td>Состояние OSPF GR для процесса 0</td></tr> <tr> <td>GR status</td><td>Состояние мягкого перезапуска GR, "GR in progress" означает, что коммутатор находится в процессе обработки мягкого перезапуска</td></tr> <tr> <td>GR remaining time</td><td>время, оставшееся до завершения процесса мягкого перезапуска</td></tr> </tbody> </table> Show GR state of all processes on GR helper: <pre>Switch#show ip ospf graceful-restart</pre> OSPF process 0 graceful-restart information: GR status : Helper Neighbor ID Interface Remaining time 1.1.1.1 Vlan1 100 2.2.2.2 Vlan1 200 <table border="1"> <thead> <tr> <th>Информация, отображаемая на экране</th><th>Описание</th></tr> </thead> <tbody> <tr> <td>OSPF process 0 graceful-restart information</td><td>Состояние OSPF GR для процесса 0</td></tr> <tr> <td>GR status</td><td>Состояние мягкого перезапуска GR, "Helper" означает, что коммутатор работает в качестве помощника</td></tr> </tbody> </table>	Информация, отображаемая на экране	Описание	OSPF process 0 graceful-restart information	Состояние OSPF GR для процесса 0	GR status	Состояние мягкого перезапуска GR, "GR in progress" означает, что коммутатор находится в процессе обработки мягкого перезапуска	GR remaining time	время, оставшееся до завершения процесса мягкого перезапуска	Информация, отображаемая на экране	Описание	OSPF process 0 graceful-restart information	Состояние OSPF GR для процесса 0	GR status	Состояние мягкого перезапуска GR, "Helper" означает, что коммутатор работает в качестве помощника
Информация, отображаемая на экране	Описание														
OSPF process 0 graceful-restart information	Состояние OSPF GR для процесса 0														
GR status	Состояние мягкого перезапуска GR, "GR in progress" означает, что коммутатор находится в процессе обработки мягкого перезапуска														
GR remaining time	время, оставшееся до завершения процесса мягкого перезапуска														
Информация, отображаемая на экране	Описание														
OSPF process 0 graceful-restart information	Состояние OSPF GR для процесса 0														
GR status	Состояние мягкого перезапуска GR, "Helper" означает, что коммутатор работает в качестве помощника														



	Neighbor ID	идентификатор маршрутизатора-помощника при перезапуске
	Interface	Интерфейс уровня 3, подключенный к перезапущенному
	Remaining time	время, оставшееся до завершения процесса мягкого перезапуска

16.3. Команды для протокола BGP

16.3.1. Настройка агрегированных элементов BGP таблиц (aggregate-address)

Команда	aggregate-address <ip-address/M> [summary-only] [as-set] no aggregate-address <ip-address/M> [summary-only] [as-set] Команда используется для настройки агрегированных записей (aggregate-address). Команда "no aggregate-address <ip-address/M> [summary-only] [as-set]" удаляет записи
Параметр	<ip-address/M>: IP-адрес, длина маски. [summary-only] : анонс только префикса, подавляя более конкретные маршруты. [as-set] : выводит автономную систему (АС) на маршруте в списке, каждая АС отображается один раз
По умолчанию	Отсутствует конфигурация
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Агрегация адресов сокращает передаваемую информацию о маршрутизации. Параметр "summary-only" передает агрегированный маршрут, подавляя более конкретные маршруты к соседним узлам. Параметр "as-set" перечислит АС из каждого агрегируемого маршрута только один раз без повторения
Пример	<pre>Switch(config-router)# aggregate-address 100.1.0.0/16 summary-only Switch(config-router)# aggregate-address 100.2.0.0/16 summary-only as-set Switch(config-router)# aggregate-address 100.3.0.0/16 as-set</pre>



16.3.2. Выполнение агрегации на следующем узле (bgp aggregate-nexthop-check)

Команда	bgp aggregate-nexthop-check no bgp aggregate-nexthop-check Указывает необходимость проверки BGP всех следующих узлов (next-hop) маршрутов при агрегации. Команда "no bgp aggregate-nexthop-check" отменяет эту настройку, т.е. следующего узла агрегированному маршруту не проверяется
Параметр	-
По умолчанию	Проверка узла при суммировании маршрутов не выполняется
Режим ввода команды	Режим глобальной конфигурации
Руководство по использованию	Команда позволяет задать выполнение суммирования только в том случае, если следующий узел (next-hop) соответствует указанному. Если проверка отключена, все охватываемые маршруты будут объединены в агрегированный
Пример	Switch(config)#bgp aggregate-nexthop-check

16.3.3. Сравнение MED для маршрутов от соседних узлов из различных автономных систем (bgp always-compare-med)

Команда	bgp always-compare-med no bgp always-compare-med Команда позволяет установить постоянное выполнение сравнения MED (дискриминатор множественного выхода). Команда "no bgp always-compare-med" отменяет конфигурацию
Параметр	-
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Как правило BGP сравнивает MED только между путями из одной и той же автономной системы (АС). С помощью этой команды MED маршрутов, поступающих из разных АС, также будет сравниваться



Пример	АС (200) получает один и тот же префикс маршрута из двух АС (100 и 300), содержащих разные MED, поэтому сравнение MED будет выполняться всегда. Switch(config-router)#bgp always-compare-med

16.3.4. Метод ASDOT для записи АС (bgp asnotation asdot)

Команда	bgp asnotation asdot no bgp asnotation asdot Отображает номер АС и использует метод ASDOT для соответствия регулярному выражению. Команда с "no" в начале отменяет данный способ
Параметр	-
По умолчанию	Применяется метод ASPLAIN
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	После установки этой команды, чтобы изменить метод отображения номера АС и соответствия регулярному выражению, необходимо настроить команду «clear ip bgp *» для восстановления всех отношений BGP-соседей
Пример	Показать номер АС и сопоставить регулярное выражение по методу ASDOT. Switch(config)#router bgp 200 Switch(config-router)#bgp asnotation asdot

16.3.5. Предотвращение учета as-path в алгоритме выбора маршрута (bgp bestpath as-path ignore)

Команда	bgp bestpath as-path ignore no bgp bestpath as-path ignore Задаёт игнорирование длины AS-PATH. Команда "no bgp bestpath as-path ignore" отменяет конфигурацию
Параметр	-
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP



Руководство по использованию	Длина AS-PATH будет сравниваться в алгоритме выбора маршрута BGP, и ее можно игнорировать, используя эту настройку
Пример	Задать игнорирование длины AS-PATH: Switch(config)#router bgp 200 Switch(config-router)#bgp bestpath as-path ignore

16.3.6. Сравнение длины пути конфедерации AC (bgp bestpath compare-confed-aspah)

Команда	bgp bestpath compare-confed-aspah no bgp bestpath compare-confed-aspah Команда позволяет сравнивать длину пути AC конфедерации. Команда "no bgp bestpath compare-confed-aspah" отменяет данную настройку
Параметр	-
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Обычно в процессе принятия решения о маршруте в BGP сравнивается только длина внешнего AS-PATH. Эта команда указывает, что длина пути AC внутренней конфедерации AS-PATH должна также использоваться в процессе принятия решения
Пример	Настроить конфедерацию длины AS-PATH. Switch(config-router)#bgp bestpath compare-confed-aspah

16.3.7. Сравнение идентификаторов маршрутизаторов для одинаковых путей BGP (bgp bestpath compare-routerid)

Команда	bgp bestpath compare-routerid no bgp bestpath compare-routerid Устанавливает сравнение идентификаторов маршрутизаторов. Команда "no bgp bestpath compare-routerid" отменяет конфигурацию
Параметр	-
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP



Руководство по использованию	Обычно, при прочих равных условиях, в качестве лучшего маршрута выбирается первый маршрут от одной АС. Данная команда используется для включения сравнения идентификатора маршрутизаторов в процесс выбора
Пример	Устройство (10.1.1.66, AS200) получает одинаковый префикс маршрута от двух устройств (10.1.1.64 и 10.1.1.68) одной автономной системы (АС) (100), задать на устройстве сравнение идентификаторов маршрутов. Switch(config-router)#bgp bestpath compare-routerid

16.3.8. Сравнение атрибута MED при выборе путей (bgp bestpath med)

Команда	bgp bestpath med {[confed] [missing-as-worst]} no bgp bestpath med {[confed] [missing-as-worst]} Команда задает выполнение сравнения атрибутов MED в конфедерации, а при отсутствии MED считать путь наилучшим. Команда “no bgp bestpath med {[confed] [missing-as-worst]}” отменяет данную конфигурацию
Параметр	[confed] : сравнение MED среди путей конфедерации [missing-is-worst] : обрабатывать отсутствующий MED как наилучшее значение
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Команда выполнение учета атрибута MED при сравнении маршрутов в конфедерации. При отсутствии MED параметру “missing-is-worst” присваивается значение 0, делая путь с отсутствующим атрибутом MED наилучшим путем
Пример	Установить сравнение атрибутов MED в пути конфедерации и принимать значение как наибольшее, если MED недоступен. Switch(config-router)#bgp bestpath med confed missing-as-worst

16.3.9. Пересылка маршрутов от клиента к клиенту (bgp client-to-client reflection)

Команда	bgp client-to-client reflection no bgp client-to-client reflection
	Команда позволяет настроить пересылку маршрутов. Команда “no bgp client-to-client reflection” отменяет данную конфигурацию



Параметр	-
По умолчанию	При настройке клиента пересылка маршрутов включена по умолчанию
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	После настройки клиентов отражения при помощи "neighbor {<ip-address> <TAG>} route-reflector-client", маршрутизатор выполняет отражение маршрутов между клиентами по умолчанию. Форма NO этой команды отменяет отражение маршрутов между клиентами (отражение маршрутов между клиентами и не клиентами не нарушается)
Пример	Отменить отражение маршрутов. Switch(config-router)#no bgp client-to-client reflection

16.3.10. Настройка идентификатора кластера (bgp cluster-id)

Команда	bgp cluster-id {<ip-address> <01-4294967295>} no bgp cluster-id {[<ip-address>] <0-4294967295>} Команда устанавливает идентификатор кластера отражателя маршрутов. Команда "no bgp cluster-id {[<ip-address>] <0-4294967295>}" отменяет конфигурацию
Параметр	<ip-address> <1-4294967295> : идентификатор кластера отражателя маршрутов в десятично-точечной записи или 32-значное число
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Кластер включает в себя отражатель маршрутов и его клиентов в области. Но в целях повышения резервирования кластер иногда может иметь более одного отражателя маршрутов. В таком случае параметр "Router-id" служит для идентификации исключительно маршрутизатора в области, а "cluster-id" необходим для идентификации двух или более отражателей маршрутов
Пример	Установить "cluster-id" отражателей маршрутов как 1.1.1.1. Switch(config-router)#bgp cluster-id 1.1.1.1



16.3.11. Идентификатор BGP конфедерации (bgp confederation identifier)

Команда	bgp confederation identifier <as-id> no bgp confederation identifier [<as-id>] Создает конфигурацию конфедерации. Команда “no bgp confederation identifier [<as-id>]” удаляет конфедерацию
Параметр	<as-id> : идентификационный номер АС конфедерации маршрутов в диапазоне от 1 до 4294967295, может быть представлен в десятичной записи (например, 6553700) или в записи с разделителем (например, 100.100)
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Конфедерация позволяет подразделить большую АС на несколько АС, которые будут рассматриваться как одна крупная АС. Команда создает большое количество АС
Пример	Switch(config-router)# bgp confederation identifier 600

16.3.12. Определение участников конфедерации (bgp confederation peers)

Команда	bgp confederation peers <as-id> [<as-id>..] no bgp confederation peers <as-id> [<as-id>..] Команда позволяет добавлять автономные системы в конфедерацию и удалять их из нее
Параметр	<as-id>: идентификаторы АС, включенные в конфедерацию в диапазоне от 1 до 4294967295. Могут быть представлены в десятичной записи (например, 6553700) или в записи с разделителем (например, 100.100), которых может быть несколько
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Конфедерация позволяет подразделить большую АС на несколько АС, которые будут рассматриваться как одна крупная АС. Команда позволяет добавлять участников конфедерации и удалять их из нее



Пример	Создать конфедерацию с ID-номером 600, добавить участников 100, 200, 100.300. <pre>Switch(config-router)# bgp confederation identifier 600 Switch(config-router)#bgp confederation peers 100 200 100.300</pre>

16.3.13. Подавление маршрутов в BGP (bgp dampening)

Команда	<pre>bgp dampening [<1-45>] [<1-20000> <1-20000> <1-255>] [<1-45>] no bgp dampening</pre> Разрешает подавление маршрутов. Команда “no bgp dampening” отменяет функцию подавления маршрутов
Параметр	<1-45>: половина времени достижимости или недостижимости маршрута; время, в течение которого штраф уменьшится до половины своего текущего значения, в минутах <1-20000>: предельное значение повторного использования. <1-255>: максимальная продолжительность подавления маршрута в минутах
По умолчанию	Половина времени достижимости по умолчанию 15 минут, для недостижимости 15 минут. Предел подавления по умолчанию равен 2000, предел повторного использования равен 750, максимальное время подавления 60 минут
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Подавление маршрутов минимизирует нестабильность, вызванную частыми изменениями в маршрутах. Каждому нестабильному маршрута назначается штраф и как только штраф превышает пороговое значение подавления, анонсирование маршрута прекращается. Штраф уменьшается в соответствии с настроенным значением времени полураспада, при сохранении стабильности маршрута. Как только штраф становится меньше порога или время подавления превышает заданный предел, анонсирование маршрута снова разрешается. Эта команда предназначена для включения/выключения подавления маршрута и настройки его параметров
Пример	Включить подавление маршрута и применить настройки по умолчанию. <pre>Switch(config-router)# bgp dampening</pre>



16.3.14. Параметры BGP по умолчанию (bgp default)

Команда	<pre>bgp default {ipv4-unicast local-preference <0-4294967295>}</pre> <pre>no bgp default {ipv4-unicast local-preference [<0-4294967295>]}</pre> Команда задает настройки BGP по умолчанию. Команда “no bgp default {ipv4-unicast local-preference [<0-4294967295>]}” отменяет данную конфигурацию
Параметр	ipv4-unicast : активировать одноадресный режим IPv4 для обмена с соседними маршрутизаторами по умолчанию. local-preference<0-4294967295> : значения локального приоритета по умолчанию
По умолчанию	Одноадресный режим IPv4 подключен по умолчанию при включении протокола BGP. Приоритет по умолчанию равен 100
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Семейство адресов IPv4 unicast по умолчанию включено в BGP. Команда “no bgp default ipv4-unicast” используется для отключения семейства адресов. Локальный приоритет по умолчанию можно настроить с помощью команды “bgp default local-preference”
Пример	Установить локальный приоритет по умолчанию равным 500. Configure in 10.1.1.66: <pre>Switch(config)#router bgp 200</pre> <pre>Switch(config-router)# bgp default local-preference 500</pre>

16.3.15. Сравнение MED, анонсируемой разными узлами в общей автономной системе (bgp deterministic-med)

Команда	<pre>bgp deterministic-med no bgp deterministic-med</pre> Команда применяет наилучшую переменную MED для одного префикса в автономной системе (АС) для сравнения с другими автономными системами. Команда “no bgp deterministic-med” отменяет данную конфигурацию
Параметр	-
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP



Руководство по использованию	Обычно, сравнение выполняется для всех путей с одним и тем же префиксом. При вводе данной команды система применит маршрут с наименьшим MED в AC (когда другие основные атрибуты одинаковы) для сравнения с остальными автономными системами. После выбора лучшего пути он выбирается в AC независимо от значения MED
Пример	Задать на BGP использование лучшего MED для одного и того же префикса в AC для сравнения с другими AC. Switch(config-router)#bgp deterministic-med

16.3.16. Принудительная подстановка номеров AC (bgp enforce-first-as)

Команда	bgp enforce-first-as no bgp enforce-first-as Обеспечивает принудительную подстановку номеров AC в начало атрибута AS_PATH во всех входящих обновлениях для узлов BGP, в противном случае пир отключается. Команда “no bgp enforce-first-as” отменяет данную конфигурацию
Параметр	-
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Команда запрещает трафик из небезопасных или неавторизованных систем
Пример	Switch(config-router)#bgp enforce-first-as

16.3.17. Немедленный сброс сеанса BGP (bgp fast-external-failover)

Команда	bgp fast-external-failover no bgp fast-external-failover Быстрый сброс при изменении подключения соседей BGP на интерфейсе, в дополнение к ожиданию таймаута TCP. Команда “no bgp fast-external-failover” отменяет данную конфигурацию
Параметр	-
По умолчанию	Задано
Режим ввода команды	Режим маршрутизации BGP



Руководство по использованию	Команда используется для немедленного сброса подключения соседнего узла, если интерфейс, используемый для соединения BGP, выходит из строя
Пример	Switch(config-router)# bgp fast-external-failover

16.3.18. Включить входной фильтр маршрутов (bgp inbound-route-filter)

Команда	bgp inbound-route-filter no bgp inbound-route-filter Протокол bgp не устанавливает маршрутную информацию, которая не совпадает с локально настроенным значением идентификатора маршрута RD. Форма команды с "no" в начале задает запись RD не зависимо от наличия локального идентификатора маршрута
Параметр	-
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Обычно, когда коммутатор выступает в роли PE (граничного маршрутизатора провайдера), сохранение маршрута bgp, полученного из VPN, в BGP зависит от того, получил ли VRF (комплекс маршрутизации и пересылки), настроенный в этом PE, соответствующую информацию. При вводе команды с "no" BGP сохранит сообщение о маршрутизации без учета совпадающей информации
Пример	Switch(config)#router bgp 100 Switch(config-router)#no bgp inbound-route-filter

16.3.19. Максимальное количество маршрутизаторов в процессе BGP (bgp inbound-max-route-num)

Команда	bgp inbound-max-route-num <0-500000> no bgp inbound-max-route-num Задаёт ограничение на количество маршрутизаторов, получаемых процессом bgp от своих соседей
Параметр	Ограничение на количество маршрутизаторов, в диапазоне от 0 до 500000
По умолчанию	50000



Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Команда устанавливает максимальное количество маршрутизаторов, получаемых процессом bgp от соседних узлов
Пример	Следующая конфигурация ограничит максимальное количество маршрутизаторов, которые процесс bgp получает от своих соседей, до 20000. Switch(config-router)#bgp inbound-max-route-num 20000

16.3.20. Запись сообщений об изменении состояния соседних устройств без включения отладки BGP (bgp log-neighbor-changes)

Команда	bgp log-neighbor-changes no bgp log-neighbor-changes Команда регистрирует в журнале изменения состояния соседнего узла BGP. Команда "no bgp log-neighbor-changes" отменяет данную конфигурацию
Параметр	-
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Позволяет вывести на экран сообщения об изменении состояния соседнего узла
Пример	Switch(config-router)# bgp log-neighbor-changes

16.3.21. Проверка маршрутов на наличие префикса в таблице маршрутизации (bgp network import-check)

Команда	bgp network import-check no bgp network import-check Эта команда используется для проверки доступности маршрутов IGP в таблице маршрутизации BGP. Команда "no bgp network import-check" указывает не проверять доступность IGP
Параметр	-
По умолчанию	-



Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Проверка доступности IGP в маршруте, объявляемом BGP, заключается в проверке существования следующего хопа и доступности его IGP
Пример	Установить проверку доступности IGP в маршрутизации BGP. Switch(config-router)# bgp network import-check

16.3.22. Установить выбор пути, совместимого с RFC 1771 (bgp rfc1771-path-select)

Команда	bgp rfc1771-path-select no bgp rfc1771-path-select После установки этого атрибута выбор маршрута будет происходить в соответствии со стандартом rfc 1771, т.е. не будут проверяться внутренние метрики AC и не будут сравниваться внутренние METRIC
Параметр	-
По умолчанию	-
Режим ввода команды	Режим глобальной конфигурации
Руководство по использованию	После установки этого атрибута выбор пути будет осуществляться в соответствии с правилами, определенными в rfc 1771, т.е. внутренняя метрика AC не проверяется при наличии различных AS, что должно происходить при отсутствии этого атрибута
Пример	Задать выбор маршрута в соответствии с rfc1771. Switch(config)# bgp rfc1771-path-select

16.3.23. Строгое выполнение протокола RFC 1771 (bgp rfc1771-strict)

Команда	bgp rfc1771-strict no bgp rfc1771-strict Устанавливает соблюдение ограничений rfc1771. Команда "no bgp rfc1771-strict" снимает строгое следование ограничениям
Параметр	-
По умолчанию	Ограничения rfc 1771 отсутствуют



Режим ввода команды	Режим глобальной конфигурации
Руководство по использованию	С этим атрибутом типы генерации маршрутов из протоколов RIP, OSPF, ISIS и т.д., будут считаться IGP (внутренне сгенерированными), в противном случае источник будет всегда установлен как "неполный" (incomplete). Например: задать строгое соблюдение ограничений rfc1771
Пример	Задать строгое соблюдение ограничений rfc1771. Switch(config)#bgp rfc1771-strict

16.3.24. Настройка ID-маршрутизатора вручную (bgp router-id)

Команда	bgp router-id <A.B.C.D>
	no bgp router-id [<A.B.C.D>] Ручная настройка ID маршрутизатора. "no" в начале команды отменяет данную конфигурацию
Параметр	<A.B.C.D> : идентификатор маршрутизатора
По умолчанию	Идентификатор маршрутизатора получается автоматически
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Команда позволяет вручную задать ID маршрутизатора
Пример	Задать ID маршрутизатора как 1.1.1.1. Switch(config-router)#bgp router-id 1.1.1.1

16.3.25. Интервалы сканирования маршрутизаторов BGP (bgp scan-time)

Команда	bgp scan-time <0-60> no bgp scan-time [<0-60>] Команда задает интервал сканирования следующего хопа маршрута BGP. Команда "no bgp scan-time [<0-60>]" восстанавливает значение по умолчанию
Параметр	<0-60> : интервал проверки действительности
По умолчанию	60 секунд



Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Этот интервал является периодом, после которого маршрутизатор проверяет действительность следующего хопа в маршруте BGP. Если выполнять проверку нет необходимости, установите параметр 0
Пример	Установить интервал периодической проверки следующего хопа равным 30 секундам. Switch(config-router)# bgp scan-time 30

16.3.26. Сброс соединения BGP (clear ip bgp)

Команда	clear ip bgp * [vrf <vrf-name>] [in out soft [in out]] Сброс соединения между BGP vrf-name и всеми пирами
Параметр	<vrf-name> : имя экземпляра VPN-маршрутизации, в диапазоне от 1 до 64; in : входящее обновление без сброса соединения out : исходящее обновление без сброса соединения soft : перезапуск без сброса соединения
По умолчанию	-
Режим ввода команды	Привилегированный режим
Руководство по использованию	По команде clear ip bgp * BGP перезапускается; при настройке параметра in запросы отправляются соседям; маршруты отправляются соседям при настройке параметра out; Если установлено значение soft, сброс соединения для BGP не выполняется
Пример	Switch#clear ip bgp * vrf VRF-A Switch#

16.3.27. Удаление информации о подавленных маршрутах (clear ip bgp dampening)

Команда	clear ip bgp [<address-family>] dampening [<ip-address> <ip-address/M>] Используется для сброса всех подавленных маршрутов BGP
Параметр	<address-family> : семейство адресов, например, "ipv4 unicast". <ip-address> : IP-адрес.



