

# Руководство по настройке линейки промышленных коммутаторов в 19” стойку

## Управление через CLI



Интерфейс командной  
строки



## Оглавление

|  |    |
|--|----|
| Введение.....  | 18 |
| Условные обозначения .....                                     | 18 |
| 1. Подготовка к настройке .....                                | 19 |
| 1.1 Номер порта коммутатора .....                              | 19 |
| 1.2 Подготовка к запуску коммутатора.....                      | 19 |
| 1.3 Получение помощи.....                                      | 20 |
| 1.4 Командные режимы .....                                     | 20 |
| 1.5 Отмена команды.....  | 21 |
| 1.6 Сохранение конфигурации .....                              | 21 |
| 2. Настройка управления системой .....                         | 22 |
| 2.1 Настройка управления файлами .....                         | 22 |
| 2.1.1 Управление файловой системой.....                        | 22 |
| 2.1.2 Команды для файловой системы .....                       | 22 |
| 2.1.3 Запуск из файла вручную .....                            | 23 |
| 2.1.4 Обновление программного обеспечения .....                | 23 |
| 2.1.5 Обновление конфигурации.....                             | 25 |
| 2.1.6 Обновление при помощи FTP.....                           | 25 |
| 2.2 Базовые настройки управления системой .....                | 27 |
| 2.2.1 Настройка IP-адреса Ethernet .....                       | 27 |
| 2.2.2 Настройка маршрута по умолчанию.....                     | 27 |
| 2.2.3 Команда ping .....                                       | 28 |
| 2.3 Настройка HTTP .....                                       | 28 |
| 2.3.1 Включение службы HTTP.....                               | 28 |
| 2.3.2 Изменение номера порта службы HTTP.....                  | 29 |
| 2.3.3 Настройка пароля доступа для службы HTTP.....            | 29 |
| 2.3.4 Указание списка управления доступом для службы HTTP..... | 29 |
| 2.3.5 Примеры настройки HTTP .....                             | 29 |
| 3. Настройка терминала .....                                   | 30 |
| 3.1 Введение.....  | 30 |
| 3.2 Связь между линией и интерфейсом.....                      | 30 |
| 3.3 Пример настройки VTU.....                                  | 30 |
| 4. Настройка управления сетью.....                             | 31 |



|        |   |    |
|--------|---|----|
| 4.1    | Настройка SNMP.....   | 31 |
| 4.1.1  | Введение.....   | 31 |
| 4.1.2  | Задачи настройки SNMP.....  | 33 |
| 4.1.3  | Настройка представления SNMP .....  | 34 |
| 4.1.4  | Создание или изменение контроля доступа для SNMP-комьюнити .....                | 34 |
| 4.1.5  | Настройка способа связи системного администратора и местоположения системы..... | 35 |
| 4.1.6  | Определение максимальной длины пакета данных агента SNMP .....                  | 35 |
| 4.1.7  | Мониторинг состояния SNMP .....   | 35 |
| 4.1.8  | Настройка локального ядра SNMP .....  | 35 |
| 4.1.9  | Настройка SNMP Trap .....   | 36 |
| 4.1.10 | Настройка адреса источника SNMP .....   | 37 |
| 4.1.11 | Пример настройки .....  | 37 |
| 4.2    | Настройка RMON.....   | 37 |
| 4.2.1  | Задачи настройки RMON .....   | 37 |
| 4.2.2  | Настройка сигнализации .....  | 38 |
| 4.2.3  | Настройка события .....   | 39 |
| 4.2.4  | Настройка статистики .....  | 40 |
| 4.2.5  | Настройка истории.....  | 40 |
| 4.2.6  | Отображение конфигурации RMON коммутатора .....                                 | 41 |
| 4.3    | Настройка PDP .....   | 42 |
| 4.3.1  | Введение.....   | 42 |
| 4.3.2  | Задачи настройки PDP .....  | 42 |
| 4.3.3  | Конфигурация PDP по умолчанию .....   | 43 |
| 4.3.4  | Настройка частоты PDP и времени хранения информации.....                        | 43 |
| 4.3.5  | Установка версии PDP.....   | 43 |
| 4.3.6  | Запуск PDP на коммутаторе .....   | 43 |
| 4.3.7  | Запуск PDP на порту.....  | 44 |
| 4.3.8  | Мониторинг и управление PDP .....   | 45 |
| 4.3.9  | Примеры настройки PDP .....   | 45 |
| 4.4    | Команды настройки SSH.....  | 46 |
| 4.4.1  | Введение.....   | 46 |
| 4.4.2  | Настройка методов аутентификации .....  | 46 |



|       |   |    |
|-------|---|----|
| 4.4.3 | Настройка списка управления доступом .....                  | 46 |
| 4.4.4 | Настройка времени ожидания аутентификации .....             | 46 |
| 4.4.5 | Настройка количества повторных попыток аутентификации ..... | 47 |
| 4.4.6 | Включение SSH-сервера .....                                 | 47 |
| 4.4.7 | Пример настройки SSH-сервера .....                          | 47 |
| 5.    | Настройка основных параметров интерфейсов .....             | 48 |
| 5.1   | Введение .....  | 48 |
| 5.2   | Настройка общих атрибутов интерфейса .....                  | 50 |
| 5.2.1 | Добавление описания .....                                   | 50 |
| 5.2.2 | Настройка полосы пропускания .....                          | 51 |
| 5.2.3 | Настройка временной задержки .....                          | 51 |
| 5.3   | Мониторинг и поддержка интерфейса .....                     | 51 |
| 5.3.1 | Проверка состояния интерфейса .....                         | 52 |
| 5.3.2 | Инициализация и удаление интерфейса .....                   | 52 |
| 5.3.3 | Выключение и включение интерфейса .....                     | 52 |
| 5.4   | Настройка интерфейса Ethernet .....                         | 53 |
| 5.4.1 | Выбор интерфейса Ethernet .....                             | 53 |
| 5.4.2 | Настройка скорости .....                                    | 53 |
| 5.4.3 | Настройка дуплексного режима интерфейса .....               | 54 |
| 5.4.4 | Настройка управления потоком на интерфейсе .....            | 54 |
| 5.5   | Настройка логического интерфейса .....                      | 54 |
| 5.5.1 | Настройка нулевого интерфейса .....                         | 55 |
| 5.5.2 | Настройка интерфейса Loopback .....                         | 55 |
| 5.5.3 | Настройка интерфейса агрегации .....                        | 56 |
| 5.5.4 | Настройка интерфейса VLAN .....                             | 56 |
| 5.5.5 | Настройка интерфейса Super VLAN .....                       | 56 |
| 5.6   | Примеры настройки интерфейса .....                          | 57 |
| 6.    | Настройка расширенных параметров интерфейсов .....          | 58 |
| 6.1   | Port Security .....   | 58 |
| 6.1.1 | Введение .....  | 58 |
| 6.1.2 | Настройка MAC-адресов и привязка IP-адреса .....            | 58 |
| 6.2   | Блокировка трафика .....                                    | 59 |
| 6.3   | Изоляция портов .....                                       | 59 |



|  |    |
|--|----|
| 6.4 Управление штормами.....   | 59 |
| 6.5 Ограничение скорости порта.....  | 60 |
| 6.6 Обнаружение петель на порту .....                                      | 61 |
| 6.7 Настройка диапазона интерфейсов .....                                  | 61 |
| 6.7.1 Вход в режим настройки диапазона интерфейсов.....                    | 61 |
| 6.7.2 Пример настройки .....   | 62 |
| 6.8 Зеркалирование портов .....  | 62 |
| 6.8.1 Настройка зеркалирования .....                                       | 62 |
| 6.8.2 Отображение информации о зеркалировании .....                        | 64 |
| 7. VLAN .....  | 64 |
| 7.1 Введение.....  | 64 |
| 7.2 Туннель Dot1Q.....   | 65 |
| 7.2.1 Описание .....   | 65 |
| 7.2.2 Реализация .....   | 65 |
| 7.2.3 Изменение значения TPID.....   | 66 |
| 7.3 Настройка VLAN.....  | 67 |
| 7.3.1 Добавление/удаление VLAN.....  | 67 |
| 7.3.2 Настройка порта коммутатора .....                                    | 68 |
| 7.3.3 Создание/удаление интерфейса VLAN .....                              | 69 |
| 7.3.4 Настройка интерфейса Super VLAN .....                                | 69 |
| 7.3.5 Мониторинг конфигурации и состояния VLAN.....                        | 70 |
| 7.3.6 Глобальное включение/отключение туннеля Dot1Q и настройка TPID ..... | 71 |
| 7.3.7 Настройка режима передачи VLAN и трансляционной записи .....         | 71 |
| 7.4 Примеры настройки .....  | 72 |
| 7.4.1 Пример настройки Super VLAN .....                                    | 72 |
| 7.4.2 Примеры настройки туннеля Dot1Q .....                                | 73 |
| 8. Настройка связующего дерева .....                                       | 78 |
| 8.1 Введение.....  | 78 |
| 8.2 Выбор режима STP.....  | 79 |
| 8.3 Отключение/включение STP .....   | 80 |
| 8.4 Настройка приоритета коммутатора.....                                  | 80 |
| 8.5 Настройка времени приветствия.....                                     | 81 |
| 8.6 Настройка максимального возраста .....                                 | 81 |



|         |  |     |
|---------|--|-----|
| 8.7     | Настройка времени задержки передачи.....           | 81  |
| 8.8     | Настройка приоритета порта .....                   | 82  |
| 8.9     | Настройка стоимости пути .....                     | 82  |
| 8.10    | Настройка автоматически назначаемого порта.....    | 82  |
| 8.11    | Мониторинг состояния STP .....                     | 83  |
| 8.12    | VLAN STP.....                                      | 83  |
| 8.12.1  | Обзор .....  | 83  |
| 8.12.2  | Команды настройки VLAN STP .....                   | 84  |
| 8.13    | RSTP .....   | 86  |
| 8.13.1  | Включение/отключение RSTP на коммутаторе.....      | 86  |
| 8.13.2  | Настройка приоритета коммутатора .....             | 87  |
| 8.13.3  | Настройка времени задержки передачи.....           | 87  |
| 8.13.4  | Настройка времени приветствия .....                | 88  |
| 8.13.5  | Настройка максимального возраста .....             | 88  |
| 8.13.6  | Настройка стоимости пути .....                     | 89  |
| 8.13.7  | Настройка приоритета порта .....                   | 90  |
| 8.13.8  | Настройка проверки согласованности протоколов..... | 90  |
| 8.14    | MTSP.....  | 91  |
| 8.14.1  | Введение.....                                      | 91  |
| 8.14.2  | Домен MST .....                                    | 91  |
| 8.14.3  | IST, CST, CIST и MSTI .....                        | 92  |
| 8.14.4  | Роли порта .....                                   | 93  |
| 8.14.5  | MSTP BPDU.....                                     | 96  |
| 8.14.6  | Стабильное состояние .....                         | 98  |
| 8.14.7  | Подсчет переходов .....                            | 99  |
| 8.14.8  | Совместимость с STP.....                           | 99  |
| 8.14.9  | Задачи настройки MSTP .....                        | 99  |
| 8.14.10 | Конфигурация MSTP по умолчанию.....                | 100 |
| 8.14.11 | Включение и отключение MSTP .....                  | 100 |
| 8.14.12 | Настройка региона MST .....                        | 101 |
| 8.14.13 | Настройка корневого моста сети.....                | 102 |
| 8.14.14 | Настройка вторичного корневого моста .....         | 103 |
| 8.14.15 | Настройка приоритета моста .....                   | 104 |



|         |   |     |
|---------|---|-----|
| 8.14.16 | Настройка параметров времени STP .....                      | 105 |
| 8.14.17 | Настройка диаметра сети.....                                | 106 |
| 8.14.18 | Настройка максимального количества переходов.....           | 107 |
| 8.14.19 | Настройка приоритета порта .....                            | 107 |
| 8.14.20 | Настройка стоимости пути порта .....                        | 108 |
| 8.14.21 | Настройка типа подключения порта .....                      | 109 |
| 8.14.22 | Активация режима совместимости с MST .....                  | 109 |
| 8.14.23 | Перезапуск проверки конвертации протоколов .....            | 110 |
| 8.14.24 | Проверка информации MSTP .....                              | 111 |
| 8.15    | Дополнительные функции STP .....                            | 112 |
| 8.15.1  | Введение.....   | 112 |
| 8.15.2  | Port Fast.....  | 112 |
| 8.15.3  | BPDU Guard .....  | 113 |
| 8.15.4  | BPDU Filter.....  | 114 |
| 8.15.5  | Uplink Fast .....   | 114 |
| 8.15.6  | Backbone Fast.....  | 116 |
| 8.15.7  | Root Guard .....  | 118 |
| 8.15.8  | Loop Guard .....  | 119 |
| 8.15.9  | Настройка Port Fast .....                                   | 119 |
| 8.15.10 | Настройка BPDU Guard .....                                  | 120 |
| 8.15.11 | Настройка BPDU Filter .....                                 | 121 |
| 8.15.12 | Настройка Uplink Fast .....                                 | 122 |
| 8.15.13 | Настройка Backbone Fast .....                               | 122 |
| 8.15.14 | Настройка Root Guard.....                                   | 124 |
| 8.15.15 | Настройка Loop Guard .....                                  | 124 |
| 9.      | Настройка таблицы MAC-адресов .....                         | 125 |
| 9.1     | Настройка статического MAC-адреса .....                     | 125 |
| 9.2     | Настройка времени устаревания MAC-адреса.....               | 126 |
| 9.3     | Настройка совместного изучения MAC-адреса разными VLAN..... | 126 |
| 9.4     | Отображение MAC-адресов.....                                | 127 |
| 9.5     | Удаление динамических MAC-адресов .....                     | 127 |
| 10.     | Агрегация каналов .....                                     | 128 |
| 10.1    | Введение.....   | 128 |



|       |   |     |
|-------|---|-----|
| 10.2  | Настройка логического канала, используемого для агрегации .....                             | 129 |
| 10.3  | Агрегация физических портов .....   | 129 |
| 10.4  | Выбор режима балансировки нагрузки агрегированных портов .....                              | 130 |
| 10.5  | Отслеживание состояния агрегации .....  | 131 |
| 11.   | Настройка GVRP .....  | 131 |
| 11.1  | Введение.....   | 131 |
| 11.2  | Глобальное включение/отключение GVRP .....  | 131 |
| 11.3  | Включение/отключение GVRP на интерфейсе .....   | 132 |
| 11.4  | Мониторинг и обслуживание GVRP .....  | 132 |
| 11.5  | Пример настройки .....  | 133 |
| 12.   | IGMP Snooping .....   | 134 |
| 12.1  | Введение.....   | 134 |
| 12.2  | Включение/отключение IGMP Snooping для VLAN .....   | 135 |
| 12.3  | Добавление/удаление статического мультикастового адреса VLAN .....                          | 135 |
| 12.4  | Настройка немедленного выхода VLAN из группы .....  | 136 |
| 12.5  | Настройка фильтрации многоадресных сообщений без зарегистрированного адреса назначения..... | 136 |
| 12.6  | Настройка таймера Router Age .....  | 137 |
| 12.7  | Настройка таймера Response Time.....  | 138 |
| 12.8  | Настройка генератора запросов IGMP Snooping.....  | 138 |
| 12.9  | Мониторинг и поддержка IGMP Snooping.....   | 139 |
| 12.10 | Пример настройки IGMP Snooping .....  | 142 |
| 13.   | Настройка 802.1x.....   | 142 |
| 13.1  | Настройка аутентификации 802.1x на основе портов .....                                      | 143 |
| 13.2  | Настройка мульти-аутентификации 802.1x .....  | 144 |
| 13.3  | Настройка максимального количества запросов аутентификации ID 802.1x .....                  | 144 |
| 13.4  | Настройка повторной аутентификации 802.1x .....   | 145 |
| 13.5  | Настройка частоты передачи сообщений 802.1x.....  | 145 |
| 13.6  | Настройка привязки пользователя 802.1x.....   | 146 |
| 13.7  | Настройка метода аутентификации 802.1x для порта.....                                       | 146 |
| 13.8  | Выбор типа аутентификации 802.1x для порта .....  | 146 |
| 13.9  | Настройка учета 802.1x.....   | 147 |
| 13.10 | Настройка гостевой VLAN 802.1x .....  | 147 |



|         |  |     |
|---------|--|-----|
| 13.11   | Запрет клиенту использования нескольких сетевых карт .....                   | 148 |
| 13.12   | Восстановление настроек 802.1x по умолчанию .....                            | 148 |
| 13.13   | Мониторинг конфигурации и состояния аутентификации 802.1x.....               | 149 |
| 13.14   | Пример настройки .....   | 149 |
| 14.     | Настройка MAC ACL.....   | 150 |
| 14.1    | Создание списка управления доступом .....                                    | 150 |
| 14.2    | Настройка элементов списка .....   | 150 |
| 14.3    | Применение списка .....  | 152 |
| 15.     | Настройка IP ACL .....   | 152 |
| 15.1    | Фильтрация IP-пакетов .....  | 152 |
| 15.2    | Создание стандартного и расширяемого IP ACL .....                            | 153 |
| 15.3    | Применение IP ACL .....  | 154 |
| 15.4    | Примеры применения расширяемого списка доступа .....                         | 154 |
| 16.     | QoS.....   | 155 |
| 16.1    | Основные понятия .....   | 155 |
| 16.2    | Модель QoS между терминалами .....   | 156 |
| 16.3    | Алгоритмы очереди QoS .....  | 156 |
| 16.4    | Настройка QoS.....   | 157 |
| 16.4.1  | Настройка очереди глобальных приоритетов CoS .....                           | 158 |
| 16.4.2  | Настройка полосы пропускания для приоритетной очереди CoS .....              | 158 |
| 16.4.3  | Настройка политики планирования приоритетных очередей CoS .....              | 159 |
| 16.4.4  | Настройка стандарта планирования для приоритетных очередей CoS .....         | 160 |
| 16.4.5  | Установка значения CoS по умолчанию для порта .....                          | 160 |
| 16.4.6  | Настройка приоритетной очереди CoS для порта .....                           | 161 |
| 16.4.7  | Создание карты политики QoS .....  | 161 |
| 16.4.8  | Настройка описания карты политики QoS.....                                   | 163 |
| 16.4.9  | Настройка сопоставления потока данных с картой политики QoS .....            | 163 |
| 16.4.10 | Настройка действий для потока данных в рамках управления политикой QoS ..... | 164 |
| 16.4.11 | Применение политики QoS к порту .....  | 165 |
| 16.4.12 | Отображение карты политики QoS .....   | 166 |
| 16.4.13 | Установка ограничения скорости на порту .....                                | 166 |
| 16.5    | Пример настройки QoS .....   | 167 |



|   |     |
|---|-----|
| 17. Туннель протокола второго уровня .....                          | 167 |
| 17.1 Введение.....  | 167 |
| 17.2 Настройка туннеля .....  | 168 |
| 17.3 Пример настройки туннеля.....                                  | 168 |
| 18. AAA .....   | 169 |
| 18.1 Введение.....  | 169 |
| 18.1.1 Служба безопасности AAA .....                                | 169 |
| 18.1.2 Преимущества использования AAA .....                         | 170 |
| 18.1.3 Принципы AAA .....   | 170 |
| 18.1.4 Список методов AAA.....                                      | 171 |
| 18.1.5 Процесс настройки AAA .....                                  | 172 |
| 18.2 Настройка аутентификации .....                                 | 172 |
| 18.2.1 Настройка аутентификации при входе с помощью AAA .....       | 173 |
| 18.2.2 Аутентификация на привилегированном уровне .....             | 176 |
| 18.2.3 Настройка баннеров сообщений для аутентификации AAA.....     | 177 |
| 18.2.4 Изменение текста приглашения ввода имени пользователя .....  | 178 |
| 18.2.5 Изменение текста приглашения ввода пароля пользователя ..... | 178 |
| 18.2.6 Создание аутентификации на основе имени пользователя.....    | 178 |
| 18.2.7 Создание пароля enable .....                                 | 179 |
| 18.2.8 Пример настройки аутентификации AAA .....                    | 179 |
| 18.3 Настройка авторизации.....                                     | 180 |
| 18.3.1 Настройка авторизации EXEC с помощью AAA .....               | 180 |
| 18.3.2 Пример авторизации AAA .....                                 | 182 |
| 18.4 Настройка учета .....  | 183 |
| 18.4.1 Настройка учета подключений с помощью AAA.....               | 183 |
| 18.4.2 Настройка сетевого учета с помощью AAA.....                  | 184 |
| 18.4.3 Настройка обновления учета через AAA .....                   | 185 |
| 18.4.4 Ограничение учета пользователей без имени .....              | 185 |
| 19. RADIUS.....   | 185 |
| 19.1 Введение.....  | 186 |
| 19.1.1 Описание RADIUS .....  | 186 |
| 19.1.2 Принцип работы .....   | 187 |
| 19.2 Настройка RADIUS .....   | 187 |



|        |   |     |
|--------|---|-----|
| 19.2.1 | Настройка связи коммутатора с сервером RADIUS .....                         | 188 |
| 19.2.2 | Настройка коммутатора под атрибуты RADIUS, специфичные для поставщика ..... | 189 |
| 19.2.3 | Назначение RADIUS для аутентификации.....                                   | 189 |
| 19.2.4 | Назначение RADIUS для авторизации.....                                      | 189 |
| 19.2.5 | Назначение RADIUS для учета .....   | 190 |
| 19.3   | Примеры настройки RADIUS .....  | 190 |
| 19.3.1 | Пример аутентификации RADIUS .....  | 190 |
| 19.3.2 | Применение RADIUS в AAA .....   | 190 |
| 20.    | Веб-аутентификация .....  | 191 |
| 20.1   | Введение.....   | 191 |
| 20.1.1 | Описание .....  | 191 |
| 20.1.2 | Подготовка к настройке .....  | 194 |
| 20.2   | Настройка веб-аутентификации .....  | 195 |
| 20.2.1 | Глобальная конфигурация .....   | 195 |
| 20.2.2 | Настройка интерфейса .....  | 197 |
| 20.2.3 | Включение веб-аутентификации.....   | 198 |
| 20.3   | Мониторинг и поддержка веб-аутентификации .....                             | 198 |
| 20.3.1 | Проверка глобальной конфигурации .....                                      | 198 |
| 20.3.2 | Проверка конфигурации интерфейса .....                                      | 198 |
| 20.3.3 | Проверка состояния пользователей .....                                      | 198 |
| 20.3.4 | Принудительное отключение пользователей .....                               | 199 |
| 20.4   | Пример настройки веб-аутентификации .....                                   | 199 |
| 21.    | DHCP Snooping .....   | 201 |
| 21.1   | Включение/выключение функции DHCP Snooping .....                            | 202 |
| 21.2   | Включение DHCP Snooping в VLAN .....  | 202 |
| 21.3   | Настройка интерфейса в качестве доверенного порта DHCP .....                | 203 |
| 21.4   | Включение DAI в VLAN .....  | 203 |
| 21.5   | Настройка интерфейса в качестве доверенного порта ARP.....                  | 204 |
| 21.6   | Включение мониторинга исходного IP-адреса в VLAN .....                      | 204 |
| 21.7   | Настройка интерфейса, доверенного для мониторинга исходного IP-адреса ..... | 204 |
| 21.8   | Настройка TFTP-сервера для резервного копирования привязок адресов .....    | 205 |
| 21.9   | Настройка имени файла для резервного копирования привязок адресов .....     | 206 |



|          |   |     |
|----------|---|-----|
| 21.10    | Настройка интервала резервного копирования привязок адресов ..... | 206 |
| 21.11    | Ручная настройка привязки интерфейса .....                        | 206 |
| 21.12    | Мониторинг и поддержка DHCP Snooping .....                        | 207 |
| 21.13    | Пример настройки DHCP Snooping .....                              | 208 |
| 22.      | LLDP .....  | 209 |
| 22.1     | Введение.....   | 209 |
| 22.2     | Включение/отключение LLDP .....                                   | 210 |
| 22.3     | Настройка времени удержания.....                                  | 210 |
| 22.4     | Настройка таймера .....   | 211 |
| 22.5     | Настройка реинициализации .....                                   | 211 |
| 22.6     | Настройка TLV для отправки.....                                   | 212 |
| 22.7     | Настройка режима передачи или приема .....                        | 212 |
| 22.8     | Отображение информации LLDP .....                                 | 212 |
| 22.9     | Удаление информации LLDP.....                                     | 213 |
| 23.      | Протоколы защиты кольцевых соединений Ethernet .....              | 214 |
| 23.1     | Введение.....   | 214 |
| 23.1.1   | Обзор протоколов.....   | 214 |
| 23.1.2   | Базовые сведения о настройке кольцевого резервирования .....      | 214 |
| 23.2     | EAPS.....   | 216 |
| 23.2.1   | Основные понятия .....  | 216 |
| 23.2.2   | Роли кольцевых узлов .....  | 216 |
| 23.2.3   | Роли кольцевых портов.....  | 217 |
| 23.2.4   | Управляющая VLAN и VLAN для передачи данных.....                  | 217 |
| 23.2.5   | Символ замкнутой кольцевой сети.....                              | 218 |
| 23.2.6   | Типы пакетов EAPS.....  | 218 |
| 23.2.7   | Механизм работы EAPS.....   | 219 |
| 23.2.7.1 | Работа главного узла.....   | 219 |
| 23.2.7.2 | Уведомление о нерабочем канале транзитного узла .....             | 219 |
| 23.2.7.3 | Возобновление соединения транзитного узла.....                    | 219 |
| 23.2.8   | Настройка EAPS .....  | 220 |
| 23.2.8.1 | Введение .....  | 220 |
| 23.2.8.2 | Настройка главного узла .....                                     | 221 |
| 23.2.8.3 | Настройка транзитного узла .....                                  | 222 |
| 23.2.8.4 | Настройка кольцевого порта .....                                  | 223 |



|          |   |     |
|----------|---|-----|
| 23.2.8.5 | Просмотр состояния протокола .....  | 223 |
| 23.2.9   | Пример настройки EAPS .....   | 224 |
| 23.3     | ERPS .....  | 226 |
| 23.3.1   | Основные понятия .....  | 226 |
| 23.3.1.1 | Роли кольцевых узлов.....   | 226 |
| 23.3.1.2 | Роли кольцевых портов .....   | 227 |
| 23.3.1.3 | Управляющая VLAN и VLAN данных.....   | 227 |
| 23.3.1.4 | Автоматическое обнаружение и проверка согласованности кольцевого порта..... | 228 |
| 23.3.1.5 | Типы пакетов ERPS.....  | 228 |
| 23.3.2   | Механизм защиты кольца ERPS.....  | 229 |
| 23.3.2.1 | Стабильное состояние.....   | 229 |
| 23.3.2.2 | Обработка неисправного локального канала связи.....                         | 229 |
| 23.3.2.3 | Обработка восстановления локального канала связи .....                      | 230 |
| 23.3.2.4 | Восстановление кольца ERPS .....  | 230 |
| 23.3.3   | Настройка ERPS .....  | 230 |
| 23.3.3.1 | Введение .....  | 230 |
| 23.3.3.2 | Настройка кольцевого узла .....   | 231 |
| 23.3.3.3 | Настройка кольцевого порта .....  | 232 |
| 23.3.3.4 | Просмотр состояния протокола .....  | 233 |
| 23.3.4   | Примеры настройки ERPS .....  | 234 |
| 23.3.4.1 | Фиксированные настройки RPL.....  | 234 |
| 23.3.4.2 | Простые настройки для применения автоматического обнаружения.....           | 235 |
| 24.      | Протоколы маршрутизации .....   | 235 |
| 24.1     | RIP .....   | 235 |
| 24.1.1   | Введение.....   | 235 |
| 24.1.2   | Запуск RIP.....   | 236 |
| 24.1.3   | Включение одноадресной рассылки сообщений об обновлении маршрута RIP .....  | 237 |
| 24.1.4   | Изменение метрики маршрута .....  | 237 |
| 24.1.5   | Настройка таймеров .....  | 238 |
| 24.1.6   | Указание номера версии RIP .....  | 238 |
| 24.1.7   | Активация аутентификации RIP .....  | 240 |
| 24.1.8   | Запрет суммирования маршрутов .....   | 241 |
| 24.1.9   | Запрет аутентификации исходного IP-адреса .....                             | 242 |



|           |   |     |
|-----------|---|-----|
| 24.1.10   | Настройка максимального количества маршрутов.....                         | 242 |
| 24.1.11   | Мониторинг и поддержка RIP .....  | 244 |
| 24.1.12   | Пример настройки RIP .....  | 245 |
| 24.2      | BEIGRP .....  | 246 |
| 24.2.1    | Введение.....   | 246 |
| 24.2.2    | Активация протокола BEIGRP .....  | 247 |
| 24.2.3    | Настройка процента используемой пропускной способности.....               | 247 |
| 24.2.4    | Настройка арифметического коэффициента суммарного расстояния BEIGRP ..... | 247 |
| 24.2.5    | Использование смещения для настройки суммарного расстояния .....          | 248 |
| 24.2.6    | Отключение автосуммирования .....   | 248 |
| 24.2.7    | Настройка обобщения маршрутов.....  | 249 |
| 24.2.8    | Импортирование других маршрутов в процесс BEIGRP .....                    | 249 |
| 24.2.9    | Настройка дополнительных параметров BEIGRP .....                          | 250 |
| 24.2.10   | Мониторинг и поддержка BEIGRP .....                                       | 252 |
| 24.2.11   | Пример настройки BEIGRP .....   | 252 |
| 24.3      | OSPF.....   | 252 |
| 24.3.1    | Введение.....   | 253 |
| 24.3.2    | Запуск OSPF.....  | 254 |
| 24.3.3    | Настройка параметров интерфейса OSPF.....                                 | 254 |
| 24.3.4    | Настройка OSPF в разных физических сетях.....                             | 255 |
| 24.3.5    | Настройка области OSPF.....   | 256 |
| 24.3.6    | Настройка суммирования маршрутов в области OSPF .....                     | 257 |
| 24.3.7    | Настройка сбора данных пересылающим маршрутизатором .....                 | 257 |
| 24.3.8    | Создание маршрута по умолчанию .....                                      | 258 |
| 24.3.9    | Выбор идентификатора маршрутизатора через интерфейс Loopback .....        | 258 |
| 24.3.10   | Настройка административной дистанции OSPF .....                           | 259 |
| 24.3.11   | Настройка таймера расчета маршрута .....                                  | 259 |
| 24.3.12   | Мониторинг и поддержка OSPF .....   | 260 |
| 24.3.13   | Примеры настройки OSPF .....  | 261 |
| 24.3.13.1 | Пример конфигурации VLSM.....   | 261 |
| 24.3.13.2 | Примеры настройки маршрута OSPF и распределения маршрутов.....            | 262 |
| 24.3.13.3 | Пример комплексной настройки OSPF на коммутаторе ABR .....                | 266 |
| 24.4      | BGP .....   | 269 |