	<ip-address/M> : IP-адрес и маска
По умолчанию	-
Режим ввода команды	Привилегированный режим
Руководство по использованию	Команда позволяет очистить сообщения о подавлении маршрутизации BGP и состоянии по различным параметрам (например, семейство адресов или IPv4-адрес)
Пример	Удалить подавление маршрутизации BGP и состояние кластера одноадресной рассылки IPv4. Switch# clear ip bgp ipv4 unicast dampening

16.3.28. Удалить статистику нестабильностей BGP (clear ip bgp flap-statistics)

Команда	clear ip bgp [<address-family>] flap-statistics [<ip-address> <ip-address/M>] Используется для сброса статистики колебания маршрутов BGP
Параметр	<address-family> : семейство адресов, например, "ipv4 unicast". <ip-address> : IP-адрес. <ip-address/M> : IP-адрес и маска
По умолчанию	-
Режим ввода команды	Привилегированный режим
Руководство по использованию	Команда позволяет очистить статистику колебаний маршрутов BGP и состояний по различным параметрам (например, семейство адресов или IPv4-адрес)
Пример	Удалить статистику подавления маршрутизации BGP и состояния кластера одноадресной рассылки IPv4. Switch#clear ip bgp ipv4 unicast flap-statistics



16.3.29. Установка административной дистанции маршрутов для указанного префикса (distance)

Команда	distance <1-255> <ip-address/M> [<WORD>] no distance <1-255> <ip-address/M> [<WORD>] Определяет административную дистанцию для указанного префикса маршрута. Команда “no distance <1-255> <ip-address/M> [<WORD>]” восстанавливает значение по умолчанию
Параметр	<1-255> : административная дистанция. <ip-address/M> : префикс маршрутизации <WORD> : имя списка доступа
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Задаёт административную дистанцию для указанного маршрута BGP в качестве основы для выбора маршрута
Пример	Задать административную дистанцию для маршрута 90 10.1.1.64/32 равной 90. Switch(config-router)# distance 90 10.1.1.64/32

16.3.30. Установка административной дистанции для маршрутов BGP (distance bgp)

Команда	distance bgp <1-255> <1-255> <1-255> no distance bgp [<1-255> <1-255> <1-255>] Устанавливает административную дистанцию для протокола BGP. Команда “no distance bgp [<1-255> <1-255> <1-255>]” восстанавливает административную дистанцию до значения по умолчанию
Параметр	<1-255> : Соответственно административная дистанция EBGP, IBGP и LOCAL для BGP
По умолчанию	EBGP равно 20, остальные 200
Режим ввода команды	Режим маршрутизации BGP



Руководство по использованию	: Задаёт административную дистанцию для маршрутизации BGP в качестве основы для выбора маршрута NSM
Пример	Установить административную дистанцию для маршрутизации BGP равной 15, административную дистанцию для IBGP и локальной маршрутизации равной 150. <pre>Switch(config-router)# distance bgp 15 150 150</pre>

16.3.31. Создать список доступа к пути автономной системы (AC) BGP (ip as-path access-list)

Команда	<pre>ip as-path access-list <.LINE> {<permit> <deny>} <LINE> no ip as-path access-list <.LINE> {<permit> <deny>} <LINE></pre> Создает список доступа к автономной системе AS-PATH. Команда “no ip as-path access-list <.LINE>{<permit> <deny>} <LINE>” удаляет список доступа
Параметр	<.LINE> : имя списка доступа. <LINE> : выражение для сопоставления путей в AS-PATH
По умолчанию	-
Режим ввода команды	Режим глобальной конфигурации
Руководство по использованию	Команда задает список доступа, связанный с AS-PATH, определяющий условия прохождения/фильтра
Пример	Настроить список доступа с именем ASPF, фильтрующий AS-PATH, содержащий маршрут 100. <pre>Switch(config)#ip as-path access-list ASPF deny ^100\$</pre>

16.3.32. Список сообществ (ip community-list)

Команда	<pre>ip community-list {<LISTNAME> <1-199> [expanded <WORD>]][standard <WORD>]} {deny permit} <.COMMUNITY></pre> <pre>no ip community-list {<LISTNAME> <1-199> [expanded <WORD>]][standard <WORD>]} [{deny permit} <.COMMUNITY>]</pre> Создает список сообществ "community-list". Команда “no ip community-list {<LISTNAME> <1-199> [expanded <WORD>]][standard <WORD>]} [{deny permit} <.COMMUNITY>]” удаляет список



Параметр	<LISTNAME> : имя списка сообществ. <1-199>: Номер стандартного или увеличенного списка <WORD>: Номер стандартного или увеличенного списка <.COMMUNITY > : Члены списка сообществ в формате aa: nn, internet, local-AS, no-advertise, and no-export. Для расширенного списка применяются регулярные выражения
По умолчанию	-
Режим ввода команды	Режим глобальной конфигурации
Руководство по использованию	Данная команда позволяет сконфигурировать "community-list" для реализации политики пропуска/фильтрации/поиска
Пример	Настроить "ip community-list" с именем LN, установить для атрибута "permit" community значение 100: 10. Switch(config)# ip community-list LN permit 100: 10

16.3.33. Расширенный список сообществ (ip extcommunity-list)

Команда	<pre>ip extcommunity-list {<LISTNAME> <1-199> [expanded <WORD>]][standard <WORD>]} {deny permit} <.COMMUNITY> no ip extcommunity-list {<LISTNAME> <1-199> [expanded <WORD>]][standard <WORD>]} {deny permit} <.COMMUNITY></pre> Создает расширенный список сообществ. Команда "no ip extcommunity-list {<LISTNAME> <1-199> [expanded <WORD>]][standard <WORD>]} {deny permit} <.COMMUNITY>" удаляет расширенный список сообществ
Параметр	<LISTNAME> : имя списка сообществ. <1-199> : Номер стандартного или увеличенного списка <WORD> : Номер стандартного или увеличенного списка <.COMMUNITY > : Члены списка сообществ в формате aa: nn, internet, local-AS, no-advertise, and no-export. Для расширенного списка применяются регулярные выражения
По умолчанию	-
Режим ввода команды	Режим глобальной конфигурации



Руководство по использованию	Данная команда позволяет сконфигурировать "community-list" для реализации политики пропуска/фильтрации/поиска
Пример	Настроить "excommunity-list" с именем LN, установить для атрибута "permit" community значение 100: 10. Switch(config)#ip extcommunity-list LN permit 100: 10

16.3.34. Разрешение на обмен маршрутами с соседним узлом (neighbor activate)

Команда	neighbor {<ip-address> <TAG>} activate no neighbor {<ip-address> <TAG>} activate Команда используется для настройки параметров передачи информации, т.е. разрешения или запрещения обмена указанной информацией "address-family" с соседним маршрутизатором BGP. Команда "no neighbor {<ip-address> <TAG>} activate" отключает обмен информацией с соседним узлом
Параметр	<ip-address> : IP-адрес соседнего узла <TAG> : имя группы пиров
По умолчанию	Включает обмен маршрутами IP unicast address-family, и отключает остальные семейства адресов
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	IP unicast задается в режиме маршрутизации BGP. Переопределяет настройки для указанного семейства адресов в режиме "address-family". Если эта опция не включена ни на одной из сторон между локальным узлом и соседним, соседний узел не будет получать семейства адресов, и даже если соответствующий маршрут был ранее получен, он будет отменен при отключении этой опции
Пример	Настроить обмен одноадресным маршрутом с соседом 2002: : 2. Switch(config-router)#neighbor 2002: : 2 activate



16.3.35. Минимальный интервал между отправкой обновлений маршрутизации BGP (neighbor advertisement-interval)

Команда	<code>neighbor {<ip-address> <TAG>} advertisement-interval <0-600></code> <code>no neighbor {<ip-address> <TAG>} advertisement-interval [<0-600>]</code> Устанавливает интервал обновления определенной маршрутной информации. Команда “no neighbor {<ip-address> <TAG>} advertisement-interval [<0-600>]” восстанавливает настройки по умолчанию
Параметр	<code><ip-address></code> : IP-адрес соседнего узла <code><TAG></code> : имя группы пиров. <code><0-600></code> : интервал объявления в секундах
По умолчанию	Для IBGP интервал 5 секунд, для EBGP интервал 30 секунд
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Уменьшение этого значения повышает скорость обновления маршрута, но при этом потребляет больше полосы пропускания
Пример	Установить интервал обновления маршрута 20 секунд для соседнего узла 10.1.1.64. <code>Switch(config-router)#neighbor 10.1.1.64 advertisement-interval 20</code>

16.3.36. Анонсирование префиксов, содержащих дублирующиеся номера автономных систем (neighbor allowas-in)

Команда	<code>neighbor {<ip-address> <TAG>} allowas-in [<1-10>]</code> <code>no neighbor {<ip-address> <TAG>} allowas-in</code> Управляет числом раз, когда один и тот же номер АС может появляться в таблице маршрутизации АС соседних узлов. Команда “no neighbor {<ip-address> <TAG>} allowas-in” restores to not allow any repeat
Параметр	<code><ip-address></code> : IP-адрес соседнего узла <code><TAG></code> : имя группы пиров. <code><1-10></code> : допустимое количество вхождений номера АС
По умолчанию	По умолчанию не допускается повторения АС в одном и том же маршруте, если задано дублирование, по умолчанию устанавливается значение 3, если параметры <1-10> не заданы



Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Обычно BGP не позволяет одному и тому же номеру AC появляться в маршруте более одного раза. Если номер AC появляется в AS-PATH, система отклоняет маршрут. Однако для поддержки некоторых особых потребностей, особенно поддержки VPN, расширенный BGP позволяет повторно отображать AC, определяя, с помощью данной команды, число повторных появлений AC
Пример	Разрешить одной и той же AC появляться в маршруте три раза для соседнего устройства 10.1.1.66. Switch(config-router)#neighbor 10.1.1.66 allowas-in

16.3.37. Передача соседнему устройству неизменных атрибутов (neighbor attribute-unchanged)

Команда	neighbor {<ip-address> <TAG>} attribute-unchanged [as-path][med][next-hop] no neighbor {<ip-address> <TAG>} attribute-unchanged [as-path] [med] [next-hop] Указывает определенные атрибуты, которые остаются неизменными при передаче, т.е. прозрачная передача атрибута. Команда "no neighbor {<ip-address> <TAG>} attribute-unchanged [as-path] [med] [next-hop]" означает, что прозрачная передача атрибута не выполняется
Параметр	<ip-address> : IP-адрес соседнего узла <TAG> : имя группы пиров
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	При применении данной настройки атрибуты определенного маршрута передаются указанному соседу неизменными. Режим маршрутизации BGP это режим конфигурации одноадресной рассылки "IPv4 unicast address". Если параметры не указаны, это значит, что три вышеуказанных параметра заданы вместе
Пример	Установить атрибут маршрута as-path, med, next-hop неизменным для соседнего узла 10.1.1.64. Switch(config-router)#neighbor 10.1.1.64 attribute-unchanged



16.3.38. Анонсирование возможностей обновления (neighbor capability)

Команда	neighbor {<ip-address> <TAG>} capability {dynamic route-refresh} no neighbor {<ip-address> <TAG>} capability {dynamic route-refresh} Настраивает динамическое обновление между соседними устройствами и согласование возможности обновления маршрута. Команда "no neighbor {<ip-address> <TAG>} capability {dynamic route-refresh}" отключает согласование возможностей
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров
По умолчанию	Возможность динамического обновления не настроена, но настроена возможность обновления маршрута
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Это расширенная возможность BGP. При такой конфигурации поддерживаемые обеими сторонами возможности будут согласовываться в сообщениях OPEN, соседнее устройство отвечает при наличии возможности или отправляет NOTIFICATION, если таковой нет. После этого отправляющая сторона пошлет сообщение OPEN, исключающее возможность восстановления соединения. Динамическая возможность относится к тому, что при изменении согласования семейства адресов соединение не нужно перезапускать. "Route refresh" означает отправку запроса на обновление при настройке некоторых реконфигурируемых без сброса соединения атрибутов, и соседнее устройство повторно передает существующий маршрут на сторону отправителя. При использовании атрибута "route refresh" соединение не нужно перезапускать, его можно обновить с помощью команды "clear ip bgp * soft in"
Пример	Switch(config-router)#neighbor 10.1.1.64 capability dynamic Switch(config-router)# no neighbor 10.1.1.64 capability route-refresh



16.3.39. Анонсирование возможностей обновления ORF (neighbor capability orf prefix-list)

Команда	neighbor {<ip-address> <TAG>} capability orf prefix-list {<both> <send> <receive>} no neighbor {<ip-address> <TAG>} capability orf prefix-list {<both> <send> <receive>} Задаёт возможность фильтрации отправляемых маршрутов между соседями. Команда “no neighbor {<ip-address> <TAG>} capability orf prefix-list {<both> <send> <receive>}” отключает возможность согласования
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Это расширенная возможность BGP. При такой конфигурации поддерживаемые обеими сторонами возможности будут согласовываться в сообщениях OPEN, соседнее устройство отвечает при наличии возможности или отправляет NOTIFICATION, если таковой нет. После этого отправляющая сторона пошлет сообщение OPEN, исключающее возможность восстановления соединения. Используя эту функцию, сторона с настроенным правилом фильтрации списка префиксов отправляет свое собственное правило фильтрации пиру, а группа пиров применит это правило в качестве собственного правила вывода, чтобы избежать отправки маршрутов, которые будут отклонены другим устройством
Пример	Задать выполнение согласования возможностей фильтрации исходящих маршрутов с соседним узлом 10.1.1.66. Switch(config-router)#neighbor 10.1.1.66 capability orf prefix-list both



16.3.40. Определение наличия и решение для устранения коллизий (neighbor collide-established)

Команда	neighbor {<ip-address> <TAG>} collide-established no neighbor {<ip-address> <TAG>} collide-established Команда подключает проверку наличия коллизий TCP соединения и их решений. Команда “no neighbor {<ip-address> <TAG>} collide-established” отключает выполнение решений для коллизии TCP соединений
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя пира
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Эта команда предназначена для решения проблемы множественных соединений между пирами, вызванных коллизиями TCP-соединений. Соединение, созданное с помощью этой опции, проверяется даже в установленном состоянии. При возникновении коллизии проверяется, превышает ли локальный IP-адрес IP-адрес партнера; если да, то исходное соединение удаляется; если нет, то опция настраивается на проверку только в том случае, если соединение создано с локальной стороны и находится в состояниях open sent и open confirm
Пример	Установить выполнение проверки коллизий TCP-соединений с соседним узлом 10.1.1.64 и решения. Switch(config-router)#neighbor 10.1.1.64 collide-established

16.3.41. Отправка соседнему узлу маршрута по умолчанию от локального маршрутизатора (neighbor default-originate)

Команда	neighbor {<ip-address> <TAG>} default-originate [route-map <WORD>] no neighbor {<ip-address> <TAG>} default-originate [route-map <WORD>] Разрешает передачу маршрута по умолчанию определенному соседу. Команда “no neighbor {<ip-address> <TAG>} default-originate [route-map <WORD>]” отменяет отправку
Параметр	<ip-address> : IP-адрес соседнего узла <TAG> : имя пира. <WORD> : имя карты маршрута
По умолчанию	-



Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	С помощью этой опции маршрут по умолчанию от локальной стороны будет передан соседнему узлу. Здесь указываются варианты того, какой маршрут передать по умолчанию. Если несколько соседних устройств предоставляют маршруты по умолчанию, лучший маршрут выбирается на основе принципа выбора маршрута. Согласно зеркалу маршрутов, можно выбрать, когда отправлять маршрут по умолчанию
Пример	Установить передачу локального маршрута по умолчанию соседнему узлу 10.1.1.64. <pre>Switch(config-router)#neighbor 10.1.1.64 default-originate</pre> Switch(config-router)# После этого в списке маршрутов соседних устройств появится маршрут по умолчанию из BGP

16.3.42. Описание соседнего маршрутизатора (neighbor description)

Команда	neighbor {<ip-address> <TAG>} description <.LINE> no neighbor {<ip-address> <TAG>} description Задаёт строку с описанием пира или группы пиров. Команда "no neighbor {<ip-address> <TAG>} description" удаляет данное описание
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров. <.LINE> : Строка описания, состоящая из отображаемых символов, не более 80
По умолчанию	Строка описания пустая
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Применяется для комментария с описанием пира или группы пиров
Пример	Задать строку описания соседнего узла 10.1.1.64 как "tester". <pre>Switch(config-router)#neighbor 10.1.1.64 description tester</pre> Switch(config-router)#



16.3.43. Фильтрация обновлений от конкретного соседа BGP (neighbor distribute-list)

Команда	<pre>neighbor {<ip-address> <TAG>} distribute-list {<1-199> <1300-2699> <WORD>} {in out}</pre> <pre>no neighbor {<ip-address> <TAG>} distribute-list {<1-199> <1300-2699> <WORD>} {in out}</pre> Настраивает политику, применяемую при передаче обновлений маршрутов от соседних устройств. Команда “no neighbor {<ip-address> <TAG>} distribute-list {<1-199> <1300-2699> <WORD>} {in out}” отменяет конфигурацию политики
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров. <1-199> <1300-2699> <WORD> : номер или имя списка доступа
По умолчанию	Политика не применяется
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	При помощи команды “access-list” выполняется конфигурация политики, а описываемая команда применяется при отправке и получении маршрута. При параметре “in” выполняется фильтрация входящих обновлений; при параметре “out” выполняется фильтрация исходящих от локального узла обновлений на соседний узел
Пример	Отправить соседнему маршрутизатору 10.1.1.66 правило фильтрации маршрута с целью 100.1.0.0. <pre>Switch(config)#access-list 101 deny ip 100.1.0.0 0.0.1.255 any</pre> <pre>Switch(config)#access-list 101 permit ip any any</pre> <pre>Switch(config)#router bgp 100</pre> <pre>Switch(config-router)# neighbor 10.1.1.66 distribute-list 101 in</pre>

16.3.44. Не выполнение согласований (neighbor dont-capability-negotiate)

Команда	<pre>neighbor {<ip-address> <TAG>} dont-capability-negotiate</pre> <pre>no neighbor {<ip-address> <TAG>} dont-capability-negotiate</pre> Указывает не выполнять согласование возможностей при создании соединений. Команда “no neighbor {<ip-address> <TAG>} dont-capability-negotiate” отменяет данную конфигурацию



Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров
По умолчанию	Согласование возможностей выполняется
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Поскольку по умолчанию используется согласование, этот параметр можно использовать для отключения согласования, если известно, что версия BGP соседнего устройства старше и не поддерживает согласование возможностей
Пример	При следующих настройках последнее добавленное согласование возможностей не будет реализовано в соединении. Switch(config-router)#neighbor 10.1.1.64 dont-capability-negotiate

16.3.45. Предоставление участия в динамической маршрутизации узлам, не соединенным напрямую (neighbor ebgp-multihop)