|  |     |
|--|-----|
| 24.4.1 Введение.....   | 269 |
| 24.4.1.1 Описание .....  | 269 |
| 24.4.1.2 Выбор пути .....  | 270 |
| 24.4.2 Настройка BGP.....  | 271 |
| 24.4.2.1 Базовая настройка .....   | 271 |
| 24.4.2.2 Расширенная настройка.....  | 276 |
| 24.4.3 Мониторинг и поддержка BGP .....  | 282 |
| 24.4.4 Примеры настройки BGP .....   | 284 |
| 24.4.4.1 Примеры использования карты маршрутизации .....                                 | 284 |
| 24.4.4.2 Пример конфигурации соседей .....   | 286 |
| 24.4.4.3 Пример фильтрации маршрутов BGP на основе соседей.....                          | 286 |
| 24.4.4.4 Примеры фильтрации маршрутов BGP на основе интерфейса.....                      | 286 |
| 24.4.4.5 Примеры использования списка префиксов для настройки фильтрации маршрутов ..... | 287 |
| 24.4.4.6 Примеры агрегации маршрутов BGP .....   | 288 |
| 24.4.4.7 Пример настройки маршрутного рефлектора .....                                   | 289 |
| 24.4.4.8 Пример конфедерации BGP .....   | 291 |
| 24.4.4.9 Примеры карты маршрутизации с атрибутом группы BGP .....                        | 294 |
| 25. Многоадресная рассылка .....   | 296 |
| 25.1 Введение.....   | 296 |
| 25.2 Реализация многоадресной маршрутизации .....  | 296 |
| 25.3 Задачи настройки многоадресной маршрутизации.....                                   | 297 |
| 25.3.1 Задачи основной настройки многоадресной рассылки.....                             | 297 |
| 25.3.2 Задачи настройки IGMP.....  | 297 |
| 25.3.3 Задачи настройки PIM-DM .....   | 298 |
| 25.3.4 Задачи настройки PIM-SM.....  | 298 |
| 25.3.5 Задачи настройки DVMRP .....  | 298 |
| 25.4 Основные настройки многоадресной маршрутизации .....                                | 298 |
| 25.4.1 Запуск многоадресной маршрутизации .....  | 299 |
| 25.4.2 Запуск функции многоадресной рассылки на порту .....                              | 299 |
| 25.4.2.1 Запуск OLNK.....  | 299 |
| 25.4.2.2 Запуск PIM-DM .....   | 299 |
| 25.4.2.3 Запуск PIM-SM.....  | 300 |
| 25.4.2.4 Настройка порога TTL.....   | 300 |
| 25.4.2.5 Настройка быстрой многоадресной передачи .....                                  | 300 |



|          |  |     |
|----------|--|-----|
| 25.4.2.6 | Настройка статического многоадресного маршрута.....                | 301 |
| 25.4.3   | Настройка границы многоадресной IP-передачи.....                   | 302 |
| 25.4.4   | Настройка управления скоростью многоадресной IP-передачи .....     | 302 |
| 25.4.5   | Настройка помощника многоадресной передачи .....                   | 303 |
| 25.4.6   | Настройка тупикового многоадресного маршрута .....                 | 305 |
| 25.4.7   | Мониторинг и поддержка многоадресного маршрута.....                | 306 |
| 25.5     | IGMP .....   | 307 |
| 25.5.1   | Введение.....  | 307 |
| 25.5.2   | Изменение текущей версии IGMP.....                                 | 307 |
| 25.5.3   | Настройка интервала запросов IGMP .....                            | 308 |
| 25.5.4   | Настройка интервала проверки запросчика IGMP .....                 | 308 |
| 25.5.5   | Настройка максимального времени ответа IGMP.....                   | 309 |
| 25.5.6   | Настройка интервала запросов IGMP для последнего члена группы..... | 310 |
| 25.5.7   | Статическая конфигурация IGMP.....                                 | 310 |
| 25.5.8   | Настройка списка немедленного выхода из группы IGMP .....          | 311 |
| 25.5.9   | Примеры настройки функций IGMP .....                               | 312 |
| 25.6     | PIM-DM.....  | 314 |
| 25.6.1   | Введение.....  | 314 |
| 25.6.2   | Настройка таймера .....  | 315 |
| 25.6.3   | Настройка обновления состояния.....                                | 316 |
| 25.6.4   | Настройка списка фильтрации.....                                   | 316 |
| 25.6.5   | Установка приоритета DR.....                                       | 317 |
| 25.6.6   | Очистка элемента (S, G).....                                       | 317 |
| 25.7     | PIM-SM .....   | 318 |
| 25.7.1   | Введение.....  | 318 |
| 25.7.2   | Запуск PIM-SM .....  | 319 |
| 25.7.3   | Настройка статического RP .....                                    | 320 |
| 25.7.4   | Настройка кандидата на роль BSR .....                              | 320 |
| 25.7.5   | Настройка кандидата на роль RP .....                               | 320 |
| 25.7.6   | Отображение маршрута многоадресной рассылки PIM-SM .....           | 321 |
| 25.7.7   | Удаление маршрутов многоадресной рассылки PIM-SM.....              | 321 |
| 25.7.8   | Примеры настройки PIM-SM .....                                     | 321 |
| 25.7.8.1 | Настройка маршрутизации.....                                       | 321 |



|                               |     |
|-------------------------------|-----|
| 25.7.8.2 Настройка BSR.....   | 323 |
| Расшифровка аббревиатур ..... | 325 |



## Введение

В руководстве описаны основные команды, используемые для настройки коммутатора и управления при помощи интерфейса командной строки (CLI).

## Условные обозначения

### 1. Условные обозначения в тексте

| Формат | Описание  |
|--------|---|
| < >    | Скобки < > обозначают «кнопки». Например, нажмите кнопку <Set>  |
| [ ]    | Скобки [ ] обозначают имя окна или имя меню. Например, нажмите пункт меню [File]  |
| →      | Мультиуровневое меню разделяется посредством знака «→». Например, [Start] → [All Programs] → [Accessories]. Нажмите меню [Start], войдите в подменю [All programs], затем войдите в подменю [Accessories] |
| /      | Выбор одной, двух или более опций при помощи символа «/». Например, «Add/Subtract» означает добавить или удалить  |

### 2. Условные обозначения CLI

| Формат            | Описание  |
|-------------------|---|
| <b>Bold</b>       | Означает команды и ключевые слова. Например, <b>show version</b> будет показываться с использованием шрифта <b>Bold</b>   |
| { <i>Italic</i> } | Указывает на значение параметра, которое необходимо ввести. Например, для команды <b>show vlan {vlan id}</b> вместо {vlan id} следует вводить актуальный идентификатор VLAN |

### 3. Условные символы

| Символ   | Описание   |
|--|--|
| <br>Заметка | Необходимые пояснения к содержимому выполняемых операций с устройством |



## 1. Подготовка к настройке

В данной главе в основном описываются следующие подготовительные работы перед первой настройкой коммутатора:

- номер порта коммутатора;
- подготовка коммутатора к запуску;
- как получить помощь;
- командный режим;
- отмена команды;
- сохранение конфигурации.

### 1.1 Номер порта коммутатора

Физический порт коммутатора нумеруется в формате `<type><slot>/<port>`. Таблица преобразования типа в имя выглядит следующим образом:

| Тип интерфейса     | Имя          | Упрощенное имя |
|--------------------|--------------|----------------|
| 10M Ethernet       | Ethernet     | e              |
| 100M fast Ethernet | FastEthernet | f              |
| 1000M Ethernet     | GigaEthernet | g              |

Номер слота расширения для маркировки и настройки портов должен быть равен **0**. Другие слоты расширения нумеруются слева направо, начиная с **1**.

Порты в одном слоте расширения нумеруются в порядке снизу вверх и слева направо, начиная с **1**. Если существует только один порт, его номер равен **1**.



Порты в модулях каждого вида должны быть последовательно пронумерованы снизу вверх и слева направо.

### 1.2 Подготовка к запуску коммутатора

Перед настройкой коммутатора выполните следующие подготовительные работы:

1. Настройте оборудование коммутатора в соответствии с требованиями руководства.
2. Настройте программу моделирования терминала на ПК.
3. Определите структуру IP-адресов для сетевых протоколов IP.



## 1.3 Получение помощи

Используйте знак вопроса (?) и стрелки направления для облегчения ввода команд:

- Введите вопросительный знак. Отобразится текущий список доступных команд.

Switch> ?

- Введите несколько знакомых символов и нажмите клавишу пробела. Отобразится список доступных команд, начиная с введенных знакомых символов.

Switch> s?

- Введите команду, нажмите клавишу пробела и введите вопросительный знак. Отобразится список параметров команды.

Switch> show ?

- Нажмите клавишу «вверх», чтобы отобразить ранее введенные команды. Продолжайте нажимать клавишу «вверх», и отобразятся дополнительные команды. После этого нажмите клавишу «вниз», и под текущей командой отобразится следующая вводимая команда.

## 1.4 Командные режимы

Интерфейсы командной строки для коммутатора можно разделить на несколько режимов. Каждый командный режим позволяет настраивать различные группы программ. Команда, которую можно использовать в настоящее время, зависит от командного режима, в котором вы находитесь. Чтобы получить доступный список команд можно ввести знак вопроса в различных командных режимах,. Наиболее распространенные режимы перечислены в следующей таблице:

| Командный режим              | Способ входа   | Подсказка | Способ выхода                         |
|------------------------------|--|-----------|---------------------------------------|
| Режим системного мониторинга | Введите <b>Ctrl-p</b> после включения питания                    | monitor#  | Выполните <b>quit</b>                 |
| Пользовательский режим       | Аутентификация пользователя                                      | Switch>   | Выполните <b>exit</b> или <b>quit</b> |
| Режим управления (EXEC)      | Введите <b>enter</b> или <b>enable</b> в пользовательском режиме | Switch#   | Выполните <b>exit</b> или <b>quit</b> |



|   |  |                     |  |
|---|--|---------------------|--|
| Режим глобальной конфигурации (общая настройка) | Введите <b>config</b> или <b>configure</b> в режиме управления                                     | Switch_config#      | Выполните <b>exit</b> или <b>quit</b> или введите <b>Ctrl-z</b> , чтобы вернуться в режим управления |
| Режим настройки интерфейса                      | Введите команду <b>interface</b> в режиме глобальной конфигурации, например, <b>interface f0/1</b> | Switch_config_f0/1# | Выполните <b>exit</b> или <b>quit</b> или введите <b>Ctrl-z</b> , чтобы вернуться в режим управления |

Для каждого режима существует определенный набор команд, с которыми он может работать. Если при вводе команд возникает проблема, проверьте подсказку и введите вопросительный знак, чтобы получить список команд, доступных для текущего режима. Проблема может возникнуть при запуске в неправильном командном режиме или при неправильном написании команды.

В следующем примере показано изменение подсказки интерфейса относительно выбранного командного режима:

```
Switch> enter
Password: <enter password>
Switch# config
Switch_config# interface f0/1
Switch_config_f0/1# quit
Switch_config# quit
Switch#
```

## 1.5 Отмена команды

Чтобы отменить команду или восстановить ее функции по умолчанию, перед большинством команд можно добавить ключевое слово «no». Например:

```
no ip routing
```

## 1.6 Сохранение конфигурации

На случай перезапуска системы или внезапного отключения питания рекомендуется периодически сохранять текущую конфигурацию. Это поможет быстро восстановить ее. Вы



можете выполнить **write** для сохранения конфигурации в режиме управления или в режиме глобальной конфигурации.

## 2. Настройка управления системой

### 2.1 Настройка управления файлами

#### 2.1.1 Управление файловой системой

Имя файла во флеш-памяти состоит не более чем из 20 символов. Имена файлов нечувствительны к регистру.

#### 2.1.2 Команды для файловой системы

Жирным шрифтом во всех командах выделены ключевые слова. Остальные слова и символы – это параметры. Содержимое квадратных скобок «[]» не является обязательным.

| Команда                        | Описание   |
|--------------------------------|--|
| <b>format</b>                  | Форматирует файловую систему и удаляет все данные  |
| <b>dir</b> [ <i>filename</i> ] | Отображает имена файлов и каталогов. Имя файла в скобках «[]» означает отображение файлов, начинающихся с нескольких букв. Файл отображается в следующем формате:<br>Index number file name <FILE> length established time, где:<br>1. Index number – порядковый номер файла<br>2. File name – имя файла<br>3. <FILE> – это обозначение типа файла, которое может быть использовано для идентификации типа файла в системе<br>4. Length – длина файла в байтах<br>5. Established time – время создания файла |
| <b>delete</b> <i>filename</i>  | Удаляет файл. Система подскажет, если файл не существует   |
| <b>md</b> <i>dirname</i>       | Создает каталог  |
| <b>rd</b> <i>dirname</i>       | Удаляет каталог. Система подскажет, если каталог не существует   |
| <b>more</b> <i>filename</i>    | Отображает содержимое файла. Если содержимое файла не может быть отображено на одной странице, оно будет отображено на нескольких  |
| <b>cd</b>                      | Изменяет текущую директорию. Позволяет перейти в другую директорию или подкаталог, где хранятся файлы  |



|                  |                         |
|------------------|-------------------------|
| <code>pwd</code> | Отображает текущий путь |
|------------------|-------------------------|

## 2.1.3 Запуск из файла вручную

```
monitor# boot flash <local_filename>
```

Данная команда предназначена для запуска программного обеспечения коммутатора из флеш-памяти, которая может содержать несколько различных программ для коммутатора.

### ➤ Параметры

| Параметр                    | Описание  |
|-----------------------------|---|
| <code>flash</code>          | Запуск из флеш-памяти   |
| <code>local_filename</code> | Имя файла, сохраненное во флеш-памяти. Пользователи должны ввести имя файла |

### ➤ Пример

```
monitor# boot flash switch.bin
```

## 2.1.4 Обновление программного обеспечения

Пользователь может использовать эту команду для загрузки системного программного обеспечения коммутатора локально или удаленно, чтобы получить обновление версии или пользовательскую версию, содержащую определенную функцию (например, шифрование данных и т. д.).

Обновление программного обеспечения осуществляется в режиме системного мониторинга.

### ➤ Загрузка файла при помощи TFTP

```
monitor# copy tftp flash: [ip_addr]
```

Данная команда предназначена для копирования файла с TFTP-сервера на флеш-память в системе. После ввода команды система предложит указать имя удаленного сервера и имя удаленного файла.

### ➤ Параметры

| Параметр             | Описание  |
|----------------------|---|
| <code>flash</code>   | Устройство хранения – флеш-память   |
| <code>ip_addr</code> | IP-адрес TFTP-сервера<br>Если IP-адрес не указан, система предложит ввести IP-адрес после запуска команды <b>copy</b> |





### ➤ Пример

В следующем примере показано, как файл **main.bin** считывается с сервера, записывается на носитель коммутатора и переименовывается в **switch.bin**.

```
monitor# copy tftp flash
```

```
Prompt: Source file name[]?main.bin
```

```
Prompt: Remote-server ip address[]?192.168.20.1
```

```
Prompt: Destination file name[main.bin]?switch.bin
```

```
please wait ...
```

```
#####  
#####  
#####  
#####  
#####  
#####
```

```
TFTP:successfully receive 3377 blocks ,1728902 bytes
```

```
monitor#
```

## 2.1.5 Обновление конфигурации

Конфигурация коммутатора сохраняется в виде файла с именем startup-config. Для обновления конфигурации используются те же команды, что и для обновления программного обеспечения.

```
monitor# copy tftp flash startup-config
```

## 2.1.6 Обновление при помощи FTP

```
switch# copy ftp {flash | cf} [ip_addr | option]
```

Для обновления программного обеспечения и конфигурации в режиме управления можно использовать FTP. Введите команду **copy** для загрузки файла с FTP-сервера на коммутатор, а также для выгрузки файла из файловой системы коммутатора на FTP-сервер. После ввода команды система предложит ввести имя удаленного сервера и имя удаленного файла.

```
copy {ftp:[[/login-name:[login-password]@]location]/directory]/filename]} {flash<:filename>}  
{flash<:filename>}|ftp:[[/login-name: [login-password]@] location]/directory]/filename}  
<blksize> <mode> <type>
```



## ➤ Параметры

| Параметр       | Описание  |
|----------------|---|
| login-name     | Имя пользователя FTP-сервера<br>Если имя пользователя не указано, система предложит вам ввести его после запуска команды <b>copy</b>      |
| login-password | Пароль пользователя FTP-сервера<br>Если пароль пользователя не указан, система предложит вам ввести его после запуска команды <b>copy</b> |
| nchecksize     | Не проверять размер файла на сервере  |
| blksize        | Размер блока передаваемых данных<br>Значение по умолчанию: 512  |
| ip_addr        | IP-адрес FTP-сервера<br>Если IP-адрес не указан, система предложит ввести его после запуска команды <b>copy</b>                           |
| active         | Означает подключение FTP-сервера в активном режиме  |
| passive        | Означает подключение FTP-сервера в пассивном режиме   |
| type           | Установить режим передачи данных (ascii или binary)   |

## ➤ Пример

В следующем примере показано, как файл **main.bin** считывается с сервера, записывается на носитель коммутатора и переименовывается в **switch.bin**.

```
config# copy ftp flash
```

```
Prompt: ftp user name[anonymous]? login-name
```

```
Prompt: ftp user password[anonymous]? login-password
```

```
Prompt: Source file name[]?main.bin
```

```
Prompt: Remote-server ip address[]?192.168.20.1
```

```
Prompt: Destination file name[main.bin]?switch.bin
```

или

```
config# copy ftp://login-nam:login-password@192.168.20.1/main.bin flash:switch.bin
```

```
#####
```

```
#####
```

```
FTP:successfully receive 3377 blocks ,1728902 bytes
```



config#

Когда FTP-сервер не работает, время ожидания увеличивается. Если эта проблема вызвана временем ожидания TCP (значение по умолчанию – 75 с), вы можете настроить глобальную команду **ip tcp synwait-time** для изменения времени подключения TCP. Однако использовать эту функцию не рекомендуется.

При использовании FTP в некоторых сетевых средах скорость передачи данных может быть относительно низкой. Вы можете должным образом настроить размер блока передачи для получения наилучшего эффекта. Размер по умолчанию — 512 символов, что гарантирует относительно высокую скорость работы в большинстве сетей.

## 2.2 Базовые настройки управления системой

### 2.2.1 Настройка IP-адреса Ethernet

monitor# ip address <ip\_addr> <net\_mask>

Эта команда предназначена для настройки IP-адреса Ethernet. IP-адрес по умолчанию — 192.168.0.1, маска подсети — 255.255.255.0.

#### ➤ Параметры

| Параметр        | Описание               |
|-----------------|------------------------|
| <i>ip_addr</i>  | IP-адрес Ethernet      |
| <i>net_mask</i> | Маска подсети Ethernet |

#### ➤ Пример

monitor# ip address 192.168.1.1 255.255.255.0

### 2.2.2 Настройка маршрута по умолчанию

monitor# ip route default <ip\_addr>

Эта команда используется для настройки маршрута по умолчанию. Можно настроить только один такой маршрут.

#### ➤ Параметры

| Параметр       | Описание                    |
|----------------|-----------------------------|
| <i>ip_addr</i> | IP-адрес шлюза по умолчанию |

#### ➤ Пример

monitor# ip route default 192.168.1.1



## 2.2.3 Команда ping

```
monitor# ping <ip_address>
```

Эта команда предназначена для проверки состояния сетевого подключения.

### ➤ Параметры

| Параметр          | Описание            |
|-------------------|---------------------|
| <i>ip_address</i> | IP-адрес получателя |

### ➤ Пример

```
monitor# ping 192.168.20.100
```

```
PING 192.168.20.100: 56 data bytes
```

```
64 bytes from 192.168.20.100: icmp_seq=0. time=0. ms
```

```
64 bytes from 192.168.20.100: icmp_seq=1. time=0. ms
```

```
64 bytes from 192.168.20.100: icmp_seq=2. time=0. ms
```

```
64 bytes from 192.168.20.100: icmp_seq=3. time=0. ms
```

```
----192.168.20.100 PING Statistics----
```

```
4 packets transmitted, 4 packets received, 0% packet loss
```

```
round-trip (ms) min/avg/max = 0/0/0
```

## 2.3 Настройка HTTP

- Включение службы HTTP
- Изменение номера порта службы HTTP
- Настройка пароля доступа для службы HTTP
- Указание списка контроля доступа для службы HTTP

### 2.3.1 Включение службы HTTP

По умолчанию служба HTTP отключена. Она включается в режиме глобальной конфигурации с помощью следующей команды:

| Команда               | Описание              |
|-----------------------|-----------------------|
| <b>ip http server</b> | Запускает службу HTTP |



### 2.3.2 Изменение номера порта службы HTTP

Номер порта прослушивания для службы HTTP – 80. Его можно изменить в режиме глобальной конфигурации с помощью следующей команды:

| Команда                          | Описание                  |
|----------------------------------|---------------------------|
| <b>ip http port</b> {portNumber} | Изменяет номер HTTP-порта |

### 2.3.3 Настройка пароля доступа для службы HTTP

В качестве пароля доступа HTTP использует «enable». Если вы хотите выполнять аутентификацию для HTTP-доступа, необходимо установить пароль enable. Он устанавливается в режиме глобальной конфигурации с помощью следующей команды:

| Команда                           | Описание                    |
|-----------------------------------|-----------------------------|
| <b>enable password</b> {0 7} line | Устанавливает пароль enable |

### 2.3.4 Указание списка управления доступом для службы HTTP

Чтобы контролировать доступ хоста к HTTP-серверу, вы можете указать список контроля доступа для службы HTTP. Для этого используйте следующую команду в режиме глобальной конфигурации:

| Команда                            | Описание   |
|------------------------------------|--|
| <b>ip http access-class</b> STRING | Указывает список управления доступом для службы HTTP |

### 2.3.5 Примеры настройки HTTP

В следующем примере в качестве порта службы HTTP используется порт по умолчанию (80), а доступ ограничен адресом 192.168.20.0/24:

➤ **Настройка ip acl:**

```
ip access-list standard http-acl
permit 192.168.20.0 255.255.255.0
```

➤ **Глобальная конфигурация:**

```
ip http access-class http-acl
ip http server
```



## 3. Настройка терминала

### 3.1 Введение

Система использует команду **line** для настройки параметров терминала. С помощью нее можно настроить ширину и высоту окна, отображаемого терминалом.

В системе есть четыре типа линий: консоль, aid (асинхронный ввод-вывод), асинхронный и виртуальный терминал. Разные системы имеют разное количество линий этих типов. Обратитесь к руководству по настройке программного и аппаратного обеспечения для правильной настройки.

| Тип линии | Интерфейс                 | Описание  | Нумерация              |
|-----------|---------------------------|---|------------------------|
| CON(СТУ)  | Консоль                   | Для входа в систему с целью настройки   | 0                      |
| VTY       | Виртуальный и асинхронный | Для подключения Telnet, X.25 PAD, HTTP и удаленного входа в систему (rlogin) на синхронных портах, таких как Ethernet и последовательный порт | 32 номера, начиная с 1 |

### 3.2 Связь между линией и интерфейсом

Линия виртуального терминала обеспечивает синхронный интерфейс для доступа к системе. Когда вы подключаетесь к системе через линию VTY, вы фактически подключаетесь к виртуальному порту на интерфейсе. Для каждого синхронного интерфейса может быть много виртуальных портов.

Например, если к интерфейсу (Ethernet или последовательному порту) подключаются несколько Telnet, вам необходимо выполнить следующие процедуры настройки VTY:

- 1) войти в режим настройки линии;
- 2) настроить параметры терминала.

Для настройки VTY обратитесь к разделу 3.3 «Пример настройки VTY».

Чтобы проверить конфигурацию VTY, запустите команду **showline**.

### 3.3 Пример настройки VTY.

Данный пример показывает, как отменить ограничение количества строк на экран для всех VTY без запросов **more**:

```
config# line vty 0 32
```



config\_line# length 0

## 4. Настройка управления сетью

### 4.1 Настройка SNMP

#### 4.1.1 Введение

Система SNMP включает следующие части:

- Система управления SNMP (NMS)
- Агент SNMP (AGENT)
- Информационная база управления (MIB)

SNMP – это протокол управления сетевыми устройствами через TCP/IP, работающий на прикладном уровне. С помощью него NMS и агенты обмениваются пакетами данных для управления сетью.

Система управления SNMP может быть частью системы управления сетью. Агент и MIB хранятся в системе. Перед настройкой SNMP в системе необходимо определить взаимосвязь между системой управления сетью и агентом.

Агент SNMP содержит переменные MIB. Система управления SNMP может проверять или изменять значения этих переменных. Система управления может получить значение переменной от агента или сохранить значение переменной для агента. Агент собирает данные из MIB. MIB — это база данных параметров устройства и сетевых настроек. Агент также может реагировать на загрузку системы управления или запрос на настройку данных. Агент SNMP может отправлять прерывания в систему управления. Агенты отправляют в NMS Trap-сообщения, содержащие информацию о тревоге при определенном состоянии сети. Trap-сообщение может указывать на неправильную аутентификацию пользователя, перезагрузку, состояние канала связи (включено или выключено), закрытие TCP-соединения, потерю соединения с соседними системами или другие важные события.

#### ➤ SNMP-уведомление

Когда происходят какие-то особые события, система отправляет информационные сообщения в NMS. Например, когда агент обнаруживает ненормальное состояние сети, он отправляет информацию в систему управления.

SNMP-уведомления можно рассматривать как trap-сообщения или информационные запросы (inform request). Поскольку принимающая сторона не отправляет никакого ответа при получении trap-сообщения, это приводит к тому, что принимающая сторона не может быть уверена, что сообщение было получено. Поэтому система уведомлений посредством Trap-сообщений ненадежна. Для сравнения, система управления SNMP, которая получает информационный запрос, использует PDU, который SNMP отображает в качестве ответа на эту информацию. Если в NMS не получен информационный запрос, эхо-ответ не будет отправлен. Если принимающая сторона не отправляет никакого ответа, агент может повторно отправить информационный запрос. Так уведомления в конечном итоге достигают своего назначения.



Поскольку информационные запросы более надежны, они потребляют больше ресурсов системы и сети. Trap-сообщение удаляется после отправки. Информационный запрос должен храниться в памяти до тех пор, пока не будет получено эхо или не истечет время ожидания. Кроме того, trap отправляется только один раз, а inform request может быть неоднократно отправлен повторно. Повторная отправка запроса создает дополнительную коммуникационную активность и увеличивает нагрузку на сеть. Таким образом, чередование отправки сообщений типа trap и inform request обеспечивает баланс между надежностью и использованием ресурсов. Если системе управления SNMP очень важно получать каждое уведомление, имеет смысл использовать информационный запрос. Если приоритет отдается количеству коммуникационных сообщений в сети, и нет необходимости получать каждое уведомление, то можно использовать trap.

Данный коммутатор поддерживает только trap-сообщения, но для него может быть предоставлено расширение, позволяющее отправлять запросы типа inform request.

### ➤ Версия SNMP

Система поддерживает следующие версии SNMP:

SNMPv1 – простой протокол управления сетью, полный интернет-стандарт, определенный в документе сетевых стандартов RFC1157.

SNMPv2C – архитектура управления, основанная на группах. Интернет-стандарт протокола для тестирования, который определен в документе сетевых стандартов RFC1901.

Коммутатор 3-го уровня также поддерживает следующие SNMP:

SNMPv3 – простой протокол управления сетью версии 3, определенный в RFC3410.

SNMPv1 применяет групповой формат безопасности. Используйте список управления доступом к IP-адресу и пароль, чтобы определить группу NMS, которая может получить доступ к MIB агента.

SNMPv3 обеспечивает безопасный доступ к устройствам за счет комбинации проверки подлинности и шифрования пакетов по сети.

В SNMPv3 реализованы следующие функции безопасности:

целостность сообщения — гарантия того, что пакет не был изменен при передаче;

аутентификация — определение того, что сообщение получено из достоверного источника;

шифрование — шифрование содержимого пакета предотвращает его просмотр неавторизованным источником.

SNMPv3 обеспечивает как модели безопасности, так и уровни безопасности. Модель безопасности — это стратегия проверки подлинности, настроенная для пользователя и группы, в которой находится пользователь. Уровень безопасности — это допустимый уровень безопасности в рамках модели безопасности. Сочетание модели безопасности и уровня безопасности определяет, какой механизм безопасности используется при обработке SNMP-пакета. Доступны три модели безопасности, то есть аутентификация и шифрование, аутентификация и отсутствие шифрования, отсутствие аутентификации.

Вам необходимо настроить агент SNMP на версию SNMP, которую поддерживает рабочая станция управления. Агент может общаться со многими NMS.



### ➤ Поддерживаемые MIB

SNMP данной системы поддерживает все переменные MIBII (RFC 1213) и trap-сообщения SNMP (RFC 1215).

Для каждой системы предоставляется собственное расширение MIB.

## 4.1.2 Задачи настройки SNMP

Команды настройки SNMP включают:

- настройку представления SNMP;
- создание или изменение контроля доступа для сообщества SNMP;
- настройку способа связи системного администратора и системы;
- определение максимальной длины пакета данных агента SNMP;
- мониторинг состояния SNMP;
- настройку локального ядра SNMP;
- настройку Trap-сообщений SNMP;
- настройку группы SNMPv3;
- настройку пользователя SNMPv3;
- настройку шифрования SNMP-сервера;
- настройку источника Trap-сообщений SNMP-сервера;
- настройку времени ожидания Trap-сообщений SNMP-сервера;
- настройку SNMP-сервера для отправки трапов на указанный хост с использованием имен хостов;
- настройку trap-логов SNMP-сервера;
- настройку количества повторных сообщений;
- настройку времени поддержания активности;
- настройку кодирования SNMP-сервера;
- настройку идентификатора события SNMP-сервера;
- настройку тайм-аута для SNMP getBulk-запросов;
- настройку задержки для SNMP getBulk-запросов;
- отображение информации о работе SNMP;
- отображение отладочной информации SNMP.



### 4.1.3 Настройка представления SNMP

Представления SNMP предназначены для регулирования прав доступа (включение или исключение) для MIB. Используйте следующую команду для настройки представления:

| Команда   | Описание   |
|---|--|
| <b>snmp-server view</b> <i>name oid</i> [ <b>excluded</b>   <b>included</b> ] | Добавляет поддерево или таблицу определяемой идентификатором OID базы MIB в SNMP-представление. В процессе также указывается уровень доступа к этому объекту (идентификатору) в рамках данного представления |

Подмножества, к которым можно получить доступ в представлении SNMP, – это оставшиеся объекты, которые «включают» объекты MIB, разделенные «исключаемыми» объектами. Объекты, которые не настроены, по умолчанию недоступны.

После создания и настройки представления SNMP вы можете добавить его к конфигурации определенной группы, чтобы ограничить доступ этой группы только к тем объектам, которые разрешены в соответствующем SNMP-представлении.

### 4.1.4 Создание или изменение контроля доступа для SNMP-КОМЬЮНИТИ

Символьную строку комьюнити можно использовать для определения связи между управляющей системой SNMP и агентом. Эта строка аналогична паролю, который разрешает системе доступ к агенту. Вы можете указать одно или несколько свойств, относящихся к строке комьюнити. Эти свойства являются необязательными:

- разрешение использовать строку комьюнити для получения списка доступа по IP-адресу в системе управления SNMP;
- определение представлений MIB всех подмножеств объектов MIB, которые могут получить доступ к указанному комьюнити;
- указание комьюнити с правами на чтение и запись доступных объектов MIB.

Настройте символьную строку комьюнити в режиме глобальной конфигурации с помощью следующей команды:

| Команда   | Описание                             |
|---|--------------------------------------|
| <b>snmp-server community</b> [ <b>0 7</b> ] <i>string</i> [ <b>view view-name</b> ] [ <b>ro</b>   <b>rw</b> ] [ <i>word</i> ] | Определяет строку группового доступа |

Вы можете настроить одну или несколько строк группового доступа. Запустите команду **no snmp-server community**, чтобы удалить указанную строку.



#### 4.1.5 Настройка способа связи системного администратора и местоположения системы

SysContact и sysLocation — это переменные управления в системной группе MIB, соответственно определяющие идентификатор оператора связи и фактическое местоположение контролируемого узла. Доступ к этой информации можно получить через config-файлы. Используйте следующие команды в режиме глобальной конфигурации:

| Команда                          | Описание                                       |
|----------------------------------|--|
| <b>snmp-server contact text</b>  | Задаёт символьную строку контактного лица узла |
| <b>snmp-server location text</b> | Задаёт символьную строку местонахождения узла  |

#### 4.1.6 Определение максимальной длины пакета данных агента SNMP

Когда агент SNMP получает запросы или отправляет ответы, пакеты данных имеют определённую длину. Для настройки максимальной длины пакета используйте следующую команду в режиме глобальной конфигурации:

| Команда                                  | Описание                          |
|--|-----------------------------------|
| <b>snmp-server packetsize byte-count</b> | Задаёт максимальный размер пакета |

#### 4.1.7 Мониторинг состояния SNMP

Вы можете запустить следующую команду в режиме глобальной конфигурации, чтобы отслеживать статистику вывода/ввода SNMP, включая недопустимые элементы символьной строки комьюнити, количество ошибок и переменные запроса.

| Команда          | Описание                    |
|------------------|-----------------------------|
| <b>show snmp</b> | Отслеживание состояния SNMP |

#### 4.1.8 Настройка локального ядра SNMP

Используйте следующую команду, чтобы настроить систему для отправки данных локального ядра SNMP:



| Команда   | Описание                       |
|---|--------------------------------|
| <b>snmp-server engineID local</b> <i>engineID</i> | Настройка локального ядра SNMP |

## 4.1.9 Настройка SNMP Trap

Используйте следующую команду, чтобы настроить систему для отправки trap-сообщений (вторая задача не является обязательной):

### ➤ Настройка системы для отправки

Запустите следующие команды в режиме глобальной конфигурации, чтобы настроить систему для отправки сообщений на хост.

| Команда   | Описание   |
|---|--|
| <b>snmp-server host hostv6</b> <i>host community-string</i> [ <i>trap-type</i> ]  | Указывает получателя Trap-сообщения  |
| <b>snmp-server host</b> <i>host</i> [traps   informs] {version {v1   v2c   v3 {auth   noauth   priv}}} <i>community-string</i> [ <i>trap-type</i> ] | Указывает получателя, номер версии и имя пользователя для Trap-сообщения<br><br>В SNMPv3 необходимо указать engine ID для хоста до того, как хост будет настроен на получение trap-сообщений |

При запуске системы автоматически запускается агент SNMP. Активируются все типы Trap-сообщений. Вы можете использовать команду **snmp-server host**, чтобы указать, какой хост будет получать какие сообщения.

Некоторыми сообщениями нужно управлять с помощью других команд. Например, если вы хотите, чтобы сообщения о состоянии связи отправлялись при открытии или закрытии интерфейса, вам нужно запустить **snmp trap link-status** в режиме настройки интерфейса. Чтобы отключить эти trap-сообщения, запустите команду **snmp trap link-stat**.

Вы должны настроить команду **snmp-server host**, чтобы хост получал trap-сообщения.

### ➤ Изменение текущего параметра trap

В качестве необязательного элемента можно указать исходный интерфейс, на котором возникают сообщения, длину очереди сообщений или значение интервала повторной отправки для каждого хоста.

Чтобы изменить параметры trap, вы можете запустить следующие необязательные команды в режиме глобальной конфигурации:



| Команда   | Описание  |
|---|---|
| <b>snmp-server trap-source</b> <i>interface</i> | Определяет исходный интерфейс, на котором создаются trap-сообщения, и задает для них исходный IP-адрес    |
| <b>snmp-server queue-length</b> <i>length</i>   | Создает длину очереди сообщений для каждого хоста, имеющего функцию trap. Значение по умолчанию: 10       |
| <b>snmp-server trap-timeout</b> <i>seconds</i>  | Определяет частоту отправки trap-сообщений в очереди повторной отправки. Значение по умолчанию: 30 секунд |

## 4.1.10 Настройка адреса источника SNMP

Выполните следующую команду в режиме глобальной конфигурации, чтобы задать исходный адрес для сообщения SNMP:

| Команда                                  | Описание  |
|--|---|
| <b>snmp source-addr</b> <i>ipaddress</i> | Устанавливает исходный адрес для сообщений SNMP |

## 4.1.11 Пример настройки

```
snmp-server community public RO
```

```
snmp-server community private RW
```

```
snmp-server host 192.168.10.2 public
```

Вы можете использовать строку комьюнити **public** для чтения переменных MIB в системе. Вы также можете использовать строку комьюнити **private** для чтения переменных MIB и записи записываемых переменных MIB в системе.

Приведенная выше команда указывает общедоступную строку сообщества для отправки trap-сообщений на 192.168.10.2, когда этого требует система. Например, когда порт находится в нерабочем состоянии, система отправит информационное сообщение linkdown по адресу 192.168.10.2.

## 4.2 Настройка RMON

### 4.2.1 Задачи настройки RMON

Задачи настройки RMON включают в себя:



- настройку функции аварийного сигнала;
- настройку функции события;
- настройку функции статистики;
- настройку функции истории;
- отображение конфигурации коммутатора.

## 4.2.2 Настройка сигнализации

Вы можете настроить функцию тревоги RMON через командную строку или SNMP NMS. Если вы настраиваете через SNMP NMS, вначале необходимо настроить SNMP коммутатора. После настройки функции тревоги устройство может отслеживать определенные статистические значения в системе. В следующей таблице показано, как настроить функцию аварийного сигнала RMON:

| Команда   | Описание  |
|---|---|
| <b>config</b>   | Вход в режим глобальной конфигурации  |
| <b>rmon alarm</b> <i>index variable interval {absolute   delta} rising-threshold value [eventnumber] falling-threshold value [eventnumber] [owner string]</i> | <p>Добавление элемента тревоги RMON</p> <p><b>index</b> – это номер элемента тревоги. Диапазон составляет от 1 до 65535</p> <p><b>variable</b> – переменная, объект в отслеживаемой MIB. Объект должен быть активным и корректно функционировать в системе MIB. могут быть обнаружены только объекты определенных типов, таких как Integer (целочисленные значения), Counter (счетчики), Gauge (измерительные приборы) или Time Ticks (единицы времени)</p> <p><b>interval</b> – временной интервал для выборки. Единица измерения – секунда. Значение — от 1 до 4 294 967 295</p> <p><b>absolute</b> – используется для прямого контроля значения объекта MIB.</p> <p><b>delta</b> – используется для отслеживания изменения значений объектов MIB между двумя выборками</p> <p><b>value</b> — это пороговое значение, при котором генерируется аварийный сигнал</p> <p><b>event number</b> — это индекс события, которое генерируется при достижении порога. Не является обязательным</p> |



|              |  |
|--------------|--|
|              | <b>owner string</b> – строка владельца, предназначена для информации о тревоге |
| <b>exit</b>  | Вернуться в режим управления   |
| <b>write</b> | Сохранить настройки  |

После настройки элемента аварийного сигнала RMON устройство через определенный интервал времени получит значение указанного в переменной OID. Полученное значение будет сравниваться с предыдущим значением в зависимости от типа тревоги (абсолютная или дельта). Если значение, полученное из определенного OID, превышает предыдущее значение и пороговое значение, будет сгенерировано событие с указанным индексом **eventnumber**. Если значение **eventnumber** равно 0 или событие с указанным индексом отсутствует в таблице событий, ничего не произойдет. Если невозможно получить значение из указанного в переменной OID, состояние элемента тревоги в этой строке определяется как недопустимое. Если вы запускаете **rmon alarm** много раз для настройки элементов сигналов тревоги с одним и тем же индексом, действительной будет только последняя конфигурация. Для отмены конфигураций с определенным индексом можно использовать команду **no rmon alarm index**.

### 4.2.3 Настройка события

Этапы настройки события RMON показаны в следующей таблице:

| Команда   | Описание   |
|---|--|
| <b>config</b>   | Вход в режим глобальной конфигурации   |
| <b>rmon event index</b><br>[ <b>description string</b> ]<br>[ <b>log</b> ] [ <b>owner string</b> ]<br>[ <b>trap community</b> ] | Добавление события RMON<br><b>index</b> – означает номер элемента события. Диапазон составляет от 1 до 65 535<br><b>description</b> – описание, означает информацию о событии<br><b>log</b> – означает добавление части информации в таблицу журнала при возникновении события<br><b>trap</b> – означает, что при возникновении события генерируется trap-сообщение<br><b>community</b> – означает имя сообщества<br><b>owner string</b> – строка владельца, предназначена для информации о событии. |
| <b>exit</b>   | Вернуться в режим управления   |
| <b>write</b>  | Сохранить настройки  |



После того как вы настроили событие RMON, необходимо установить параметр **eventLastTimeSent** для этого события в значение **sysUpTime** при срабатывании сигнала тревоги. Если для события RMON задан атрибут **log**, в таблицу журнала добавляется сообщение. Если для события RMON задан атрибут **trap**, от имени комьюнити отправляется trap-сообщение. Если вы запускаете **rmon event** много раз для настройки элементов событий с одним и тем же индексом, будет действительна только последняя конфигурация. Для отмены элементов событий с определенным индексом можно использовать команду **no rmon event index**.

## 4.2.4 Настройка статистики

Группа статистики RMON используется для мониторинга статистической информации по каждому порту устройства. Этапы настройки статистики следующие:

| Команда   | Описание  |
|---|---|
| <b>config</b>                                     | Вход в режим глобальной конфигурации  |
| <b>interface iftype ifid</b>                      | Вход в режим настройки интерфейса<br><b>iftype</b> – означает тип порта<br><b>ifid</b> – означает идентификатор интерфейса                                    |
| <b>rmon collection stats index [owner string]</b> | Разрешить сбор статистики на порту<br><b>index</b> – означает индекс статистики<br><b>owner</b> – строка владельца, предназначена для информации о статистике |
| <b>exit</b>                                       | Вернуться в режим глобальной конфигурации   |
| <b>exit</b>                                       | Вернуться в режим управления  |
| <b>write</b>                                      | Сохранить настройки   |

Если вы запускаете **rmon collection stat** много раз для настройки элементов статистики с одним и тем же индексом, будет актуальна только последняя конфигурация. Вы можете запустить **no rmon collection stats index**, чтобы отменить элементы статистики с указанным индексом.

## 4.2.5 Настройка истории

Группа истории RMON используется для сбора статистической информации в различных временных интервалах на порту устройства. Функция истории настраивается следующим образом:



| Команда   | Описание  |
|---|---|
| <b>config</b>   | Вход в режим глобальной конфигурации  |
| <b>interface</b> <i>iftype ifid</i>   | Вход в режим настройки интерфейса<br><b>iftype</b> – означает тип порта<br><b>ifid</b> – означает идентификатор интерфейса  |
| <b>rmon collection history</b> <i>index</i><br>[ <b>buckets</b> <i>bucket-number</i> ] [ <b>interval</b> <i>second</i> ] [ <b>owner</b> <i>string</i> ] | Включить функцию истории на порту<br><b>index</b> – порядковый номер элемента истории<br><b>bucket-number</b> – определяет количество «корзин» или записей, которые будут храниться в истории. Каждая «корзина» содержит данные за определённый интервал времени. Значение по умолчанию обычно составляет 50<br><b>second</b> – означает временной интервал получения статистических данных. Значение по умолчанию – 1800 секунд<br><b>owner</b> – строка владельца используется для информации об элементе истории |
| <b>exit</b>   | Вернуться в режим глобальной конфигурации   |
| <b>exit</b>   | Вернуться в режим управления  |
| <b>write</b>  | Сохранить настройки   |

После добавления элемента истории RMON устройство будет получать данные статистики с указанного порта через интервал, равный значению **second**. Эти данные будут добавлены к элементу истории как часть информации. Если вы запускаете **rmon collection history index** много раз для настройки элементов истории с одним и тем же индексом, действительной будет только последняя конфигурация. Вы можете запустить **no rmon collection history index**, чтобы отменить элементы истории с указанным индексом.



Если значение «bucket-number» слишком велико или значение интервала «second» слишком мало, сбор истории потребует много системных ресурсов.

## 4.2.6 Отображение конфигурации RMON коммутатора

Запустите **show**, чтобы отобразить конфигурацию коммутатора.

| Команда | Описание |
|---------|----------|
|         |          |



|  |  |
|--|--|
| <pre>show rmon [alarm] [event]    [statistics] [history]</pre> | <p>Отображает информацию о настройках</p> <p><b>alarm</b> – означает отображение конфигурации элемента тревоги</p> <p><b>event</b> – означает отображение конфигурации элемента события и элементов, которые генерируются при возникновении событий и содержатся в таблице журнала</p> <p><b>statistics</b> – означает отображение конфигурации элемента статистики и значений статистики, которые устройство собирает с порта</p> <p><b>history</b> – означает отображение настроек элемента истории и значений статистики, которые устройство собирает с порта в последние заданные промежутки времени</p> |
|--|--|

## 4.3 Настройка PDP

### 4.3.1 Введение

PDP (Protocol Discovery Protocol) – двухуровневый протокол, применяемый для обнаружения сетевого оборудования. Он используется в NMS для определения всех соседей уже известного устройства. PDP позволяет вам узнать адрес агента SNMP и типы соседних устройств. После обнаружения соседних устройств через PDP, NMS может запрашивать соседние устройства через SNMP для получения топологии сети.

Коммутаторы данной серии могут обнаруживать соседние устройства при помощи PDP, но не могут запрашивать соседние устройства через SNMP. Поэтому эти коммутаторы должны располагаться на границе сетей. В противном случае не удастся получить полную сетевую топологию.

PDP можно настроить на всех SNAP (например, Ethernet).

### 4.3.2 Задачи настройки PDP

- Конфигурация PDP по умолчанию
- Настройка частоты PDP и времени хранения информации
- Установка версии PDP
- Запуск PDP на коммутаторе
- Запуск PDP на порту
- Мониторинг и управление PDP



### 4.3.3 Конфигурация PDP по умолчанию

| Функция   | Настройки по умолчанию |
|---|------------------------|
| Режим глобальной настройки                      | Выключено              |
| Режим настройки интерфейса                      | Запускается            |
| Тактовая частота PDP (частота передачи пакетов) | 60 секунд              |
| Хранение информации PDP                         | 180 секунд             |
| Версия PDP                                      | 2                      |

### 4.3.4 Настройка частоты PDP и времени хранения информации

Чтобы установить частоту передачи пакетов PDP и время хранения информации PDP, вы можете выполнить следующие команды в режиме глобальной настройки:

| Команда                     | Описание                                    |
|-----------------------------|---|
| <b>pdp timer seconds</b>    | Устанавливает частоту передачи пакетов PDP  |
| <b>pdp holdtime seconds</b> | Устанавливает время хранения информации PDP |

### 4.3.5 Установка версии PDP

Чтобы установить версию PDP, вы можете запустить следующую команду в режиме глобальной настройки:

| Команда                  | Описание                 |
|--------------------------|--------------------------|
| <b>pdp version {1 2}</b> | Устанавливает версию PDP |

### 4.3.6 Запуск PDP на коммутаторе

Чтобы включить PDP, вы можете запустить следующую команду в режиме глобальной настройки:

| Команда        | Описание                    |
|----------------|-----------------------------|
| <b>pdp run</b> | Включает PDP на коммутаторе |



### 4.3.7 Запуск PDP на порту

Чтобы включить PDP на порту, вы можете запустить следующую команду в режиме настройки интерфейса:



| Команда           | Описание                           |
|-------------------|------------------------------------|
| <b>pdp enable</b> | Запускает PDP на порту коммутатора |

### 4.3.8 Мониторинг и управление PDP

Для мониторинга PDP выполните следующие команды в режиме EXEC:

| Команда                           | Описание  |
|-----------------------------------|---|
| <b>show pdp traffic</b>           | Отображает количество полученных и переданных пакетов PDP |
| <b>show pdp neighbor [detail]</b> | Отображает соседние устройства, которые обнаруживает PDP  |

### 4.3.9 Примеры настройки PDP

➤ **Пример 1. Запуск PDP**

```
Switch_config# pdp run
Switch_config# int g0/1
Switch_config_g0/1# pdp enable
```

➤ **Пример 2. Настройка частоты PDP и времени хранения информации**

```
Switch_config# pdp timer 30
Switch_config# pdp holdtime 90
```

➤ **Пример 3. Установка версии PDP**

```
Switch_config# pdp version 1
```

➤ **Пример 4. Мониторинг PDP**

```
Switch_config# show pdp neighbor
```

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater

```
Device-ID Local-Intf Hldtme Port-ID Platform Capability
Switch Gig0/1 169 Gig0/1 COM, RISC R S
```



## 4.4 Команды настройки SSH

### 4.4.1 Введение

Безопасное и зашифрованное коммуникационное соединение может быть создано между клиентом SSH и устройством через сервер SSH. Соединение имеет telnet-подобные функции. Сервер SSH поддерживает алгоритмы шифрования, включая des, 3des и blowfish.

Клиент SSH – это приложение, работающее по протоколу SSH. Он может обеспечивать аутентификацию и шифрование, поэтому гарантирует безопасную связь между коммуникационными устройствами или устройствами, поддерживающими SSH, даже если они работают в небезопасных сетевых условиях. Клиент SSH поддерживает алгоритмы шифрования, включая des, 3des и blowfish.

Сервер и клиент поддерживают версию SSH 1.5. Оба они поддерживают только приложение оболочки.

### 4.4.2 Настройка методов аутентификации

SSH-сервер использует режим аутентификации по логину и паролю. По умолчанию он использует список методов аутентификации **default**.

Выполните следующую команду в командном режиме глобальной конфигурации, чтобы настроить список методов аутентификации:

| Команда                                  | Описание                                  |
|--|---|
| <b>ip sshd auth_method</b> <i>STRING</i> | Настраивает список методов аутентификации |

### 4.4.3 Настройка списка управления доступом

Чтобы контролировать доступ к SSH-серверу, необходимо настроить для него список управления доступом. Выполните следующую команду в режиме глобальной конфигурации:

| Команда                                   | Описание                               |
|---|--|
| <b>ip sshd access-class</b> <i>STRING</i> | Настраивает список управления доступом |

### 4.4.4 Настройка времени ожидания аутентификации

После установления соединения между клиентом и сервером сервер прерывает связь, если аутентификация не может быть подтверждена в течение установленного времени. Выполните следующую команду в режиме глобальной конфигурации, чтобы настроить значение времени ожидания аутентификации:



| Команда                                       | Описание                                  |
|---|---|
| <code>ip sshd timeout &lt;60-65535&gt;</code> | Настраивает время ожидания аутентификации |

#### 4.4.5 Настройка количества повторных попыток аутентификации

Если количество неудачных попыток аутентификации превышает максимальное количество, SSH-сервер не позволит вам повторить аутентификацию, пока не будет установлено новое соединение. По умолчанию допускается 3 повторных попытки аутентификации.

Выполните следующую команду в режиме глобальной конфигурации, чтобы настроить максимальное количество повторных попыток аутентификации:

| Команда   | Описание   |
|---|--|
| <code>ip sshd auth-retries &lt;0-65535&gt;</code> | Настраивает максимальное количество повторных попыток аутентификации |

#### 4.4.6 Включение SSH-сервера

SSH-сервер по умолчанию отключен. Когда сервер SSH включен, устройство будет генерировать пару ключей RSA, а затем прослушивать запросы на подключение от клиента. Процесс занимает одну-две минуты.

Выполните следующую команду в режиме глобальной конфигурации, чтобы включить сервер SSH:

| Команда                     | Описание  |
|-----------------------------|---|
| <code>ip sshd enable</code> | Включает SSH-сервер. Используется 1024-битный ключ для шифрования |

#### 4.4.7 Пример настройки SSH-сервера

Следующая конфигурация разрешает доступ к SSH-серверу только хосту с IP-адресом 192.168.20.40. Для распознавания идентификатора пользователя применяется локальная база данных пользователей.

##### ➤ Список контроля доступа

```
ip access-list standard ssh-acl
permit 192.168.20.40
```



➤ **Глобальная настройка**

```
aaa authentication login ssh-auth local
ip sshd auth-method ssh-auth
ip sshd access-class ssh-acl
ip sshd enable
```

## 5. Настройка основных параметров интерфейсов

### 5.1 Введение

Этот раздел описывает различные типы интерфейсов, поддерживаемые коммутатором, и их конфигурации. Также рассматриваются основные команды, используемые при настройке интерфейсов.

➤ **Поддерживаемые типы интерфейсов**

Информацию о типах интерфейсов см. в следующей таблице:

| Тип интерфейса       | Описание   |
|----------------------|--|
| Интерфейс Ethernet   | Ethernet<br>Fast Ethernet<br>Gigabit Ethernet  |
| Логический интерфейс | Интерфейс Loopback<br>Нулевой интерфейс<br>Интерфейс VLAN<br>Интерфейс SuperVLAN<br>Интерфейс группы агрегации |

Поддерживаются два типа интерфейса: интерфейс Ethernet и логический интерфейс. Тип Ethernet-интерфейса зависит от конфигурации конкретного устройства, а также наличия сетевой карты или модуля, установленного на коммутаторе. Логический интерфейс – это виртуальный порт, изначально не имеющий соответствующего физического устройства, который настраивается пользователем вручную.

Поддерживаемые интерфейсы Ethernet данного коммутатора включают:

- интерфейс Ethernet;
- интерфейс Fast Ethernet;
- интерфейс Gigabit Ethernet.

Поддерживаемые логические интерфейсы включают:



- интерфейс Loopback
- нулевой интерфейс
- интерфейс группы агрегации;
- интерфейс VLAN.

#### ➤ Общие принципы настройки

Данное описание относится к процессу настройки всех интерфейсов. Выполните следующие шаги в режиме глобальной конфигурации.

1. Запустите команду **interface**, чтобы войти в режим настройки интерфейса. В это время подсказка в командной строке показывает «config\_» и сокращенную форму названия интерфейса, который необходимо настроить. Используйте интерфейсы в порядке возрастания их номеров. Номера назначаются во время установки или при добавлении сетевой карты в систему. Запустите команду **show interface**, чтобы отобразить эти интерфейсы. Каждый интерфейс, поддерживаемый устройством, отображает собственное состояние следующим образом:

```
Switch# show interface g1/1
GigaEthernet1/1 is down, line protocol is down
Hardware is Fast Ethernet, Address is 0009.7cf7.7dc1
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Auto-duplex, Auto-speed
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 17:52:52, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1 packets input, 64 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
```



0 input packets with dribble condition detected  
1 packets output, 64 bytes, 0 underruns  
0 output errors, 0 collisions, 1 interface resets  
0 babbles, 0 late collision, 0 deferred  
0 lost carrier, 0 no carrier, 0 PAUSE output  
0 output buffer failures, 0 output buffers swapped out

Чтобы настроить интерфейс Gigabit Ethernet g1/1, введите следующую команду:

```
interface GigaEthernet1/1
```

Коммутатор выведет запрос «config\_g1/1».



Нет необходимости добавлять пробел между типом интерфейса и его номером. Например, в приведенном примере возможны оба варианта написания: g1/1 или g 1/1.

2. Вы можете проверить действие различных команд в режиме настройки интерфейса. Команды определяют протоколы и прикладные программы, которые должны выполняться на интерфейсе. Эти команды будут действовать до тех пор, пока пользователь не выйдет из режима настройки интерфейса или не переключится на другой интерфейс.

3. После завершения настройки интерфейса для проверки его состояния используйте команду **show** (см. раздел «Мониторинг и поддержка интерфейса»).

## 5.2 Настройка общих атрибутов интерфейса

Далее описываются команды настройки общих атрибутов, которые можно выполнить на интерфейсе любого типа. Настраиваемые общие атрибуты включают описание интерфейса, пропускную способность, задержку и т.д.

### 5.2.1 Добавление описания

Добавление описания интерфейса помогает запомнить установленные на нем настройки. Это описание служит только примечанием к интерфейсу, чтобы помочь определить цель его использования, и не влияет на какие-либо функции. Описание возвращается командами **show running-config** и **show interface**. Для добавления описания введите следующую команду в режиме настройки интерфейса:



| Команда                          | Описание   |
|----------------------------------|--|
| <b>description</b> <i>string</i> | Добавляет описание для настраиваемого интерфейса |

Для получения более полной информации см. раздел «Примеры настройки интерфейса».

## 5.2.2 Настройка полосы пропускания

Протокол передачи данных использует информацию о пропускной способности интерфейса для принятия решения о ходе выполнения операции. Введите следующую команду, чтобы настроить пропускную способность интерфейса:

| Команда                         | Описание  |
|---------------------------------|---|
| <b>bandwidth</b> <i>kilobps</i> | Указывает ширину полосы пропускания настраиваемого интерфейса |

Полоса пропускания – это всего лишь параметр маршрутизации, который не влияет на скорость передачи данных по фактическому физическому интерфейсу.

## 5.2.3 Настройка временной задержки

Протокол передачи данных использует информацию о временной задержке интерфейса для принятия решения о ходе выполнения операции. В режиме настройки интерфейса введите следующую команду, чтобы настроить временную задержку:

| Команда                                | Описание   |
|--|--|
| <b>delay</b> <i>tensofmicroseconds</i> | Указывает временную задержку для настраиваемого интерфейса |

Конфигурация временной задержки является просто информационным параметром. Эта команда не может настроить фактическую задержку интерфейса.

## 5.3 Мониторинг и поддержка интерфейса

При помощи следующих операций можно контролировать и поддерживать интерфейс:

- проверка состояния интерфейса;
- инициализация и удаление интерфейса;
- выключение и включение интерфейса.



### 5.3.1 Проверка состояния интерфейса

Коммутатор поддерживает несколько команд, связанных с отображением информации об интерфейсе, включая номер версии программного и аппаратного обеспечения, состояние интерфейса. В следующей таблице перечислены некоторые команды для мониторинга интерфейса:

| Команда                                  | Описание                                   |
|--|--|
| <b>show interface</b> [type [slot port]] | Отображает состояние интерфейса            |
| <b>show running-config</b>               | Отображает текущую конфигурацию            |
| <b>show version</b>                      | Отображает версию программного обеспечения |

### 5.3.2 Инициализация и удаление интерфейса

Вы можете динамически устанавливать и удалять логические интерфейсы. Это также относится к субинтерфейсу и многоканальному интерфейсу. Используйте следующую команду для инициализации и удаления интерфейса в режиме глобальной конфигурации:

| Команда                                | Описание  |
|--|---|
| <b>no interface</b> [type [slot port]] | Инициализирует физический интерфейс или удаляет виртуальный |

### 5.3.3 Выключение и включение интерфейса

Когда интерфейс закрыт, все функции этого интерфейса отключаются, а сам он помечается как недоступный во всех командах мониторинга. Эта информация может передаваться другим коммутаторам по протоколу динамической маршрутизации.

Используйте следующую команду, чтобы отключить или включить интерфейс в режиме настройки интерфейса:

| Команда            | Описание            |
|--------------------|---------------------|
| <b>shutdown</b>    | Выключает интерфейс |
| <b>no shutdown</b> | Включает интерфейс  |

Вы можете использовать команду **show interface** и команду **show running-config**, чтобы проверить, был ли закрыт интерфейс. Отключенный интерфейс, отображается как «administratively down» в ответе команды **show interface**. Для получения более подробной информации см. раздел «Примеры настройки интерфейса».



## 5.4 Настройка интерфейса Ethernet

В этом разделе описана процедура настройки интерфейса Ethernet. Подробная процедура включает несколько шагов, среди которых обязательным является только первый.