Команда	neighbor {<ip-address> <TAG>} ebgp-multihop [<1-255>] no neighbor {<ip-address> <TAG>} ebgp-multihop [<1-255>] Указывает, какие соседи EBGП могут существовать в разных сегментах, а также количество транзитных участков-хопов (TTL). Команда “no neighbor {<ip-address> <TAG>} ebgp-multihop [<1-255>]” определяет, что соседи EBGП обязаны находиться в одном сегменте
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров. <1-255> : допустимое количество хопов
По умолчанию	Должны находиться в одном сегменте
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Без этой команды пиры EBGП должны находиться в одном сегменте, а после ввода этой команды адреса пиров могут находиться в разных сегментах. Если максимальное количество хопов не задано, количество хопов равно 255



Пример	Три устройства 10.1.1.64(AS100) и 11.1.1.120(AS300) подключены соответственно к двум интерфейсам 10.1.1.66 и 10.1.1.100 другого устройства. Доступность IGP для 10.1.1.64 и 11.1.1.120 на обеих сторонах маршрутов обеспечиваются посредством статической конфигурации. Отношения смежности устанавливаются только после того, как обе стороны настроены следующим образом: на 10.1.1.64 <pre>Switch(config-router)#neighbor 11.1.1.120 ebgp-multihop</pre> на 11.1.1.120 <pre>Switch(config-router)#neighbor 10.1.1.64 ebgp-multihop</pre> После этого коммутаторы в разных сегментах смогут создавать отношения смежности BGP

16.3.46. Принудительно установить многохоповые переходы (neighbor enforce-multihop)

Команда	<pre>neighbor {<ip-address> <TAG>} enforce-multihop</pre> <pre>no neighbor {<ip-address> <TAG>} enforce-multihop</pre> Принудительно устанавливает многоходовое соединение с соседним устройством. Команда "no neighbor {<ip-address> <TAG>} enforce-multihop" отменяет конфигурацию
Параметр	<ip-address> : IP-адрес соседнего устройства <TAG> : имя группы пиров
По умолчанию	Не соблюдается
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	На самом деле, прямые маршруты нельзя заставить работать как многохоповые, но при данной настройке они будут рассматриваться как многохоповые соединения, что означает, что проверки не прямых маршрутов, которые выполнялись бы только на IBGP и EBGP, будут выполняться на всех маршрутах после установки данного атрибута. В случае обязательного многоходового соединения проверка прямого соединения "nexthop" при выходе не выполняется
Пример	Принудительно установить соседнее устройство 10.1.1.66 в качестве многоходового соединения. <pre>Switch(config-router)#neighbor 10.1.1.66 enforce-multihop</pre>



16.3.47. Настройка фильтра BGP (neighbor filter-list)

Команда	<pre>neighbor {<ip-address> <TAG>} filter-list <.LINE> {<in> <out>}</pre> <pre>no neighbor {<ip-address> <TAG>} filter-list <.LINE> {<in> <out>}</pre> Задаёт список управления доступом для AS-PATH. Команда “no neighbor {<ip-address> <TAG>} filter-list <.LINE> {<in> <out>}” отменяет список управления доступом AS-PATH
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров. <.LINE> : имя списка доступа AS-PATH, настроенное через ip as-path access-list <.LINE> <permit deny> <LINE>
По умолчанию	Не сконфигурировано
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	После первоначальной настройки списка доступа IP AS-PATH данная опция, примененная к указанным соседним устройствам, позволит отправлять/получать маршруты с указанными номерами АС из списка АС. Принятие или отклонение зависит от настроек списка доступа, а отправка и получение задаются этой командой
Пример	Установить список управления доступом AS-PATH с именем "ASPF". Маршрут с номером АС100 не может обновиться у соседнего узла из-за фильтрации по таблице контроля. <pre>Switch(config)#ip as-path access-list ASPF deny 100</pre> <pre>Switch(config)#router bgp 100</pre> <pre>Switch(config-router)# redistribute static</pre> <pre>Switch(config-router)#neighbor 10.1.1.66 filter-list aspf out</pre>

16.3.48. Интерфейс соседнего устройства (neighbor interface)

Команда	<pre>neighbor <ip-address> interface <IFNAM></pre> <pre>no neighbor <ip-address> interface <IFNAM></pre> Задаёт интерфейс соседнего устройства. Команда “no neighbor <ip-address>interface <IFNAM>” отменяет данную конфигурацию
Параметр	<ip-address> : IP-адрес соседнего узла. <IFNAME> : имя интерфейса, например, “Vlan 2”



По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Команда указывает интерфейс выхода к соседнему узлу. Необходимо обеспечить доступность интерфейса назначения
Пример	Установить интерфейс для соседа 10.1.1.64 как интерфейс vlan 2 Switch(config-router)# neighbor 10.1.1.64 interface vlan2

16.3.49. Установка максимального числа префиксов, принимаемых узлом (neighbor maximum-prefix)

Команда	<pre>neighbor {<ip-address> <TAG>} maximum-prefix <1-4294967295> [<1-100> <warning-only>]</pre> <pre>no neighbor {<ip-address> <TAG>} maximum-prefix <1-4294967295> [<1-100> <warning-only>]</pre> Позволяет настроить количество префиксов, которые разрешено получать от соседнего маршрутизатора. Команда "no neighbor {<ip-address> <TAG>} maximum-prefix <1-4294967295> [<1-100> <warning-only>]" отменяет данную конфигурацию
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя пира. <1-4294967295> : максимальное количество префиксов, разрешенное к получению. <1-100> : пороговое значение в процентах, при котором появится предупреждение. <warning-only> : предупреждение при превышении лимита
По умолчанию	Не ограничено
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Из-за опасений по поводу слишком большого количества обновлений маршрутов от соседей (например, при атаках), максимальное количество префиксов, получаемых от соседнего устройства, ограничивается и при превышении определенного количества будет выдано предупреждение. Если опция warning-only не используется, при получении лишних префиксов маршрутизатор разрывает связь с соседним устройством. Соединение останется разорванным до тех пор, пока не будет использована команда "clear ip bgp"



Пример	Задать максимальное количество префиксов маршрута от соседнего устройства 10.1.1.64 равным 12, выдачу предупреждений, когда количество префиксов маршрута достигнет 6, и разрыв соединения, когда их количество достигнет 13. Switch(config-router)#neighbor 10.1.1.64 maximum-prefix 12 50

16.3.50. Настроить маршрутизатор как следующий узел для соседнего BGP (neighbor next-hop-self)

Команда	<pre>neighbor {<ip-address> <TAG>} next-hop-self</pre> <pre>no neighbor {<ip-address> <TAG>} next-hop-self</pre> Команда задает режим, в котором соседнее устройство указывает next-hop маршрута, отправляемого между внутренними узлами. Команда “no neighbor {<ip-address> <TAG>} next-hop-self” отменяет данную конфигурацию
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	В среде EBGP nexthop автоматически указывает на соседний узел-источник. Однако в среде IBGP значение "nexthop" для маршрутов в пределах одного сегмента остается неизменным. Если это не широкоэвещательная сеть, будут возникать ошибки. Эта команда предназначена для принудительного указания себя в качестве "nexthop" соседнего узла в среде IBGP
Пример	Switch(config-router)#neighbor 10.1.1.66 next-hop-self

16.3.51. Переопределение результата согласования возможностей (neighbor override-capability)

Команда	<pre>neighbor {<ip-address> <TAG>} override-capability</pre> <pre>no neighbor {<ip-address> <TAG>} override-capability</pre> Указывает включить ли согласование переопределения возможностей. Команда “no neighbor {<ip-address> <TAG>} override-capability” восстанавливает согласование возможностей
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров



По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	При использовании этого атрибута не будут отправляться уведомления об ошибках, вызванных узлами, который не поддерживает согласование возможностей
Пример	Switch(config-router)#neighbor 10.1.1.64 override-capability

16.3.52. Предписание маршрутизатору не инициировать соединение (neighbor passive)

Команда	neighbor {<ip-address> <TAG>} passive no neighbor {<ip-address> <TAG>} passive Указывает отправлять или нет согласие на соединение с указанным узлом. Команда "no neighbor {<ip-address> <TAG>} passive" возвращает отправку положительного ответа на запрос соединения
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров
По умолчанию	Отправка положительного ответа на запрос соединения
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Если этот атрибут установлен, локальная сторона не будет активно отправлять TCP-запрос на соединение после настройки соседнего узла, но будет осуществлять прием входящих сообщений, ожидая запроса на подключение
Пример	Switch(config-router)#neighbor 10.1.1.64 passive После настройки этого атрибута и восстановления соединения, локальная сторона не пытается создать соединение, а остается в состоянии ACTIVE, ожидая TCP запрос на соединение от партнера



16.3.53. Создание группы пиров (neighbor peer-group (Creating))

Команда	neighbor < TAG> peer-group no neighbor < TAG> peer-group Создает/удаляет группы пиров. Команда "no neighbor < TAG> peer-group" удаляет группу пиров
Параметр	<TAG> : имя группы пиров, максимальная длина 26 символов
По умолчанию	Группы пиров не существует
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Соседние маршрутизаторы с одинаковыми атрибутами могут быть объединены в группы пиров, что уменьшает затраты на конфигурирование. Члены группы задаются с помощью команды "neighbor <ip-address> peer-group <TAG>"
Пример	Switch(config-router)#neighbor pg peer-group Switch(config-router)#neighbor 10.1.1.64 peer-group pg Switch(config-router)#neighbor pg remote-as 100

16.3.54. Управление членами группы пиров (neighbor peer-group (Configuring group members))

Команда	"neighbor <ip-address> peer-group <TAG> no neighbor <ip-address> peer-group <TAG>" позволяет добавлять пиры в группу и удалять из нее. Команда "no neighbor <ip-address>peer-group <TAG>" удаляет пиры из группы пиров
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров
По умолчанию	Группа пиров отсутствует
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Соседние маршрутизаторы с одинаковыми атрибутами могут быть объединены в группы пиров, что уменьшает затраты на конфигурирование. Для создания группы пиров применяется команда, приведенная ранее, а данная команда позволяет назначать членов группы
Пример	См. пример выше



16.3.55. Порт для соседнего узла (neighbor port)

Команда	neighbor <ip-address> port <0-65535> no neighbor <ip-address> port [<0-65535>] Указывает номер TCP-порта соседнего узла, через который осуществляется связь. Команда “no neighbor <ip-address> port [<0-65535>]” восстанавливает значение по умолчанию
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров. <0-65535> : номер TCP-порта
По умолчанию	Номер порта по умолчанию 179
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Команда позволяет устройству подключаться через порты, не указанные BGP
Пример	Switch(config-router)#neighbor 10.1.1.64 port 1023

16.3.56. Применение префиксного списка для фильтрации обновлений от узла (neighbor prefix-list)

Команда	neighbor {<ip-address> <TAG>} prefix-list <LISTNAME number> {<in out>} no neighbor {<ip-address> <TAG>} prefix-list <LISTNAME number>{<in> <out>} Команда задает ограничения для фильтрации маршрутных обновлений, принимаемых от соседнего узла либо передаваемых соседним узлом. Команда “no neighbor {<ip-address> <TAG>} prefix-list <LISTNAME number> {<in> <out>}” отменяет конфигурацию
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров. <LISTNAME number> : имя или порядковый номер в списке префиксов. <in out> : направление фильтрации
По умолчанию	Фильтрация по префиксу не применяется



Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Команда позволяет указать префикс и его диапазон, создавая запись "ip prefix-list" и определяет разрешения для данного диапазона. Отправляются или принимаются только маршруты с разрешенными префиксами
Пример	<pre>Switch(config)#ip prefix-list prw permit 100.1.0.0/22 ge 23 le 25 Switch(config)#router bgp 200 Switch(config-router)#redistribute static Switch(config-router)#neighbor 10.1.1.66 prefix-list prw out</pre>

16.3.57. Номер автономной системы соседнего узла BGP (neighbor remote-as)

Команда	<pre>neighbor {<ip-address> <TAG>} remote-as <as-id> no neighbor {<ip-address> <TAG>} [remote-as <as-id>]</pre> Данная команда конфигурирует соседний узел BGP. Команда с "no" в начале удаляет соседние узлы BGP
Параметр	<ip-address> : IP-адрес соседнего устройства <TAG> : имя группы пиров <as-id> : Номер АС соседнего устройства в диапазоне от 1 до 4294967295. Могут быть представлены в десятичной записи (например, 6553700) или в записи с разделителем (например, 100.100)
По умолчанию	Соседние узлы отсутствуют
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Соседние устройства BGP создаются исключительно командой конфигурирования. Действительные взаимоотношения между соседними устройствами устанавливаются только при взаимном конфигурировании. В конфигурации необходимо указать номер АС партнера. При некорректном номере АС взаимоотношения между соседними узлами невозможно установить. Номер АС партнера должен совпадать с номером автономной системы локального узла
Пример	Настроить 2 соседние АС как 100 и 100.200. <pre>Switch(config)#router bgp 200 Switch(config-router)# neighbor 10.1.1.64 remote-as 100 Switch(config-router)# neighbor 10.2.1.64 remote-as 100.200</pre>



16.3.58. Исключение частных AC из обновлений (neighbor remove-private-AS)

Команда	neighbor {<ip-address> <TAG>} remove-private-AS no neighbor {<ip-address> <TAG>} remove-private-AS Устанавливает необходимость удалять номер частной AC из отправляемых обновлений. Команда “no neighbor {<ip-address> <TAG>} remove-private-AS” отменяет данную конфигурацию
Параметр	<ip-address> : IP-адрес соседнего устройства <TAG> : имя группы пиров
По умолчанию	Не сконфигурировано
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Установка этого атрибута предотвращает присвоение внутреннего номера AC внешней AC. Внутренний номер AC находится в диапазоне 64512-65535, и этот номер AC не может быть отправлен в INTERNET, поскольку он не является действительным внешним номером AC. Здесь удаляется частный номер AC для полностью частной маршрутизации AC. Маршруты с частными номерами AC, которые также имеют публичные номера AC, не обрабатываются
Пример	Switch(config-router)#neighbor 10.1.1.64 remove-private-AS

16.3.59. Применение карты маршрута (neighbor route-map)

Команда	neighbor {<ip-address> <TAG>} route-map <NAME> {<in out>} no neighbor {<ip-address> <TAG>} route-map <NAME> {<in out>} Задаёт политику сопоставления маршрутов при отправке или получении маршрута. Команда “no neighbor {<ip-address> <TAG>} route-map <NAME> {<in out>}” отменяет конфигурацию
Параметр	<ip-address> : IP-адрес соседнего устройства <TAG> : имя группы пиров <NAME> : имя карты маршрутов <in out> : направление карты маршрутов
По умолчанию	Не задано
Режим ввода команды	Режим маршрутизации BGP



Руководство по использованию	Сначала необходимо настроить отображение маршрутов в глобальном режиме, создав карту маршрутов с помощью команды "route-map" и настроив условие соответствия и действия, после чего можно применить команду
Пример	<pre>Switch(config)#route-map test permit 5 Switch(config-route-map)#match interface Vlan1 Switch(config-route-map)#set as-path prepend 65532 Switch(config-route-map)#exit Switch(config)#router bgp 200 Switch(config-router)#neighbor 10.1.1.64 route-map test out</pre>

16.3.60. Настройка маршрутизатора в качестве отражателя маршрутов BGP и указанного соседа в качестве его клиента (neighbor route-reflector-client)

Команда	<pre>neighbor {<ip-address> <TAG>} route-reflector-client no neighbor {<ip-address> <TAG>} route-reflector-client</pre> Команда определяет клиента для отражателя маршрутов. Команда "no neighbor {<ip-address> <TAG>}route-reflector-client" отменяет конфигурацию
Параметр	<ip-address> : IP-адрес соседнего устройства <TAG> : имя группы пиров
По умолчанию	Не сконфигурировано
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Отражение маршрута используется для уменьшения количества пиров, когда внутренних IBGP-маршрутизаторов внутри AC слишком много. Клиент обменивается сообщениями только с отражателем маршрута, а отражатель обрабатывает обмен сообщениями между каждым клиентом и другими маршрутизаторами IBGP, EBGP. Эта команда настраивает маршрутизатор в качестве отражателя маршрутов, а определенную группу пиров в качестве клиентов. Примечание: эта настройка доступна только в пределах AC
Пример	<pre>Switch(config)#router bgp 100 Switch(config-router)#neighbor 10.1.1.66 remote 100 Switch(config-router)#neighbor 10.1.1.66 route-reflector-client Switch(config-router)#neighbor 10.1.1.68 remote 100 Switch(config-router)#neighbor 10.1.1.68 route-reflector-client</pre>



16.3.61. Настроить соседний узел как клиент сервера маршрутизации (neighbor route-server-client)

Команда	<pre>neighbor {<ip-address> <TAG>} route-server-client no neighbor {<ip-address> <TAG>} route-server-client</pre> Позволяет указать клиента сервера маршрутизации. Команда "no neighbor {<ip-address> <TAG>} route-server-client" отменяет конфигурацию.
Параметр	<ip-address> : IP-адрес соседнего устройства <TAG> : имя группы пиров
По умолчанию	Не сконфигурировано
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Служба маршрутизации предназначена для сокращения количества пиров, когда в среде EBGP слишком много маршрутизаторов между АС. Сервер прозрачно преобразует сообщения маршрутизации для других клиентов, при этом клиенты обмениваются сообщениями через сервер маршрутизации.
Пример	Имеется три маршрутизатора: 10.1.1.64 (AS100) и 10.1.1.68 (AS300) соответственно создают соседские отношения с подключенным 10.1.1.66 AS200, конфигурация следующая: <pre>Switch(config)#router bgp 200 Switch(config-router)#neighbor 10.1.1.64 remote-as 100 Switch(config-router)#neighbor 10.1.1.64 route-server-client Switch(config-router)# neighbor 10.1.1.68 remote-as 300 Switch(config-router)# neighbor 10.1.1.68 route-server-clien</pre>

16.3.62. Отправка соседним узлам BGP атрибутов сообщества (neighbor send-community)

Команда	<pre>neighbor {<ip-address> <TAG>} send-community [both extended standard] no neighbor {<ip-address> <TAG>} send-community [both extended standard]</pre> Задаёт необходимость отправки атрибутов сообщества соседним узлам. Команда "no neighbor {<ip-address> <TAG>} send-community [both extended standard]" отключает отправку.



Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров [both extended standard] : стандартное сообщество, расширенное сообщество или оба
По умолчанию	Отправка атрибутов выполняется
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Атрибуты сообщества можно отправлять или не отправлять во внешнюю среду. Значение по умолчанию для нашей компании - отправлять, а значение по умолчанию для стандартных протоколов - не отправлять. Если установить этот атрибут, атрибуты сообщества будут отправляться при отправке информации о маршрутизации соседям. Отсутствие следующего выбора будет равно стандартному
Пример	<pre>Switch(config-router)#no neighbor 10.1.1.66 send-community Switch(config-router)#neighbor 10.1.1.66 send-community</pre>

16.3.63. Отключение соседнего маршрутизатора (neighbor shutdown)

Команда	<pre>neighbor {<ip-address> <TAG>} shutdown no neighbor {<ip-address> <TAG>} shutdown</pre> Команда применяется для разрыва связи с соседним устройством. Команда "no neighbor {<ip-address> <TAG>} shutdown" отменяет конфигурацию
Параметр	<ip-address> : IP-адрес соседнего устройства <TAG> : имя группы пиров
По умолчанию	Разрыв связи не происходит
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Напрямую разрывает подключение/выполняет подключение к пиру (группе) без отмены конфигурации соседнего устройства
Пример	<pre>Switch(config-router)#neighbor 10.1.1.64 shutdown</pre>



16.3.64. Сохранение полученных маршрутных обновлений на локальном маршрутизаторе (neighbor soft-reconfiguration inbound)

Команда	neighbor {<ip-address> <TAG>} soft-reconfiguration inbound no neighbor {<ip-address> <TAG>} soft-reconfiguration inbound Устанавливает выполнение функции "inbound soft reconfiguration" (хранения базы маршрутов от соседнего узла, без каких-либо модификаций, на локальном маршрутизаторе и последующего обновления без разрыва сессии) Команда "no neighbor {<ip-address> <TAG>} soft-reconfiguration inbound" отменяет выполнение "inbound soft reconfiguration"
Параметр	<ip-address> : IP-адрес соседнего устройства <TAG> : имя группы пиров
По умолчанию	Выполнение "inbound soft reconfiguration" Не задано
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	После настройки мягкой реконфигурации "soft reconfiguration" система сохраняет входящие сообщения в буфере и применяет их немедленно при перезагрузке, чтобы минимизировать затраты на коммутацию с другими маршрутизаторами. Команда доступна только в том случае, если не включена возможность обновления маршрута
Пример	Switch(config-router)#neighbor 11.1.1.120 soft-reconfiguration inbound

16.3.65. Строгое соответствие возможностям узла (neighbor strict-capability-match)

Команда	neighbor {<ip-address> <TAG>} strict-capability-match no neighbor {<ip-address> <TAG>} strict-capability-match Указывает на необходимость строгого соответствия возможностям узла при установлении соединений. Команда "no neighbor {<ip-address> <TAG>} strict-capability-match" используется для отключения этой функции
Параметр	<ip-address> : IP-адрес соседнего устройства <TAG> : имя группы пиров
По умолчанию	Строгое соответствие возможностям не задано



Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Эта команда действительна только для MP-BGP. Позволяет установить соединение с соседним узлом только полным совпадении возможностей MP-BGP обеих сторон, иначе соединение отключается. При этом совпадение других возможностей не влияет на установление соседства
Пример	Switch(config-router)#neighbor 10.1.1.64 strict-capability-match

16.3.66. Установка таймера для определенного BGP узла (neighbor timers)

Команда	neighbor {<ip-address> <TAG>} timers <0-65535> <0-65535> no neighbor {<ip-address> <TAG>} timers <0-65535> <0-65535> Команда задает интервал KEEPALIVE и время ожидания получения сообщения hold time. Команда "no neighbor {<ip-address> <TAG>} timers <0-65535> <0-65535>" восстанавливает значение по умолчанию
Параметр	<ip-address> : IP-адрес соседнего устройства <TAG> : имя группы пиров <0-65535> : значение параметров KEEPALIVE и HOLD TIME соответственно
По умолчанию	Для значения KEEPALIVE - 60 секунд. Для значения HOLD TIME - 240 секунд
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Позволяет настроить значение интервалов отправки KEEPALIVE и HOLD TIME для соседнего устройства. Время удержания "holdtime" - это период времени для поддержания соединения, в течение которого маршрутизатор ожидает получения сообщения "keepalive" от соседнего маршрутизатора, если сообщение не получено в течение этого периода, соединение будет прервано
Пример	Switch(config-router)#neighbor 10.1.1.64 timers 50 200



16.3.67. Таймер подключения BGP (neighbor timers connect)

Команда	neighbor {<ip-address> <TAG>} timers connect <0-65535> no neighbor {<ip-address> <TAG>} timers connect [<0-65535>] Задаёт интервал времени повторного подключения. Команда "no neighbor {<ip-address> <TAG>} timers connect [<0-65535>]" восстанавливает значение по умолчанию
Параметр	<ip-address> : IP-адрес соседнего устройства <TAG> : имя группы пиров <0-65535> : интервал повторного запроса
По умолчанию	120 с
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Задаёт временной интервал для соединения при подключении к пиру. Форма команды с "NO" в начале восстанавливает значение по умолчанию
Пример	Switch(config-router)#neighbor 10.1.1.64 timers connect 100

16.3.68. Выборочная передача маршрутов определенному узлу BGP (neighbor unsuppress-map)

Команда	neighbor {<ip-address> <TAG>} unsuppress-map <WORD> no neighbor {<ip-address> <TAG>} unsuppress-map <WORD> Устанавливает или отменяет подавление условий соответствия указанной карте маршрута. Команда "no neighbor {<ip-address> <TAG>} unsuppress-map <WORD>" отменяет данную конфигурацию
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя группы пиров. <WORD> : имя карты маршрутов
По умолчанию	Не задано
Режим ввода команды	Режим маршрутизации BGP



Руководство по использованию	Эта команда обычно используется для маршрутов, подавляемых при распространении условиями "aggregated" и "summary-only". Маршруты, удовлетворяющие условиям карты маршрутов, по-прежнему будут передаваться по отдельности и не будут подавляться
Пример	<pre>Switch(config-router)#neighbor 10.1.1.66 unsuppress-map rmp Switch(config)#access-list 10 permit 10.1.1.100 0.0.0.255 Switch(config)#route-map rmp permit 5 Switch(config-route-map)#match ip next-hop 10</pre> Маршрут с nexthop 10.1.1.100 не будет подавляться

16.3.69. Источник для обновлений BGP (neighbor update-source)

Команда	<pre>neighbor {<ip-address> <TAG>} update-source <IFNAME> no neighbor {<ip-address> <TAG>} update-source <IFNAME></pre> Определяет источник обновлений. Команда "no neighbor {<ip-address> <TAG>} update-source <IFNAME>" отменяет конфигурацию
Параметр	<ip-address> : IP-адрес соседнего устройства <TAG> : имя группы пиров <IFNAME> : имя или IP-адрес интерфейса
По умолчанию	Не сконфигурировано, используется ближайший интерфейс
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Указанный источник обновления может подключаться к любому доступному интерфейсу маршрутизатора. Интерфейс "loopback" - это интерфейс, который чаще всего используется с этой командой. Форма "NO" команды восстанавливает связь с ближайшим источником обновления интерфейса. Неправильное использование источника обновления может привести к недоступности соседних соединений и возникновению проблем с недействительными интерфейсами, поэтому мы используем интерфейс "loop back". Примечание: интерфейс "loop back" должен поддерживать доступность своего адреса, чтобы была возможность устанавливать соединения в качестве источника обновлений
Пример	<pre>Switch(config-router)#neighbor 10.1.1.66 update-source 192.168.0.1</pre>



16.3.70. Применение конкретной версии BGP (neighbor version 4)

Команда	neighbor {<ip-address> <TAG>} version 4 Настройка версии BGP маршрутизатора
Параметр	<ip-address> : IP-адрес соседнего устройства <TAG> : имя группы пиров 4 : разрешенная версия BGP, только 4
По умолчанию	4
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Пока поддерживается только версия 4, поэтому, какой бы ни была конфигурация, версия остается 4
Пример	Switch(config-router)#neighbor 10.1.1.66 version 4 Switch(config-router)#

16.3.71. Определение веса для маршрутов от указанного узла (neighbor weight)

Команда	neighbor {<ip-address> <TAG>} weight <0-65535> no neighbor {<ip-address> <TAG>} weight [<0-65535>] Определяет значение веса маршрута, получаемого от соседнего узла. Команда “no neighbor {<ip-address> <TAG>} weight [<0-65535>]” восстанавливает значение по умолчанию
Параметр	<ip-address> : IP-адрес соседнего узла. <TAG> : имя или IP-адрес. <0-65535> : значение веса
По умолчанию	Вес по умолчанию маршрутов, полученный от других маршрутизаторов, равен 0. Вес по умолчанию в локальной статической конфигурации равен 32768
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Значение веса может повлиять на выбор маршрута. Веса относятся только к маршрутизатору и не являются атрибутами, которые могут быть переданы вовне



Пример	Switch(config-router)#neighbor 10.1.1.66 weight 500

16.3.72. Анонсирование сетей в процессе маршрутизации BGP (network (BGP))

Команда	network <ip-address/M> [route-map <WORD>] [backdoor] no network <ip-address/M> [route-map <WORD>] [backdoor] Команда позволяет настроить сеть анонсируемую BGP, карту маршрутов в сети или обходной маршрут (backdoor) для сети. Команда “no network <ip-address/M>[route-map <WORD>] [backdoor]” отменяет конфигурацию
Параметр	<ip-address/M> : идентификатор префикса сети <WORD> : имя карты маршрутов
По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Данная команда используется для анонсирования сетей в процессе маршрутизации BGP. При использовании сети, заданной этой командой, одноранговая сеть будет распространяться в карте маршрутов соседа, даже если локально маршрут отсутствует. При помощи атрибутов, задаваемых в применяемой сети, при указании маршрута из EBGP или внутри сети в параметре backdoor, внутренний маршрут будет предпочтительным, даже если внешний маршрут имеет меньшее расстояние
Пример	Switch(config-router)# network 172.16.0.0/16

16.3.73. Перераспределение входящих маршрутов в BGP (redistribute (BGP))

Команда	redistribute <ROUTES> [route-map <WORD>] no redistribute <ROUTES> [route-map <WORD>] Задаёт перераспределение протоколов маршрутизации, полученных без помощи протокола BGP, в процесс BGP. Команда “no redistribute <ROUTES> [route-map <WORD>]” отменяет данную конфигурацию
Параметр	<ROUTES> : источник маршрута или протокол маршрутизации, включая: connected (присоединённые), ISIS, kernel (маршруты ядра), ospf и rip static (статические), <WORD> : имя карты маршрута



По умолчанию	-
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	Команда предназначена для перераспределения маршрутов, полученных без помощи протокола BGP, в таблицу маршрутизации BGP и передачи таких маршрутов соседним узлам
Пример	С помощью команды ввести статический маршрут в BGP и анонсировать его соседним устройствам. Switch(config-router)# redistribute static

16.3.74. Перераспределять маршруты OSPF (redistribute ospf)

Команда	redistribute ospf [<process-id>] [route-map<word>] no redistribute ospf [<process-id>] Определяет перераспределение информации о маршрутизации из OSPF в BGP. "no" в начале команды удаляет конфигурацию
Параметр	process-id это идентификатор процесса OSPF, в пределах от 1 до 65535. Если "process-id" не указан, будет использован идентификатор процесса по умолчанию. route-map <word> указатель на представленную карту маршрутизации
По умолчанию	Перераспределение не выполняется
Режим ввода команды	Режим маршрутизации BGP
Руководство по использованию	-
Пример	Перераспределить маршрутизацию OSPF v2 в BGP (номер равен 1). Switch(config)#router bgp 1 Switch(config-router)#redistribute ospf 2



16.3.75. Запуск процесса BGP (router bgp)

Команда	<code>router bgp <as-id></code> <code>no router bgp <as-id></code> Включение экземпляра BGP. Команда “no router bgp <as-id>” удаляет экземпляр BGP
Параметр	<as-id> : Номер AC в диапазоне от 1 до 4294967295, может быть представлен в десятичной записи (например, 6553700) или в записи с разделителем (например, 100.100)
По умолчанию	Процесс BGP не запущен
Режим ввода команды	Режим глобальной конфигурации
Руководство по использованию	Команда позволяет запустить BGP в указанной AC, а затем зайти в режим "config-router" для настройки протокола
Пример	Включить BGP, номер AC - 4294967295 в десятичной записи. <code>Switch(config)#router bgp 4294967295</code> <code>Switch(config-router)#exit</code> Включить BGP, номер AC - 4294967295 в записи с разделителем. <code>Switch(config)#router bgp 65535.65535</code> <code>Switch(config-router)#exit</code>

16.3.76. Глобальная настройка таймеров для BGP (timers bgp)

Команда	<code>timers bgp <0-65535> <0-65535></code> <code>no timers bgp [<0-65535> <0-65535>]</code> Настраивает значения таймеров, используемые BGP, для всех соседних узлов. Команда “no timers bgp [<0-65535> <0-65535>]” возвращает значения по умолчанию
Параметр	<0-65535> : значение параметров KEEPALIVE и HOLD TIME соответственно
По умолчанию	Для значения KEEPALIVE - 60 секунд. Для значения HOLD TIME - 240 секунд
Режим ввода команды	Привилегированный режим и режим конфигурации



Руководство по использованию	Аналогично настройке времени для соседнего устройства, только выполняется для всех соседних устройств
Пример	Switch(config-router)# timers bgp 50 200

16.3.77. Просмотр информации о сети BGP (show ip bgp)

Команда	show ip bgp [<ADDRESS-FAMILY>] [<ip-address> <ip-address/M> [longer-prefixes]] cidr-only Выводит на экран сообщения маршрутизации, выполняемой BGP
Параметр	<ADDRESS-FAMILY> : семейство адресов, например, "ipv4 unicast" ; <ip-address> : IP-адрес; <ip-address/M> : IP-адрес и маска
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Позволяет вывести на экран сообщения маршрутизации BGP на основе различных параметров (например, семейства адресов или IPv4-адрес), маршруты с определенным префиксом, или просто показать сообщения маршрутизации, которые не соответствуют самому раннему семейству IP-адресов (то есть маршрут не является адресом типа A или B или C)
Пример	Switch#show ip bgp BGP table version is 147, local router ID is 10.1.1.64 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale Origin codes: i - IGP, e - EGP, ? – incomplete Network Next Hop Metric LocPrf Weight Path *> 12.0.0.0 10.1.1.121 0 32768 ? *> 100.1.1.0/24 10.1.1.200 0 32768 ? *> 100.1.2.0/24 10.1.1.200 0 32768 ? *> 172.0.0.0/8 0.0.0.0 32768 i Total number of prefixes 4



16.3.78. Просмотр информации об атрибутах сети BGP (show ip bgp attribute-info)

Команда	show ip bgp attribute-info Выводит на экран информацию об атрибутах BGP
Параметр	-
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Применяется для вывода информации об атрибутах BGP
Пример	Switch#show ip bgp attribute-info attr[1] nexthop 0.0.0.0 attr[1] nexthop 10.1.1.64 attr[3] nexthop 10.1.1.64 attr[1] nexthop 10.1.1.121 attr[2] nexthop 10.1.1.200

16.3.79. Просмотр маршрутов, принадлежащих определённым сообществам BGP (show ip bgp community)

Команда	show ip bgp [<ADDRESS-FAMILY>] community <TYPE> [exact-match] Выводит на экран маршруты, принадлежащие определённым сообществам BGP
Параметр	<ADDRESS-FAMILY> : семейство адресов, например, "ipv4 unicast" <TYPE> : идентификатор сообщества в формате AA: NN или комбинации из local-AS, no-advertise и no-export
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Допускается выбрать несколько сообществ одновременно, при точном совпадении будут показаны только идеально совпадающие записи



Пример	<pre>Switch#show ip bgp community BGP table version is 10, local router ID is 10.1.1.64 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path * 100.1.1.0/24 0.0.0.0 32768 700 800 i *> 172.0.0.0/8 0.0.0.0 32768 700 800 i Total number of prefixes 2</pre>

16.3.80. Просмотр информации о сообществе BGP (show ip bgp community-info)

Команда	<pre>show ip bgp community-info</pre> Используется для просмотра всей доступной информации о сообществах BGP
Параметр	
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Несколько сообщений об одном сообществе могут быть закрыты одновременно
Пример	<pre>Switch#show ip bgp community-info Address Refcnt Community [0x3312558] (3) 100: 50</pre>

16.3.81. Просмотр маршрутов, соответствующих списку сообществ (show ip bgp community-list)

Команда	<pre>show ip bgp [<ADDRESS-FAMILY>] community-list <NAME> [exact-match]</pre> Выводит на экран маршруты, принадлежащие сообществам из определённого списка сообществ BGP
Параметр	<ADDRESS-FAMILY> : семейство адресов, например, "ipv4 unicast" <NAME> : список сообществ
По умолчанию	-



Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Используйте команду "ip community-list" для настройки списка сообществ, а также для включения в него сообществ. При выводе на экран имени сообщества, отображаются сообщества, включенные во все списки
Пример	<pre>Switch(config)#ip community-list commu per 100: 50 Switch#show ip bgp community-list commu BGP table version is 25, local router ID is 10.1.1.64 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale Origin codes: i - IGP, e - EGP, ? – incomplete Network Next Hop Metric LocPrf Weight Path * 100.1.1.0/24 0.0.0.0 32768 700 800 i *> 172.0.0.0/8 0.0.0.0 32768 700 800 i</pre>

16.3.82. Просмотр информации о подавленных маршрутах (show ip bgp dampening)

Команда	<pre>show ip bgp [<ADDRESS-FAMILY>] dampening {<dampened-paths> <flap-statistics> <parameters>}</pre> Выводит на экран маршрутизацию BGP и соответствующие подавленные маршруты
Параметр	<ADDRESS-FAMILY> : семейство адресов, например, "ipv4 unicast"
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Будут отображаться только подавленные маршруты. <parameters> отображает конфигурации, не относящиеся к определенным маршрутам. Две другие опции будут соответственно показывать ограниченные маршруты и сообщения о подавленной (недавно восстановленной из недействительной) маршрутизации



Пример	<pre>Switch#show ip bgp dampening dampened-paths BGP table version is 12, local router ID is 10.1.1.66 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale Origin codes: i - IGP, e - EGP, ? - incomplete Network From Reuse Path *d 100.1.3.0/24 10.1.1.64 00: 27: 40 100 ? Total number of prefixes 1 Switch#show ip bgp dampening flap-statistics BGP table version is 13, local router ID is 10.1.1.66 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale Origin codes: i - IGP, e - EGP, ? - incomplete Network From Flaps Duration Reuse Path *d 100.1.3.0/24 10.1.1.64 3 00: 06: 05 00: 27: 00 100 ? Switch#show ip bgp dampening parameters dampening 15 750 2000 60 15 (route-map rmp) Reachability Half-Life time : 15 min Reuse penalty : 750 Suppress penalty : 2000 Max suppress time : 60 min Un-reachability Half-Life time : 15 min Max penalty (ceil) : 11999 Min penalty (floor) : 375 Total number of prefixes 1</pre>

16.3.83. Просмотр маршрутов, соответствующих списку фильтрации (show ip bgp filter-list)

Команда	<pre>show ip bgp [<ADDRESS-FAMILY>]filter-list [<WORD >]</pre> Выводит на экран маршруты в BGP, соответствующие определенному списку фильтрации AC
Параметр	<ADDRESS-FAMILY> : семейство адресов, например, "ipv4 unicast". < WORD > : имя списка доступа в AS-PATH
По умолчанию	-



Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Командой "ip as-path access-list" задается список доступа автономной системы АС. Данная команда отображает маршруты, соответствующие списку доступа
Пример	<pre>Switch#show ip bgp filter-list FL BGP table version is 2, local router ID is 11.1.1.100 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path *> 100.1.1.0/24 10.1.1.64 0 0 100 ? Total number of prefixes 1</pre>

16.3.84. Просмотр маршрутов с несогласованными путями АС (show ip bgp inconsistent-as)

Команда	<pre>show ip bgp [<ADDRESS-FAMILY>] inconsistent-as</pre> Выводит на экран маршруты с несогласованными путями АС BGP
Параметр	<ADDRESS-FAMILY> : семейство адресов, например, "ipv4 unicast"
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Если один и тот же префикс получается из разных АС, то эти системы будут считаться несовместимыми. Данная команда применяется для отображения таких маршрутов
Пример	<pre>Switch#show ip bgp inconsistent-as BGP table version is 2, local router ID is 11.1.1.100 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path * 100.1.1.0/24 10.1.1.68 0 0 300 ? *> 10.1.1.64 0 0 100 ? Total number of prefixes 1</pre>



16.3.85. Просмотр информации о распространении маршрутов (show ip bgp neighbors)

Команда	show ip bgp [<ADDRESS-FAMILY>] neighbors [IP-ADDRESS] [advertised-routes received {prefix-filter routes} routes] Выводит на экран информацию о соседних узлах BGP
Параметр	<ADDRESS-FAMILY> : семейство адресов, например, "ipv4 unicast" <ip-address> : IP-адрес соседнего устройства
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Команда выводит подробные сведения обо всех соседних узлах. При указании IP-адреса будет показана подробная информация о соседних узлах с указанным IP-адресом. Параметры "advertised-routes" , "received prefix-filter" , "received routes" , "routes" соответственно отображают анонсируемые локально маршруты, префиксные списки для фильтрации, полученные маршруты (включена мягкая реконфигурация) и сообщение о маршрутизации от конкретного узла
Пример	<pre>Switch#show ip bgp neighbor BGP neighbor is 10.1.1.66, remote AS 200, local AS 100, external link BGP version 4, remote router ID 11.1.1.100 BGP state = Established, up for 00: 13: 43 Last read 00: 13: 43, hold time is 240, keepalive interval is 60 seconds Neighbor capabilities: Route refresh: advertised and received (old and new) Address family IPv4 Unicast: advertised and received Received 17 messages, 0 notifications, 0 in queue Sent 17 messages, 0 notifications, 0 in queue Route refresh request: received 0, sent 0 Minimum time between advertisement runs is 30 seconds For address family: IPv4 Unicast BGP table version 2, neighbor version 2 Index 1, Offset 0, Mask 0x2 Community attribute sent to this neighbor (both) 0 accepted prefixes 1 announced prefixes Connections established 7; dropped 6</pre>



16.3.86. Просмотр путей BGP (show ip bgp paths)

Команда	show ip bgp [<ADDRESS-FAMILY>] paths Выводит на экран информацию о всех путях BGP
Параметр	<ADDRESS-FAMILY> : семейство адресов, например, "ipv4 unicast"
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Команда выводит сообщения о пути BGP, включая статус использования
Пример	Switch#show ip bgp paths Address Refcnt Path [0x331dad0: 0] (1) [0x331d850: 93] (1) 600 [0x331d8d8: 249] (2) 200 300

16.3.87. Просмотр маршрутов, соответствующих списку префиксов (show ip bgp prefix-list)

Команда	show ip bgp [<ADDRESS-FAMILY>] prefix-list [<NAME>] Выводит на экран маршруты BGP, префиксы которых совпадают с префиксами из определённого списка префиксов
Параметр	<ADDRESS-FAMILY> : семейство адресов, например, "ipv4 unicast". <NAME> : имя списка префиксов
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Позволяет выбрать необходимый маршрут BGP, применив список фильтрации в виде регулярного выражения



Пример	<pre>Switch(config)#ip prefix-list PL permit any Switch#show ip bgp prefix-list PL BGP table version is 1, local router ID is 10.1.1.64 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale Origin codes: i - IGP, e - EGP, ? – incomplete Network Next Hop Metric LocPrf Weight Path * 100.1.1.0/24 10.1.1.66 0 200 300 ? *> 10.1.1.100 0 32768 ? Total number of prefixes 1</pre>

16.3.88. Просмотр маршрутов BGP, содержащих указанное регулярное выражение (show ip bgp quote-regexp)