### 5.4.1 Выбор интерфейса Ethernet

Выполните следующую команду в режиме глобальной настройки, чтобы войти в режим настройки интерфейса Ethernet:

| Команда   | Описание   |
|---|--|
| <b>interface fastethernet</b> [ <i>slot</i>   <i>port</i> ] | Вход в режим настройки интерфейса Fast-Ethernet    |
| <b>interface gigaethernet</b> [ <i>slot</i>   <i>port</i> ] | Вход в режим настройки интерфейса Gigabit-Ethernet |

Для отображения состояния интерфейса может использоваться команда **show interface gigaethernet** [**fastethernet**] [*slot* | *port*].

### 5.4.2 Настройка скорости

Скорость Ethernet может быть реализована с помощью автосогласования или с помощью настройки интерфейса.

| Команда  | Описание  |
|--|---|
| <b>speed</b> { <b>10</b>   <b>100</b>   <b>auto</b> } (T port)<br><b>speed</b> { <b>100</b>   <b>1000</b>   <b>auto</b> } (SFP port) | Устанавливает скорость Ethernet на 10М, 100М, 1000М или автосогласование                  |
| <b>no speed</b>  | Восстанавливает настройки по умолчанию. Скорость устанавливается в режим автосогласования |



Скорость SFP зависит от его модели. Например, скорость GBIC и GE-FX составляет 1000 Мбит/с, но при настройке ее также можно указать равной 100 Мбит/с. Скорость FE-FX составляет 100М. Если после команды **speed** есть параметр **auto**, интерфейс может включить функцию автоматического согласования. В противном случае скорость является фиксированной и не может быть согласована. Гигабитный порт может автоматически поддерживать режим 10 100 1000, тогда как для порта 100М автосогласование отключено.



### 5.4.3 Настройка дуплексного режима интерфейса

По умолчанию интерфейсы Ethernet могут автоматически согласовывать, будут ли они дуплексными или полудуплексными. Дуплексный режим для гигабитного интерфейса всегда автоматический.

| Команда                            | Описание   |
|------------------------------------|--|
| <b>duplex {full   half   auto}</b> | Устанавливает дуплексный режим интерфейса Ethernet                                 |
| <b>No duplex</b>                   | Восстанавливает настройки по умолчанию. Дуплексный режим согласуется автоматически |

### 5.4.4 Настройка управления потоком на интерфейсе

Когда интерфейс находится в полнодуплексном режиме, управление потоком осуществляется с помощью кадра паузы, определенного в стандарте 802.3X. В полудуплексном режиме данная функция реализуется обратным давлением (back pressure).

| Команда                             | Описание   |
|-------------------------------------|--|
| <b>flow-control on   off   auto</b> | Включает или отключает управление потоком на интерфейсе                                      |
| <b>no flow-control</b>              | Восстанавливает настройки по умолчанию, то есть управление потоком на интерфейсе отсутствует |



Разница между «flow-control auto» и «flow-control on» заключается в том, что во втором случае кадр управления потоком принимается принудительно. В то время как при использовании параметра «flow-control auto» кадр управления потоком пересылается только при успешном согласовании устройств в сети.

## 5.5 Настройка логического интерфейса

В этом разделе описывается, как настроить логический интерфейс. Возможны следующие варианты:

- настройка нулевого интерфейса;
- настройка интерфейса Loopback;



- настройка интерфейса агрегации;
- настройка интерфейса VLAN;
- настройка интерфейса SuperVLAN

### 5.5.1 Настройка нулевого интерфейса

Вся система поддерживает только один нулевой интерфейс. Его функции аналогичны функциям нулевых устройств, применяемых в большинстве операционных систем. Нулевой интерфейс всегда доступен, но он никогда не отправляет и не получает коммуникационную информацию. Команда конфигурации интерфейса **no ip unreachable** — единственная команда, доступная нулевому интерфейсу. Нулевой интерфейс предоставляет дополнительный метод фильтрации коммуникации. То есть, нежелательная сетевая коммуникация может быть направлена на нулевой интерфейс. Также нулевой интерфейс может функционировать как список управления доступом.

Вы можете выполнить следующую команду в режиме глобальной конфигурации, чтобы указать нулевой интерфейс:

| Команда                 | Описание                                      |
|-------------------------|---|
| <b>interface null 0</b> | Переход в режим настройки нулевого интерфейса |

Нулевой интерфейс может быть применен в любой команде, которая принимает тип интерфейса в качестве параметра.

В следующем примере показано, как настроить нулевой интерфейс для маршрутизации IP 192.168.20.0.

```
ip route 192.168.20.0 255.255.255.0 null 0
```

### 5.5.2 Настройка интерфейса Loopback

Интерфейс Loopback является логическим интерфейсом. Он всегда функционирует и продолжает сеанс BGP, даже если внешний интерфейс отключен. Интерфейс Loopback может использоваться в качестве конечного адреса для сеанса BGP. Если другие коммутаторы пытаются достичь интерфейса Loopback, протокол динамической маршрутизации должен быть настроен для трансляции маршрутов с адресом этого интерфейса. Сообщения, которые направляются на интерфейс Loopback, могут быть перенаправлены на коммутатор и обработаны локально. Сообщения, направленные на интерфейс Loopback, но пункт назначения которых не является IP-адресом этого интерфейса, будут отброшены. Это означает, что интерфейс loopback функционирует как нулевой интерфейс.

Выполните следующую команду в режиме глобальной конфигурации, чтобы указать интерфейс обратной связи и войти в режим настройки интерфейса:



| Команда                                 | Описание                                      |
|---|---|
| <b>interface loopback</b> <i>number</i> | Переход в режим настройки интерфейса Loopback |

### 5.5.3 Настройка интерфейса агрегации

Проблема недостаточной пропускной способности одного интерфейса Ethernet решается путем создания виртуального интерфейса агрегации. Он может связать вместе несколько полнодуплексных физических интерфейсов с одинаковой скоростью, что значительно повышает пропускную способность.

Выполните следующую команду, чтобы определить интерфейс агрегации:

| Команда  | Описание                        |
|--|---------------------------------|
| <b>interface port-aggregator</b> <i>number</i> | Настраивает интерфейс агрегации |

### 5.5.4 Настройка интерфейса VLAN

Интерфейс VLAN – это интерфейс маршрутизации в коммутаторе. Команда **vlan** в режиме глобальной конфигурации только добавляет в систему VLAN второго уровня, не определяя, как поступать с IP-пакетом, адрес назначения которого находится в VLAN. Если интерфейса VLAN нет, такие пакеты будут отброшены.

Выполните следующую команду, чтобы определить интерфейс VLAN:

| Команда                             | Описание                   |
|-------------------------------------|----------------------------|
| <b>interface vlan</b> <i>number</i> | Настраивает интерфейс VLAN |

### 5.5.5 Настройка интерфейса Super VLAN

Технология Super VLAN обеспечивает следующий механизм: hosts в разных VLAN одного коммутатора могут быть размещены в одной подсети IPv4 и использовать один и тот же шлюз по умолчанию; таким образом, сохраняется множество IP-адресов. Технология Super VLAN объединяет разные VLAN в группу, где VLAN используют один и тот же интерфейс управления, а hosts используют один и тот же сетевой раздел IPv4 и шлюз. VLAN, принадлежащая Super VLAN, называется SubVLAN. Ни одна SubVLAN не может иметь назначенный IP-адрес на интерфейсе управления.

Интерфейс Super VLAN можно настроить через командную строку. Процедура настройки показана ниже:



| Команда   | Описание   |
|---|--|
| <b>[no] interface supervlan <i>index</i></b>              | <p>Вход в режим настройки интерфейса Super VLAN. Если указанный интерфейс не существует, система сама создаст его</p> <p><b>index</b> – номер интерфейса Super VLAN. Значения находятся в диапазоне от 1 до 32</p> <p><b>no</b> – удаление интерфейса Super VLAN</p>   |
| <b>[no] subvlan [setstr] [add addstr] [remove remstr]</b> | <p>Настраивает SubVLAN в Super VLAN. Добавленная SubVLAN не может обладать иметь адреса на интерфейсе управления и не может принадлежать другим Super VLAN. В исходном состоянии Super VLAN не содержит никаких SubVLAN. Одновременно можно использовать только одну подкоманду</p> <p><b>setstr</b> означает настройку списка SubVLAN. Например, 2,4-6 указывает VLAN 2, 4, 5 и 6</p> <p><b>add</b> означает добавление VLAN в исходный список SubVLAN</p> <p><b>addstr</b> означает строку символов, формат которой такой же, как указано выше</p> <p><b>remove</b> означает удаление VLAN в исходном списке SubVLAN</p> <p><b>remstr</b> – строка символов, формат которой такой же, как указано выше.</p> <p><b>no</b> означает удаление всех SubVLAN в Super VLAN. Команда <b>no</b> не может использоваться с другими подкомандами</p> |

После создания интерфейса Super VLAN вы можете настроить его IP-адрес. Интерфейс Super VLAN также является портом маршрутизации, который можно настроить так же, как и другие порты.

## 5.6 Примеры настройки интерфейса

### ➤ Пример 1. Описание интерфейса

В следующем примере показано, как добавить описание, относящееся к интерфейсу. Это описание отображается в файле конфигурации и на командном дисплее интерфейса.

```
interface vlan 1
```

```
ip address 192.168.1.23 255.255.255.0
```



### ➤ Пример 2. Отключение и включение интерфейса

В следующем примере показано, как отключить интерфейс Ethernet 0/1:

```
interface GigaEthernet0/1  
shutdown
```

В следующем примере показано, как включить интерфейс Ethernet 0/1:

```
interface GigaEthernet0/1  
no shutdown
```

## 6. Настройка расширенных параметров интерфейсов

### 6.1 Port Security

#### 6.1.1 Введение

Вы можете управлять функцией Port Security для защиты порта, позволяя ему работать в определенном диапазоне сети в соответствии с вашей конфигурацией. Чтобы активировать защиту, вам нужно установить максимальное количество безопасных MAC-адресов, которые могут взаимодействовать с выбранным портом. Если количество использованных MAC-адресов превышает установленный вами лимит, и некоторые из этих адресов не считаются безопасными, для защиты порта будут предприняты определенные действия в соответствии с установленными настройками.

Port Security имеет следующие функции:

- Настройка допустимого количества безопасных MAC-адресов;
- Настройка статических безопасных MAC-адресов. Если защищенный порт не имеет статического безопасного MAC-адреса или количество статических безопасных MAC-адресов меньше настроенного общего допустимого количества безопасных MAC-адресов, порт будет изучать динамические MAC-адреса.
- Отбрасывание нелегальных пакетов при нарушении безопасности порта

В разделе описывается, как настроить защищенный порт для коммутатора.

#### 6.1.2 Настройка MAC-адресов и привязка IP-адреса.

Коммутатор может привязать к порту как IP-адрес, так и MAC-адрес или же привязать только один из них.

После того, как IP-адрес привязан к MAC-адресу на порту, IP-сообщения, несовместимые с привязанными MAC-адресами, будут фильтроваться.

Войдите в режим настройки интерфейса и выполните следующую команду, чтобы отобразить информацию о конфигурации защищенного порта:



| Команда   | Описание                                 |
|---|--|
| <b>switchport port-security bind {ip A.B.C.D mac H.H.H}</b> | Привязка IP-адреса к MAC-адресу на порту |

## 6.2 Блокировка трафика

По умолчанию интерфейс Ethernet будет транслировать неизвестные сообщения в VLAN, где он расположен. В некоторых случаях следует запрещать такого рода пересылку.

| Команда  | Описание  |
|--|---|
| <b>switchport block {unicast   multicast   broadcast}</b>    | Интерфейс не пересылает одноадресные, многоадресные или широковещательные сообщения |
| <b>no switchport block {unicast   multicast   broadcast}</b> | Интерфейс пересылает все типы сообщений   |

## 6.3 Изоляция портов

В нормальных условиях пакет данных может быть перенаправлен между различными портами коммутаторов. Иногда требуется ограничить передачу данных между портами, и для этого используется функция изоляции портов. Изолированные порты не могут передавать данные между собой. Пакеты могут нормально пересылаться между портами без функции изоляции или между изолированными и неизолированными портами.

| Команда                        | Описание                   |
|--------------------------------|----------------------------|
| <b>switchport protected</b>    | Включает функцию изоляции  |
| <b>no switchport protected</b> | Выключает функцию изоляции |

## 6.4 Управление штормами

Порты коммутатора могут быть атакованы постоянными аномальными одноадресными (сбой определения MAC-адреса), многоадресными или широковещательными сообщениями. Это может привести к выходу из строя портов коммутатора и даже всего коммутатора. Поэтому был предусмотрен механизм для сдерживания этого явления. Функция управления штормом может устанавливать разные скорости на входе для разных типов сообщений, которым разрешено поступать на коммутатор.



| Команда  | Описание  |
|--|---|
| <code>storm-control {broadcast   multicast   unicast} threshold count</code> | <p>Настройка функции управления штормом на порту</p> <p><b>Unicast</b> означает, что контролируются неизвестные одноадресные пакеты</p> <p><b>Multicast</b> означает, что контролируется многоадресная рассылка</p> <p><b>Broadcast</b> означает, что контролируется широковещательная рассылка</p> <p><b>Count</b> означает пороговое значение, которое необходимо настроить</p> |
| <code>no storm-control {broadcast   multicast   unicast} threshold</code>    | Отмена управления штормом на порту  |

## 6.5 Ограничение скорости порта

Данная функция используется для ограничения скорости входящего и исходящего потока порта. Используйте следующие команды для ограничения скорости потока после входа в режим управления:

| Команда   | Описание  |
|---|---|
| <code>config</code>   | Вход в режим глобальной конфигурации  |
| <code>interface g0/1</code>                                     | Вход в режим настройки выбранного интерфейса  |
| <code>[no] switchport rate-limit band {ingress   egress}</code> | <p>Настройка ограничения скорости потока для порта</p> <p><b>band</b> – предельная скорость потока</p> <p><b>percent</b> – ограничение потока в процентах</p> <p><b>ingress</b> – настройка для входящего потока</p> <p><b>egress</b> – настройка для исходящего потока</p> |
| <code>exit</code>   | Вернуться в режим глобальной конфигурации   |
| <code>exit</code>   | Вернуться в режим управления  |



## 6.6 Обнаружение петель на порту

Вы можете определить наличие петли на порту, настроив периодическую отправку сообщений `keepalive` в режиме глобальной конфигурации:

| Команда                         | Описание   |
|---------------------------------|--|
| <code>[no] keepalive</code>     | Включение/отключение функции обнаружения петель  |
| <code>keepalive [second]</code> | <p>Настройка временного интервала для тестовых сообщений, отправляемых портом</p> <p><b>second</b> – временной интервал отправки сообщений в секундах. Диапазон: 0–32767</p> |

## 6.7 Настройка диапазона интерфейсов

В процессе настройки бывают случаи, когда приходится настраивать один и тот же атрибут на портах одного типа. Во избежание повторной настройки на каждом порту и для снижения трудозатрат рекомендуется использовать режим настройки диапазона интерфейсов. В этом режиме можно настраивать порты, относящиеся к одному типу и имеющие одинаковый номер слота.



Перед входом в режим настройки диапазона интерфейсов следует убедиться, что все интерфейсы диапазона установлены и инициализированы.

### 6.7.1 Вход в режим настройки диапазона интерфейсов

Выполните следующую команду, чтобы войти в режим настройки диапазона интерфейсов:

| Команда   | Описание   |
|---|--|
| <code>interface range type slot/&lt;port - port2   port3&gt;[ , &lt;port1 - port2   port3&gt;]</code> | <p>Вход в режим настройки диапазона интерфейсов. Все порты, входящие в диапазон, соответствуют следующим условиям:</p> <p><b>type:</b> относится к типу настраиваемых интерфейсов;</p> |



|  |  |
|--|--|
|  | <p><b>slot:</b> определяет номер конкретного модуля или шасси, на котором расположены порты;</p> <p>Номера портов до/после «-» должны находиться в диапазоне от port1 до port2 или быть равными port3;</p> <p>Перед/после «-» или «,» должен быть пробел</p> |
|--|--|

## 6.7.2 Пример настройки

С помощью команды **interface range** включите в диапазон настройки слот 0 и его порты Fast Ethernet 1, 2, 3, 6, 8, 10, 11, 12:

```
switch_config# interface range 1 – 3 , 6 , 8 , 10 - 12
```

## 6.8 Зеркалирование портов

### 6.8.1 Настройка зеркалирования

Настроив зеркалирование, вы можете использовать один порт коммутатора для наблюдения за трафиком, относящемся к группе портов.

Для настройки войдите в привилегированный режим и выполните следующие действия:

| Команда  | Описание   |
|--|--|
| config   | Вход в режим глобальной конфигурации   |
| <b>mirror session</b> <i>session_number</i> { <b>destination</b> { <b>interface</b> <i>interface-id</i> } <b>source</b> { <b>interface</b> <i>interface-id</i> [,   -] rx   tx   both} } | <p>Настройка зеркалирования портов</p> <p><b>session-number</b> – порядковый номер конфигурации зеркалирования</p> <p><b>destination</b> – порт назначения</p> <p><b>source</b> – порт источника зеркалирования.</p> <p><b>rx</b> – входящие данные.</p> <p><b>tx</b> – исходящие данные.</p> <p><b>both</b> – входящие и исходящие данные</p> |
| exit   | Вернуться в режим управления   |
| write  | Сохранить настройки  |





## 6.8.2 Отображение информации о зеркалировании

Запустите **show**, чтобы отобразить информацию о конфигурации зеркалирования портов.

| Команда  | Описание   |
|--|--|
| <b>show mirror [session <i>session_number</i>]</b> | <p>Отображает информацию о настройке зеркалирования портов</p> <p><b>session-number</b> – порядковый номер конфигурации зеркалирования</p> |

## 7. VLAN

### 7.1 Введение

Понятие VLAN (виртуальная локальная сеть) относится к группе логических сетевых устройств в одной или нескольких локальных сетях, которые настроены таким образом, что могут взаимодействовать так же, как если бы были физически подключены к одному и тому же проводу, хотя на самом деле они расположены в нескольких разных сегментах сети. В 1999 году IEEE разработал проект стандарта протокола IEEE 802.1Q, используемый для стандартизации методов реализации VLAN. Поскольку VLAN основаны на логических, а не физических соединениях, они очень предоставляют широкие возможности для управления пользователями/хостами, а также распределения полосы пропускания и оптимизации ресурсов.

Существует несколько различных типов виртуальных локальных сетей и различные режимы работы их портов-участников.

- VLAN на основе портов (Port-Based): каждый порт физического коммутатора настраивается со списком доступа, определяющим членство в определенных VLAN.
- Интерфейс поддерживает магистральный режим (802.1Q trunk mode).
- Интерфейс поддерживает режим доступа (access mode).

Port-Based VLAN предназначена для назначения порта одному из подмножеств VLAN, поддерживаемых коммутатором. Если в этом подмножестве имеется только VLAN, то этот порт является портом доступа. Если же сетей несколько, то этот порт является магистральным (транковым). Среди множества виртуальных сетей есть одна сеть по умолчанию, и каждому порту назначается PVID (идентификатор порта VLAN), соответствующий этой VLAN.

- На интерфейсе поддерживается диапазон допустимых значений VLAN (VLAN-allowed range).

Параметр VLAN-allowed используется для управления диапазоном виртуальных локальных сетей, которому принадлежит порт. Параметр VLAN-untagged используется при настройке порта для отправки пакетов без тега VLAN в соответствующую виртуальную сеть.



## 7.2 Туннель Dot1Q

### 7.2.1 Описание

Dot1Q Tunnel – это название туннельного протокола, основанного на инкапсуляции 802.1Q, определенной в IEEE 802.1ad. Его основная идея состоит в том, чтобы инкапсулировать тег VLAN частной сети в тег публичной сети. Пакет переносит двухуровневую метку через магистральную сеть поставщика услуг, предоставляя пользователю относительно простой VPN-туннель уровня 2. Протокол Dot1Q Tunnel прост и удобен в управлении. Он не требует поддержки сигнализации и может быть реализован только посредством статической конфигурации, особенно там, где основой корпоративной сети или маломасштабной MAN являются небольшие L3-коммутаторы.

Являясь дешевым и компактным решением VPN L2, Dot1Q Tunnel становится все более популярным среди пользователей малых сетей, когда требуется VPN. Внутри сети оператора Р-устройству не обязательно поддерживать функцию туннеля Dot1Q. То есть традиционные коммутаторы L3 могут полностью удовлетворить требования, что делает сеть простой и экономичной. Коммутатор выполняет следующие функции:

- Включает Dot1Q Tunnel глобально;
- Поддерживает взаимную трансляцию между VLAN клиента и SPVLAN на порту нисходящей линии связи, включая трансляцию в плоском режиме и в режиме QinQ;
- Поддерживает настройку восходящего порта;
- Поддерживает различные значения TPID.

### 7.2.2 Реализация

Существует два режима реализации туннеля Dot1Q: туннель Dot1Q на основе порта и туннель Dot1Q на основе внутренней классификации тегов CVLAN.

#### 1. Туннель Dot1Q на основе порта

Когда порт коммутатора получает пакеты, независимо от того, имеют ли пакеты тег VLAN, коммутатор добавит к этим пакетам тег VLAN по умолчанию, к которой относится данный порт. Таким образом, если полученный пакет имеет тег VLAN, он становится пакетом с двойным тегом; если полученный пакет изначально не помечен, к нему будет добавлен тег VLAN по умолчанию для этого порта.

Пакет с одним тегом VLAN имеет структуру, показанную в таблице 1:

Таблица 1 – Пакет с одним тегом VLAN

|            |            |                     |                  |               |                   |             |
|------------|------------|---------------------|------------------|---------------|-------------------|-------------|
| DA<br>(6B) | SA<br>(6B) | ETYPE(8100)<br>(2B) | VLAN TAG<br>(2B) | ETYPE<br>(2B) | DATA<br>(0~1500B) | FCS<br>(4B) |
|------------|------------|---------------------|------------------|---------------|-------------------|-------------|

Пакет с двумя тегами VLAN имеет структуру, показанную в таблице 2:



Таблица 2 – Пакет с двумя тегами VLAN

|            |            |                     |                     |                   |               |               |                   |             |
|------------|------------|---------------------|---------------------|-------------------|---------------|---------------|-------------------|-------------|
| DA<br>(6B) | SA<br>(6B) | ETYPE(8100)<br>(2B) | ETYPE(8100)<br>(2B) | CVLAN Tag<br>(2B) | ETYPE<br>(2B) | ETYPE<br>(2B) | DATA<br>(0~1500B) | FCS<br>(4B) |
|------------|------------|---------------------|---------------------|-------------------|---------------|---------------|-------------------|-------------|

## 2. Туннель Dot1Q на основе внутреннего тега CVLAN

Служба функционирует в соответствии с зоной CVLAN ID внутреннего тега CVLAN туннеля Dot1Q. Зону CVLAN можно преобразовать в идентификатор SPVLAN. Существует два режима трансляции VLAN: плоская (flat) и QinQ. В режиме трансляции VLAN QinQ, когда один и тот же пользователь использует разные службы с разными идентификаторами CVLAN, услуги могут распределяться в соответствии с этими идентификаторами. Например, идентификатор CVLAN службы передачи данных (bandwidth service) находится в диапазоне от 101 до 200. Идентификатор CVLAN службы VOIP находится в диапазоне от 201 до 300. Идентификатор CVLAN службы IPTV находится в диапазоне от 301 до 400. В соответствии с диапазоном идентификаторов CVLAN, когда PE-устройство получает пользовательские данные, оно добавляет SPVLAN-тег с ID 1000 к услуге передачи данных и SPVLAN-тег с ID 3000 к услуге IPTV.

Основное различие между режимами Flat VLAN и QinQ VLAN заключается в том, как SPVLAN-тег добавляется или заменяет существующий CVLAN-тег.

- В режиме Flat VLAN трансляции, SPVLAN-тег заменяет CVLAN-тег напрямую, не добавляясь как внешний слой.
- В режиме QinQ VLAN трансляции, SPVLAN-тег добавляется к внешнему слою CVLAN-тега, создавая двойную тегированную структуру, что облегчает управление трафиком и сегментацию сети, особенно для поставщиков услуг.

### 7.2.3 Изменение значения TPID

Значение TPID можно изменить. В следующей таблице показана структура тега, определенная IEEE802.1Q:

Таблица 3 – Структура тега VLAN

|                 |                                  |              |                   |
|-----------------|----------------------------------|--------------|-------------------|
| TPID<br>2 байта | Приоритет пользователя<br>3 бита | CFI<br>1 бит | VLAN ID<br>12 бит |
|-----------------|----------------------------------|--------------|-------------------|

TPID – это поле в теге VLAN. Значение поля, определенное IEEE 802.1Q, равно 0x8100. Коммутатор использует значение TPID (0x8100), указанное протоколом по умолчанию. Устройства некоторых поставщиков не устанавливают значение TPID внешнего тега в пакете туннеля Dot1Q на 0x8100. Для совместимости с этими устройствами большинство коммутаторов могут изменять значение TPID пакетов туннеля Dot1Q. Значение TPID устройства PE может быть настроено пользователем. Когда порт этих устройств получает пакет, значение TPID во внешнем теге VLAN пакета будет заменено значением,



установленным пользователем, и отправлено в общедоступную сеть. Затем эти пакеты могут быть идентифицированы устройствами других поставщиков.

## 7.3 Настройка VLAN

- Добавление/удаление VLAN
- Настройка порта коммутатора
- Создание/удаление интерфейса VLAN
- Настройка интерфейса Super Vlan
- Мониторинг конфигурации и состояния VLAN
- Настройка списка управления доступом на основе VLAN
- Глобальное включение/отключение туннеля Dot1Q и настройка TPID
- Настройка режима передачи VLAN и трансляционной записи

### 7.3.1 Добавление/удаление VLAN

Являясь виртуальной логической сетью, VLAN имеет те же атрибуты, что и физическая локальная сеть, но позволяет группировать конечные станции, даже если они не расположены в одном сегменте локальной сети. VLAN может иметь несколько портов, и все одноадресные, многоадресные и широковещательные сообщения будут пересылаться только на устройства внутри одной VLAN, т. е. по умолчанию они не будут передаваться на устройства в других VLAN. Если данные необходимо передать в другую VLAN, их следует пересылать через маршрутизатор или мост.

Запустите следующую команду для настройки VLAN:

| Команда   | Описание   |
|---|--|
| <b>vlan</b> <i>vlan-id</i>                        | Вход в режим настройки VLAN                            |
| <b>name</b> <i>str</i>                            | Имя в режиме настройки VLAN                            |
| <b>exit</b>                                       | Выход из режима настройки с сохранением созданной VLAN |
| <b>vlan</b> <i>vlan-range</i>                     | Одновременное создание нескольких VLAN                 |
| <b>no vlan</b> <i>vlan-id</i>   <i>vlan-range</i> | Удаление одной или нескольких VLAN                     |

VLAN могут быть динамически добавлены и удалены через протокол управления VLAN GVRP.



## 7.3.2 Настройка порта коммутатора

Порт коммутатора поддерживает следующие режимы: access, trunk, dot1q-tunnel, dot1q-translating-tunnel, dot1q-tunnel-uplink.

- Режим доступа (access) указывает, что этот порт принадлежит одной VLAN, отправляя и принимая только нетегированные кадры Ethernet.
- Транковый режим (trunk) указывает, что порт соединяет другие коммутаторы, и может передавать и принимать тегированные кадры Ethernet.
- Туннельный режим Dot1Q (dot1q-tunnel) принимает полученные пакеты безоговорочно как пакеты без тега. Чип коммутатора автоматически добавляет PVID порта в качестве нового тега, тем самым позволяя коммутатору игнорировать различные разделы VLAN, подключенные к сети. Затем пакет будет доставлен без изменений на другой порт в другой подсети того же клиента. Таким образом реализуется прозрачная передача.
- Режим трансляции (dot1q-translating-tunnel) основан на транковом режиме. Порт может обращаться к таблице трансляции VLAN для поиска соответствующей метки SPVLAN в зависимости от VLAN-тега входящего пакета. Чип коммутатора использует SPVLAN для замены оригинального тега или добавляет тег SPVLAN к внешнему слою оригинального тега. Когда пакет выходит из порта, тег SPVLAN заменяется оригинальным тегом или удаляется. Коммутатор может игнорировать различные VLAN-разделы в доступной сети и передавать пакеты одному и тому же клиенту в другой подсети через другой порт, обеспечивая прозрачную передачу.
- Режим туннелирования на порту восходящей линии связи (dot1q-tunnel-uplink) также является производным от транкового режима. Для отправки пакетов через порт необходимо настроить диапазон VLAN с нетегированным трафиком для SPVLAN. Если пакеты соответствуют этому диапазону, они передаются через порт без изменений. При получении пакетов портом происходит проверка их TPID. В случае обнаружения различий или если пакеты нетегированные, им добавляется SPVLAN-тег с собственным TPID в качестве тега внешнего уровня.

Каждый порт имеет одну VLAN по умолчанию и один PVID, и все данные без тега VLAN, полученные на порту, относятся к пакетам данных VLAN.

Транковый режим позволяет присваивать порту сразу несколько сетей VLAN и также настраивать, какие типы пакетов будут пересылаться и к какому числу VLAN относится порт. То есть, пакеты, отправленные через этот порт, могут быть помечены тегам (таким образом порт является членом нескольких VLAN) или быть без тегов, а список VLAN, к которым относится порт, определяется системой управления сетью.

Выполните следующую команду, чтобы настроить порт коммутатора:

| Команда  | Описание                           |
|--|------------------------------------|
| <code>switchport pvid <i>vlan-id</i></code>  | Настройка PVID порта коммутатора   |
| <code>switchport mode {access   trunk   dot1q-translating-tunnel   dot1q-tunnel-uplink}</code> | Настройка режима порта коммутатора |



|   |  |
|---|--|
| <b>switchport trunk vlan-allowed ...</b>  | Настройка списка VLAN, разрешенных для передачи по сетевому интерфейсу. Эта команда ограничивает передачу трафика только разрешенным VLAN, предотвращая возможность обращения устройств к другим VLAN через данный сетевой интерфейс |
| <b>switchport trunk vlan-untagged ...</b> | Определяет диапазон VLAN, который будет использоваться для немаркированного трафика, проходящего через данный магистральный порт   |

### 7.3.3 Создание/удаление интерфейса VLAN

Интерфейс VLAN может быть установлен для реализации управления сетью или выполнения функций маршрутизации третьего уровня. Также его можно использовать для указания IP-адреса и маски. Выполните следующую команду для настройки интерфейса VLAN:

| Команда                                   | Описание                          |
|---|-----------------------------------|
| <b>[no] interface vlan <i>vlan-id</i></b> | Создание/удаление интерфейса VLAN |

### 7.3.4 Настройка интерфейса Super VLAN

Интерфейс Super VLAN поддерживается только на коммутаторе уровня 3.

Super VLAN – это технология виртуализации локальной сети, позволяющая объединять несколько VLAN в единый логический домен. Технология позволяет подсетям разных VLAN позволяет использовать IP-адрес интерфейса управления Super VLAN, что значительно сокращает потребность в IP-адресах. Хосты в группе используют один и тот же сетевой раздел IPv4 и шлюз. VLAN, принадлежащие Super VLAN, называются SubVLAN. Они не имеют собственного настраиваемого управляющего интерфейса.

Интерфейс Super VLAN можно настроить через командную строку. Процедура настройки показана ниже:

| Команда                                      | Описание   |
|--|--|
| <b>[no] interface supervlan <i>index</i></b> | Вход в режим настройки интерфейса. Если указанный интерфейс Super VLAN не существует, система создаст его сама |



|   |  |
|---|--|
|   | <p><b>index</b> – номер интерфейса Super VLAN. Значение находится в диапазоне от 1 до 32</p> <p><b>no</b> – удаление соответствующего интерфейса Super VLAN</p>  |
| <p><b>[no] subvlan</b> [<i>setstr</i>] [<b>add</b> <i>addstr</i>] [<b>remove</b> <i>remstr</i>]</p> | <p>Настраивает SubVLAN в Super VLAN. Добавленная SubVLAN не может иметь интерфейса управления. В исходном состоянии Super VLAN не включает SubVLAN. Одновременно можно использовать только одну подкоманду</p> <p><b>setstr</b> – задать список SubVLAN. Например, список 2,4-6 указывает VLAN 2, 4, 5 и 6</p> <p><b>add</b> – добавить указанные SubVLAN в исходный список</p> <p><b>addstr</b> – строка символов, формат которой такой же, как указано выше</p> <p><b>remove</b> – удалить указанные SubVLAN в из исходного списка</p> <p><b>remstr</b> – строка символов, формат которой такой же, как указано выше</p> <p><b>no</b> – удалить все SubVLAN в Super VLAN. Команда <b>no</b> не может использоваться с другими подкомандами</p> |

После создания интерфейса Super VLAN вы можете настроить для него IP-адрес. Интерфейс Super VLAN также является портом маршрутизации, который можно настроить так же, как и другие порты.

### 7.3.5 Мониторинг конфигурации и состояния VLAN

Выполните следующие команды в режиме EXEC, чтобы просмотреть настройки и состояние VLAN и туннеля Dot1Q:

| Команда  | Описание  |
|--|---|
| <b>show vlan</b> [ <i>id x</i>   <b>interface</b> <i>intf</i>   <b>dot1q-tunnel</b> [ <i>interface intf</i> ]] | Отображение конфигурации и состояния VLAN или туннеля Dot1Q |
| <b>show interface</b> { <i>vlan</i>   <i>supervlan</i> } <i>x</i>  | Отображение состояния выбранного интерфейса VLAN/Super VLAN |



### 7.3.6 Глобальное включение/отключение туннеля Dot1Q и настройка TPID

После глобального включения туннеля Dot1Q порт линейной карты станет нижним портом туннеля Dot1Q по умолчанию, и будет принудительно добавлять тег SPVLAN к входящему пакету.

После настройки глобального TPID, когда пакет выходит из верхнего порта коммутатора, глобальный TPID будет использован в качестве TPID тега SPVLAN. Когда пакет поступает на верхний коммутатор, если тег SPVLAN не соответствует заданному глобальному TPID или если пакет не имеет тега, то коммутатор добавит тег SPVLAN с собственным TPID в качестве внешнего тега пакета.

Ниже приведена команда для включения глобального туннеля Dot1Q и глобального TPID.

| Команда                  | Описание  |
|--------------------------|---|
| <b>dot1q-tunnel tpid</b> | Настраивает глобальную функцию dot1q-tunnel и глобальный TPID коммутатора |

### 7.3.7 Настройка режима передачи VLAN и трансляционной записи

Линейная карта поддерживает туннельную трансляцию VLAN Dot1Q. После настройки режима трансляции VLAN и соответствующей записи, VLAN будет работать в туннеле интерфейса. Существует 2 режима трансляции: плоский режим и режим QinQ. В плоском режиме пакет, входящий в порт нисходящей линии туннеля, будет использован в качестве индекса для выполнения поиска в таблице трансляции VLAN. Найденный тег SPVLAN добавляется к внешнему тегу CVLAN. Когда пакет выходит из порта, тег SPVLAN удаляется.

Режим QinQ подразумевает использование тегирования VLAN, где пакеты могут содержать два уровня тегов. Для интерфейса режимом трансляции VLAN по умолчанию является QinQ.

При настройке записи трансляции VLAN в режиме интерфейса, плоский режим позволяет настроить только сопоставление «один к одному» между CVLAN и SPVLAN. В режиме QinQ между CVLAN и SPVLAN можно настроить сопоставление «много-один».

Ниже приведена команда для настройки режима передачи и записей VLAN:

| Команда   | Описание                                 |
|---|--|
| <b>switchport dot1q-translating-tunnel</b><br>{mode [flat   qinq]   translate<br>{oldvlanlist   oldvlanid} newvlan<br>[priority]} | Настройка режима передачи VLAN и записей |



## 7.4 Примеры настройки

### 7.4.1 Пример настройки Super VLAN

Ниже представлена сетевая среда:

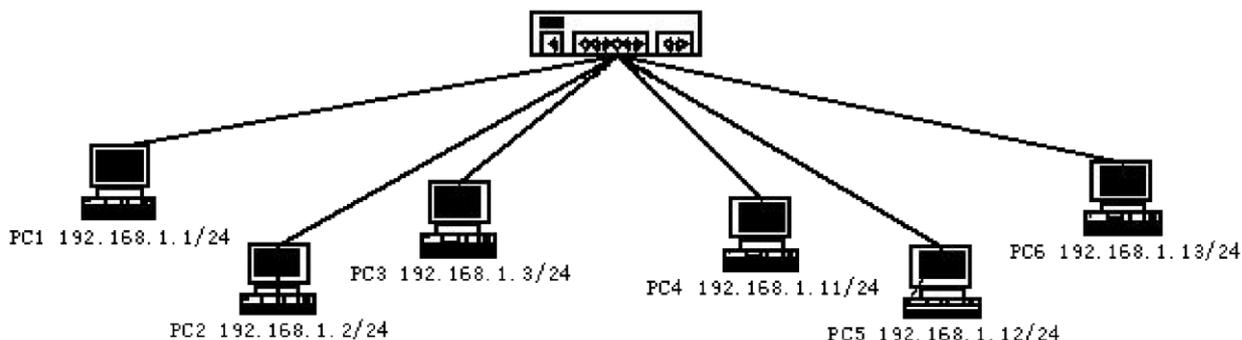


Рисунок 1 – Топология сети

Пользователи персональных компьютеров PC1–PC6 подключаются к коммутатору через порты 1–6. IP-адреса этих ПК принадлежат сетевому разделу 192.168.1.0/24. Хотя группа PC1–PC3 и группа PC4–PC6 расположены в разных широковещательных доменах уровня 2, PC1–PC6 могут пинговать друг друга и управлять коммутатором через IP-адрес 192.168.1.100. Для этого необходимо настроить порты 1–3 на VLAN1 и порты 4–6 на VLAN. Затем добавить VLAN 1 и 2 в Super VLAN в качестве ее SubVLAN. На коммутаторе следует выполнить следующие настройки:

```
interface fastethernet 0/4
switchport pvid 2
!
interface fastethernet 0/5
switchport pvid 2
!
interface fastethernet 0/6
switchport pvid 2
!
interface supervlan 1
subvlan 1,2
ip address 192.168.1.100 255.255.255.0
ip proxy-arp subvlan
!
```



## 7.4.2 Примеры настройки туннеля Dot1Q

Ниже приведены несколько типичных сетевых сценариев, иллюстрирующих применение туннеля Dot1Q.

### ➤ Пример 1

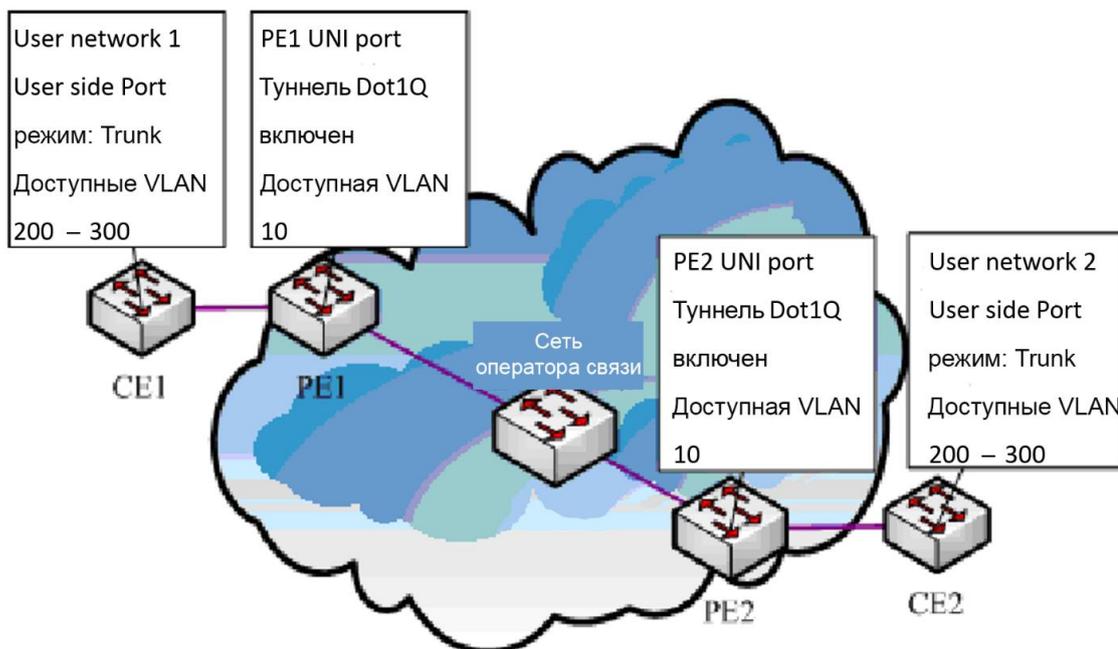


Рисунок 2 – Настройка туннеля Dot1Q

Как показано на рисунке выше, порт F0/1 CE1 соединяет порт F0/1 (или порт G0/1) PE1; PE1 подключается к S8510 на порту F0/2 (или порту G0/2); PE2 подключается к S8510 на порту F0/2 (или порту G0/2); а порт F0/1 (или порт G0/1) PE2 соединяет порт F0/1 CE1.

Порты PE настроены как порты доступа VLAN 10, и на них включен туннель Dot1Q. Однако портам CE по-прежнему требуется Trunk VLAN 200–300, что позволяет каналу между CE и PE быть асимметричным. В этом случае общедоступной сети достаточно предоставить пользователям только идентификатор VLAN, равный 10. Независимо от того, сколько VLAN ID частной сети запланировано в сети пользователя, вновь распространяемый VLAN ID общедоступной сети будет в обязательном порядке внесен в тегированные пакеты, когда они попадают в магистральную сеть интернет-провайдера. Затем эти пакеты с идентификатором общедоступной сети проходят через магистральную сеть, достигают другой ее стороны, то есть устройств PE, избавляются от тега VLAN общедоступной сети, возобновляют передачу пользовательских пакетов и в конечном итоге передаются на CE-устройства пользователей. Таким образом, пакеты, пересылаемые в магистральной сети, имеют два уровня заголовков тегов 802.1Q, один из которых является тегом общедоступной сети, а другой – тегом частной сети. Подробный процесс пересылки пакетов показан ниже:



1. Поскольку выходной порт CE1 является магистральным портом, все пакеты, передаваемые пользователями в PE1, содержат тег VLAN частной сети (в диапазоне от 200 до 300). Один из таких пакетов показан в таблице 4.

Таблица 4 – Структура пакета CE1

|            |            |                     |                  |               |                   |             |
|------------|------------|---------------------|------------------|---------------|-------------------|-------------|
| DA<br>(6B) | SA<br>(6B) | ETYPE(8100)<br>(2B) | VLAN TAG<br>(2B) | ETYPE<br>(2B) | DATA<br>(0~1500B) | FCS<br>(4B) |
|------------|------------|---------------------|------------------|---------------|-------------------|-------------|

2. Когда пакеты поступают на устройство PE1, оно, игнорирует тег VLAN частной сети, поскольку входной порт является портом доступа туннеля Dot1Q, но добавляет в эти пакеты тег дефолтной VLAN 10, как показано в таблице 5.

Таблица 5 – Структура пакета PE1

|            |            |                     |                       |                         |                      |               |                   |             |
|------------|------------|---------------------|-----------------------|-------------------------|----------------------|---------------|-------------------|-------------|
| DA<br>(6B) | SA<br>(6B) | ETYPE(8100)<br>(2B) | SPVLAN<br>Tag<br>(2B) | ETYPE<br>(8100)<br>(2B) | CVLAN<br>Tag<br>(2B) | ETYPE<br>(2B) | DATA<br>(0~1500B) | FCS<br>(4B) |
|------------|------------|---------------------|-----------------------|-------------------------|----------------------|---------------|-------------------|-------------|

3. В магистральной сети пакеты передаются по порту VLAN 10. Тег частной сети сохраняется в прозрачном состоянии до тех пор, пока эти пакеты не достигнут PE2.

4. PE2 обнаруживает, что порт, через который он соединен с CE2, является портом доступа VLAN 10, удаляет заголовок тега VLAN 10 согласно 802.1Q, восстанавливает изначальные пакеты пользователей и передает их на CE2, как показано в таблице 6.

Таблица 6 – Структура пакета PE2

|            |            |                     |                  |               |                   |             |
|------------|------------|---------------------|------------------|---------------|-------------------|-------------|
| DA<br>(6B) | SA<br>(6B) | ETYPE(8100)<br>(2B) | VLAN TAG<br>(2B) | ETYPE<br>(2B) | DATA<br>(0~1500B) | FCS<br>(4B) |
|------------|------------|---------------------|------------------|---------------|-------------------|-------------|

Если смотреть на поток пересылки, Dot1Q Tunnel очень лаконичен. Особенность данной технологии заключается в отсутствии необходимости сигнализации для поддержания туннеля, что обеспечивает простоту использования и статическую конфигурацию.

Что касается типичной конфигурации Dot1Q Tunnel, коммутаторы настраиваются следующим образом, когда они работают как PE (PE1 имеет ту же конфигурацию, что и PE2):

```
Switch_config# dot1q-tunnel
```

```
Switch_config_g0/1# switchport pvid 10
```

```
Switch_config_g0/2# switchport mode trunk
```

```
Switch_config_g0/2# switchport trunk vlan-untagged 1-9,11-4094
```

или:



```
Switch_config_g0/1#switchport mode dot1q-tunnel
Switch_config_g0/1#switchport pvid 10
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#switchport trunk vlan-untagged 1-9,11-4094
```

## ➤ Пример 2

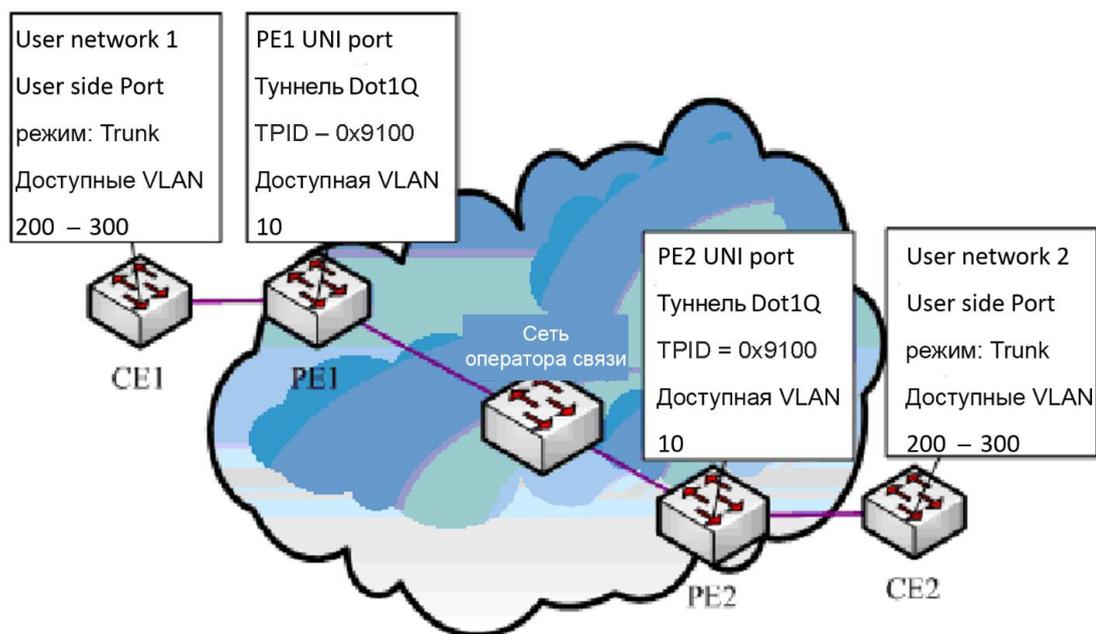


Рисунок 3 – Настройка туннеля Dot1Q

Как показано на рисунке 3, пакет, отправленный устройством PE, имеет TPID тега SPVLAN 0x9100. Устройство PE необходимо использовать коммутатор, поддерживающий модификацию TPID. Настройки для устройств PE1 и PE2 следующие:

```
Switch_config# dot1q-tunnel 0x9100
Switch_config_f0/1# switchport pvid 10
Switch_config_f0/2# switchport mode dot1q-tunnel-uplink
Switch_config_f0/2# switchport trunk vlan-untagged 1-9,11-4094
или:
Switch_config# dot1q-tunnel
Switch_config_f0/1# switchport mode dot1q-tunnel 0x9100
Switch_config_f0/1# switchport pvid 10
Switch_config_f0/2# switchport mode dot1q-tunnel-uplink 0x9100
Switch_config_f0/2# switchport trunk vlan-untagged 1-9,11-4094
```



или:

```
Switch_config# dot1q-tunnel
Switch_config_g0/1# switchport pvid 10
Switch_config_g0/2# switchport mode dot1q-tunnel-uplink 0x9100
Switch_config_g0/2# switchport trunk vlan-untagged 1-9,11-4094
```

### ➤ Пример 3

Когда пользователь подключен к различным услугам, его доступ будет завершён на UNI-порту коммутатора PE. Чтобы различать разные сервисы и реализовывать разные стандарты QOS, необходимо трансляцию VLAN через туннель Dot1Q.

Как показано на рисунке 4, оператор назначает каждому пользователю три VLAN, по одной для каждой услуги. Например, для пользователя 1 назначаются VLAN с тегами 1001, 2001 и 3001 соответственно. VLAN 1001 соответствует широкополосным услугам (broadband), VLAN 2001 – услугам VoIP, а VLAN 3001 – услугам IPTV. Когда услуга поступает на UNI-порт коммутатора PE, тег VLAN дополняется различными внешними тегами в зависимости от VLAN ID пользователя. Если внешний тег пользователя равен 1001, то тег 1001 добавляется непосредственно к внешнему уровню. Аналогично, для пользователя 2 его различным услугам также могут быть назначены разные VLAN-теги. Основное отличие при назначении внешних тегов для пользователей заключается в различии местоположения CE и в конечной идентификации пользователя.

Таблица 7 – Маркировка пакетов клиентских устройств

| Устройство | Служба    | Внутренний тег CVLAN | Внешний тег SPVLAN | Принцип классификации потоков |
|------------|-----------|----------------------|--------------------|-------------------------------|
| CE1        | broadband | 101–200              | 1001               | Раздел CVLAN                  |
|            | VOIP      | 201–300              | 2001               |                               |
|            | IPTV      | 301–400              | 3001               |                               |
| CE2        | broadband | 101–200              | 1002               |                               |
|            | VOIP      | 201–300              | 2002               |                               |
|            | IPTV      | 301–400              | 3002               |                               |

В этой сетевой схеме внутренний и внешний теги четко различаются. Внешний тег идентифицирует местоположение устройства конечного пользователя (CE), а внутренний тег указывает на конкретного пользователя. Внешний тег помогает определить местоположение устройства CE и тип сервиса, в то время как внутренний тег обозначает местоположение пользователя внутри устройства CE. Таким образом, комбинация



внутреннего и внешнего тегов позволяет эффективно управлять трафиком и обеспечивать правильную маршрутизацию данных.

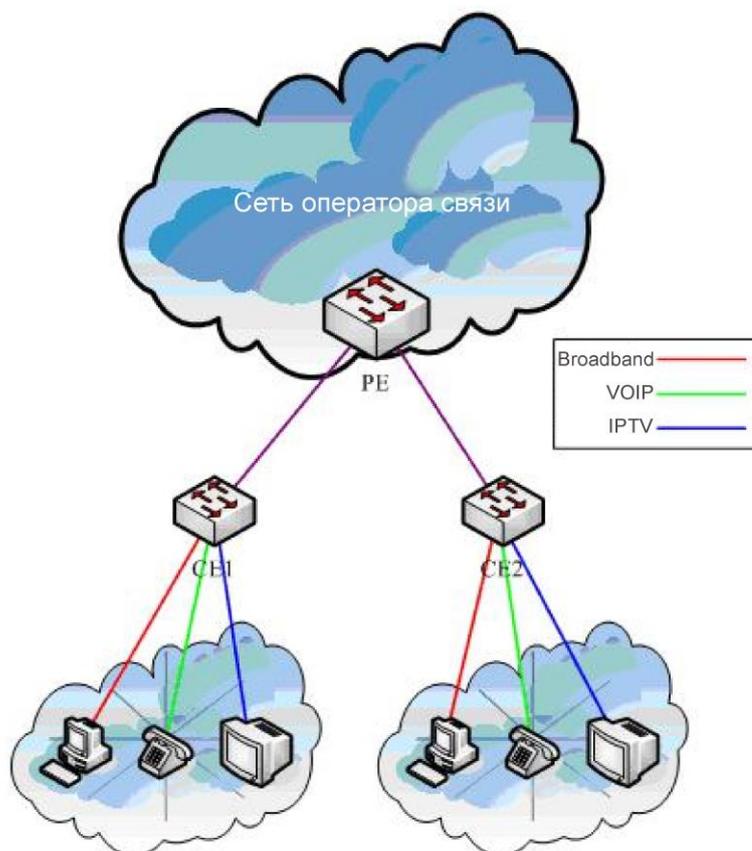


Рисунок 4 – Туннелирование трафика различных служб

Предположим, что CE1 подключен к порту G0/1 устройства PE1, CE2 подключен к порту G0/2 устройства PE1, а NNI-порт туннеля Dot1Q устройства PE – это g0/3. Для вышеуказанной топологии необходимо выполнить следующую настройку:

```
Switch_config# dot1q-tunnel
```

```
Switch_config_g0/1# switchport mode dot1q-translating-tunnel
```

```
Switch_config_g0/1# switchport dot1q-translating-tunnel mode QinQ (конфигурация по умолчанию)
```

```
Switch_config_g0/1# switchport dot1q-translating-tunnel translate 101-200 1001
```

```
Switch_config_g0/1# switchport dot1q-translating-tunnel translate 201-300 2001
```

```
Switch_config_g0/1# switchport dot1q-translating-tunnel translate 301-400 3001
```

```
Switch_config_g0/2# switchport mode dot1q-translating-tunnel
```

```
Switch_config_g0/2# switchport dot1q-translating-tunnel mode QinQ (конфигурация по умолчанию)
```

```
Switch_config_g0/2# switchport dot1q-translating-tunnel translate 101-200 1002
```

```
Switch_config_g0/2# switchport dot1q-translating-tunnel translate 201-300 2002
```



```
Switch_config_g0/2# switchport dot1q-translating-tunnel translate 301-400 3002
```

```
Switch_config_g0/3# switchport mode dot1q-tunnel-uplink
```

## 8. Настройка связующего дерева

### 8.1 Введение

Стандартный протокол связующего дерева (STP) определен в IEEE 802.1D. Это объединяет топологию локальной сети, состоящую из нескольких мостов, в единое связующее дерево, предотвращая возникновение петель и обеспечивая стабильную работу сети. Стек коммутаторов для остальной части сети выглядит как единый узел связующего дерева; все члены стека используют один и тот же идентификатор моста. Если не указано иное, термин «коммутатор» может относиться к автономному коммутатору и к стеку коммутаторов.

STP использует алгоритм связующего дерева для выбора одного коммутатора резервируемой сети в качестве корня этого дерева. Алгоритм вычисляет наилучший путь без петель через коммутируемую сеть второго уровня, назначая каждому порту роль в зависимости от его функции в активной топологии.

STP – это протокол управления связью второго уровня, который обеспечивает избыточность путей, предотвращая при этом образование петель в сети. Для правильной работы сети Ethernet на втором уровне между любыми двумя станциями может существовать только один активный путь. Несколько активных путей между конечными станциями приводят к образованию петель. Если в сети существует петля, конечные станции могут получать дублирующиеся сообщения. Коммутаторы также могут изучать MAC-адреса конечных станций на нескольких интерфейсах второго уровня. Эти условия приводят к нестабильной работе сети. Работа STP прозрачна для конечных станций, которые не могут определить, подключены ли они к одному сегменту локальной сети или к коммутируемой локальной сети из нескольких сегментов.

Алгоритм STP создает активную топологию сети с простыми соединениями, выбирая одно дерево, которое охватывает все узлы сети. В активной топологии некоторые порты, которые участвуют в процессе выбора корневого моста и определения пути к корню дерева, могут пропускать кадры, в то время как другие находятся в состоянии блокировки и не могут передавать информацию. В зависимости от состояния сети порты могут быть включены или исключены из активной топологии. Когда сетевое устройство становится неэффективным или добавляется в сеть, или удаляется из нее, порты могут изменять своё состояние, например, переходить в состояние передачи.

В топологии STP коммутатор может рассматриваться как корень. Для каждого сегмента локальной сети (LAN) порт моста будет передавать данные от этого сегмента к корню. Этот порт считается назначенным портом для данного сегмента сети. Мост, на котором расположен этот порт, рассматривается как назначенный мост локальной сети. Корень является назначенным мостом для всех сегментов сети, к которым он подключен. На каждом мосту порт, ближайший к корню, называется корневым портом. Только корневой порт и назначенный порт (если он существует) находятся в состоянии передачи. Порты другого типа не отключены, но не являются ни корневыми, ни назначенными; их называют резервными портами.



Следующие параметры определяют структуру стабилизированной активной топологии:

- идентификатор каждого моста;
- стоимость пути для каждого порта;
- идентификатор для каждого порта моста.

В качестве корневого выбирается мост с наивысшим приоритетом (значение идентификатора наименьшее). Порты каждого моста имеют атрибут Root Path Cost, то есть минимальное значение стоимости пути всех портов от корня до моста. Назначенный порт – это порт, через который происходит пересылка трафика для определенного сегмента сети. Он выбирается на основе наименьшей стоимости пути от коммутатора до корня топологии сети (или корневого коммутатора).

Когда два порта на коммутаторе находятся в петле, настройки приоритета порта и стоимости пути протокола STP определяют, какой порт будет находиться в состоянии передачи, а какой – в состоянии блокировки. Значение приоритета порта отражает его положение в топологии сети и его способность передавать трафик. Значение стоимости пути указывает на скорость передачи данных через медиасреду.

Данная серия коммутаторов поддерживает два режима протокола связующего дерева: 802.1D STP и 802.1w RSTP. Некоторые модели также поддерживают распределенный режим STP в зависимости от VLAN, а также протокол MSTP.

В этой главе описывается настройка стандартного протокола связующего дерева, поддерживаемого коммутатором.



802.1D STP и 802.1w RSTP в этой статье обозначаются сокращенно SSTP и RSTP. SSTP означает «единое связующее дерево».

#### Задачи настройки SSTP

- Выбор режима STP
- Отключение/включение STP
- Настройка приоритета коммутатора
- Настройка времени приветствия
- Настройка максимального возраста
- Настройка времени задержки пересылки
- Настройка приоритета порта
- Настройка стоимости пути
- Настройка автоматически назначаемого порта
- Мониторинг состояния STP

## 8.2 Выбор режима STP



Выполните следующую команду, чтобы настроить режим STP:

| Команда  | Описание               |
|--|------------------------|
| <b>spanning-tree mode {sstp   rstp   mstp}</b> | Выбор конфигурации STP |

### 8.3 Отключение/включение STP

По умолчанию связующее дерево включено. Отключайте связующее дерево только в том случае, если вы уверены, что в топологии сети нет петель.

Выполните следующие действия, чтобы отключить связующее дерево:

| Команда                 | Описание      |
|-------------------------|---------------|
| <b>no spanning-tree</b> | Отключает STP |

Чтобы включить связующее дерево, используйте следующую команду:

| Команда  | Описание                               |
|--|--|
| <b>spanning-tree</b>                           | Включает режим STP по умолчанию (SSTP) |
| <b>spanning-tree mode {sstp   rstp   mstp}</b> | Включает определенный режим STP        |

### 8.4 Настройка приоритета коммутатора

Вы можете настроить приоритет коммутатора и повысить вероятность того, что автономный коммутатор или коммутатор в стеке будет выбран в качестве корневого.

Выполните следующие действия, чтобы настроить приоритет коммутатора:

| Команда   | Описание  |
|---|---|
| <b>spanning-tree sstp priority <i>value</i></b> | Изменяет значение приоритета SSTP                         |
| <b>no spanning-tree sstp priority</b>           | Возвращает приоритет SSTP к значению по умолчанию (32768) |



## 8.5 Настройка времени приветствия

Пользователь может настроить интервал между блоками данных STP, отправляемыми корневым коммутатором, изменив время приветствия.