Команда	<pre>show ip bgp [<ADDRESS-FAMILY>] quote-regexp [<WORD>]</pre> Выводит на экран маршруты BGP, содержащие указанное регулярное выражение для определенной AC
Параметр	<ADDRESS-FAMILY> : семейство адресов, например, "ipv4 unicast". <WORD> : Обычное выражение
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Позволяет выбрать нужный маршрут с помощью регулярных выражений
Пример	<pre>Switch#show ip bgp quote-regexp ^300\$ BGP table version is 2, local router ID is 11.1.1.100 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path *> 100.1.1.0/24 10.1.1.68 0 0 300 ? Total number of prefixes 1 Switch#sh ip bgp quote-regexp 100 BGP table version is 2, local router ID is 11.1.1.100</pre>



	Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path * 100.1.1.0/24 10.1.1.64 0 0 500 100 600 ? Total number of prefixes 1

16.3.89. Просмотр информации о перераспределении из внешних процессов (show ip bgp redistribute)

Команда	show ip bgp redistribute Выводит информацию о перераспределенной маршрутизации из внешних процессов в BGP
Параметр	-
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим ввода команд
Руководство по использованию	-
Пример	Switch#show ip bgp redistribute

16.3.90. Просмотр информации о соседних устройствах (show ip bgp neighbors)

Команда	show ip bgp neighbors Позволяет просмотреть информацию о соседних узлах указанного BGP или всего BGP-процесса
Параметр	
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим ввода команд
Руководство по использованию	-



Пример	Switch#show ip bgp neighbors

16.3.91. Просмотр маршрутов BGP, содержащих указанное регулярное выражение (show ip bgp regexp)

Команда	show ip bgp [<ADDRESS-FAMILY>] regexp [<LINE>] Выводит на экран маршруты BGP, соответствующие регулярному выражению пути определенной AC
Параметр	<ADDRESS-FAMILY > : семейство адресов, например, "ipv4 unicast". <LINE> : Обычное выражение
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Команда позволяет выбрать маршруты BGP определенной AC, удовлетворяющие регулярному выражению
Пример	Switch#show ip bgp regexp 100 BGP table version is 2, local router ID is 11.1.1.100 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path * 100.1.1.0/24 10.1.1.64 0 0 500 100 600 ? Total number of prefixes 1

16.3.92. Просмотр маршрутов BGP, входящих в указанную карту маршрутов (show ip bgp route-map)

Команда	show ip bgp [<ADDRESS-FAMILY>] route-map [<NAME>] Выводит на экран маршруты BGP, входящие в указанную карту маршрутов
Параметр	<ADDRESS-FAMILY > : например, "ipv4 unicast". <NAME> : имя карты маршрутов
По умолчанию	-



Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Используйте команду "route-map" для настройки карт маршрутов, с помощью которых можно отображать обрабатываемые маршруты. Данная команда отобразит маршруты, соответствующие конкретной карте маршрутов
Пример	<pre>Switch#show ip bgp route-map rmp BGP table version is 2, local router ID is 11.1.1.100 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path * 100.1.1.0/24 10.1.1.64 0 0 500 100 600 ? *> 10.1.1.68 0 0 300 ? Total number of prefixes 1</pre>

16.3.93. Отображение статуса сканирования BGP (show ip bgp scan)

Команда	<pre>show ip bgp scan</pre> Выводит на экран сообщения о сканировании BGP
Параметр	
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Сообщения "nexthop" необходимо регулярно сканировать. Команда показывает текущий интервал сканирования и связанные с ним маршруты
Пример	<pre>Switch#show ip bgp scan BGP Instance: (Default) AS 200, router-id 11.1.1.100 BGP scan interval is 60 Current BGP nexthop cache:</pre>



16.3.94. Просмотр сводной информации о BGP (show ip bgp summary)

Команда	show ip bgp [<ADDRESS-FAMILY>] summary Выводит на экран сводную информацию о BGP	
Параметр	<ADDRESS-FAMILY> : семейство адресов, например, "ipv4 unicast"	
По умолчанию	-	
Режим ввода команды	Привилегированный режим и режим конфигурации	
Руководство по использованию	Отображает основную сводную информацию о BGP	
Пример	Switch#show ip bgp summary BGP router identifier 10.1.1.66, local AS number 200 BGP table version is 1 1 BGP AS-PATH entries 0 BGP community entries Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 10.1.1.68 4 300 0 0 0 0 never Active Total number of neighbors 1	
	Информация, отображаемая на экране	Описание
	identifier	идентификатор локального устройства
	local AS number	номер AC локального маршрутизатора
	table version	номер версии внутренней базы данных BGP
	AS-PATH entries	таблица записей AS-PATH
	community entries	записи сообществ
	Neighbor	Адрес работающего соседнего узла
	V	Версия BGP работающего соседнего узла



	AS	номер AC соседнего устройства, частью которой является
	MsgRcvd	Количество сообщений, полученных от соседнего узла
	MsgSent	Количество сообщений, отправленных соседнему узлу
	TblVer	версия таблицы маршрутизации
	Up/Down	Если состояние с соседним узлом установлено, отображается продолжительность связи, в противном случае отображается текущий статус.
	State/PfxRcd	Если состояние установлено, показано количество префиксов, полученных маршрутизатором. В противном случае отображается текущий статус соседей.

16.3.95. Просмотр информации о виде BGP (show ip bgp view)

Команда	show ip bgp view [<NAME>] [<ip-address> <ip-address/M>][<ADDRESS-FAMILY>] summary] Выводит информацию об указанном экземпляре BGP
Параметр	<NAME> : имя экземпляра BGP <ip-address> : IP address <ip-address/M> : IP-адрес или маска <ADDRESS-FAMILY> : семейство адресов, например, "ipv4 unicast"
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Команда позволяет просмотреть информацию об указанном экземпляре BGP



Пример	Switch#show ip bgp view as300 100.1.1.0/24

16.3.96. Просмотр информации о соседних узлах указанного экземпляра BGP (show ip bgp view neighbors)

Команда	show ip bgp view [<NAME>] neighbors [<ip-address>] Выводит на экран информацию о соседних узлах указанного экземпляра BGP
Параметр	<NAME> : имя экземпляра BGP <ip-address> : IP-адрес соседнего узла
По умолчанию	-
Режим ввода команды	Привилегированный режим и режим конфигурации
Руководство по использованию	Выводит на экран информацию о соседних узлах указанного экземпляра BGP
Пример	Switch#show ip bgp view as300 neighbors

16.3.97. Параметры отладки для протокола BGP (debug bgp)

Команда	debug bgp [<MODULE> all] no debug bgp [<MODULE> all] Открывает параметры отладки для протокола BGP. Команда “no debug bgp [<MODULE> all]” закрывает параметры отладки
Параметр	<MODULE>: имя модулей BGP, включая dampening, events, filters, fsm, keepalives, nsm, updates и т.д
По умолчанию	Не задано
Режим	Привилегированный режим
Руководство по использованию	Применяется для мониторинга событий BGP и обнаруженных ошибок, предупреждающих сообщений
Пример	Вывести на экран отладочные сообщения всех модулей bgp. Switch#debug bgp all



16.3.98. Параметры отладки отправленных сообщений перераспределения (debug bgp redistribute message send)

Команда	debug bgp redistribute message send no debug bgp redistribute message send Команда позволяет применять параметры отладки отправки сообщений для перераспределения маршрутизации из внешних процессов, например, OSPF и RIP, в BGP. "no" в начале команды отключает процесс отладки
Параметр	-
По умолчанию	Параметры отладки закрыты
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Switch# debug bgp redistribute message send Switch# no debug bgp redistribute message send

16.3.99. Параметры отладки полученных сообщений о перераспределении маршрута (debug bgp redistribute route receive)

Команда	debug bgp redistribute route receive no debug bgp redistribute route receive Команда используется для подключения параметров отладки получаемых сообщений от NSM для BGP. Форма команды с "no" в начале отключает отладку получаемых от NSM сообщений для BGP
Параметр	-
По умолчанию	Параметры отладки закрыты
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Switch#debug bgp redistribute route receive Switch#no debug bgp redistribute route receive



16.3.100. Включить возможность мягкого перезапуска BGP (bgp graceful-restart)

Команда	bgp graceful-restart no bgp graceful-restart Поддерживает для BGP возможность мягкого перезапуска (GR) и задает значения restart-time (время перезапуска) и stale-path-time (время хранения пути) по умолчанию, команда с "no" в начале отключает GR
Параметр	-
По умолчанию	BGP не поддерживает мягкий перезапуск
Режим	Режим конфигурации маршрутизатора BGP
Руководство по использованию	-
Пример	Настроить мягкий перезапуск. Switch(config-router)# bgp graceful-restart

16.3.101. Время ожидания для восстановления узла при мягком перезапуске (bgp graceful-restart restart-time)

Команда	bgp graceful-restart restart-time <1-3600> no bgp graceful-restart restart-time <1-3600> Команда задает время восстановления связи при мягком перезапуске BGP (принимающий узел (Receiving Speaker) включает таймер таймаута для соседнего устройства, для этого используется restart-time). Параметр restart-time задает максимальное время ожидания от момента, когда принимающий узел обнаружит перезапуск, до получения сообщений OPEN. Если принимающий узел не получает сообщений OPEN по истечении этого времени, он может удалить маршрут SATLE, сохраненный соседним устройством. Команда с "No" в начале восстанавливает значение времени перезапуска по умолчанию 120 секунд
Параметр	<1-3600> : время в секундах
По умолчанию	значение по умолчанию для restart-time - 120 секунд
Режим	Режим конфигурации маршрутизатора BGP
Руководство по использованию	-



Пример	Установить для GR на BGP время restart-time в 60 секунд. Switch(config-router)# bgp graceful-restart restart-time 60

16.3.102. Время хранения пути при мягком перезапуске (bgp graceful-restart stale-path-time)

Команда	bgp graceful-restart stale-path-time <1-3600> no bgp graceful-restart stale-path-time <1-3600> Позволяет настроить "stale-path-time" для мягкого перезапуска BGP. Задаёт для принимающего узла максимальное время, в течение которого сохраняются устаревшие маршруты из полученных сообщений OPEN в полученные EOR. Команда с "No" в начале восстанавливает значение "stale-path-time" по умолчанию, равное 360 секундам
Параметр	<1-3600> : время в секундах
По умолчанию	значение по умолчанию для "stale-path-time" — 360 секунд
Режим	Режим конфигурации маршрутизатора BGP
Руководство по использованию	-
Пример	Установить для BGP GR время "stale-path-time" в 460 секунд. Switch(config-router)# bgp graceful-restart stale-path-time 460

16.3.103. Установка таймера до выбора маршрута для перезапускаемого узла (bgp selection-deferral-time)

Команда	bgp selection-deferral-time <1-3600> no bgp selection-deferral-time <1-3600> Позволяет установить время отсрочки выбора "selection-deferral-time" для BGP GR. Задаёт для перезапускаемого узла (Restarting Speaker) максимальное время ожидания с момента получения сообщения OPEN до получения EOR для начала выбора маршрутов. Если Restarting Speaker не получает EOR после превышения этого времени, выбор маршрутов может начинаться. Команда с "No" в начале восстанавливает для selection-deferral-time значение по умолчанию равное 120 секундам
Параметр	<1-3600> : время в секундах
По умолчанию	Значение по умолчанию для selection-deferral-time - 120 секунд



Режим	Режим конфигурации маршрутизатора BGP
Руководство по использованию	-
Пример	Установить время "selection-deferral-time" для BGP GR равное 240 секундам. Switch(config-router)# bgp selection-deferral-time 240

16.3.104. Поддержка мягкого перезапуска на соседнем узле (neighbor capability graceful-restart)

Команда	neighbor (A.B.C.D X: X: : X: X WORD) capability graceful-restart no neighbor (A.B.C.D X: X: : X: X WORD) capability graceful-restart Позволяет установить возможность поддержки мягкого перезапуска (GR) соседним узлам. Команда с "no" в начале отменяет поддержку GR
Параметр	(A.B.C.D X: X: : X: X WORD) : адрес соседнего узла или группа соседних узлов для BGP
По умолчанию	Мягкий перезапуск не сконфигурирован
Режим	Режим семейства одноадресных адресов протокола BGP
Руководство по использованию	-
Пример	Задать анонсирование возможности мягкого перезапуска соседнему узлу 1.1.1.1. Switch(config-router)#neighbor 1.1.1.1 capability graceful-restart

16.3.105. Время перезапуска для соседних узлов (neighbor restart-time)

Команда	neighbor (A.B.C.D X: X: : X: X WORD) restart-time <1-3600> no neighbor (A.B.C.D X: X: : X: X WORD) restart-time <1-3600> Устанавливает время перезапуска (restart-time) для соседних узлов, команда с "no" восстанавливает значения по умолчанию
Параметр	(A.B.C.D X: X: : X: X WORD) : адрес соседнего узла или группа соседних узлов для BGP <1-3600> : время в секундах



По умолчанию	Время перезапуска для соседнего узла по умолчанию составляет 120 секунд
Режим	Режим семейства одноадресных адресов протокола BGP
Руководство по использованию	-
Пример	Установить соседнему узлу 1.1.1.1 время restart-time в 60 секунд. Switch(config-router)# neighbor restart-time 60

16.4. Команды протокола RIP

16.4.1. Удаление записей из таблицы маршрутизации (clear ipv6 rip route)

Команда	clear ipv6 rip route { <ipv6-address > kernel static connected rip ospf isis bgp all } Удаляет указанные записи из таблицы маршрутизации RIPng
Параметр	Команда удаляет записи, которые точно соответствуют адресу назначения из таблицы маршрутизации RIP. <ipv6-address > адрес назначения в шестнадцатеричном формате с длиной префикса. kernel удалить маршрут kernel из таблицы маршрутов RIPng static удалить статический маршрут из таблицы маршрутов RIPng connected удалить прямой маршрут из таблицы маршрутов RIPng rip удалить маршрут RIPng только из таблицы маршрутов RIPng ospf удалить маршрут IPv6 OSPF только из таблицы маршрутов RIPng bgp удалить маршрут IPv6 BGP только из таблицы маршрутов RIPng ISIS удалить маршрут ipv6 isis только из таблицы маршрутов RIPng all удалить все маршруты из таблицы маршрутов RIPng
По умолчанию	Конфигурация по умолчанию отсутствует
Режим	Привилегированный режим
Руководство по использованию	При использовании этой команды со всеми параметрами все маршруты в таблице маршрутизации RIPng будут удалены
Пример	Switch#clear ipv6 rip route 2001:1:1::/64 Switch#clear ipv6 rip route ospf



16.4.2. Анонс маршрута по умолчанию в RIP (default-information originate)

Команда	default-information originate no default-information originate Разрешает перераспределение сети 0: : в RIPv6. Команда "no default-information originate" отключает данную функцию
Параметр	-
По умолчанию	Отключено
Режим	Режим маршрутизации
Руководство по использованию	-
Пример	Switch# config terminal Switch(config)# router ipv6 rip Switch(config-router)# default-information originate

16.4.3. Метрика по умолчанию (default-metric)

Команда	default-metric <value> no default-metric Устанавливает значение метрики маршрутизации по умолчанию для внедренных маршрутов; команда "no default-metric" восстанавливает значение по умолчанию
Параметр	<value> значение метрики маршрута, которое необходимо задать, в диапазоне от 1 до 16
По умолчанию	Значение метрики маршрута по умолчанию равно 1
Режим	Режим маршрутизации
Руководство по использованию	Команда "default-metric" используется для установки значения метрики маршрута по умолчанию для маршрутов из других протоколов маршрутизации при распределении в маршруты RIPv6. При использовании команд "redistribute" для внедрения маршрутов из других протоколов, если не указана конкретная метрика маршрута, будет использоваться значение метрики маршрута по умолчанию, заданное командой "default-metric"



Пример	Установить значение метрики маршрута по умолчанию для маршрутов из других протоколов маршрутизации при распределении в маршруты RIPv6 равным 3. <pre>Switch(config)# router ipv6 rip Switch(config-router)# default-metric 3</pre>

16.4.4. Административная дистанция (distance)

Команда	<pre>distance <number> [<ipv6-address>] [<access-list-name access-list-number>]</pre> <pre>no distance [<ipv6-address>]</pre> Устанавливает административную дистанцию. Команда “no distance [<A.B.C.D/M>]” восстанавливает значение по умолчанию 120
Параметр	<number> задает значение дистанции, в диапазоне 1-255. < ipv6-address > адрес локального канала или его префикс. <access-list-name access-list-number > номер или имя применяемого списка доступа
По умолчанию	По умолчанию значение административной дистанции равно 120
Режим	Режим маршрутизации и режим семейства адресов
Руководство по использованию	Если существует два маршрута к одному и тому же адресу назначения с разными протоколами маршрутизации, для выбора маршрута используется административная дистанция. Чем меньше административная дистанция протокола маршрутизации, тем надежнее будет маршрут, полученный от протокола
Пример	<pre>Switch# config terminal Switch(config)# router ipv6 rip Switch(config-router)# distance 8 fe80:1111::4200:21ff:fe00:11 mylist</pre>

16.4.5. Фильтрация обновлений маршрута (distribute-list)

Команда	<pre>distribute-list{<access-list-number access-list-name> prefix<prefix-list-name>} {in out} [<ifname>]</pre> <pre>no distribute-list{<access-list-number access-list-name> prefix<prefix-list-name>} {in out} [<ifname>]</pre> Команда предназначена для фильтрации входящих (исходящих) обновлений маршрута с помощью списка доступа access-list или списка префиксов prefix-list. Команда “no distribute-list {access-list-name> prefix<prefix-list-name>} {in out} [<ifname> vlan <vlan-id>]” отменяет функцию фильтрации



Параметр	<access-list-number access-list-name> имя или номер списка доступа, который будет применяться. <prefix-list-name> имя списка префиксов, который будет применяться. <ifname> имя интерфейса, к которому будет применяться фильтрация маршрутов
По умолчанию	Функция отключена в RIPv6 по умолчанию
Режим	Режим маршрутизации
Руководство по использованию	Если не указан конкретный интерфейс фильтрация будет применяться ко всем интерфейсам
Пример	<pre>Switch# config terminal Switch(config)# router ipv6 rip Switch(config-router)# distribute-list prefix myfilter in vlan 1</pre>

16.4.6. Параметры отладки для RIPv6 (debug ipv6 rip)

Команда	<pre>debug ipv6 rip [events nsm packet[recv send][detail]] all] no debug ipv6 rip [events nsm packet[recv send][detail]] all]</pre> Используется для вывода отладочной информации для RIPv6 и отображения различных отладочных сообщений. Команда “no debug ipv6 rip [events nsm packet [recv send][detail]] all]” закрывает отладку
Параметр	events показывает отладочные сообщения о событиях RIPv6 nsm показывает сообщения связи между RIPv6 и NSM. packet показывает отладочные сообщения пакетов данных RIPv6 recv показывает сообщения о принятых пакетах данных send показывает сообщения отправленных пакетов данных detail показывает сообщения о полученных или отправленных пакетах данных
По умолчанию	Не включено
Режим	Привилегированный режим
Руководство по использованию	-



Пример	<pre>Switch#debug ipv6 rip packet Switch#1970/01/01 21: 15: 08 IMI: SEND[Ethernet1/4]: Send to [ff02: : 9]: 521 1970/01/01 21: 15: 08 IMI: SEND[Ethernet1/2]: Send to [ff02: : 9]: 521 1970/01/01 21: 15: 09 IMI: RECV[Ethernet1/4]: Receive from [fe80: : 20b: 46ff: fe57: 8e60]: 521 1970/01/01 21: 15: 09 IMI: RECV[Ethernet1/4]: 3000: 1: 1: : /64 is filtered by access-list dclist 1970/01/01 21: 15: 09 IMI: RECV[Ethernet1/4]: 3ffe: 1: 1: : /64 is filtered by access-list dclist 1970/01/01 21: 15: 15 IMI: RECV[Ethernet1/2]: Прием от [fe80: : 203: fff: fe01: 257c]: 521</pre>

16.4.7. Параметры отладки отправленных сообщений перераспределения маршрута (debug ipv6 rip redistribute message send)

Команда	<pre>debug ipv6 rip redistribute message send no debug ipv6 rip redistribute message send</pre> Открывает параметры отладки, показывающие сообщения о перераспределении маршрутов, отправленных в RIPv6 из OSPFv3 или прочих внешних процессов. "no" в начале команды отключает параметры отладки
Параметр	Не задано
По умолчанию	Параметры отладки закрыты
Режим	Привилегированный режим
Руководство по использованию	-
Пример	<pre>Switch#debug ipv6 rip redistribute message send Switch#no debug ipv6 rip redistribute message send</pre>



16.4.8. Параметры отладки полученных сообщений о перераспределении маршрута (debug ipv6 rip redistribute route receive)

Команда	debug ipv6 rip redistribute route receive no debug ipv6 rip redistribute route receive Открывает параметры отладки, показывающие сообщения о перераспределении маршрутов, полученных RIPng от NSM. "no" в начале команды отключает отладку
Параметр	Не задано
По умолчанию	Параметры отладки закрыты
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Switch#debug ipv6 rip redistribute route receive Switch#no debug ipv6 rip redistribute route receive

16.4.9. Агрегированные адреса (ipv6 rip aggregate-address)