Используйте следующую команду для настройки времени приветствия SSTP:

| Команда   | Описание  |
|---|---|
| <b>spanning-tree sstp hello-time</b> <i>value</i> | Настраивает время приветствия SSTP                              |
| <b>no spanning-tree sstp hello-time</b>           | Возвращает время приветствия SSTP к значению по умолчанию (4 с) |

## 8.6 Настройка максимального возраста

Используйте параметр **max-age** (максимальный возраст) SSTP, чтобы настроить значение интервала времени (в секундах), которое коммутатор ждет перед тем, как попытаться изменить конфигурацию связующего дерева при отсутствии входящих конфигурационных сообщений. Если в течение указанного времени коммутатор не получает новых сообщений от других устройств, он считает текущую топологию устаревшей и начинает процесс реконфигурации.

Выполните следующие действия, чтобы настроить время интервала:

| Команда  | Описание  |
|--|---|
| <b>spanning-tree sstp max-age</b> <i>value</i> | Настраивает значение max-age SSTP                 |
| <b>no spanning-tree sstp max-age</b>           | Возвращает max-age к значению по умолчанию (20 с) |

## 8.7 Настройка времени задержки передачи

Настройте задержку передачи SSTP, чтобы определить количество секунд, в течение которых интерфейс ожидает перехода из состояний обучения и прослушивания связующего дерева в состояние передачи данных.

Используйте следующую команду для настройки задержки:

| Команда   | Описание                                 |
|---|--|
| <b>spanning-tree sstp forward-time</b> <i>value</i> | Настраивает время задержки передачи SSTP |



|   |  |
|---|--|
| <b>no spanning-tree sstp forward-time</b> | Возвращает время задержки к значению по умолчанию (15 с) |
|---|--|

## 8.8 Настройка приоритета порта

Если возникает петля, связующее дерево использует приоритет порта при выборе интерфейса для перевода в состояние передачи. Вы можете назначить более высокие значения приоритета (более низкие числовые значения) интерфейсам, которые вы хотите выбрать первыми, и значения более низкого приоритета (более высокие числовые значения) для интерфейсов, которые будут выбираться в последнюю очередь. Если все интерфейсы имеют одинаковое значение приоритета, связующее дерево переводит интерфейс с наименьшим номером в состояние передачи и блокирует остальные.

Выполните следующие действия, чтобы настроить приоритет интерфейса:

| Команда                                       | Описание   |
|---|--|
| <b>spanning-tree port-priority value</b>      | Настраивает значение приоритета порта для интерфейса     |
| <b>spanning-tree sstp port-priority value</b> | Изменяет приоритет порта SSTP                            |
| <b>no spanning-tree sstp port-priority</b>    | Возвращает приоритет порта к значению по умолчанию (128) |

## 8.9 Настройка стоимости пути

Выполните следующие действия, чтобы настроить стоимость пути для интерфейса:

| Команда                              | Описание  |
|--------------------------------------|---|
| <b>spanning-tree cost value</b>      | Настраивает стоимость пути для интерфейса         |
| <b>spanning-tree sstp cost value</b> | Изменяет стоимость пути SSTP                      |
| <b>no spanning-tree sstp cost</b>    | Возвращает стоимость пути к значению по умолчанию |

## 8.10 Настройка автоматически назначаемого порта

Специальная функция автоматического назначения порта позволяет линейной карте автоматически отправлять BPDU на автоматически назначенный порт, снижая нагрузку на управляющее устройство. Функция эффективна в режиме STP. В режиме глобальной конфигурации выполните следующие команды для настройки функции автоматического назначения порта коммутаторов серии S8500:



| Команда                                 | Описание   |
|---|--|
| <b>spanning-tree designated-auto</b>    | Включает функцию автоматического назначения порта  |
| <b>no spanning-tree designated-auto</b> | Отключает функцию автоматического назначения порта |

## 8.11 Мониторинг состояния STP

Чтобы отслеживать конфигурацию и состояние STP, используйте следующие команды в режиме управления:

| Команда                             | Описание  |
|-------------------------------------|---|
| <b>show spanning-tree</b>           | Отображает информацию связующего дерева только на активных интерфейсах        |
| <b>show spanning-tree detail</b>    | Отображает подробную сводку информации о связующем дереве на всех интерфейсах |
| <b>show spanning-tree interface</b> | Отображает информацию о связующем дереве для указанного интерфейса            |

## 8.12 VLAN STP

### 8.12.1 Обзор

В режиме SSTP в сети существует только один экземпляр STP. Состояние порта коммутатора в STP определяет его состояние во всех VLAN. Если в сети присутствует несколько VLAN, разделение единого STP и сетевой топологии может привести к перегрузкам в некоторых сегментах сети.

Коммутаторы данной серии поддерживает запуск независимого SSTP в определенном количестве VLAN, гарантируя, что порт будет иметь разное состояние в разных VLAN и между VLAN реализуется балансировка нагрузки. Важно отметить, что количество VLAN, в которых можно независимо запускать протокол связующего дерева, равно 30, а другие топологии VLAN, превышающие ограничение по количеству, не будут управляться при помощи STP.



### 8.12.2 Команды настройки VLAN STP

Чтобы настроить параметры SSTP в VLAN, выполните эти команды в режиме глобальной конфигурации:



| Команда  | Описание  |
|--|---|
| <b>spanning-tree mode pvst</b>                                       | Запуск режима настройки STP для VLAN  |
| <b>spanning-tree vlan <i>vlan-list</i></b>                           | Назначение экземпляра STP указанным VLAN<br><b>vlan-list</b> – список VLAN<br>В списке можно указать до 30 VLAN |
| <b>no spanning-tree vlan <i>vlan-list</i></b>                        | Удаление экземпляра связующего дерева из указанных VLAN   |
| <b>spanning-tree vlan <i>vlan-list</i> priority <i>value</i></b>     | Настройка уровня приоритета связующего дерева в указанных VLAN  |
| <b>no spanning-tree <i>vlan-list</i> priority</b>                    | Сброс приоритета связующего дерева в указанных VLAN на значение по умолчанию                                    |
| <b>spanning-tree vlan <i>vlan-list</i> forward-time <i>value</i></b> | Настройка задержки пересылки для указанных VLAN   |
| <b>no spanning-tree vlan <i>vlan-list</i> forward-time</b>           | Сброс задержки пересылки для указанных VLAN на значение по умолчанию  |
| <b>spanning-tree vlan <i>vlan-list</i> max-age <i>value</i></b>      | Настройка максимального возраста для указанных VLAN   |
| <b>no spanning-tree vlan <i>vlan-list</i> max-age</b>                | Сброс максимального возраста для указанных VLAN на значение по умолчанию  |
| <b>spanning-tree vlan <i>vlan-list</i> hello-time <i>value</i></b>   | Настройка времени приветствия для указанных VLAN  |
| <b>no spanning-tree vlan <i>vlan-list</i> hello-time</b>             | Сброс времени приветствия указанных VLAN на значение по умолчанию   |

Чтобы настроить атрибуты порта, выполните следующие команды в режиме настройки интерфейса:

| Команда   | Описание  |
|---|---|
| <b>spanning-tree vlan <i>vlan-list</i> cost</b> | Настройка стоимости пути порта в указанных VLAN |



|   |  |
|---|--|
| <b>no spanning-tree vlan <i>vlan-list</i> cost</b>          | Сброс стоимости пути порта в указанных VLAN на значение по умолчанию |
| <b>spanning-tree vlan <i>vlan-list</i> port-priority</b>    | Настройка приоритета порта в указанных VLAN                          |
| <b>no spanning-tree vlan <i>vlan-list</i> port-priority</b> | Сброс приоритета порта в указанных VLAN на значение по умолчанию     |

Запустите эту команду в режиме управления тли мониторинга, чтобы проверить состояние связующего дерева в VLAN:

| Команда   | Описание                                    |
|---|---|
| <b>show spanning-tree vlan <i>vlan-list</i></b> | Проверка состояния связующего дерева в VLAN |

## 8.13 RSTP

Задачи настройки RSTP

- Включение/отключение RSTP на коммутаторе
- Настройка приоритета коммутатора
- Настройка времени задержки передачи
- Настройка времени приветствия
- Настройка максимального возраста
- Настройка стоимости пути
- Настройка приоритета порта
- Настройка проверки согласованности протоколов

### 8.13.1 Включение/отключение RSTP на коммутаторе

Выполните следующие команды в режиме глобальной конфигурации:

| Команда                        | Описание                                   |
|--------------------------------|--|
| <b>spanning-tree mode rstp</b> | Включает RSTP                              |
| <b>no spanning-tree mode</b>   | Возвращает STP в режим по умолчанию (SSTP) |



## 8.13.2 Настройка приоритета коммутатора

Вы можете настроить приоритет коммутатора и повысить вероятность того, что автономный коммутатор или коммутатор в стеке будет выбран в качестве корневого.

Выполните следующие команды в режиме глобальной конфигурации:

| Команда                                  | Описание   |
|--|--|
| <b>spanning-tree rstp priority value</b> | Изменяет значение приоритета RSTP                |
| <b>no spanning-tree rstp priority</b>    | Возвращает приоритету rstp значение по умолчанию |



Если приоритет всех мостов во всей сети имеет одно и то же значение, то в качестве корневого будет выбран мост с наименьшим MAC-адресом. В ситуации, когда включен протокол RSTP, изменение значения приоритета моста приведет к перерасчету связующего дерева.

По умолчанию значение приоритета моста равно 32768.

## 8.13.3 Настройка времени задержки передачи

Сбои канала связи могут привести к тому, что сеть пересчитает структуру связующего дерева. Но сообщение об обновлении конфигурации не может быть передано по всей сети одновременно. И, если вновь выбранный корневой порт и назначенный порт немедленно начнут пересылку данных, это может привести к появлению временного замкнутого пути (петли). Поэтому протокол использует своего рода «механизм перехода состояний». Прежде чем корневой и назначенный порт начинают пересылать данные, они проходят через промежуточное состояние. После прохождения времени задержки (Forward Delay Time), они переходят в состояние пересылки данных. Это время задержки гарантирует, что вновь созданное сообщение будет передано по всей сети. Характеристика задержки передачи моста связана с диаметром сети коммутатора. Как правило, чем больше диаметр сети и количество хопов, тем дольше должно быть время задержки.

Выполните следующие команды в режиме глобальной конфигурации:

| Команда                                      | Описание   |
|--|--|
| <b>spanning-tree rstp forward-time value</b> | Настраивает задержку передачи                            |
| <b>no spanning-tree rstp forward-time</b>    | Возвращает время задержки к значению по умолчанию (15 с) |



Если настроить задержку передачи на относительно небольшое значение, это может привести к временному перенасыщению путей. При слишком большом значении система может не возобновить подключение в течение неоправданно длительного времени. Рекомендуется использовать значение по умолчанию.

Время задержки по умолчанию составляет 15 секунд.

### 8.13.4 Настройка времени приветствия

Правильное значение времени приветствия может гарантировать, что мост обнаружит свои связи в сети, не забирая слишком много сетевых ресурсов.

Выполните следующие команды в режиме глобальной конфигурации:

| Команда   | Описание   |
|---|--|
| <b>spanning-tree rstp hello-time</b> <i>value</i> | Настраивает время приветствия                        |
| <b>no spanning-tree rstp hello-time</b>           | Возвращает время приветствия к значению по умолчанию |

Следует отметить, что слишком большое значение времени приветствия может привести к тому, что сетевой мост не сможет получить сообщение «Hello» из-за потери пакетов канала. Таким образом, сетевой мост решит, что соединение нарушено, и пересчитает связующее дерево. Если значение времени приветствия слишком мало, это может привести к тому, что сетевой мост будет часто отправлять сообщения о конфигурации, нерационально занимая при этом полосу пропускания. Это увеличивает нагрузку на сеть и процессор.



Рекомендуется использовать значение по умолчанию, которое составляет 4 секунды.

### 8.13.5 Настройка максимального возраста

Максимальный возраст (*max-age*) определяет время жизни каждого BPDU (пакета данных протокола моста), отправленного корневым мостом, до того, как он должен быть отброшен. Если корневой мост не получает BPDU из определенного порта в течение этого времени, он считает, что связь через данный порт неактивна и начинает искать другой путь через связующее дерево.

Выполните следующие команды в режиме глобальной конфигурации:

| Команда | Описание |
|---------|----------|
|---------|----------|



|   |   |
|---|---|
| <b>spanning-tree rstp max-age value</b> | Настраивает значение max-age                      |
| <b>no spanning-tree rstp max-age</b>    | Возвращает max-age к значению по умолчанию (20 с) |



Очень низкое значение max-age приводит к частым перерасчетам и ненужным блокировкам, в то время как слишком высокое значение может привести к тому, что изменения состояния узлов останутся без внимания, а это также рискует оказаться проблемой для стабильности сети.

Рекомендуется использовать значение по умолчанию, которое составляет 20 секунд.

## 8.13.6 Настройка стоимости пути

Значение по умолчанию для стоимости пути выводится из скорости передачи данных конкретного интерфейса. Если возникает петля, связующее дерево использует значение **rstp cost** при выборе интерфейса для перевода в активное состояние. Вы можете назначить более низкие значения стоимости для интерфейсов, которые желательно выбрать в первую очередь, и более высокие – для интерфейсов, которые хотите выбрать последними. Если все интерфейсы имеют одинаковое значение стоимости, связующее дерево переводит в состояние передачи интерфейс с наименьшим номером, а остальные блокирует.

Для настройки стоимости пути выполните следующие действия в режиме настройки интерфейса:

| Команда                              | Описание  |
|--------------------------------------|---|
| <b>spanning-tree rstp cost value</b> | Настраивает стоимость пути для интерфейса         |
| <b>no spanning-tree rstp cost</b>    | Возвращает стоимость пути к значению по умолчанию |



Изменение стоимости пути для порта Ethernet приведет к перерасчету связующего дерева. Рекомендуется использовать значение по умолчанию и позволить протоколу RSTP самостоятельно рассчитать стоимость пути для текущего интерфейса.

Когда скорость порта 10 Мбит/с, стоимость пути интерфейса Ethernet составляет 2000000. Когда скорость порта 100 Мбит/с, стоимость пути интерфейса Ethernet составляет 200000.



### 8.13.7 Настройка приоритета порта

Если возникает петля, связующее дерево использует приоритет порта при выборе интерфейса для перевода в состояние передачи данных. Вы можете назначить более высокий приоритет (более низкие числовые значения) интерфейсам, которые хотите выбрать первыми, и низкий приоритет (более высокие числовые значения), для интерфейсов, которые будут выбираться в последнюю очередь. Если все интерфейсы имеют одинаковое значение приоритета, связующее дерево переводит интерфейс с наименьшим номером в состояние передачи и блокирует остальные.

Выполните следующие действия в режиме настройки интерфейса:

| Команда                                       | Описание   |
|---|--|
| <b>spanning-tree rstp port-priority value</b> | Настраивает приоритет порта для интерфейса         |
| <b>no spanning-tree rstp port-priority</b>    | Возвращает приоритет порта к значению по умолчанию |



Изменение приоритета интерфейса Ethernet приведет к перерасчету связующего дерева.

Приоритет интерфейса Ethernet по умолчанию – 128.

### 8.13.8 Настройка проверки согласованности протоколов

Протокол RSTP позволяет коммутатору работать совместно с традиционным коммутатором 802.1D STP с помощью механизма преобразования протокола. Если один порт коммутатора получает информацию о конфигурации STP, этот порт перестроится на отправку только сообщений STP.

Если порт перестает получать BPDU STP после нахождения в состоянии совместимости со стандартом 802.1D STP, он автоматически возвращается к RSTP. В то же время через команду **spanning-tree rstp migration-check** можно запустить проверку преобразования протокола портом и восстановление порта в RSTP-режим.

Команду можно запустить в режиме глобальной конфигурации для проверки конвертации протоколов на всех портах, или в режиме настройки интерфейса для проверки отдельного указанного порта.



| Команда                                   | Описание   |
|---|--|
| <b>spanning-tree rstp migration-check</b> | Перезапуск проверки процесса преобразования протокола всех портов или текущего порта |

## 8.14 MTSP

### 8.14.1 Введение

Протокол множественного связующего дерева (MSTP) используется для предотвращения петель во взаимосвязанных сегментах сетей, построенных на основе Ethernet. Он позволяет сетевым администраторам настроить более одного дерева связанных устройств на сетевой сегмент, что снижает время восстановления сети в случае отказа коммутатора. MSTP совместим с более ранним протоколом связующего дерева (STP) и протоколом быстрого связующего дерева (RSTP).

И STP, и RSTP могут создавать единую топологию STP. Все сообщения VLAN пересылаются через единственное связующее дерево. STP работает медленнее, в то время как RSTP обеспечивает более быструю и надежную топологию, благодаря механизму квитирования для управления взаимодействием между сетевыми устройствами.

MSTP наследует механизм быстрого установления связи, использованный в RSTP. В то же время MST позволяет распределять разные VLAN по разным связующим деревьям, создавая в сети несколько топологий. В сетях, созданных по протоколу MSTP, кадры разных VLAN могут пересылаться по разным путям, благодаря чему реализуется балансировка нагрузки этих VLAN.

MSTP позволяет использовать несколько VLAN внутри одной топологии STP и эффективно сократить количество STP, необходимых для поддержки множества VLAN, что улучшает производительность и уменьшает нагрузку на сеть. Таким образом, MSTP предлагает более эффективный способ управления VLAN, чем STP.

### 8.14.2 Домен MST

В MSTP связь между VLAN и STP описывается с помощью таблицы конфигурации MSTP. Таблица, имя и номер редактирования конфигурации составляют идентификатор конфигурации MST.

В сети взаимосвязанные мосты с одинаковым идентификатором конфигурации MST рассматриваются в одном и том же регионе MST. Мосты в одном и том же регионе всегда имеют одинаковую конфигурацию VLAN, что гарантирует успешную отправку кадров VLAN в регионе MST.



### 8.14.3 IST, CST, CIST и MSTI

На рисунке 5 показана сеть MSTP, включающая три региона MST и коммутатор, работающий по протоколу 802.1D STP.

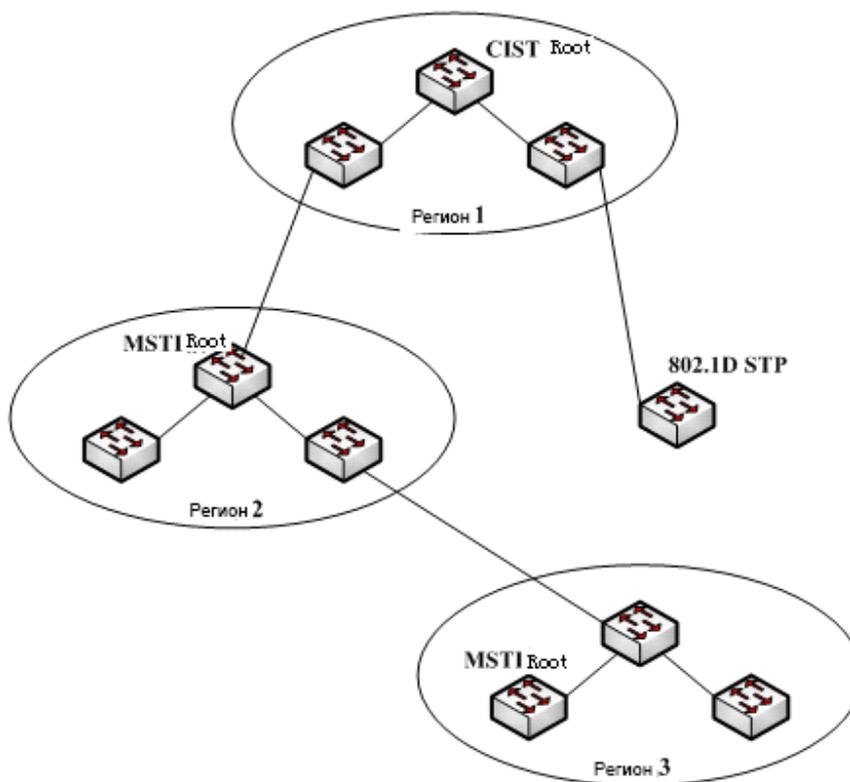


Рисунок 5 – Топология MSTP

#### 1. CIST

Общее и внутреннее связующее дерево (CIST) означает связующее дерево, состоящее из всех отдельных коммутаторов и взаимосвязанных локальных сетей. Эти коммутаторы могут принадлежать разным регионам MST. Это могут быть коммутаторы, работающие по традиционному протоколу STP или RSTP. Коммутаторы, использующие STP или RSTP в регионах MST, считаются находящимися в своих регионах.

После того как топология сети стабилизируется, все узлы CIST выбирают корневой мост CIST. В каждом регионе будет выбран внутренний корневой мост, который является кратчайшим путем от центра региона к корню CIST.

#### 2. CST

Если каждый регион MST рассматривать как один коммутатор, общее связующее дерево (CST) – это связующее дерево, соединяющее все «одиночные коммутаторы». Как показано на рисунке 5, регионы 1, 2, 3 и коммутаторы STP составляют сеть CST.

#### 3. IST

Внутреннее связующее дерево (IST) относится к части CIST, которая находится в регионе MST, то есть IST и CST вместе составляют CIST.



## 4. MSTI

Протокол MSTP позволяет распределять разные VLAN по разным связующим деревьям. Затем создается несколько экземпляров связующего дерева (MSTI). Обычно экземпляр связующего дерева №0 относится к дереву CIST, которое можно расширить на всю сеть. Каждый экземпляр связующего дерева, начиная с №1, находится в определенном регионе. В каждом экземпляре связующего дерева может быть несколько VLAN. В исходном состоянии все VLAN распределены в CIST.

MSTI в регионах MST является независимыми. Они могут выбирать разные коммутаторы в качестве собственных корней.

### 8.14.4 Роли порта

Порты в MSTP могут выполнять разные роли, подобно портам в RSTP.

#### 1. Корневой порт (root port)

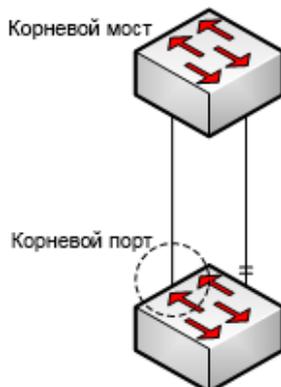


Рисунок 6 – Корневой порт

Корневой порт – это наилучший порт для создания соединения между текущим коммутатором и корневым мостом, который имеет минимальную стоимость пути.

#### 2. Альтернативный порт (alternate port)

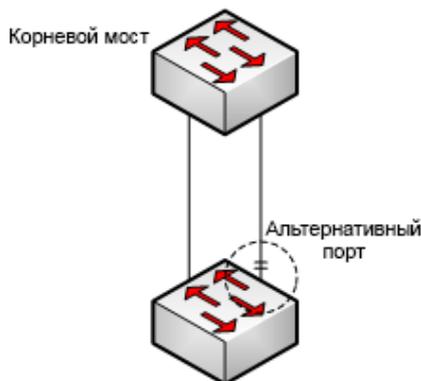


Рисунок 7 – Альтернативный порт



Альтернативный порт – это резервный порт для связи между текущим коммутатором и корневым мостом. Если соединение корневого порта выходит из строя, альтернативный порт может быстро превратиться в новый корневой без прерывания связи.

### 3. Назначенный порт (designated port)

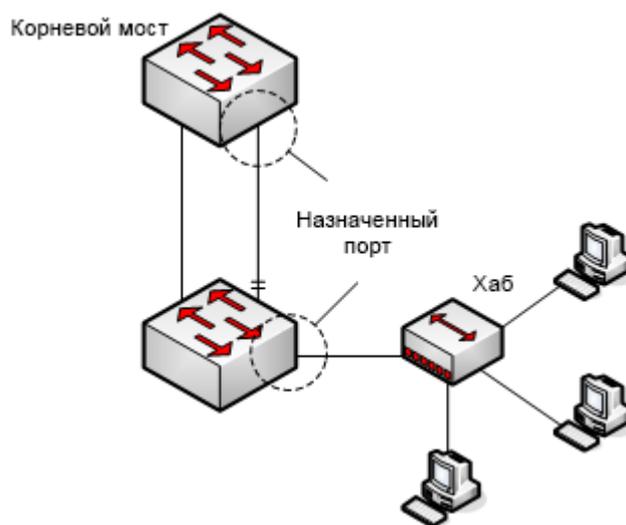


Рисунок 8 – Назначенный порт

Назначенный порт может подключаться к коммутаторам или локальной сети в следующем регионе. Это путь между текущей локальной сетью и корневым мостом.

### 4. Резервный порт (backup port)

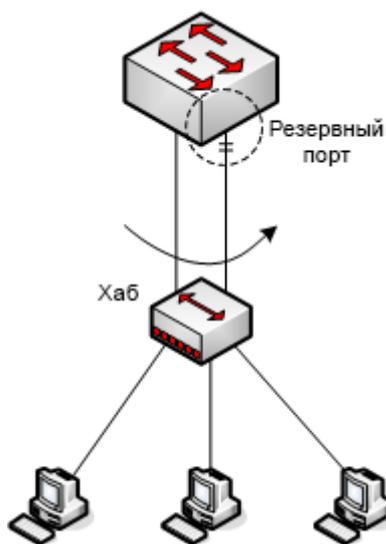


Рисунок 9 – Резервный порт



Когда два порта коммутатора подключаются напрямую или оба подключаются к одной и той же локальной сети, порт с более высоким приоритетом должен быть назначенным портом, а другой порт – резервным. Если назначенный порт выходит из строя, резервный берёт на себя его роль для продолжения бесперебойной работы.

## 5. Мастер-порт (master port)

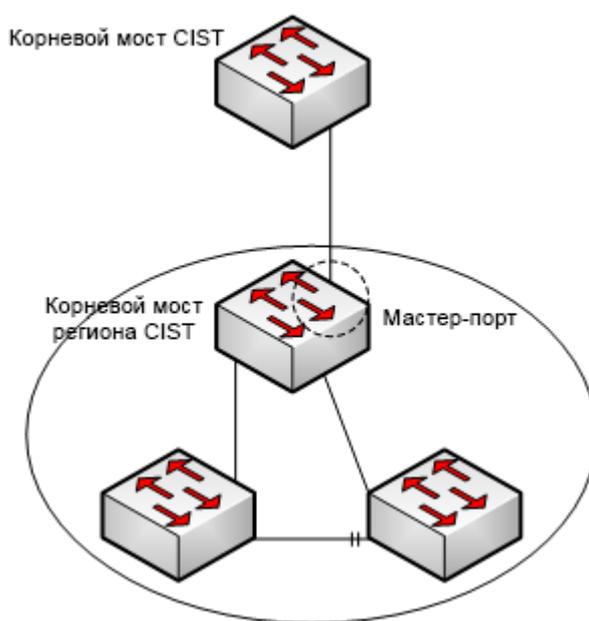


Рисунок 10 – Мастер-порт

Мастер-порт – порт, который соединяет регион MST с общим корневым мостом и имеет к нему кратчайший путь. Мастер-порт – это корневой порт корневого моста в регионе CIST.

## 6. Граничный порт (boundary port)

Граничные порты, относящиеся к CIST, имеют небольшое отличие от поведения граничных портов других экземпляров MSTI. Граничный порт внутри MSTI ограничивает расширение связующего дерева через этот порт, что может быть полезным при разделении сети на несколько взаимосвязанных областей.

## 7. Конечный порт (edge port)

В протоколах RSTP или MSTP конечный порт означает порт, напрямую соединяющий сетевой хост. Эти порты могут сразу переходить в состояние передачи, минуя состояния прослушивания и обучения и не создавая петель в сети.

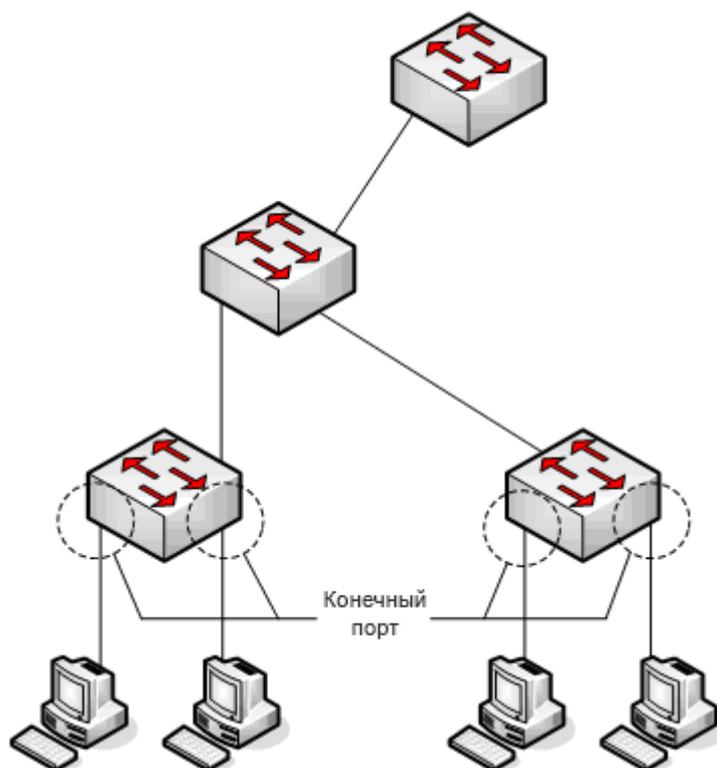


Рисунок 11 – Конечный порт

В исходном состоянии MSTP и RSTP не используют все порты в качестве конечных, что обеспечивает возможность быстрого создания топологии сети. Если порт получает BPDU от других коммутаторов, он возобновляет работу в нормальном режиме. Если порт получает BPDU 802.1D STP, он должен подождать время, равное удвоенному значению Forward Delay, а затем перейти в состояние передачи данных.

### 8.14.5 MSTP BPDU

Подобно STP и RSTP, коммутаторы, работающие под управлением MSTP, могут взаимодействовать друг с другом при помощи обмена сообщениями, в которых содержится блок данных протокола моста (BPDU). Вся информация о конфигурации CIST и MSTI может передаваться через BPDU. В таблицах 8 и 9 представлена структура BPDU, используемая MSTP.

Таблица 8 – MSTP BPDU

| Имя поля   | Номер байта |
|--|-------------|
| Protocol Identifier (идентификатор протокола)                | 1–2         |
| Protocol Version Identifier (идентификатор версии протокола) | 3           |
| BPDU Type (тип BPDU)   | 4           |



|  |        |
|--|--------|
| CIST Flags (флаги CIST)  | 5      |
| CIST Root Identifier (идентификатор корневого моста CIST)                        | 6–13   |
| CIST External Root Path Cost (затраты на внешний путь корневого моста CIST)      | 14–17  |
| CIST Regional Root Identifier (идентификатор регионального корневого моста CIST) | 18–25  |
| CIST Port Identifier (идентификатор порта CIST)                                  | 26–27  |
| Message Age (возраст сообщения)  | 28–29  |
| Max Age (максимальный возраст)   | 30–31  |
| Hello Time (время приветствия)   | 32–33  |
| Forward Delay (задержка передачи)  | 34–35  |
| Version 1 Length (длина версии 1)  | 36     |
| Version 3 Length (длина версии 3)  | 37–38  |
| Format Selector (выбор формата)  | 39     |
| Configuration Name (название конфигурации)                                       | 40–71  |
| Revision (ревизия)   | 72–73  |
| Configuration Digest (дайджест конфигурации)                                     | 74–89  |
| CIST Internal Root Path Cost (затраты на внутренний корневой путь CIST)          | 90–93  |
| CIST Bridge Identifier (идентификатор моста CIST)                                | 94–101 |
| CIST Remaining Hops (оставшиеся хопы CIST)                                       | 102    |
| MSTI Configuration Messages (сообщения о конфигурации MSTI)                      | 103~   |

Таблица 9 – Информация о конфигурации MSTI

| Имя поля                | Номер байта |
|-------------------------|-------------|
| MSTI FLAGS (флаги MSTI) | 1           |



|  |       |
|--|-------|
| MSTI Regional Root Identifier (идентификатор регионального корневого моста MSTI) | 2–9   |
| MSTI Internal Root Path Cost (затраты на внутренний корневой путь MSTI)          | 10–13 |
| MSTI Bridge Priority (приоритет моста MSTI)                                      | 14    |
| MSTI Port Priority (приоритет порта MSTI)  | 15    |
| MSTI Remaining Hops (оставшиеся хопы MSTI)                                       | 16    |

## 8.14.6 Стабильное состояние

Коммутатор MSTP выполняет вычисления и сравнивает операции в соответствии с полученными BPDU и, наконец, гарантирует, что:

1. Один коммутатор выбирается в качестве корня CIST всей сети.
2. Каждый коммутатор и сегмент локальной сети могут определить минимальную стоимость пути к корню CIST, обеспечивая устойчивое соединение и предотвращая образование петель.
3. Каждый регион имеет коммутатор в качестве регионального корня CIST. Коммутатор имеет путь к корню CIST с минимальной стоимостью.
4. Каждый MSTI может независимо выбирать коммутатор в качестве регионального корня MSTI.
5. Каждый коммутатор в регионе и сегменте локальной сети может определить путь с минимальной стоимостью к корню MSTI.
6. Корневой порт CIST обеспечивает путь с минимальной стоимостью между региональным корнем CIST и корнем CIST.
7. Назначенный порт CIST предоставляет своей локальной сети путь с минимальной стоимостью к корню CIST.
8. Альтернативный порт и резервный порт обеспечивают соединение, когда коммутатор, порт или локальная сеть не работают или отключены.
9. Корневой порт MSTI обеспечивает путь с минимальной стоимостью к региональному корню MSTI.
10. Назначенный порт MSTI обеспечивает путь с минимальной стоимостью к региональному корню MSTI.
11. Мастер-порт обеспечивает соединение между регионом и корнем CIST. В регионе корневой порт регионального корня CIST функционирует как мастер-порт всех MSTI в регионе.



### 8.14.7 Подсчет переходов

В отличие от STP и RSTP, протокол MSTP не использует возраст сообщения и максимальный возраст в конфигурационных BPDU для расчета топологии сети. Чтобы решить эту задачу, MSTP использует счетчик переходов (хопов).

Чтобы предотвратить заикливание информации, MSTP связывает передаваемую информацию с атрибутом количества переходов в каждом связующем дереве. Атрибут количества переходов для BPDU обозначается региональным корнем CIST или региональным корнем MSTI и уменьшается на каждом принимающем порту. Если счетчик переходов на порту становится равным 0, информация будет удалена, а сам порт станет назначенным.

### 8.14.8 Совместимость с STP

MSTP позволяет коммутатору работать с традиционным коммутатором STP посредством механизма преобразования протокола. Если один порт коммутатора получает сообщение конфигурации STP, этот порт затем передает только сообщение STP. В то же время порт, который получает информацию STP, считается граничным (boundary) портом.



Когда порт находится в состоянии STP-совместимости, он не перейдет автоматически в состояние MSTP, даже если больше не получает сообщений STP. В этом случае вы можете запустить команду **spanning-tree mstp migration-check**, чтобы очистить сообщения STP, полученные портом, и вернуть порт в режим MSTP.

Коммутатор, использующий протокол RSTP, может идентифицировать и обрабатывать сообщения MSTP. Поэтому MSTP-коммутатору не требуется преобразование протокола при работе с RSTP-коммутатором.

### 8.14.9 Задачи настройки MSTP

- Конфигурация MSTP по умолчанию
- Включение и отключение MSTP
- Настройка региона MSTP
- Настройка корневого моста сети
- Настройка вторичного корневого моста
- Настройка приоритета моста
- Настройка временных параметров STP
- Настройка диаметра сети
- Настройка максимального количества переходов



- Настройка приоритета порта
- Настройка стоимости пути для порта
- Настройка конечного порта
- Настройка типа подключения порта
- Активация режима совместимости с MST
- Перезапуск проверки конвертации протоколов

## 8.14.10 Конфигурация MSTP по умолчанию

| Атрибут  | Настройки по умолчанию   |
|--|--|
| Режим STP  | SSTP (PVST, RSTP и MSTP не запущены)                           |
| Имя региона  | Символьная строка MAC-адреса                                   |
| Номер редактирования региона                                       | 0  |
| Распределение VLAN   | Все VLAN относятся к CIST (MST00)                              |
| Приоритет связующего дерева (CIST и все экземпляры MST)            | 32768  |
| Приоритет порта связующего дерева (CIST и все экземпляры MST)      | 128  |
| Стоимость пути порта связующего дерева (CIST и все экземпляры MST) | 1000 Мбит/с: 20000<br>100 Мбит/с: 200000<br>10 Мбит/с: 2000000 |
| Время приветствия (Hello Time)                                     | 2 с  |
| Задержка передачи (Forward Delay)                                  | 15 с   |
| Максимальное время устаревания (Maximum-aging Time)                | 20 с   |
| Максимальное количество переходов (Maximum hop count)              | 20   |

## 8.14.11 Включение и отключение MSTP

Протокол STP по умолчанию может быть запущен в режиме PVST или SSTP. Вы можете остановить его работу, если связующее дерево не требуется.



Выполните следующую команду, чтобы перевести STP в режим MSTP:

| Команда                        | Описание                           |
|--------------------------------|------------------------------------|
| <b>spanning-tree</b>           | Включает STP в режиме по умолчанию |
| <b>spanning-tree mode mstp</b> | Включает MSTP                      |

Выполните следующую команду, чтобы отключить STP:

| Команда                 | Описание      |
|-------------------------|---------------|
| <b>no spanning-tree</b> | Выключает STP |

## 8.14.12 Настройка региона MST

Область MST, в которой находится коммутатор, определяется тремя атрибутами: именем конфигурации, номером редактирования, сопоставлением VLAN и MSTI. Вы можете изменить их с помощью команд настройки региона. Обратите внимание, что изменение любого из трех атрибутов приведет к изменению конфигурации региона, в котором находится коммутатор.

В исходном состоянии имя конфигурации MST представляет собой строку символов MAC-адреса коммутатора. Номер редактирования равен 0, а все VLAN отображаются в CIST (MST00). Поскольку разные коммутаторы имеют разные MAC-адреса, коммутаторы, работающие под управлением MSTP, в исходном состоянии находятся в разных регионах. Вы можете запустить команду **spanning-tree mstp instance instance-id vlan vlan-list**, чтобы создать новый MSTI и сопоставить с ним выбранную VLAN. Если MSTI удален, все эти VLAN снова сопоставляются с CIST.

Выполните следующую команду, чтобы настроить информацию о регионе MST:

| Команда                                  | Описание  |
|--|---|
| <b>spanning-tree mstp name string</b>    | Настраивает имя конфигурации MST<br><b>string</b> означает строку символов имени конфигурации. Она содержит до 32 символов, с учетом заглавных букв. Значением по умолчанию является строка символов MAC-адреса |
| <b>no spanning-tree mstp name</b>        | Устанавливает для имени конфигурации MST значение по умолчанию  |
| <b>spanning-tree mstp revision value</b> | Устанавливает номер редактирования MST  |



|   |  |
|---|--|
|   | <b>value</b> представляет номер редактирования в диапазоне от 0 до 65535. Значение по умолчанию – 0  |
| <b>no spanning-tree mstp revision</b>   | Устанавливает для номера редактирования MST значение по умолчанию  |
| <b>spanning-tree mstp instance</b> <i>instance-id</i><br><b>vlan</b> <i>vlan-list</i> | Соотносит VLAN с MSTI<br><br><b>instance-id</b> – номер экземпляра MST. Независимое значение, представляющее экземпляр связующего дерева, то есть MSTI. Значение варьируется от 1 до 15<br><br><b>vlan-list</b> – список VLAN, сопоставленных со связующим деревом. Диапазон значений – от 1 до 4094. Может представлять группу VLAN, например «1,2,3», «1-5» и «1,2,5-10» |
| <b>no spanning-tree mstp instance</b><br><i>instance-id</i>                           | Отменяет сопоставление VLAN MSTI и отключает экземпляр связующего дерева<br><br><b>instance-id</b> представляет номер экземпляра связующего дерева, то есть MSTI. Значение варьируется от 1 до 15  |

Запустите следующую команду, чтобы проверить настройки региона MSTP:

| Команда                               | Описание                             |
|---------------------------------------|--------------------------------------|
| <b>show spanning-tree mstp region</b> | Отображает конфигурацию региона MSTP |

### 8.14.13 Настройка корневого моста сети

В MSTP каждый экземпляр связующего дерева имеет идентификатор моста, содержащий значение приоритета и MAC-адрес коммутатора. При построении топологии связующего дерева в качестве корня сети выбирается коммутатор со сравнительно небольшим идентификатором моста.

Команда **spanning-tree mstp instance-id root** используется для изменения приоритета коммутатора в экземпляре связующего дерева со значения по умолчанию на достаточно маленькое значение, чтобы обеспечить коммутатору успешный выбор в качестве корневого в этом экземпляре связующего дерева.

После выполнения предыдущей команды протокол автоматически проверяет идентификатор моста текущего корня сети, а затем устанавливает поле приоритета идентификатора моста на 24576, когда значение 24576 гарантирует, что текущий коммутатор станет корнем связующего дерева.



Если значение приоритета корня сети меньше значения 24576, MSTP автоматически устанавливает приоритет связующего дерева текущего моста на значение, которое на 4096 меньше значения приоритета корня. Обратите внимание, что число 4096 является шагом изменения значения сетевого приоритета.

При настройке корня вы можете запустить команду с параметром **diameter** для определения диаметра сети связующего дерева. Ключевое слово действует только в том случае, если идентификатор экземпляра связующего дерева равен 0. После установки диаметра сети MSTP автоматически вычисляет правильные параметры времени STP, чтобы обеспечить стабильность сходимости. Параметры времени включают время приветствия, задержку передачи и максимальный возраст. Подкоманду **hello-time** можно использовать для установки нового значения времени приветствия взамен настроек по умолчанию.

Выполните следующую команду, чтобы перевести коммутатор в режим корневого моста:

| Команда   | Описание   |
|---|--|
| <b>spanning-tree mstp instance-id root primary [diameter net-diameter [hello-time seconds]]</b> | <p>Настраивает коммутатор в качестве корневого в указанном MSTI</p> <p><b>instance-id</b> представляет номер экземпляра связующего дерева в диапазоне от 0 до 15</p> <p><b>net-diameter</b> представляет диаметр сети, который является необязательным параметром. Это эффективно, когда <b>instance-id</b> равен 0. Диапазон – от 2 до 7</p> <p><b>seconds</b> означает единицу измерения времени приветствия в секундах. Диапазон – от 1 до 10</p> |
| <b>no spanning-tree mstp instance-id root</b>   | <p>Отменяет корневую настройку коммутатора в связующем дереве</p> <p><b>instance-id</b> означает номер экземпляра связующего дерева в диапазоне от 0 до 15</p>   |

Выполните следующую команду, чтобы проверить состояние MSTI:

| Команда   | Описание   |
|---|--|
| <b>show spanning-tree mstp [instance instance-id]</b> | Отображает информацию о текущем состоянии MSTP для указанного экземпляра |

## 8.14.14 Настройка вторичного корневого моста

После настройки корня сети вы можете запустить команду **spanning-tree mstp instance-id root secondary**, чтобы назначить один или несколько коммутаторов вторичными (или



резервными) корневыми мостами. Они станут корнем сети, если предыдущий корневой мост по определенным причинам выйдет из строя.

В отличие от конфигурации основного корня, во время запуска команды MSTP устанавливает приоритет связующего дерева коммутатора равным 28672. Если приоритетные значения других коммутаторов в сети остаются на значениях по умолчанию (32768), то текущий коммутатор может быть назначен вторичным корнем.

При настройке вторичного корня вы можете запустить подкоманды **diameter** и **hello-time** для обновления параметров времени STP. Когда вторичный корень становится первичным и начинает работать, все эти параметры активизируются.

Выполните следующую команду, чтобы настроить коммутатор в качестве вторичного корня сети:

| Команда   | Описание  |
|---|---|
| <b>spanning-tree mstp instance-id root secondary [diameter net-diameter [hello-time seconds]]</b> | <p>Настраивает коммутатор в качестве резервного корневого в указанном MSTI</p> <p><b>instance-id</b> представляет номер экземпляра связующего дерева в диапазоне от 0 до 15</p> <p><b>net-diameter</b> представляет диаметр сети, который является необязательным параметром. Это эффективно, когда <b>instance-id</b> равен 0. Диапазон – от 2 до 7</p> <p><b>seconds</b> означает единицу измерения времени приветствия в секундах. Диапазон – от 1 до 10</p> |
| <b>no spanning-tree mstp instance-id root</b>   | <p>Отменяет корневую настройку коммутатора в связующем дереве</p> <p><b>instance-id</b> означает номер экземпляра связующего дерева в диапазоне от 0 до 15</p>  |

Выполните следующую команду, чтобы проверить состояние MSTI:

| Команда   | Описание   |
|---|--|
| <b>show spanning-tree mstp [instance instance-id]</b> | Отображает информацию о текущем состоянии MSTP для указанного экземпляра |

## 8.14.15 Настройка приоритета моста

В некоторых случаях вы можете напрямую, не запуская подкоманду **root**, настроить коммутатор в качестве корня сети, установив приоритет моста. Значение приоритета



коммутатора независимо в каждом экземпляре связующего дерева. Поэтому приоритет можно установить самостоятельно.

Выполните следующую команду, чтобы настроить приоритет моста:

| Команда  | Описание  |
|--|---|
| <b>spanning-tree mstp instance-id priority value</b> | Устанавливает приоритет коммутатора<br><b>instance-id</b> представляет номер экземпляра связующего дерева в диапазоне от 0 до 15<br><b>value</b> представляет приоритет моста. Это может быть одно из следующих значений:<br>0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440 |
| <b>no spanning-tree mstp instance-id priority</b>    | Возвращает приоритет моста коммутатора к значению по умолчанию<br><b>instance-id</b> означает номер экземпляра связующего дерева в диапазоне от 0 до 15.  |

## 8.14.16 Настройка параметров времени STP

Ниже приведены параметры времени STP:

### ➤ Hello Time (время приветствия)

Интервал отправки сообщения о конфигурации на назначенный порт, когда коммутатор выполняет функции корня сети.

### ➤ Forward Delay (задержка передачи)

Время, необходимое порту при переходе из состояния блокировки в состояние обучения и в состояние передачи данных в режиме STP.

### ➤ Max Age (максимальный возраст):

Максимальный срок действия информации о конфигурации связующего дерева.

Для снижения вероятности шока топологии сети должны выполняться следующие требования к временным параметрам:

$$2 \times (\text{fwd\_delay} - 1) \geq \text{max\_age}$$

$$\text{max\_age} \geq (\text{hello\_time} + 1) \times 2$$

Выполните следующую команду, чтобы настроить временные параметры протокола множественного связующего дерева:

| Команда | Описание |
|---------|----------|
|         |          |



|  |   |
|--|---|
| <b>spanning-tree mstp hello-time seconds</b>   | Устанавливает время приветствия<br>Параметр <b>seconds</b> – это единица измерения времени приветствия в диапазоне от 1 до 10 секунд. Его значение по умолчанию – две секунды |
| <b>no spanning-tree mstp hello-time</b>        | Возвращает время приветствия к значению по умолчанию  |
| <b>spanning-tree mstp forward-time seconds</b> | Устанавливает задержку пересылки<br>Параметр <b>seconds</b> – это единица измерения задержки в диапазоне от 4 до 40 секунд. Значение по умолчанию – 15 секунд                 |
| <b>no spanning-tree mstp forward-time</b>      | Возвращает задержку пересылки к значению по умолчанию   |
| <b>spanning-tree mstp max-age seconds</b>      | Устанавливает максимальный возраст<br>Параметр <b>seconds</b> – это единица измерения максимального возраста в диапазоне от 6 до 40 секунд. Значение по умолчанию – 20 секунд |
| <b>no spanning-tree mstp max-age</b>           | Возвращает максимальный возраст к значению по умолчанию   |

Рекомендуется изменять временные параметры STP путем настройки корневого моста или диаметра сети. Это обеспечивает наиболее оптимальное изменение параметров.

Вновь установленные временные параметры действительны, даже если они не соответствуют требованиям вышеуказанной формулы. Обратите внимание на уведомления консоли при выполнении настройки.

### 8.14.17 Настройка диаметра сети

Диаметр сети означает максимальное количество коммутаторов между двумя хостами, что отражает масштаб сети.

Вы можете установить диаметр сети MSTP, выполнив команду **spanning-tree mstp diameter net-diameter**. Параметр *net-diameter* действителен только для CIST. После настройки три временных параметра STP автоматически обновляются до оптимальных значений.

Запустите следующую команду, чтобы настроить сетевой диаметр:

| Команда | Описание |
|---------|----------|
|---------|----------|



|   |   |
|---|---|
| <b>spanning-tree mstp diameter net-diameter</b> | Настраивает диаметр сети<br>Параметр <b>net-diameter</b> находится в диапазоне от 2 до 7. Значение по умолчанию – 7 |
| <b>no spanning-tree mstp diameter</b>           | Возвращает диаметр сети к значению по умолчанию   |

Параметр **net-diameter** не сохраняется как независимая настройка в коммутаторе. Успешное сохранение настроек временных параметров возможно только после установки диаметра сети.

## 8.14.18 Настройка максимального количества переходов

Выполните следующую команду, чтобы настроить максимальное количество переходов (хопов) между узлами в топологии сети.

| Команда                                      | Описание   |
|--|--|
| <b>spanning-tree mstp max-hops hop-count</b> | Указывает максимальное количество переходов.<br>Диапазон <b>hop-count</b> от 1 до 40. Значение по умолчанию – 20 |
| <b>no spanning-tree mstp hop-count</b>       | Восстановить значение <b>hop-count</b> по умолчанию  |

## 8.14.19 Настройка приоритета порта

Если между двумя портами коммутатора возникает петля, порт с более высоким приоритетом перейдет в состояние пересылки, а порт с более низким приоритетом блокируется. Если все порты имеют одинаковый приоритет, порт с меньшим номером первым перейдет в состояние пересылки.

В режиме настройки интерфейса выполните следующие команды, чтобы установить приоритет порта STP:

| Команда  | Описание   |
|--|--|
| <b>spanning-tree mstp instance-id port-priority priority</b> | Устанавливает приоритет порта STP<br><b>instance-id</b> обозначает номер экземпляра связующего дерева в диапазоне от 0 до 15 |



|  |   |
|--|---|
|  | <p><b>priority</b> означает приоритет порта. Это может быть одно из следующих значений:</p> <p>0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240</p>   |
| <b>spanning-tree port-priority value</b>               | <p>Устанавливает приоритет порта во всех экземплярах связующего дерева</p> <p><b>value</b> обозначает приоритет порта. Это может быть одно из следующих значений:</p> <p>0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240</p> |
| <b>no spanning-tree mstp instance-id port-priority</b> | <p>Возвращает приоритет порта в MSTI к значению по умолчанию</p>  |
| <b>no spanning-tree port-priority</b>                  | <p>Возвращает приоритет порта к значению по умолчанию во всех экземплярах связующего дерева</p>   |

## 8.14.20 Настройка стоимости пути порта

В MSTP значение стоимости пути порта по умолчанию зависит от скорости соединения. Если между двумя коммутаторами возникает петля, порт с меньшей стоимостью пути перейдет в состояние пересылки. Чем меньше стоимость пути, тем выше скорость порта. Если все порты имеют одинаковую стоимость пути, порт с меньшим номером первым перейдет в состояние пересылки.

В режиме настройки интерфейса выполните следующую команду, чтобы установить стоимость пути порта:

| Команда   | Описание   |
|---|--|
| <b>spanning-tree mstp instance-id cost cost</b> | <p>Устанавливает стоимость пути для порта</p> <p><b>instance-id</b> обозначает номер экземпляра связующего дерева в диапазоне от 0 до 15</p> <p><b>cost</b> означает стоимость пути порта, которая находится в диапазоне от 1 до 200000000</p> |
| <b>spanning-tree cost value</b>                 | <p>Устанавливает стоимость пути порта во всех экземплярах связующего дерева</p> <p><b>value</b> обозначает стоимость пути, которая находится в диапазоне от 1 до 200000000</p>   |



|   |   |
|---|---|
| <b>no spanning-tree mstp instance-id cost</b> | Возвращает стоимость пути порта в MSTI к значению по умолчанию                                |
| <b>no spanning-tree cost</b>                  | Возвращает стоимость пути порта к значению по умолчанию во всех экземплярах связующего дерева |

### 8.14.21 Настройка типа подключения порта

Если соединение между коммутаторами с поддержкой MSTP является прямым соединением «точка-точка», коммутаторы могут быстро установить его с помощью механизма квитирования. При настройке типа подключения порта выберите режим **point-to-point**.

Протокол решает, использовать ли соединение «точка-точка» или нет, в зависимости от атрибута дуплекса. Если порт работает в полнодуплексном режиме, протокол считает соединение двухточечным. Если порт работает в полудуплексном режиме, протокол считает соединение общим, или разделяемым.

Если подтвердится, что коммутатор, подключенный к порту, работает по протоколу RSTP или MSTP, тип подключения порта можно настроить как «точка-точка», чтобы гарантировать возможность быстрого подтверждения связи.

Для указания типа подключения порта используйте следующую команду в режиме настройки интерфейса:

| Команда  | Описание   |
|--|--|
| <b>spanning-tree mstp point-to-point force-true</b>  | Устанавливает тип подключения порта «точка-точка»              |
| <b>spanning-tree mstp point-to-point force-false</b> | Устанавливает тип подключения порта «разделение канала»        |
| <b>spanning-tree mstp point-to-point auto</b>        | Автоматически проверяет тип подключения порта                  |
| <b>no spanning-tree mstp point-to-point</b>          | Восстанавливает тип подключения порта до настроек по умолчанию |

### 8.14.22 Активация режима совместимости с MST

Протокол MSTP, который поддерживается данной серией коммутаторов, основан на IEEE 802.1s. Чтобы быть совместимым с другими протоколами MSTP, особенно с тем, который поддерживают коммутаторы Cisco, он может работать в MST-совместимом режиме. Коммутаторы, работающие в режиме совместимости, могут идентифицировать структуру



сообщений других MSTP, проверять содержащийся региональный идентификатор MST и устанавливать регион MST.

MST- и STP-совместимые режимы основаны на механизме преобразования протокола MSTP. Если какой-либо порт коммутатора получает BPDU в совместимом режиме, он автоматически переходит в нужный режим и отправляет BPDU уже в нем. Чтобы возобновить работу порта в стандартном режиме MST, вы можете запустить команду **spanning-tree mstp migration-check**.

В режиме глобальной конфигурации выполните следующие команды, чтобы включить или отключить режим совместимости с MST:

| Команда                                     | Описание                                    |
|---|---|
| <b>spanning-tree mstp mst-compatible</b>    | Включает MST-совместимый режим коммутатора  |
| <b>no spanning-tree mstp mst-compatible</b> | Отключает MST-совместимый режим коммутатора |



- Основная функция режима совместимости – создание области MST, в которой будут коммутаторы, работающие по протоколу MSTP. В реальной сети убедитесь, что коммутатор имеет то же имя конфигурации и тот же номер редактирования. Рекомендуется настроить узел, работающий с другими протоколами MSTP, в качестве корня CIST, гарантируя, что коммутатор перейдет в режим совместимости путем получения сообщения.
- Если режим совместимости с MST не включен, то коммутатор будет неспособен корректно обрабатывать контент, совместимый с BPDU, и не сможет правильно взаимодействовать с другим коммутатором, который поддерживает MST. Из-за этого такие два коммутатора не смогут работать в одном регионе.
- Порт в режиме совместимости не может автоматически возобновить отправку стандартного MST BPDU, даже если этот режим отключен глобально. В этом случае запустите **migration-check**.

### 8.14.23 Перезапуск проверки конвертации протоколов

MSTP позволяет коммутатору работать с традиционным коммутатором STP посредством механизма преобразования протокола. Если один порт коммутатора получает конфигурационное сообщение STP, в дальнейшем он передает только сообщения STP. В то же время порт, который получает информацию STP, считается граничным портом.



Когда порт находится в состоянии STP-совместимости, он не перейдет автоматически в режим MSTP, даже если больше не получает сообщений STP. В



этом случае вы можете запустить команду **spanning-tree mstp migration-check**, чтобы очистить сообщения STP, полученные портом, и вернуть порт в режим MSTP.

Коммутатор, использующий протокол RSTP, может идентифицировать и обрабатывать сообщение MSTP. Таким образом, коммутатор MSTP не требует преобразования протокола при работе с коммутатором RSTP.

В режиме глобальной конфигурации выполните следующую команду, чтобы очистить всю информацию STP, обнаруженную всеми портами коммутатора:

| Команда                                   | Описание   |
|---|--|
| <b>spanning-tree mstp migration-check</b> | Очищает всю информацию STP, обнаруженную всеми портами коммутатора |

В режиме настройки интерфейса выполните следующую команду, чтобы очистить информацию STP, обнаруженную портом:

| Команда                                   | Описание  |
|---|---|
| <b>spanning-tree mstp migration-check</b> | Очищает всю информацию STP, обнаруженную выбранным портом |

#### 8.14.24 Проверка информации MSTP

В командном режиме системного мониторинга, глобальной конфигурации или настройки интерфейса выполните следующие команды, чтобы проверить всю информацию о настройках MSTP.

| Команда   | Описание   |
|---|--|
| <b>show spanning-tree</b>                               | Отображает информацию MSTP<br>(Можно проверить информацию о SSTP, PVST, RSTP и MSTP)           |
| <b>show spanning-tree detail</b>                        | Отображает детальную информацию MSTP<br>(Можно проверить информацию о SSTP, PVST, RSTP и MSTP) |
| <b>show spanning-tree interface <i>interface-id</i></b> | Отображает информацию STP-порта<br>(Можно проверить информацию о SSTP, PVST, RSTP и MSTP)      |



|   |   |
|---|---|
| <b>show spanning-tree mstp</b>                                  | Отображает все экземпляры MST                       |
| <b>show spanning-tree mstp region</b>                           | Отображает настройки региона MST                    |
| <b>show spanning-tree mstp instance</b><br><i>instance-id</i>   | Отображает указанный экземпляр MST                  |
| <b>show spanning-tree mstp detail</b>                           | Отображает детальную информацию MST                 |
| <b>show spanning-tree mstp interface</b><br><i>interface-id</i> | Отображает настройки MST-порта                      |
| <b>show spanning-tree mstp protocol-migration</b>               | Отображает статус преобразования протокола на порту |

## 8.15 Дополнительные функции STP

### 8.15.1 Введение

Модуль протокола связующего дерева коммутатора поддерживает семь дополнительных функций. Эти функции не настроены по умолчанию. Они поддерживаются в различных режимах протокола связующего дерева следующим образом:

| Дополнительные функции | SSTP | PVST | RSTP | MSTP |
|------------------------|------|------|------|------|
| <b>Port Fast</b>       | Да   | Да   | Нет  | Нет  |
| <b>BPDU Guard</b>      | Да   | Да   | Да   | Да   |
| <b>BPDU Filter</b>     | Да   | Да   | Нет  | Нет  |
| <b>Uplink Fast</b>     | Да   | Да   | Нет  | Нет  |
| <b>Backbone Fast</b>   | Да   | Да   | Нет  | Нет  |
| <b>Root Guard</b>      | Да   | Да   | Да   | Да   |
| <b>Loop Guard</b>      | Да   | Да   | Да   | Да   |

### 8.15.2 Port Fast

Port Fast (быстрый порт) немедленно переводит интерфейс, настроенный как порт доступа или магистральный порт, в состояние пересылки из состояния блокировки, минуя состояния прослушивания и обучения. Вы можете использовать Port Fast на интерфейсах,



подключенных к одной рабочей станции или серверу, чтобы позволить этим устройствам немедленно подключаться к сети, не дожидаясь сходимости связующего дерева.

Интерфейсы, подключенные к одной рабочей станции или серверу, не должны получать BPDU. Однако использование Port Fast может привести к появлению петель в сети, если к порту будет подключен другой коммутатор или устройство, которое может создавать дополнительные соединения. Поэтому рекомендуется использовать Port Fast только на портах, подключенных к устройствам конечных пользователей.

Функцию Port Fast можно настроить как в режиме глобальной конфигурации, так и в режиме настройки интерфейса. Если настроен глобальный режим, все порты будут считаться портами Port Fast и быстро перейдут в состояние пересылки. Таким образом увеличивается вероятность возникновения сетевых петель. Чтобы предотвратить это, вы можете использовать для защиты портов функции BPDU Guard или BPDU Filter.