Команда	ipv6 rip aggregate-address X: X: : X: X/M no ipv6 rip aggregate-address X: X: : X: X/M Команда предназначена для настройки агрегированного маршрута IPv6. "no" в начале команды удаляет агрегированный маршрут IPv6
Параметр	X: X: : X: X/M: IPv6-адрес и длина префикса
По умолчанию	По умолчанию агрегированные адреса не настроены
Режим	Режим маршрутизации или режим конфигурации интерфейса
Руководство по использованию	Если настройка агрегированного маршрута выполняется в режиме маршрутизации, протокол RIPng должен быть включен. При выполнении настройки в режиме конфигурации интерфейса, протокол RIPng может быть выключен, но агрегированная маршрутизация начнет работать, только если протокол RIPng включен на интерфейсе
Пример	Switch(config)#router ipv6 rip Switch(config-router)#ipv6 rip agg 2001:3f:ed8::99/64



16.4.10. Расщепление горизонта (ipv6 rip split-horizon)

Команда	ipv6 rip split-horizon [poisoned] no ipv6 rip split-horizon Выполняет расщепление горизонта. Команда “no ipv6 rip split-horizon” отменяет расщепление
Параметр	[poisoned] создает разделенный горизонт с блокировкой сбойного маршрута
По умолчанию	Разделенный горизонт с блокировкой сбойного маршрута
Режим	Режим конфигурации интерфейса
Руководство по использованию	Расщепление горизонта — это метод предотвращения петли маршрутизации в сети, а именно для предотвращения трансляции маршрута коммутатором уровня 3 на интерфейс, с которого этот маршрут был получен. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Switch#config terminal Switch(config)#interface Vlan1 Switch(Config-if-Vlan1)#ipv6 rip split-horizon poisoned
Команда	ipv6 rip split-horizon [poisoned] no ipv6 rip split-horizon Выполняет расщепление горизонта. Команда “no ipv6 rip split-horizon” отменяет расщепление
Параметр	[poisoned] создает разделенный горизонт с блокировкой сбойного маршрута
По умолчанию	Разделенный горизонт с блокировкой сбойного маршрута
Режим	Режим конфигурации интерфейса
Руководство по использованию	Расщепление горизонта — это метод предотвращения петли маршрутизации в сети, а именно для предотвращения трансляции маршрута коммутатором уровня 3 на интерфейс, с которого этот маршрут был получен. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен



Пример	<pre>Switch#config terminal Switch(config)#interface Vlan1 Switch(Config-if-Vlan1)#ipv6 rip split-horizon poisoned</pre>

16.4.11. Включение маршрутизации RIPng на интерфейсе (ipv6 router rip)

Команда	<pre>ipv6 router rip no ipv6 router rip</pre> Подключает маршрутизацию RIPng на интерфейсе. Команда “no ipv6 router rip” отключает RIPng на интерфейсе
Параметр	-
По умолчанию	Не сконфигурировано
Режим	Режим конфигурации интерфейса
Руководство по использованию	Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	<pre>Switch#config terminal Switch(config)#interface Vlan1 Switch(Config-if-Vlan1)#ipv6 router rip</pre>

16.4.12. Указание соседнего маршрутизатора (neighbor)

Команда	<pre>neighbor <ipv6-address> {<ifname> vlan <vlan-id>} no neighbor <ipv6-address> {<ifname> vlan <vlan-id>}</pre> Задаёт адрес назначения для фиксированной отправки. Команда “no neighbor <ipv6-address> <ifname> vlan <vlan-id>” отменяет определение указанного адреса и восстанавливает все доверенные шлюзы
Параметр	<ipv6-address> это IPv6 Link-local адрес для отправки, в шестнадцатеричном формате без длины префикса. <ifname> имя интерфейса
По умолчанию	Отправка на какой-либо фиксированный адрес назначения не выполняется
Режим	Режим маршрутизации



Руководство по использованию	При использовании в сочетании с командой конфигурации маршрутизатора "passive-interface", информация о маршрутизации направляется только указанным соседям
Пример	<pre>Switch#config terminal Switch(config)#router ipv6 rip Switch(config-router)#neighbor FE80:506::2 Vlan1</pre>

16.4.13. Смещения к входящим и исходящим метрикам (offset-list)

Команда	<pre>offset-list <access-list-number access-list-name> {in out }<number> [<ifname>] vlan <vlan-id>] no offset-list <access-list-number access-list-name> {in out }<number> [<ifname>] vlan <vlan-id>]</pre> Команда указывает значение смещения, которое добавляется к метрике маршрутизации, полученной RIPv6. Команда "no offset-list <access-list-number access-list-name> {in out} <number> [<ifname>]vlan <vlan-id>]" отключает функцию
Параметр	< access-list-number access-list-name> список доступа или имя, которое должно быть применено. <number> значение смещения для метрик, диапазон от 1 до 16; <ifname> имя интерфейса
По умолчанию	Значение смещения по умолчанию - это значение метрики интерфейса, определенное системой
Режим	Режим конфигурации маршрутизатора
Руководство по использованию	-
Пример	<pre>Switch#config terminal Switch(config)#router ipv6 rip Switch(config-router)#offset-list 1 in 5 Vlan1</pre>



16.4.14. Отключение отправки обновлений маршрутизации (passive-interface)

Команда	passive-interface[<ifname> vlan <vlan-id>] no passive-interface[<ifname> vlan <vlan-id>] Блокирует отправку коммутатором уровня 3 RIPv6 широковещательных сообщений RIPv6 на указанном интерфейсе и выполняет отправку пакетов данных RIPv6 только тому коммутатору уровня 3, который указан как соседний
Параметр	<ifname> имя конкретного интерфейса
По умолчанию	Не сконфигурировано
Режим	Режим конфигурации маршрутизатора
Руководство по использованию	-
Пример	<pre>Switch#config terminal Switch(config)#router ipv6 rip Switch(config-router)#passive-interface Vlan1</pre>

16.4.15. Перераспределение информации о маршрутизации из других протоколов (redistribute)

Команда	redistribute {kernel connected static ospf isis bgp} [metric<value>] [route-map<word>] no redistribute {kernel connected static ospf isis bgp} [metric<value>] [route-map<word>] Вводит в RIPv6 маршруты, полученные из других протоколов маршрутизации
Параметр	kernel задается из маршрутов ядра connected задается из прямых подключенных маршрутов static задается из статических маршрутов ospf из маршрутов IPv6 OSPF isis из маршрутов IPv6 ISIS bgp из маршрутов IPv6 BGP <value> значение метрики, назначаемое объявляемому маршруту, в диапазоне от 0 до 16 <word> указатель на карту маршрутов для задаваемых маршрутов
По умолчанию	-
Режим	Режим конфигурации маршрутизатора



Руководство по использованию	-
Пример	<pre>Switch#config terminal Switch(config)#router ipv6 rip Switch(config-router)#redistribute kernel route-map ipi</pre>

16.4.16. Перераспределение в OSPF (redistribute ospf)

Команда	<pre>redistribute ospf [<process-tag>] [metric<value>] [route-map<word>] no redistribute ospf [<process-tag>]</pre> Команда задает перераспределение информации о маршрутизации из внешних процессов OSPFv3 в процесс RIPng. "no" в начале команды удалит внесенные записи о маршрутизации OSPFv3
Параметр	process-tag строка тега для процесса OSPFv3 длиной не более 15 символов. Если не указан, будет использоваться процесс по умолчанию. metric <value> метрика для введенных записей маршрутизации, ограничена между 0 и 16. route-map <word> указатель на введенную карту маршрутизации
По умолчанию	Перераспределение не выполняется
Режим	Режим конфигурации RIPng
Руководство по использованию	-
Пример	Перераспределить маршрутизацию OSPFv3 ABC в RIPng. <pre>Switch(config)#router ipv6 rip Switch(config-router)#redistribute ospf abc</pre>

16.4.17. Маршрут (route)

Команда	<pre>route <ipv6-address> no route <ipv6-address></pre> Эта команда настраивает статический маршрут RIPng. Команда "no route <ipv6-address>" удаляет маршрут
Параметр	<ipv6-address> префикс IPv6-адреса назначения и его длину в шестнадцатеричной системе с двоеточием
По умолчанию	-



Режим	Режим конфигурации маршрутизатора
Руководство по использованию	Команда добавляет статический маршрут RIPng и используется в основном для отладки. Маршруты, сконфигурированные этой командой, будут отображаться не в таблице kernel маршрутов, а в базе данных маршрутов RIPng, однако их можно найти с помощью команды "show ipv6 rip"
Пример	Switch#config terminal Switch(config)#router ipv6 rip Switch(config-router)#route 3ffe: 1234: 5678: : 1/64

16.4.18. Включение процесса маршрутизации RIPng (router ipv6 rip)

Команда	router ipv6 rip no router ipv6 rip Команда обеспечивает включение процесса маршрутизации RIPng и вход в режим RIPng. Команда "no router ipv6 rip" отключает протокол маршрутизации RIPng
Параметр	
По умолчанию	Маршрутизация RIPng не запущена
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда предназначена для включения протокола маршрутизации RIPng, ее необходимо задействовать до выполнения других глобальных настроек протокола RIPng
Пример	Включите режим протокола RIPng. Switch(config)#router ipv6 rip

16.4.19. Просмотр статуса для событий и пакетов RIPng (show debugging ipv6 rip)

Команда	show debugging ipv6 rip Отображает состояние отладки RIPng для следующих опций отладки: отладка nsm, отладка событий RIPng, отладка пакетов RIPng и отладка RIPng nsm
Параметр	
По умолчанию	-



Режим	Привилегированный режим
Руководство по использованию	-
Пример	Switch#show debugging ipv6 rip RIPng debugging status: RIPng event debugging is on RIPng packet send detail debugging is on RIPng NSM debugging is on

16.4.20. Просмотр информации об интерфейсах RIPng (show ipv6 rip interface)

Команда	show ipv6 rip interface Подтверждение рабочего состояния интерфейса и протоколов линии связи	
Параметр		
По умолчанию	-	
Режим	Привилегированный режим	
Руководство по использованию	-	
Пример	Switch(config)#show ipv6 rip interface Loopback is up, line protocol is up RIPng is not enabled on this interface Vlan1 is up, line protocol is up Routing Protocol: RIPng Passive interface: Disabled Split horizon: Enabled with Poisoned Reversed IPv6 interface address: 3000: 1: 1: : 1/64 fe80: : 203: fff: fe0c: cda/64	
	Информация, отображаемая на экране	Пояснение
	Vlan1 is up, line protocol is up	Интерфейс работает



	Routing Protocol: RIP	На интерфейсе запущен протокол маршрутизации RIPv6
	Passive interface: Disabled	Пассивный интерфейс отключен
	Split horizon: Enabled with Poisoned Reversed	На интерфейсе включено разделение горизонта с блокировкой сбойного маршрута
	IP interface address: 3000: 1: 1: : 1/64 fe80: : 203: fff: fe01: 429e/64	IPv6-адрес интерфейса

16.4.21. Просмотр настроек перераспределения (show ipv6 rip redistribute)

Команда	show ipv6 rip redistribute Отображает информацию о настройках для перераспределения других выходных маршрутов в RIPv6
Параметр	-
По умолчанию	Не выводится
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Switch#show ipv6 rip redistribute

16.4.22. Просмотр таблицы маршрутизации RIPv6 (show ipv6 protocols rip)

Команда	show ipv6 protocols rip
Параметр	-
По умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Switch(config)#show ipv6 protocols rip Routing Protocol is "rIPv6"



	Sending updates every 30 seconds with +/-50%, next due in 1 seconds Timeout after 180 seconds, garbage collect after 120 seconds Outgoing update filter list for all interface is not set Incoming update filter list for all interface is not set Ethernet1/4 filtered by dclist Default redistribute metric is 1 Redistributing: static Interface Vlan10 Vlan2 Routing for Networks:	
	Информация, отображаемая на экране	Пояснение
	Sending updates every 30 seconds with +/-50%, next due in 1 seconds	Отправка обновлений каждые 30 секунд
	Timeout after 180 seconds, garbage collect after 120 seconds	Таймаут маршрутизации составляет 180 секунд, а время сбора мусора - 120 секунд
	Outgoing update filter list for all interface is not set	Список фильтров исходящих обновлений для всех интерфейсов не задан
	Incoming update filter list for all interface is not set	Список фильтров входящих обновлений для всех интерфейсов не задан
	Default redistribution metric is 1	Метрика перераспределения по умолчанию равна 1
	Redistributing: static	Перераспределение статического маршрута в маршруты RIP
	Interface Vlan10 Vlan2	Интерфейсами, на которых работает RIP, являются Vlan 10 и Vlan 2

16.4.23. Просмотр маршрутов RIP (show ipv6 rip)

Команда	show ipv6 rip Команда предназначена для отображения маршрутов RIPv6
Параметр	-
По умолчанию	-
Режим	Привилегированный режим



Руководство по использованию	-																														
Пример	Switch#show ipv6 rip Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP, a - aggregate, s - suppressed <table><thead><tr><th>Network</th><th>Next Hop</th><th>If</th><th>Met</th><th>Tag</th><th>Time</th></tr></thead><tbody><tr><td>1: : /64</td><td>::</td><td>Vlan2</td><td>1</td><td></td><td>0</td></tr><tr><td>R 2001: 1: 1: : /64</td><td>fe80: : 203: fff: fe01: 257c</td><td>Vlan2</td><td>2</td><td></td><td>0 02: 40</td></tr><tr><td>R 3000: 1: 1: : /64</td><td>::</td><td>Vlan10</td><td>1</td><td>0</td><td></td></tr><tr><td>R 3010: 1: 1: : /64</td><td>::</td><td>--</td><td>1</td><td>0</td><td></td></tr></tbody></table> Где R обозначает RIP-маршрут, а именно маршрут RIP с сетевым адресом назначения 2001:1:1::/64, адресом следующего узла fe80::203:fff:fe01:257c. Получен из Ethernet-порта VLAN2 со значением метрики 2, и у него еще есть 2 минуты 40 секунд до истечения времени	Network	Next Hop	If	Met	Tag	Time	1: : /64	::	Vlan2	1		0	R 2001: 1: 1: : /64	fe80: : 203: fff: fe01: 257c	Vlan2	2		0 02: 40	R 3000: 1: 1: : /64	::	Vlan10	1	0		R 3010: 1: 1: : /64	::	--	1	0	
Network	Next Hop	If	Met	Tag	Time																										
1: : /64	::	Vlan2	1		0																										
R 2001: 1: 1: : /64	fe80: : 203: fff: fe01: 257c	Vlan2	2		0 02: 40																										
R 3000: 1: 1: : /64	::	Vlan10	1	0																											
R 3010: 1: 1: : /64	::	--	1	0																											

16.4.24. Просмотр информации о базе данных IPv6 RIP (show ipv6 rip database)

Команда	<pre>show ipv6 rip database</pre> Выводит сообщения, связанные с базой данных RIPng
Параметр	-
По умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	-
Пример	<pre>Switch#show ipv6 rip database</pre>

16.4.25. Просмотр агрегирования (show ipv6 rip aggregate)

Команда	<pre>show ipv6 rip aggregate</pre> Выводит информацию об агрегированных маршрутах IPv6
Параметр	-
По умолчанию	-
Режим	Привилегированный режим



Руководство по использованию	Эта команда используется для отображения интерфейса, в котором настроен маршрут агрегации, параметры Metric, Count, Suppress и т.д. Если он настроен в глобальном режиме, отображается “ ”. “Metric” это метрика. “Count” - количество изученных агрегированных маршрутов. “Suppress” периодичность агрегирования																																			
Пример	Вывести на экран информацию о агрегированном маршруте IPv6. <pre>Switch(config-router)#show ipv6 rip agg</pre> Aggregate information of ripng <table><tr><th>Network</th><th>Aggregated</th><th>Ifname</th><th>Metric</th><th>Count</th><th>Suppress</th><th>2001: : /16</th></tr><tr><td>Vlan1</td><td>1</td><td></td><td>2</td><td></td><td>0</td><td></td></tr><tr><td>2001: 1: : /32</td><td>----</td><td>1</td><td>2</td><td>0</td><td></td><td></td></tr><tr><td>2001: 1: 2: : /60</td><td></td><td>Vlan1</td><td>1</td><td>1</td><td></td><td></td></tr><tr><td>----</td><td>1</td><td>1</td><td>1</td><td></td><td></td><td></td></tr></table>	Network	Aggregated	Ifname	Metric	Count	Suppress	2001: : /16	Vlan1	1		2		0		2001: 1: : /32	----	1	2	0			2001: 1: 2: : /60		Vlan1	1	1			----	1	1	1			
Network	Aggregated	Ifname	Metric	Count	Suppress	2001: : /16																														
Vlan1	1		2		0																															
2001: 1: : /32	----	1	2	0																																
2001: 1: 2: : /60		Vlan1	1	1																																
----	1	1	1																																	

16.4.26. Настройка таймеров маршрутизации RIPng (timers basic)

Команда	timers basic <update> <invalid> <garbage> no timers basic Команда позволяет задать время обновления, тайм-аута и сбора мусора таймера RIP. Команда “no timers basic” восстанавливает значение по умолчанию для каждого параметра
Параметр	<update> интервал отправки пакета обновления, указывается в секундах в диапазоне от 5 до 2147483647; <invalid> период времени, по истечении которого маршрут RIP объявляется недоступным, указывается в секундах в диапазоне от 5 до 2147483647; <garbage> время удержания, в течение которого маршрут остается в таблице маршрутизации после объявления о его недоступности, указывается в секундах в диапазоне от 5 до 2147483647;
По умолчанию	<update> по умолчанию равен 30; <invalid> по умолчанию равен 180; <garbage> по умолчанию 120
Режим	Режим конфигурации маршрутизатора
Руководство по использованию	По умолчанию система транслирует пакеты обновлений RIPng каждые 30 секунд; маршрут считается недействительным через 180 секунд, но продолжает существовать еще 120 секунд, прежде чем будет удален из таблицы маршрутизации



Пример	Установить время обновления RIP на 20 секунд и период тайм-аута на 80 секунд, время сбора мусора на 60 секунд. <pre>Switch(config)#router ipv6 rip Switch(config-router)#timers basic 20 80 60</pre>

16.5. Команды OSPFV3

16.5.1. Стоимость маршрута по умолчанию (area default-cost)

Команда	area <id> default-cost <cost> no area <id> default-cost Предназначена для указания стоимости суммарного маршрута по умолчанию, отправляемого в тупиковую область или область NSSA. Команда “no area <id> default-cost” восстанавливает значение по умолчанию
Параметр	<id> идентификатор области. Задается в формате IP-адреса или целого числа в диапазоне от 0 до 4294967295; <cost>стоимость маршрута. Диапазон <0-16777215>
По умолчанию	Стоимость OSPFv3 равна 1
Режим	Режим конфигурации OSPFv3
Руководство по использованию	Команда только на граничном маршрутизаторе области (ABR), который подключен к тупиковой области
Пример	Установите стоимость по умолчанию для области 1 на 10 <pre>Switch(config)#router ipv6 ospf Switch(config-router)#area 1 default-cost 10</pre>

16.5.2. Настройка диапазона адресов OSPF (area range)

Команда	area <id> range <ipv6address> [advertise not-advertise] no area <id> range < ipv6address> Эта команда суммирует OSPF маршруты на границе области. Команда “no area <id> range <address>” отключает данную функцию
Параметр	<id>номер области, задается в формате числа в диапазоне от 0 до 4294967295 или IPv4-адреса <ipv6address>=<X: X: X: X/M>, указывает префикс ipv6-сети области и его длину; advertise: указание анонсировать в другие области not-advertise: указание не анонсировать в другие области



	Если оба параметра не заданы, эта область по умолчанию будет анонсироваться
По умолчанию	Функция не настроена
Режим	Режим конфигурации OSPFv3
Руководство по использованию	Команда суммирует маршруты внутри области. Если идентификаторы сетей в области назначаются таким образом, что они являются смежными, данная команда конфигурирует ABR для анонсирования сводного маршрута. Этот маршрут состоит из всех отдельных сетей, принадлежащих к определенному диапазону. Этот маршрут состоит из всех отдельных сетей, принадлежащих к определенному диапазону
Пример	Switch #config terminal Switch (config)# router ipv6 ospf Switch (config-router)# area 1 range 2000: : /3

16.5.3. Задание тупиковой области OSPF (area stub)

Команда	area <id> stub [no-summary] no area <id> stub [no-summary] Команда определяет область как тупиковую. Команда "no area <id> stub [no-summary]" отменяет данную функцию
Параметр	<id>номер области, задается в формате числа в диапазоне от 0 до 4294967295 или IPv4-адреса. no-summary: пограничный маршрутизатор прекращает отправку объявлений в тупиковую область
По умолчанию	Не определена
Режим	Режим конфигурации OSPFv3
Руководство по использованию	Данную команду необходимо применить на всех маршрутизаторах, имеющих доступ к тупиковой области. Существуют две команды конфигурации маршрутизатора в тупиковой области: "stub" и "default-cost". Для всех маршрутизаторов, подключенных к тупиковой области, область должна быть настроена с использованием команды "area stub". Ключевое слово "default-cost" следует использовать только на маршрутизаторе ABR, подключенном к тупиковой области
Пример	Switch # config terminal Switch (config)# router ipv6 ospf Switch (config-router)# area 1 stub



16.5.4. Создание виртуального соединения для обмена LSA (area virtual-link)

Команда	<pre>area <id> virtual-link A.B.C.D [instance-id <instance-id> INTERVAL <value>] no area <id> virtual-link A.B.C.D [instance-id <instance-id> INTERVAL]</pre> Позволяет настроить логическую связь между двумя магистральными областями, разделенными не магистральной областью. Команда “no area <id> virtual-link A.B.C.D [instance-id <instance-id> INTERVAL]” удаляет виртуальную связь
Параметр	<id> номер области, задается в формате числа в диапазоне от 0 до 4294967295 или IPv4-адреса. <instance-id> идентификатор экземпляра интерфейса в диапазоне 0~255, по умолчанию 0. INTERVAL= [dead-interval hello-interval retransmit-interval transmit-delay] <value>: задержка или интервал в секундах, в диапазоне 1~65535 <dead-interval> : интервал, в течение которого пакеты сообщений не принимаются и по истечении которого, соседний маршрутизатор считается отключенным от сети, по умолчанию 40 секунд. <hello-interval> : интервал перед отправкой маршрутизатором пакета сообщений hello, по умолчанию 10 секунд. <retransmit-interval> : интервал перед повторной передачей маршрутизатором пакета сообщений, по умолчанию 5 секунд <transmit-delay> : время задержки перед отправкой маршрутизатором сообщения, по умолчанию 1 секунда
По умолчанию	Конфигурация по умолчанию отсутствует
Режим	Режим конфигурации OSPFv3
Руководство по использованию	В топологии OSPF все области должны граничить с магистральной областью. Если соединение с магистральной областью будет потеряно, виртуальный канал восстановит это соединение. Можно настроить виртуальную связь между любыми двумя маршрутизаторами магистральных областей, соединенными с публичной не магистральной областью. Протокол рассматривает маршрутизаторы, соединенные виртуальными каналами, как сеть в режиме точка-точка (неблокирующий обмен)
Пример	<pre>Switch#config terminal Switch(config) #router ipv6 ospf Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20 Switch(config-router) #area 1 virtual-link 10.10.11.50 instance-id 1</pre>



16.5.5. Модели пограничного маршрутизатора (abr-type)

Команда	abr-type {cisco ibm standard} no abr-type [cisco ibm standard] Команда указывает тип пограничного маршрутизатора в OSPF. Команда "no abr-type [cisco ibm standard]" восстанавливает значение по умолчанию. Команда "no abr-type [cisco ibm standard]" восстанавливает значение по умолчанию
Параметр	ciscoo, ABR с использованием реализации Cisco; ibm, ABR с использованием реализации IBM; shortcut, ABR с короткими путями; standard, Стандартный ABR (RFC2328)
По умолчанию	Cisco применяется по умолчанию
Режим	Режим конфигурации OSPFv3
Руководство по использованию	Используйте эту команду для указания типа пограничного маршрутизатора. Эта команда подходит для взаимодействия между различными протоколами OSPF, особенно в среде с несколькими хостами
Пример	Настроить стандартный ABR. Switch#config terminal Switch(config)#router ipv6 ospf Switch(config-router)#abr-type standard

16.5.6. Метрики для перераспределённых маршрутов (default-metric)

Команда	default-metric <value> no default-metric Команда устанавливает значение метрики по умолчанию для протокола маршрутизации OSPF. Команда "no default-metric" возвращает состояние по умолчанию
Параметр	<value>, значение метрики в диапазоне от 1 до 16777214
По умолчанию	Встроенный автоматический перевод значений метрики
Режим	Режим конфигурации OSPFv3
Руководство по использованию	Метрика по умолчанию упрощает обработку несовместимых метрик и обеспечивает маршрутизацию. Если метрику невозможно конвертировать, то эта метрика по умолчанию используется вместо нее. Эта команда обеспечивает применение одного и того же значения



	метрики всеми входящими маршрутами. Используйте эту команду совместно с командой "redistribute"
Пример	Switch#config terminal Switch(config)#router ipv6 ospf Switch(config-router)#default-metric 100

16.5.7. Параметры отладки событий OSPF (debug ipv6 ospf events)

Команда	[no]debug ipv6 ospf events [abr asbr os router vlink] Команда позволяет вывести отладочную информацию для событий OSPF. Команда "no debug ipv6 ospf events [abr asbr os router vlink]" закрывает отладку
Параметр	
По умолчанию	Закреты
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Switch#debug ipv6 ospf events 1970/01/01 01: 10: 35 IMI: ROUTER[Process: (null)]: GC timer expire

16.5.8. Параметры отладки состояний IFSM в OSPF (debug ipv6 ospf ifsm)

Команда	[no]debug ipv6 ospf ifsm [status events timers] Команда позволяет вывести отладочную информацию, связанную с состояниями интерфейса в OSPF. Команда "[no] debug ospf ifsm [status events timers]" закрывает параметры отладки
Параметр	
По умолчанию	Закреты
Режим	Привилегированный режим
Руководство по использованию	-



Пример	<pre>Switch#debug ipv6 ospf ifsm 1970/01/01 01: 11: 44 IMI: IFSM[Vlan1]: Hello timer expire 1970/01/01 01: 11: 44 IMI: IFSM[Vlan2]: Hello timer expire</pre>

16.5.9. Параметры отладки для LSA (debug ipv6 ospf lsa)

Команда	<pre>[no]debug ipv6 ospf lsa [generate flooding install maxage refresh]</pre> Команда открывает параметры отладки для объявлений о состоянии канала связи. Команда “no debug ospf lsa [generate flooding install maxage refresh]” закрывает параметры отладки
Параметр	Закрыты
По умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	-
Пример	-

16.5.10. Параметры отладки состояний NFSM в OSPF (debug ipv6 ospf nfsm)

Команда	<pre>[no]debug ipv6 ospf nfsm [status events timers]</pre> Команда позволяет вывести отладочную информацию, показывающую состояние конечного автомата соседей OSPF. Команда “no debug ipv6 ospf nfsm [status events timers]” закрывает отладку
Параметр	Закрыты
По умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	-
Пример	<pre>Switch#debug ipv6 ospf nfsm 1970/01/01 01: 14: 07 IMI: NFSM[192.168.2.3-000007d4]: LS update timer expire 1970/01/01 01: 14: 07 IMI: NFSM[192.168.2.1-000007d3]: LS update timer expire</pre>



	1970/01/01 01: 14: 08 IMI: NFSM[192.168.2.1-000007d3]: Full (HelloReceived) 1970/01/01 01: 14: 08 IMI: NFSM[192.168.2.1-000007d3]: nfsm_ignore called 1970/01/01 01: 14: 08 IMI: NFSM[192.168.2.1-000007d3]: Full (2-WayReceived)

16.5.11. Параметры отладки состояний NSM в OSPF (debug ipv6 ospf nsm)

Команда	[no]debug ipv6 ospf nsm [interface redistribute] Команда позволяет вывести отладочную информацию, показывающую NSM в OSPF. Команда “no debug ipv6 ospf nsm [interface redistribute]” закрывает режим отладки
Параметр	
По умолчанию	Закреты
Режим	Привилегированный режим
Руководство по использованию	-
Пример	

16.5.12. Параметры отладки для обмена пакетами (debug ipv6 ospf packet)

Команда	[no]debug ipv6 ospf packet [dd detail hello ls-ack ls-request ls-update recv send] Команда позволяет вывести отладочную информацию для пакетов OSPF. Команда “no debug ipv6 ospf packet [dd detail hello ls-ack ls-request ls-update recv send]” закрывает отладку
Параметр	
По умолчанию	Закреты
Режим	Привилегированный режим
Руководство по использованию	-



Пример	

16.5.13. Параметры отладки отправленных сообщений перераспределения (debug ipv6 ospf redistribute message send)

Команда	debug ipv6 ospf redistribute message send no debug ipv6 ospf redistribute message send Команда включает/выключает параметры отладки отправки команд из процесса IPv6 OSPF, перераспределенного в другие процессы маршрутизации IPv6 OSPF
Параметр	-
По умолчанию	Функция выключена
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Switch#debug ipv6 ospf redistribute message send

16.5.14. Параметры отладки полученных сообщений о перераспределении маршрута (debug ipv6 ospf redistribute route receive)

Команда	debug ipv6 ospf redistribute route receive no debug ipv6 ospf redistribute route receive Команда подключает и отключает отладку полученных сообщений маршрутизации от NSM для процесса IPv6 OSPF
Параметр	-
По умолчанию	Функция выключена
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Switch#debug ipv6 ospf redistribute route receive



16.5.15. Параметры отладки событий IPv6 маршрутизации (debug ipv6 ospf route)

Команда	[no]debug ipv6 ospf route [ase ia install spf] Позволяет вывести отображение отладочной информации, связанной с соответствующими маршрутами в OSPF. Команда "[no]debug ipv6 ospf route [ase ia install spf]" закрывает отладку
Параметр	-
По умолчанию	Закрываются
Режим	Привилегированный режим
Руководство по использованию	-
Пример	

16.5.16. Стоимость отправки пакета на интерфейсе (ipv6 ospf cost)

Команда	ipv6 ospf cost <cost> [instance-id <id>] no ipv6 ospf cost [instance-id <id>] Команда указывает стоимость отправки для работы протокола OSPF на интерфейсе. Команда "no ipv6 ospf cost [instance-id <id>]" восстанавливает значение по умолчанию
Параметр	<id> идентификатор экземпляра интерфейса в диапазоне от 0 до 255, по умолчанию задан 0. <cost > значение стоимости протокола OSPF, диапазон от 1 до 65535
По умолчанию	Стоимость OSPF по умолчанию равна 10
Режим	Режим конфигурации интерфейса
Руководство по использованию	Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 ospf cost 3



16.5.17. Интервал ожидания отклика до объявления соседнего устройства недоступным (ipv6 ospf dead-interval)

Команда	ipv6 ospf dead-interval <time > [instance-id <id>] no ipv6 ospf dead-interval [instance-id <id>] Задаёт интервал ожидания от соседних коммутаторов уровня 3. Команда "no ipv6 ospf dead-interval [instance-id <id>]" восстанавливает значение по умолчанию
Параметр	<id> идентификатор экземпляра интерфейса в диапазоне 0~255, по умолчанию 0. <time > интервал (в секундах), в течение которого маршрутизатор 3 уровня должен получить отклик, в диапазоне 1 ~ 65535
По умолчанию	Интервал по умолчанию — 40 секунд (4 интервала отправки hello-пакетов)
Режим	Режим конфигурации интерфейса
Руководство по использованию	Если по истечении "dead-interval" не получено ни одного пакета HELLO, данный коммутатор 3 уровня считается недоступным и недействительным. Данная команда используется для установки интервала "dead" соседних коммутаторов уровня 3, в соответствии с фактическим состоянием соединения. Задаваемое значение "dead-interval" передается в пакетах Hello. Для обеспечения нормальной работы протокола OSPF "dead-interval" между соседними коммутаторами уровня 3 должен соответствовать значению отправки hello пакетов или быть равным 4-м интервалам отправки hello-пакетов. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 ospf dead-interval 80

16.5.18. Отобразить данные о каждом маршруте в одной строке (ipv6 ospf display route single-line)

Команда	[no] ipv6 ospf display route single-line Команда "show ipv6 ospf route" меняет отображение выводов команды "show ipv6 ospf route". Команда "no ipv6 ospf display route single-line" восстанавливает отображение по умолчанию
Параметр	-



По умолчанию	Не сконфигурировано
Режим	Режим глобальной конфигурации
Руководство по использованию	Команда "show ipv6 ospf route" отображает один и тот же маршрут в нескольких строках. Данная команда позволяет вывести данные одной строкой
Пример	Switch#config terminal Switch(config)#ipv6 ospf display route single-line

16.5.19. Задать интервал между пакетами hello (ipv6 ospf hello-interval)

Команда	ipv6 ospf hello-interval <time> [instance-id <id>] no ipv6 ospf hello-interval [instance-id <id>] Указывает интервал отправки пакетов hello на интерфейсе. Команда "no ipv6 ospf hello-interval [instance-id <id>]" восстанавливает значение по умолчанию
Параметр	<id> идентификатор экземпляра интерфейса в диапазоне 0~255, по умолчанию 0. <time> интервал (в секундах), в течение которого маршрутизатор 3 уровня должен получить отклик, в диапазоне 1~ 65535
По умолчанию	Интервал отправки пакетов HELLO по умолчанию 10 секунд
Режим	Режим конфигурации интерфейса
Руководство по использованию	Пакет данных HELLO является наиболее распространенным пакетом, который периодически отправляется на соседний коммутатор уровня 3 для обнаружения и поддержания отношений смежности, выбора DR и BDR. Пользовательское значение "hello-interval" передается в пакетах HELLO. Чем меньше интервал hello, тем быстрее будут обнаружены топологические изменения, но это приведет к увеличению трафика маршрутизации. Для обеспечения нормальной работы протокола OSPF параметр "hello-interval" между соседними с интерфейсом коммутаторами уровня 3 должен быть одинаковым. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 ospf hello-interval 20



16.5.20. Приоритет маршрутизатора для определения назначенного маршрутизатора (ipv6 ospf priority)

Команда	<code>ipv6 ospf priority <priority> [instance-id <id>] no ipv6 ospf priority [instance-id <id>]</code> Команда задает приоритет маршрутизатора для определения “Defined layer 3 switch” назначенного коммутатора уровня 3 на интерфейсе. Команда “no ipv6 ospf [<ip-address>] priority” восстанавливает значения по умолчанию
Параметр	<id> идентификатор экземпляра интерфейса в диапазоне 0~255, по умолчанию 0. <priority> приоритет, допустимое значение которого находится в диапазоне 0~255
По умолчанию	Приоритет по умолчанию при выборе DR - 1
Режим	Режим конфигурации интерфейса
Руководство по использованию	Когда два маршрутизатора, подключенные к одному сегменту сети, пытаются стать назначенными маршрутизаторами, предпочтение отдается тому, у которого выше приоритет. Как правило выбирается маршрутизатор с более высоким приоритетом, но, если для двух маршрутизаторов приоритет одинаковый, предпочтение отдается маршрутизатору с более высоким ID маршрутизатора. Маршрутизатор уровня 3 с приоритетом равным 0, не может стать назначенным маршрутизатором “Defined layer 3 switch” или резервным назначенным маршрутизатором “Backup Defined layer 3 switch”. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Настроить приоритет выбора DR. Настроить интерфейс vlan 1 на отсутствие права выбора, а именно задать приоритет 0. <pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 ospf priority 0</pre>

16.5.21. Интервал между повторными передачами пакетов обновлений состояния канала связи (ipv6 ospf retransmit-interval)

Команда	<code>ipv6 ospf retransmit-interval <time> [instance-id <id>] no ipv6 ospf retransmit-interval [instance-id <id>]</code> Задает интервал повторной передачи объявлений о состоянии соединения между интерфейсом и соседними коммутаторами уровня 3. Команда “no ipv6 ospf retransmit-interval [instance-id <id>]” восстанавливает значение по умолчанию



Параметр	<id> идентификатор экземпляра интерфейса в диапазоне 0~255, по умолчанию 0. <time>интервал повторной передачи объявлений о состоянии соединения между интерфейсом и соседними коммутаторами уровня 3, указывается в секундах и находится в диапазоне 1~65535
По умолчанию	Интервал повторной передачи по умолчанию составляет 5 секунд
Режим	Режим конфигурации интерфейса
Руководство по использованию	Когда коммутатор уровня 3 передает LSA соседу, он сохраняет объявление о состоянии соединения до тех пор, пока не получит подтверждение от адресата. Если в течение этого интервала времени пакет подтверждения не получен, LSA передается повторно. Интервал повторной передачи должен быть больше, чем время, необходимое для одного раунда передачи между двумя коммутаторами уровня 3. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Задать интервал повторной передачи LSA для интерфейса vlan 1 в 10 секунд. <pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 ospf retransmit-interval 10</pre>

16.5.22. Предполагаемое время для отправки пакета LSA (ipv6 ospf transmit-delay)

Команда	ipv6 ospf transmit-delay <time> [instance-id <id>] no ipv6 ospf transmit-delay [instance-id <id>] Задаёт время задержки отправки LSA на интерфейсе. Команда "no ipv6 ospf transmit-delay [instance-id <id>]" восстанавливает значение по умолчанию
Параметр	<id> идентификатор экземпляра интерфейса в диапазоне 0~255, по умолчанию 0. <time>время задержки отправки LSA на интерфейс, которое указывается в секундах и находится в диапазоне 1~65535
По умолчанию	По умолчанию время задержки отправки LSA на интерфейс составляет 1 секунду
Режим	Режим конфигурации интерфейса



Руководство по использованию	В LSA-пакете время жизни пакета должно быть увеличено на значение, указанное в параметрах для коммутатора уровня 3, но до процесса передачи. Поэтому необходимо добавить задержку передачи перед отправкой LSA, чтобы гарантировать, что LSA будет отправлен. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен
Пример	Установить задержку отправки LSA интерфейса vlan 1 на 3 секунды. Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 ospf transmit-delay 3

16.5.23. Разрешение процесса OSPFv3 на интерфейсе (ipv6 router ospf)

Команда	<code>[no] ipv6 router ospf {area <area-id> [instance-id <instance-id> tag <tag> [instance-id <instance-id>]] tag <tag> area <area-id> [instance-id <instance-id>]}</code> Включает процесс маршрутизации ospf на интерфейсе. Команда “no ipv6 router ospf {area <area-id>[instance-id <instance-id>]} tag <tag>[instance-id <instance-id>]} tag <tag> area <area-id> [instance-id <instance-id>]}” отменяет настройку
Параметр	<area-id>это идентификатор области, который может быть представлен в виде цифр в диапазоне 0 ~ 4294967295, или как IPv4-адрес <instance-id> идентификатор экземпляра интерфейса в диапазоне 0~255, по умолчанию 0. <tag> идентификатор процесса ospfv3
По умолчанию	Не сконфигурировано
Режим	Режим конфигурации интерфейса
Руководство по использованию	Чтобы включить эту команду на интерфейсе, необходимо настроить идентификатор области. Идентификатор экземпляра и метка экземпляра являются необязательными. Процесс ospfv3 допускает один экземпляр маршрутизации для каждого идентификатора экземпляра. Маршрут может быть включен на интерфейсе с идентификатором экземпляра. Если идентификаторы экземпляров разные, на одном интерфейсе может быть запущено несколько процессов OSPF. Однако разные процессы OSPF не должны использовать один и тот же ID экземпляра. Эту команду можно настроить на туннельном интерфейсе IPv6, но она будет успешной только в том случае, если туннель тщательно настроен



Пример	<pre>Switch#config terminal Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 router ospf area 1 tag IPI instance-id 1</pre>

16.5.24. Максимальное количество одновременно обрабатываемых сообщений обмена базами данных (max-concurrent-dd)

Команда	<pre>max-concurrent-dd <value> no max-concurrent-dd</pre> Команда устанавливает максимальное количество обрабатываемых пакетов Database Descriptor (DD) в протоколе OSPF. Команда "no max-concurrent-dd" восстанавливает значение по умолчанию
Параметр	<value>в диапазоне <1-65535>, количество одновременно обрабатываемых пакетов данных dd
По умолчанию	конфигурация по умолчанию отсутствует. Нет ограничений на максимальное количество одновременно обрабатываемых сообщений dd
Режим	Режим конфигурации OSPFv3
Руководство по использованию	Команда ограничивает максимальное число текущих обменов DD, находящихся в обработке OSPF
Пример	Ограничить одновременно обрабатываемые dd до 20. <pre>Switch#config terminal Switch(config)#router ipv6 ospf Switch(config-router)#max-concurrent-dd 20</pre>

16.5.25. Отключение отправки обновлений (passive-interface)

Команда	<pre>[no] passive-interface<ifname> vlan <vlan-id></pre> Отключает отправку пакетов hello на определенные интерфейсы. Команда "no passive-interface{<ifname> vlan <vlan-id>}" отменяет данную функцию
Параметр	<ifname>конкретное имя интерфейса
По умолчанию	Не сконфигурировано
Режим	Режим конфигурации OSPFv3



Руководство по использованию	-
Пример	<pre>Switch#config terminal Switch(config)#router ipv6 ospf Switch(config-router)#passive-interface vlan1</pre>

16.5.26. Перераспределение маршрутов (redistribute)

Команда	<pre>[no]redistribute {kernel connected static rip isis bgp} [metric<value>] [metric-type {1 2}][route-map<word>]</pre> В OSPFv3 вводятся маршруты, полученные от других протоколов маршрутизации
Параметр	kernel задается из маршрутов ядра connected задается из прямых подключенных маршрутов static задается из статических маршрутов rip задается из маршрута RIP isis задается из маршрута ISIS bgp задается из маршрута BGP metric <value> метрика, которая будет использоваться для перераспределенных маршрутов, в диапазоне 0-16777214 metric-type {1 2} тип метрики задаваемого внешнего маршрута, может быть 1 или 2, значение по умолчанию 2 route-map <word> указывает на карту маршрутов для задаваемых маршрутов
По умолчанию	-
Режим	Режим конфигурации OSPFv3
Руководство по использованию	Получение и внедрение других протоколов маршрутизации в область OSPFv3 для создания маршрутов LSA от внешних источников (AS-external_LSAs.)
Пример	<pre>Switch#config terminal Switch(config)#router ipv6 ospf Switch(config-router)#redistribute bgp metric 12 metric-type 1</pre>



16.5.27. Перераспределение маршрутов OSPF (redistribute ospf)

Команда	redistribute ospf [<process-tag>] [metric<value>] [metric-type{1 2}] [route-map<word>] no redistribute ospf [<process-tag>] [metric<value>] [metric-type{1 2}] [route-map<word>] Выполняет перераспределение маршрутов по метрике "process-tag". "no" в начале команды отменяет перераспределение процесса, обозначенного тегом. При вводе необязательных параметров "metric", "metric type" и "routermap" восстанавливается конфигурация по умолчанию
Параметр	process-tag идентификатор процесса IPv6 OSPF, по умолчанию NULL. metric <value> метрика для перераспределенной маршрутизации, диапазон от 0 до 16777214. metric-type {1 2} тип метрики для перераспределенной маршрутизации, может быть только 1 или 2, по умолчанию 2. route-map <word> указатель на введенную карту маршрутизации
По умолчанию	По умолчанию маршрутизация OSPFv3 не перераспределяется
Режим	Режим конфигурации маршрутизатора IPv6 OSPF
Руководство по использованию	Если "process-id" не введен, это означает, что маршрутизация OSPFv3 будет перераспределена по умолчанию (Process-tag равен NULL). В форме команды с "no" в начале, вводятся необязательные параметры "metric", "metric-type" и "routermap", после чего восстанавливается конфигурация по умолчанию. Если необязательные параметры не указаны, маршрутизатор процесса перераспределения удаляется
Пример	Switch(config)#router ipv6 ospf Switch(config-router)#redistribute ospf

16.5.28. Идентификатор маршрутизатора (router-id)

Команда	router-id<router-id> no router-id Задание идентификатора маршрутизатора для процесса ospfv3. Команда "no router-id" восстанавливает идентификатор на 0.0.0.0
Параметр	<router-id> идентификатор маршрутизатора в формате IPv4-адреса
По умолчанию	0.0.0.0
Режим	Режим конфигурации OSPFv3



Руководство по использованию	Если идентификатор "router-id" задан как 0.0.0.0 процесс ospfv3 не включится. Необходимо настроить идентификатор маршрутизатора "router-id" для ospfv3
Пример	Switch(config)#router ipv6 ospf Switch(config-router)#redistribute ospf

16.5.29. Настройка процесса маршрутизации OSPF (router ipv6 ospf)

Команда	[no] router ipv6 ospf [<tag>] Эта команда инициализирует программу маршрутизации ospfv3 и позволяет войти в режим ospfv3 для настройки программы маршрутизации ospfv3. Команда "no router ipv6 ospf [<tag>]" останавливает соответствующий процесс
Параметр	<tag> ospfv3 метка процесса, которая может быть случайной строкой, состоящей из символов и цифр
По умолчанию	-
Режим	Режим глобальной конфигурации
Руководство по использованию	Для правильной работы процесса маршрутизации ospfv3 необходимо задать данную команду. Протокол ospfv3 должен быть включен хотя бы на одном интерфейсе. Процесс ospfv3 включается на интерфейсе, если тег, заданный командой ipv6 router ospf area в режиме интерфейса, совпадает с меткой процесса ospf
Пример	Switch#config terminal Switch(config)#router ipv6 ospf IPI

16.5.30. Просмотр общей информации о процессах маршрутизации OSPFv3 (show ipv6 ospf)

Команда	show ipv6 ospf [<tag>] Просмотр информации о реализации OSPF глобально и для областей
Параметр	<tag> тег процессов, представляет собой строку символов
По умолчанию	Информация не отображается
Режим	Все режимы



Руководство по использованию	-
Пример	<pre>Switch#show ipv6 ospf Routing Process "OSPFv3 (*null*)" with ID 192.168.2.2 SPF schedule delay 5 secs, Hold time between SPFs 10 secs Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs Number of external LSA 0. Checksum Sum 0x0000 Number of AS-Scoped Unknown LSA 0 Number of LSA originated 6 Number of LSA received 14 Number of areas in this router is 1 Area BACKBONE(0) Number of interfaces in this area is 2 SPF algorithm executed 6 times Number of LSA 8. Checksum Sum 0x43D52 Number of Unknown LSA 0</pre>

16.5.31. Просмотр базы данных OSPFv3 (show ipv6 ospf database)

Команда	<pre>show ipv6 ospf [<tag>] database[router [adv-router <advertiser_router>]]network [adv-router <advertiser_router>]] intra-prefix [adv-router <advertiser_router>]] link [adv-router <advertiser_router>] external [adv-router <advertiser_router>]] inter-prefix [adv-router <advertiser_router>]] inter-router [adv-router <advertiser_router>]]</pre> Выводит на экран сообщения базы данных о состоянии соединений OSPF
Параметр	<tag> тег процессов, представляет собой строку символов. <advertiser_router> идентификатор объявляющего маршрутизатора в формате Ipv4-адреса
По умолчанию	Информация не отображается
Режим	Все режимы
Руководство по использованию	В сообщениях, появляющихся после ввода этой команды, можно просмотреть информацию о базе данных состояния соединений OSPF



Пример	С помощью команды «show ipv6 ospf database» просмотреть LSA-сообщения протокола маршрутизации OSPF.					
	Например, на экране отображается следующее:					
	OSPFv3 Router with ID (192.168.2.2) (Process *null*)					
	Link-LSA (Interface Vlan1)					
	Link State ID	ADV Router	Age	Seq#	CkSum	Prefix
	0.0.7.211	192.168.2.2	1409	0x80000001	0x6dda	1
	0.0.7.212	192.168.2.3	1357	0x80000001	0x248e	1
	Link-LSA (Interface Vlan2)					
	Link State ID	ADV Router	Age	Seq#	CkSum	Prefix
	0.0.7.211	192.168.2.1	1450	0x80000001	0xa565	1
	0.0.7.212	192.168.2.2	1399	0x80000001	0x4305	1
	Router-LSA (Area 0.0.0.0)					
	Link State ID	ADV Router	Age	Seq#	CkSum	Link
	0.0.0.0	192.168.2.1	1390	0x80000006	0x9fe2	1
	0.0.0.0	192.168.2.2	1354	0x80000007	0x4af5	2
	0.0.0.0	192.168.2.3	1308	0x80000004	0xbbc4	1
	Network-LSA (Area 0.0.0.0)					
	Link State ID	ADV Router	Age	Seq#	CkSum	
	0.0.7.211	192.168.2.1	1390	0x80000001	0x897e	
	0.0.7.211	192.168.2.2	1354	0x80000001	0x9b69	
	Intra-Area-Prefix-LSA (Area 0.0.0.0)					
	Link State ID	ADV Router	Age	Seq#	CkSum	Prefix



	0.0.0.1	192.168.2.1	1389	0x80000005	0x7e2e	1 Reference
	0.0.0.2	192.168.2.1	1389	0x80000001	0x22cb	1
	Network-LSA					
	0.0.0.1	192.168.2.3	1306	0x80000002	0xd0d7	1 Router-LSA
Информация, отображаемая на экране			Пояснение			
Link-LSA (Interface Vlan1)			Сообщения Link LSA интерфейса Vlan1			
Router-LSA (Area 0.0.0.0)			Сообщения LSA маршрутизатора в зоне 0			
Network-LSA (Area 0.0.0.0)			Сетевые LSA в зоне 0			
Intra-Area-Prefix-LSA (Area 0.0.0.0)			Внутридоменные префиксные LSA в области 0			

16.5.32. Просмотр интерфейсов, где включен протокол OSPFv3 (show ipv6 ospf interface)

Команда	show ipv6 ospf interface <ifname> vlan <vlan-id> Выводит на экран сообщения интерфейса OSPF
Параметр	< ifname > имя интерфейса
По умолчанию	Информация не отображается
Режим	Все режимы
Руководство по использованию	-
Пример	Switch#show ipv6 ospf interface Loopback is up, line protocol is up OSPFv3 not enabled on this interface Vlan1 is up, line protocol is up Interface ID 2003



Ipv6 Prefixes

fe80: : 203: fff: fe01: 257c/64 (Link-Local Address)

2001: 1: 1: : 1/64

OSPFv3 Process (*null*), Area 0.0.0.0, Instance ID 0

Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 192.168.2.2

Interface Address fe80: : 203: fff: fe01: 257c

Backup Designated Router (ID) 192.168.2.3

Interface Address fe80: : 203: fff: fe01: d28

Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00: 00: 10

Neighbor Count is 1, Adjacent neighbor count is 1
 Vlan2 is up, line protocol is up

Interface	ID	2004

Ipv6 Prefixes

fe80: : 203: fff: fe01: 257c/64 (Link-Local Address)

2000: 1: 1: : 1/64

OSPFv3 Process (*null*), Area 0.0.0.0, Instance ID 0

Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10

Transmit Delay is 1 sec, State Backup, Priority 1

Designated	Router	(ID)	192.168.2.1

Interface	Address	fe80: : 203: fff: fe01: 429e

Backup	Designated	Router	(ID)	192.168.2.2

Interface Address fe80: : 203: fff: fe01: 257c

Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00: 00: 10

Neighbor Count is 1, Adjacent neighbor count is 1

Информация, отображаемая на экране	Пояснение
Vlan1 is up, line protocol is up	Подключение интерфейса логическое и физическое
Ipv6 Prefixes fe80: : 203: fff: fe01: 257c/64 (Link-Local Address) 2001: 1: 1: : 1/64	Ipv6-адрес интерфейса и длина префикса



OSPFv3 Process (*null*)	Процесс OspfV3, к которому принадлежит интерфейс
Area 0.0.0.1	Область, к которой принадлежит интерфейс
Instance ID 0	Идентификатор экземпляра равен 0
Router ID 192.168.2.2, Network Type BROADCAST, Cost: 10	Идентификатор процесса; Идентификатор маршрутизатора; Тип сети; Стоимость
Transmit Delay is 1 sec, State DR, Priority 1	Задержка передачи LAS на интерфейсе; состояние; выбор приоритета коммутатора уровня 3
Designated Router (ID) 192.168.2.2 Interface Address fe80: : 203: fff: fe01: 257c	Назначение коммутатора уровня 3
Backup Designated Router (ID) 192.168.2.3 Interface Address fe80: : 203: fff: fe01: d28	Резервное копирование указанного коммутатора уровня 3
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00: 00: 10	Таймер протокола OSPF; включая пакет hello, пакеты интервала опроса, интервал отказа маршрутизатора, ретрансляцию маршрутизатора
Neighbor Count is 1, Adjacent neighbor count is 1	Номера соседних коммутаторов уровня 3; номера коммутаторов уровня 3, с которыми установлены отношения смежности

16.5.33. Просмотр состояния смежности с соседними маршрутизаторами (show ipv6 ospf neighbor)

Команда	show ipv6 ospf [<tag>] neighbor [<neighbor_id> <ifname> detail detail] Отображение сообщений о смежных точках OSPF
Параметр	<tag>тег процессов, представляет собой строку символов. <neighbor_id> идентификатор соседнего маршрутизатора в формате ipv4-адреса detail: показать сведения о соседнем устройстве <ifname> имя интерфейса



По умолчанию	Информация не отображается						
Режим	Все режимы						
Руководство по использованию	Команда используется для проверки отношения смежности OSPF						
Пример	Switch#show ipv6 ospf neighbor						
	OSPFv3 Process (*null*)						
	Neighbor ID	Pri	State	Dead Time	Interface	Instance	ID
	192.168.2.3	1	Full/Backup	00: 00: 29	Vlan1	0	
	192.168.2.1	1	Full/DR	00: 00: 38	Vlan2	0	
	Vlan1						
	Информация, отображаемая на экране			Пояснение			
	Neighbor ID			Идентификатор соседнего устройства			
	Instance ID			Идентификатор экземпляра			
	Address			IP-адрес соседнего коммутатора уровня 3			
Interface			Интерфейс, к которому принадлежит соседнее устройство				
state			Состояние отношения с соседним устройством				
pri			Приоритет				

16.5.34. Просмотр маршрута (show ipv6 ospf route)

Команда	show ipv6 ospf [<tag>] route Предоставляет сведения о маршрутах OSPF, содержащихся в таблице маршрутизации
Параметр	<tag> тег процессов, представляет собой строку символов
По умолчанию	Информация не отображается
Режим	Все режимы
Руководство по использованию	-



Пример	<pre>Switch#show ipv6 ospf route</pre> Codes: C – connected, D – Discard, O – OSPF, IA – OSPF inter area E1 – OSPF external type 1, E2 - OSPF external type 2 <table> <thead> <tr> <th>Destination</th><th>Metric</th></tr> </thead> <tbody> <tr> <td>Next-hop</td><td></td></tr> <tr> <td>O 2000: 1: 1: : /64</td><td>10</td></tr> <tr> <td>directly connected, Vlan2</td><td></td></tr> <tr> <td>O 2001: 1: 1: : /64</td><td>10</td></tr> <tr> <td>directly connected, Vlan1</td><td></td></tr> <tr> <td>O 3000: 1: 1: : /64</td><td>20</td></tr> <tr> <td>via fe80: : 203: fff: fe01: 429e, Vlan2</td><td></td></tr> <tr> <td>O 3003: 1: 1: : /64</td><td>20</td></tr> <tr> <td>via fe80: : 203: fff: fe01: d28, Vlan1</td><td></td></tr> </tbody> </table>	Destination	Metric	Next-hop		O 2000: 1: 1: : /64	10	directly connected, Vlan2		O 2001: 1: 1: : /64	10	directly connected, Vlan1		O 3000: 1: 1: : /64	20	via fe80: : 203: fff: fe01: 429e, Vlan2		O 3003: 1: 1: : /64	20	via fe80: : 203: fff: fe01: d28, Vlan1	
Destination	Metric																				
Next-hop																					
O 2000: 1: 1: : /64	10																				
directly connected, Vlan2																					
O 2001: 1: 1: : /64	10																				
directly connected, Vlan1																					
O 3000: 1: 1: : /64	20																				
via fe80: : 203: fff: fe01: 429e, Vlan2																					
O 3003: 1: 1: : /64	20																				
via fe80: : 203: fff: fe01: d28, Vlan1																					

16.5.35. Просмотр информации о перераспределении в OSPF (show ipv6 ospf redistribute)

Команда	<pre>show ipv6 ospf [<process-tag>] redistribute</pre> Выводит на экран сообщения маршрутизации, которые были перераспределены от внешних процессов в OSPF
Параметр	IPv6 OSPF — идентификатор метки. Если параметр отсутствует, отображается вся информация о маршрутизации, перераспределенная из внешнего процесса IPv6 OSPF
По умолчанию	Не задано
Режим	Привилегированный режим, режим конфигурации
Руководство по использованию	Не задано
Пример	<pre>Switch#show ipv6 ospf redistribute</pre> <pre>ospf process abc redistribute information :</pre> <pre>ospf process def</pre> <pre>bgp</pre> <pre>ospf process def redistribute information :</pre> <pre>ospf process abc</pre> <pre>Switch#show ipv6 ospf abc redistribute</pre>



	ospf process abc redistribute information : ospf process def bgp

16.5.36. Просмотр информация о топологии маршрутизации OSPFv3 (show ipv6 ospf topology)

Команда	show ipv6 ospf [<tag>] topology [area <area-id>] Выводит на экран сообщения о топологии OSPF
Параметр	<tag> тег процессов, представляет собой строку символов. <area-id> это идентификатор зоны, который может быть представлен в виде цифр в диапазоне 0 ~ 4294967295 или IPv4-адрес
По умолчанию	Информация не отображается
Режим	Все режимы
Руководство по использованию	Не задано
Пример	

16.5.37. Просмотр информации о виртуальных соединениях (show ipv6 ospf virtual-links)

Команда	show ipv6 ospf [<tag>] virtual-links Выводит на экран информацию о виртуальных соединениях OSPF
Параметр	<tag> тег процессов, представляет собой строку символов
По умолчанию	Информация не отображается
Режим	Все режимы
Руководство по использованию	Не задано
Пример	Switch#show ipv6 ospf virtual-links Virtual Link VLINK1 to router 5.6.7.8 is up Transit area 0.0.0.1 via interface Vlan1, instance ID 0



	Local address 3ffe: 1234: 1: : 1/128 Remote address 3ffe: 5678: 3: : 1/128 Transmit Delay is 1 sec, State Point-To-Point, Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00: 00: 01 Adjacency state Up

16.5.38. Просмотр подробной информации о маршрутизации (show ipv6 route process-detail)

Команда	show ipv6 route [database] process-detail Выводит на экран таблицу IP-маршрутизации с указанным идентификатором процесса или меткой
Параметр	Наличие параметра "database" выводит все маршрутизаторы, при отсутствии параметра отображаются только работающие маршрутизаторы
По умолчанию	-
Режим	Привилегированный режим
Руководство по использованию	Не задано
Пример	Switch#show ipv6 route database process-detail IPv6 Routing Table Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP > - selected route, * - FIB route, p - stale info Timers: Uptime C*> :: 1/128 via :: , Loopback, 00: 29: 53 O 2001: : /64 [110/10] via :: , Vlan1, 00: 01: 07 ,process aaa C*> 2001: : /64 via :: , Vlan1, 00: 02: 54 O*> 2006: : /64 [110/10] via :: , Vlan1, 00: 01: 07, process aaa O*> 2008: : /64 [110/20] via fe80: : 203: fff: fe01: 2542, Vlan1, 00: 00: 54, process bbb



16.5.39. Время выполнения вычислений кратчайшего пути (timers spf)

Команда	timers spf <spf-delay> <spf-holdtime> no timers spf Задаёт значение таймера расчёта маршрута. Команда "no timers spf" восстанавливает соответствующее значение по умолчанию
Параметр	<spf-delay> 5 секунд по умолчанию <spf-holdtime> 10 секунд по умолчанию
По умолчанию	-
Режим	Режим конфигурации OSPFv3
Руководство по использованию	В этой команде принимается время задержки между изменением топологии получения сообщений и вычислением кратчайшего пути (SPF), а также задаётся время задержки между двумя периодическими вычислениями SPF
Пример	Switch#config terminal Switch(config)#router ipv6 ospf Switch(config-router)#timers spf 5 10

16.6. Команды MBGP4+

16.6.1. Параметры отладки отправленных сообщений перераспределения (debug ipv6 bgp redistribute message send)

Команда	debug ipv6 bgp redistribute message send no debug ipv6 bgp redistribute message send Команда позволяет применять параметры отладки отправки сообщений для перераспределения маршрутизации из внешних процессов, например, таких как OSPFv3 и прочие, в MBGP4+. "no" в начале команды отключает процесс отладки
Параметр	-
По умолчанию	Закреты
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Switch#debug ipv6 bgp redistribute message send



16.6.2. Параметры отладки полученных сообщений о перераспределении маршрута (debug ipv6 bgp redistribute route receive)

Команда	debug ipv6 bgp redistribute route receive no debug ipv6 bgp redistribute route receive Команда используется для подключения параметров отладки получаемых сообщений от NSM для MBGP4+. Форма команды с "no" в начале отключает отладку получаемых от NSM сообщений для MBGP4+
Параметр	-
По умолчанию	Закрыты
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Switch#debug ipv6 bgp redistribute route receive Switch#no debug ipv6 bgp redistribute route receive

16.6.3. Перераспределение маршрутов в OSPF (redistribute ospf (MBGP4+))

Команда	redistribute ospf [<process-tag>] [route-map<word>] no redistribute ospf [<process-tag>] Команда применяется для перераспределения информации о маршрутизации из OSPFv3 в MBGP4+. "no" в начале команды удаляет конфигурацию
Параметр	process-tag это строка символов процесса OSPFv3, длина которой не должна превышать 15. Если идентификатор процесса не указан, будет использоваться процесс по умолчанию. route-map <word> указатель на заданную карту маршрутизации
По умолчанию	Перераспределение не выполняется
Режим	Режим конфигурации BGP IPv6
Руководство по использованию	-



Пример	Перераспределить информацию о маршрутизации из процесса OSPFv3 с меткой ABC в MBGP4+ (с номером 1). Switch(config)#router bgp 1 Switch(config-router)#address-family ipv6 unicast Switch (config-router-af)#redistribute ospf abc

16.6.4. Просмотр перераспределения (show ipv6 bgp redistribute)

Команда	show ipv6 bgp redistribute Команда выводит информацию о конфигурации перераспределения других исходящих маршрутов в MBGP4+
Параметр	-
По умолчанию	Не отображается
Режим	Привилегированный режим
Руководство по использованию	-
Пример	Switch#show ipv6 bgp redistribute



17. ОБЩАЯ ИНФОРМАЦИЯ

17.1. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» → «[Гарантийное обслуживание](#)».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» → «[Взять оборудование на тест](#)».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

17.2. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться разделом технической поддержки пользователей QTECH на нашем сайте www.qtech.ru/support/.

Телефон Технической поддержки +7 (495) 269-08-81

Центральный офис +7 (495) 477-81-18

17.3. Электронная версия документа

Дата публикации 31.03.2025



https://files.qtech.ru/upload/switchers/QSW-6700/QSW-6700_config_guide.pdf