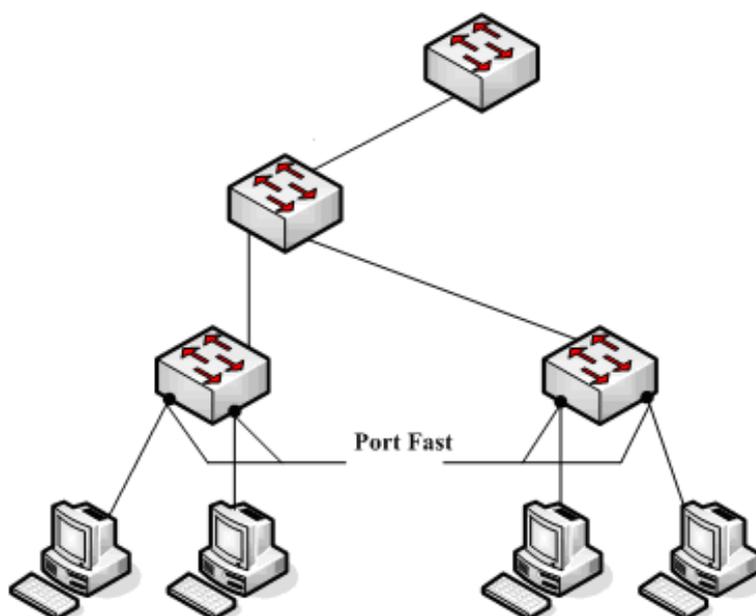


Рисунок 12 – Port Fast



Быстрые протоколы связующего дерева RSTP и MSTP могут немедленно перевести интерфейс в состояние пересылки, поэтому в таком случае нет необходимости использовать функцию Port Fast.

### 8.15.3 BPDU Guard

Функцию защиты от BPDU можно включить глобально на коммутаторе или для каждого порта в отдельности, но в работе этих режимов есть некоторые различия.



На глобальном уровне BPDU Guard включается на портах с поддержкой Port Fast, при помощи команды **spanning-tree portfast bpduguard default**. Связующее дерево отключит порты Port Fast, если на них будет получен какой-либо BPDU. В допустимой конфигурации порты с поддержкой Port Fast не получают BPDU. Их получение на порту с поддержкой Port Fast означает недопустимую конфигурацию, например, подключение неавторизованного устройства. В таком случае функция BPDU Guard переводит порт в состояние «error-disabled» (отключение из-за ошибки). Когда это происходит, коммутатор отключает весь порт, на котором произошло нарушение.

Чтобы предотвратить полное отключение порта, можно в режиме глобальной конфигурации применить команду **errdisable detect cause bpduguard shutdown vlan**. Это позволяет отключить только проблемную VLAN на порту, где произошло нарушение.

В режиме настройки интерфейса при помощи команды **spanning-tree bpduguard enable** можно включить BPDU Guard на любом порту без включения функции Port Fast. Когда порт получит BPDU, он будет переведен в состояние «error-disabled».

Функция BPDU Guard обеспечивает безопасный ответ на недопустимые конфигурации, поскольку пользователю будет необходимо вручную вернуть интерфейс в эксплуатацию. Рекомендуется включать BPDU Guard в сети поставщика услуг, чтобы предотвратить участие порта доступа в связующем дереве.

#### 8.15.4 BPDU Filter

Функция BPDU Filter может быть включена глобально на коммутаторе или для каждого интерфейса, но эта функция работает с некоторыми отличиями.

В режиме SSTP/PVST, если порт Port Fast с включенным BPDU Filter получает BPDU, функции BPDU Filter и Port Fast на порту будут автоматически отключены, и он снова станет обычным портом. Прежде чем перейти в состояние пересылки, порт должен находиться в состояниях прослушивания и обучения.

Функцию BPDU Filter можно настроить глобально или в режиме настройки интерфейса. В режиме глобальной конфигурации запустите команду **spanning-tree portfast bpdufilter**, чтобы запретить всем портам отправлять BPDU. Тем не менее, порты по-прежнему смогут получать и обрабатывать BPDU.

#### 8.15.5 Uplink Fast

Функция Uplink Fast (быстрый восходящий канал) позволяет новым корневым портам быстро переходить в состояние пересылки, когда соединение между коммутатором и корневым мостом разрывается.

Сложная сеть всегда содержит несколько уровней устройств, как показано на рисунке 13. И уровень агрегации, и уровень доступа имеют резервные соединения с верхним уровнем. Эти резервные соединения обычно блокируются STP, чтобы избежать петель.

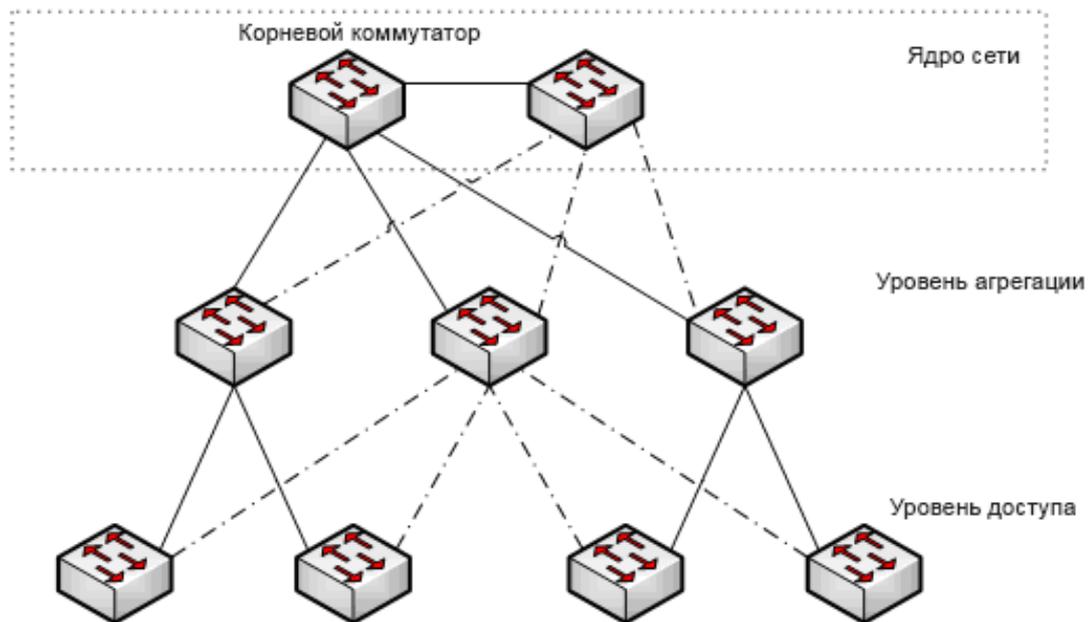


Рисунок 13 – Топология сети

Предположим, что соединение между коммутатором и верхним уровнем разорвано (это называется отказом прямого канала). STP выбирает альтернативный порт на линии резервирования в качестве корневого порта. Перед переходом в состояние пересылки альтернативный порт должен находиться в состоянии прослушивания и обучения. Если в режиме глобальной конфигурации с помощью команды **spanning-tree uplinkfast** включить функцию Uplink Fast, новый корневой порт сможет напрямую перейти в состояние пересылки, восстанавливая соединение между коммутатором и верхним уровнем.

На рисунке 14 показан принцип работы функции Uplink Fast. Порт коммутатора С, находясь в исходном состоянии, является резервным портом для подключения коммутатора В. Когда соединение между коммутатором С и корневым коммутатором А разрывается, альтернативный порт выбирается в качестве нового корневого порта и немедленно начинается передача данных.

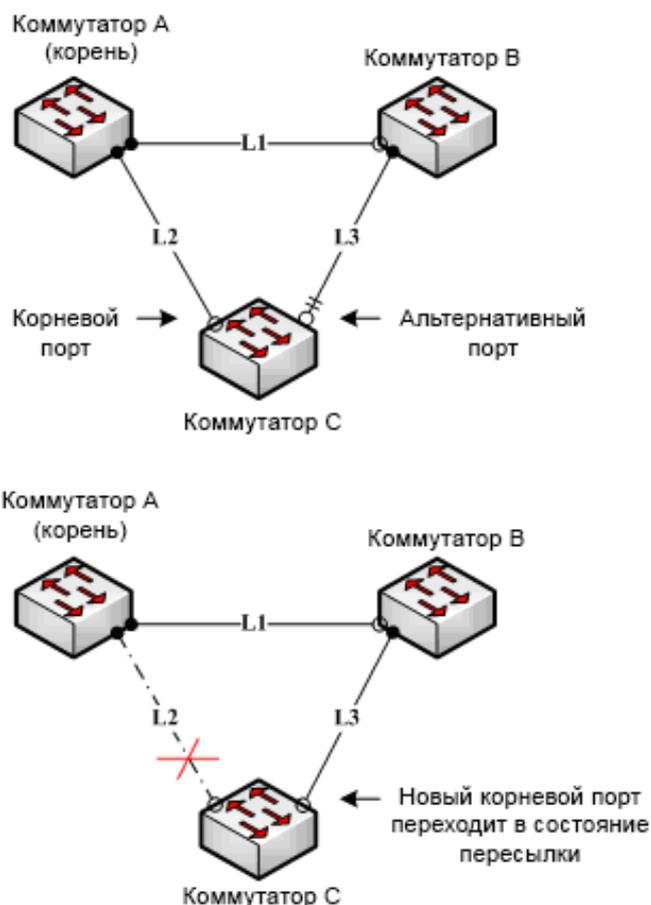


Рисунок 14 – Uplink Fast



Функция Uplink Fast оптимизирует поведение коммутатора при медленной сходимости протоколов STP (SSTP) и PVST, что обеспечивает более быстрое восстановление связности после обрыва пути. Однако в других протоколах, таких как RSTP и MSTP, новый корневой порт может быстро перейти в состояние пересылки без использования функции Uplink Fast. В этих протоколах быстрое действие восстановления связности уже заложено изначально, и для ускорения процесса Uplink Fast не требуется.

## 8.15.6 Backbone Fast

Функция Backbone Fast (быстрое магистральное соединение) является дополнением технологии Uplink Fast. Технология Uplink Fast обеспечивает быструю работу резервной линии в случае разрыва прямого соединения с назначенным коммутатором, а технология Backbone Fast помогает обнаруживать косвенные сетевые разрывы (проблемы с соединением) на верхнем уровне сети и ускоряет процесс изменения состояния портов.

На рисунке 14 соединение L2 между коммутатором С и коммутатором А называется прямым соединением между коммутатором С и корневым коммутатором А. Если



соединение разорвано, функция Uplink Fast может решить проблему. Соединение L1 между коммутаторами А и В называется косвенным каналом коммутатора С. Отключенное косвенное соединение называется косвенным сбоем, который обрабатывается функцией Backbone Fast.

Принцип работы функции Backbone Fast показан на рисунке 15.

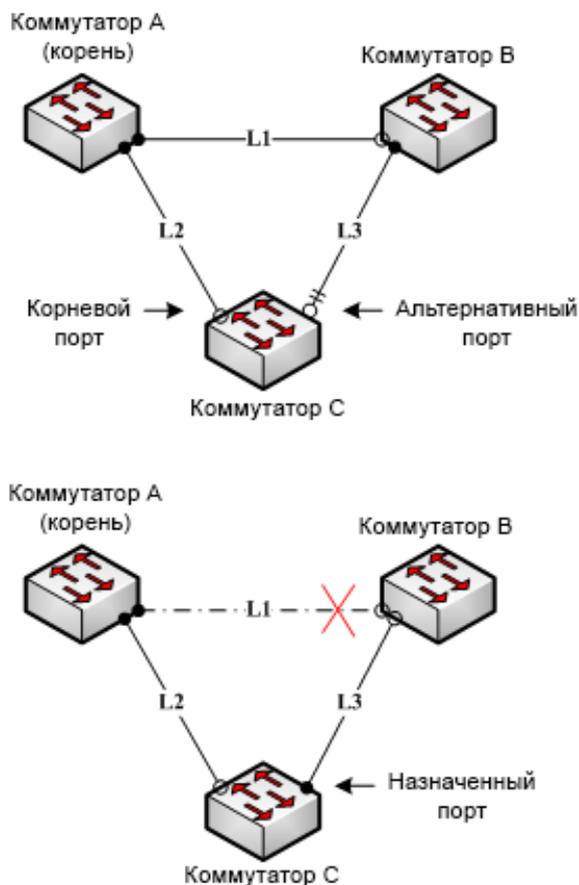


Рисунок 15 – Backbone Fast

Предположим, что приоритет моста коммутатора С выше, чем приоритет моста коммутатора В. Когда L1 отключен, коммутатор В выбирается для отправки BPDU коммутатору С, поскольку приоритет моста используется в качестве корневого приоритета. Что касается коммутатора С информация, содержащаяся в BPDU, не приоритетна информации, содержащейся в нем самом. Если Backbone Fast не включен, порт между коммутатором С и коммутатором В ожидает информацию в течение установленного времени устаревания, а затем становится назначенным портом. Это обычно занимает несколько секунд. После того, как функция включена в режиме глобальной конфигурации с помощью команды **spanning-tree backbonefast**, когда альтернативный порт коммутатора С получает BPDU с более низким приоритетом, коммутатор С считает, что соединение по косвенному каналу, способное достигнуть корневого коммутатора, на порту отключено. После этого коммутатор С незамедлительно переводит порт в статус назначенного, не дожидаясь окончания времени устаревания.



После включения Backbone Fast, если на разных портах будут получены BPDU с низким приоритетом, коммутатор будет выполнять разные действия. Если сообщение получает альтернативный порт, он становится назначенным. Если сообщение с низким приоритетом получает корневой порт, а другого резервного порта нет, коммутатор сам становится корневым.

Обратите внимание, что функция Backbone Fast просто не учитывает время устаревания информации. Новый назначенный порт по-прежнему должен следовать порядку изменения состояния: состояние прослушивания, затем состояние обучения и, наконец, состояние пересылки.



Подобно Uplink Fast, функция Backbone Fast эффективна в режимах SSTP и PVST, но не имеет смысла в RSTP и MSTP.

### 8.15.7 Root Guard

Функция Root Guard (защита корня) предотвращает превращение порта в корневой из-за получения высокоприоритетного BPDU.

Сеть второго уровня поставщика услуг (SP) может включать в себя множество подключений к коммутаторам, которые не принадлежат поставщику услуг. В такой топологии связующее дерево может переконфигурироваться и выбрать пользовательский коммутатор в качестве корневого. Вы можете избежать этой ситуации, включив Root Guard на интерфейсах коммутаторов SP, которые подключаются к коммутаторам в сети вашего клиента. Если расчеты связующего дерева приводят к выбору интерфейса в сети клиента в качестве корневого порта, Root Guard переводит интерфейс в заблокированное состояние, чтобы коммутатор клиента не стал корневым мостом.

Если коммутатор вне сети SP становится корневым, интерфейс блокируется, и связующее дерево выбирает новый корневой коммутатор. Таким образом, коммутатор клиента не становится корневым коммутатором и не находится на пути к корню.

Если коммутатор работает в режиме множественного связующего дерева (MST), Root Guard принудительно определяет интерфейс на роль назначенного порта. Если граничный порт заблокирован во внутреннем экземпляре связующего дерева (IST) из-за Root Guard, интерфейс также блокируется во всех экземплярах MST. Граничный порт – это интерфейс, который подключается к локальной сети, назначенным коммутатором которой является либо коммутатор IEEE 802.1D, либо коммутатор с другой конфигурацией региона MST.

Функция Root Guard, включенная на интерфейсе, применяется ко всем сетям VLAN, которым принадлежит интерфейс. Сети VLAN можно сгруппировать и сопоставить с экземпляром MST.

Эту функцию можно включить на интерфейсе с помощью команды **spanning-tree guard root**.



Функция Root Guard действует по-разному в SSTP/PVST и RSTP/MSTP. В режиме SSTP/PVST корневой порт всегда блокируется с помощью Root Guard. В режиме RSTP/MSTP корневой порт не будет заблокирован до получения BPDU более высокого уровня. Порт, который ранее играл роль корневого, не будет заблокирован.

### 8.15.8 Loop Guard

Функция Loop Guard (защита от петель) может быть использована, чтобы предотвратить превращение альтернативных или корневых портов в назначенные из-за сбоя, который приводит к однонаправленному соединению. Эта функция наиболее эффективна, когда она включена во всей коммутируемой сети. Loop Guard не позволяет альтернативным и корневым портам стать назначенными портами, а связующее дерево не отправляет BPDU на корневые или альтернативные порты.

Вы можете включить эту функцию с помощью команды **spanning-tree loopguard default** в режиме глобальной конфигурации.

Когда коммутатор работает в режиме PVST+ или Rapid-PVST+, Loop Guard предотвращает превращение альтернативных и корневых портов в назначенные порты, а связующее дерево не отправляет BPDU на корневые или альтернативные порты.

Когда коммутатор работает в режиме MST, BPDU не отправляются на неграничные порты только если Loop Guard блокирует интерфейс во всех экземплярах MST. На граничном порту Loop Guard блокирует интерфейс во всех экземплярах MST.



Функция Loop Guard действует по-разному в SSTP/PVST и RSTP/MSTP. В режиме SSTP/PVST нестабильный порт всегда блокируется функцией Loop Guard. В режиме RSTP/MSTP порт будет заблокирован только в том случае, если он стал назначенным из-за недоступности для приема BPDU. Loop Guard не будет блокировать порт, который выполняет роль назначенного из-за получения BPDU нижнего уровня.

### 8.15.9 Настройка Port Fast

Интерфейс с включенной функцией Port Fast переводится непосредственно в состояние пересылки сообщений связующего дерева, не дожидаясь окончания времени стандартной задержки.

Используйте следующую команду для настройки функции Port Fast в режиме глобальной конфигурации:



| Команда                                  | Описание  |
|--|---|
| <b>spanning-tree portfast default</b>    | Глобально включает функцию Port Fast. Действительно для всех интерфейсов    |
| <b>no spanning-tree portfast default</b> | Глобально отключает функция Port Fast. Не влияет на конфигурацию интерфейса |



Функция Port Fast применяется только к интерфейсу, который подключается к хосту. BPDU Guard или BPDU Filter должны быть настроены одновременно с глобальной настройкой Port Fast.

Используйте следующую команду для включения функции Port Fast в режиме настройки интерфейса:

| Команда                          | Описание  |
|----------------------------------|---|
| <b>spanning-tree portfast</b>    | Включает функцию Port Fast на интерфейсе  |
| <b>no spanning-tree portfast</b> | Отключает функцию Port Fast на интерфейсе. Это не влияет на глобальную конфигурацию |

## 8.15.10 Настройка BPDU Guard

При глобальном включении BPDU Guard на портах с активным Port Fast связующее дерево отключает порты Port Fast, которые получают BPDU.

В допустимой конфигурации порты с поддержкой Port Fast не получают BPDU. Их получение на порту с Port Fast означает недопустимую конфигурацию, например, подключение неавторизованного устройства. В таком случае функция BPDU Guard переводит порт в состояние «error-disabled» (отключение из-за ошибки). Когда это происходит, коммутатор отключает весь порт, на котором произошло нарушение.

Чтобы предотвратить полное отключение порта, можно в режиме глобальной конфигурации применить команду **errdisable detect cause bpduguard shutdown vlan**. Это позволяет отключить только проблемную VLAN на порту, где произошло нарушение.

Функция BPDU Guard обеспечивает безопасный ответ на недопустимые конфигурации, поскольку пользователю будет необходимо вручную вернуть интерфейс в эксплуатацию. Рекомендуется включать BPDU Guard в сети поставщика услуг, чтобы предотвратить участие порта доступа в связующем дереве.

Выполните следующие действия, чтобы глобально включить функцию BPDU Guard:



| Команда                                    | Описание  |
|--|---|
| <b>spanning-tree portfast bpduguard</b>    | Глобально включает функцию BPDU Guard. Это действительно для всех интерфейсов |
| <b>no spanning-tree portfast bpduguard</b> | Глобально отключает функцию BPDU Guard  |



Глобальное включение функции Port Fast может привести к широковещательному шторму. В целях защиты необходимо настроить BPDU Guard или BPDU Filter.

Выполните следующие действия, чтобы включить функцию защиты BPDU в режиме настройки интерфейса:

| Команда                                | Описание   |
|--|--|
| <b>spanning-tree bpduguard enable</b>  | Включает функцию BPDU Guard на интерфейсе  |
| <b>spanning-tree bpduguard disable</b> | Отключает функцию BPDU Guard на интерфейсе. Это не влияет на глобальную конфигурацию |
| <b>no spanning-tree bpduguard</b>      |  |

## 8.15.11 Настройка BPDU Filter

Когда вы глобально включаете BPDU Filter на интерфейсах с поддержкой Port Fast, это предотвращает отправку или получение ими BPDU. Тем не менее, интерфейсы все равно отправляют несколько BPDU при подключении, прежде чем коммутатор начнет фильтровать их. Чтобы хосты, подключенные к этим интерфейсам, не получали BPDU, следует включить BPDU Filter на коммутаторе глобально. Если BPDU получен на интерфейсе с поддержкой Port Fast, отключается и Port Fast, и BPDU Filter.

Выполните следующие действия, чтобы глобально включить функцию BPDU Filter:

| Команда                                     | Описание   |
|---|--|
| <b>spanning-tree portfast bpdufilter</b>    | Глобально включает функцию BPDU Filter. Это действительно для всех интерфейсов |
| <b>no spanning-tree portfast bpdufilter</b> | Глобально отключает функцию BPDU Filter  |



Глобальное включение функции Port Fast может привести к широковещательному шторму. В целях защиты необходимо настроить BPDU Guard или BPDU Filter.



Выполните следующие действия, чтобы включить функцию BPDU Filter в режиме настройки интерфейса:

| Команда                                  | Описание  |
|--|---|
| <b>spanning-tree bpdudfilter enable</b>  | Включает функцию BPDU Filter на интерфейсе  |
| <b>spanning-tree bpdudfilter disable</b> | Отключает функцию BPDU Filter на интерфейсе. Это не влияет на глобальную конфигурацию |
| <b>no spanning-tree bpdudfilter</b>      |   |

### 8.15.12 Настройка Uplink Fast

Если коммутатор теряет подключение, он начинает использовать альтернативные пути, как только связующее дерево выбирает новый корневой порт. Включив Uplink Fast в режиме глобальной конфигурации с помощью команды **spanning-tree uplinkfast**, вы можете ускорить выбор нового корневого порта при отказе соединения или коммутатора, а также при перенастройке связующего дерева. Корневой порт немедленно переходит в состояние пересылки, не проходя через состояния прослушивания и обучения, как это происходит при обычных процедурах связующего дерева.

Функция Uplink Fast действует только в режиме SSTP/PVST.

Выполните следующие действия для глобального включения Uplink Fast:

| Команда                            | Описание                     |
|------------------------------------|------------------------------|
| <b>spanning-tree uplinkfast</b>    | Включает функцию UplinkFast  |
| <b>no spanning-tree uplinkfast</b> | Выключает функцию UplinkFast |

### 8.15.13 Настройка Backbone Fast

BackboneFast – это дополнительная технология к функции Uplink Fast, которая реагирует на сбои в соединениях, напрямую подключенных к коммутаторам доступа. Backbone Fast оптимизирует таймер max-age, который контролирует количество времени, в течение которого коммутатор хранит информацию протокола, полученную на интерфейсе. Когда коммутатор получает низкоприоритетный BPDU от назначенного порта другого коммутатора, это является сигналом о том, что другой коммутатор мог потерять свой путь к корню, и Backbone Fast пытается найти альтернативный путь.

Функция Backbone Fast действует только в режиме SSTP/PVST.

Выполните следующие действия, чтобы глобально включить Backbone Fast:





| Команда                              | Описание                        |
|--------------------------------------|---------------------------------|
| <b>spanning-tree backbonefast</b>    | Включает функцию Backbone Fast  |
| <b>no spanning-tree backbonefast</b> | Выключает функцию Backbone Fast |

### 8.15.14 Настройка Root Guard

Root Guard, включенный на интерфейсе, применяется ко всем VLAN, которым принадлежит интерфейс. Не включайте Root Guard на интерфейсах с активной функцией Uplink Fast. С Uplink Fast резервные интерфейсы (в заблокированном состоянии) заменяют корневой порт в случае сбоя. Однако, если Root Guard также включен, все резервные интерфейсы с UplinkFast, переводятся в состояние несовместимости с корнем (заблокированы) и не могут перейти в состояние пересылки.

Функция Root Guard действует по-разному в SSTP/PVST и RSTP/MSTP. В режиме SSTP/PVST переход в статус корневого блокируется Root Guard. В режиме RSTP/MSTP переход не будет блокироваться до получения BPDU более высокого уровня. Порт, который ранее играл роль корневого, не будет блокироваться.

Выполните следующие действия, чтобы включить Root Guard на интерфейсе:

| Команда                         | Описание  |
|---------------------------------|---|
| <b>spanning-tree guard root</b> | Включает функцию Root Guard на интерфейсе               |
| <b>no spanning-tree guard</b>   | Отключает функции Root Guard и Loop Guard на интерфейсе |
| <b>spanning-tree guard none</b> |   |

### 8.15.15 Настройка Loop Guard

Вы можете использовать Loop Guard, чтобы предотвратить превращение альтернативных или корневых портов в назначенные из-за сбоя, который приводит к однонаправленному соединению. Эта функция наиболее эффективна, когда она настроена на всей коммутируемой сети. Loop Guard работает только на интерфейсах, которые рассматриваются связующим деревом как соединение «точка-точка».

Функция Loop Guard действует по-разному в SSTP/PVST и RSTP/MSTP. В режиме SSTP/PVST назначенный порт всегда блокируется при помощи Loop Guard. В режиме RSTP/MSTP порт будет заблокирован только тогда, когда он становится назначенным из-за недоступности для получения BPDU. Порт, оказавшийся в роли назначенного из-за получения BPDU более низкого уровня, не будет заблокирован Loop Guard.

Выполните следующие действия, чтобы включить Loop Guard в режиме глобальной конфигурации:



| Команда                                   | Описание  |
|---|---|
| <b>spanning-tree loopguard default</b>    | Глобально включает функцию Loop Guard. Действительно для всех интерфейсов |
| <b>no spanning-tree loopguard default</b> | Глобально отключает Loop Guard  |

Выполните следующие действия, чтобы включить Loop Guard в режиме настройки интерфейса:

| Команда                         | Описание  |
|---------------------------------|---|
| <b>spanning-tree guard loop</b> | Включает функцию Loop Guard на интерфейсе               |
| <b>no spanning-tree guard</b>   | Отключает функции Root Guard и Loop Guard на интерфейсе |
| <b>spanning-tree guard none</b> |   |

## 9. Настройка таблицы MAC-адресов

Задачи настройки таблицы MAC-адресов

- Настройка статического MAC-адреса
- Настройка времени устаревания MAC-адреса
- Настройка совместного изучения MAC-адреса разными VLAN
- Отображение MAC-адресов
- Удаление динамических MAC-адресов

### 9.1 Настройка статического MAC-адреса

Статические записи MAC-адресов – это записи, которые не устаревают и могут быть удалены только вручную. В соответствии с фактическими требованиями в процессе работы вы можете добавлять и удалять статический MAC-адрес. Для этого используйте следующую команду на привилегированном уровне:

| Команда   | Описание                                       |
|---|--|
| <b>config</b>   | Вход в режим глобальной конфигурации           |
| <b>[no] mac address-table static mac-addr vlan vlan-id interface interface-id</b> | Добавить/удалить статическую запись MAC-адреса |



|              |   |
|--------------|---|
|              | <b>mac-addr</b> – указывает MAC-адрес<br><b>vlan-id</b> – указывает номер VLAN. Диапазон допустимых значений 1–4094<br><b>interface-id</b> – указывает имя интерфейса |
| <b>exit</b>  | Вернуться в режим управления  |
| <b>write</b> | Сохранить настройки   |

## 9.2 Настройка времени устаревания MAC-адреса

Если динамический MAC-адрес не используется в течение указанного времени устаревания, коммутатор удаляет его из таблицы MAC-адресов. Время устаревания MAC-адреса можно настроить в соответствии с потребностями. По умолчанию значение составляет 300 секунд.

Настройте время устаревания MAC-адреса в привилегированном режиме следующим образом:

| Команда  | Описание   |
|--|--|
| <b>config</b>  | Вход в режим глобальной конфигурации   |
| <b>mac address-table aging-time [0   10-1000000]</b> | Настройка времени устаревания MAC-адреса<br><b>0</b> – указывает на отсутствие времени устаревания. MAC-адрес не удаляется<br>Допустимое значение: от 10 до 1000000 секунд |
| <b>exit</b>  | Вернуться в режим управления   |
| <b>write</b>   | Сохранить настройки  |

## 9.3 Настройка совместного изучения MAC-адреса разными VLAN

Когда на порту активна настройка VLAN-shared MAC address, MAC-адрес, изученный портом, будет общим для всех VLAN, то есть другие VLAN также его узнают.

Для настройки функции выполните следующие команды:



| Команда                           | Описание   |
|-----------------------------------|--|
| <b>config</b>                     | Вход в режим глобальной конфигурации                   |
| <b>interface q0/1</b>             | Вход в режим настройки выбранного интерфейса           |
| <b>switchport shared-learning</b> | Настройка совместного изучения MAC-адреса разными VLAN |
| <b>exit</b>                       | Вернуться в режим глобальной конфигурации              |
| <b>exit</b>                       | Вернуться в режим управления                           |
| <b>write</b>                      | Сохранить настройки                                    |

## 9.4 Отображение MAC-адресов

Поскольку в процессе работы требуются отладка и управление, пользователю необходимо знать содержимое таблицы MAC-адресов коммутатора. Используйте команду **show** для отображения MAC-адресов таблицы.

| Команда  | Описание   |
|--|--|
| <b>show mac address-table {dynamic [interface <i>interface-id</i>   vlan <i>vlan-id</i>]   static}</b> | <p><b>dynamic</b> отображает только динамические записи MAC-адресов</p> <p><b>interface</b> отображает динамические записи MAC-адресов на указанном интерфейсе</p> <p><b>interface-id</b> указывает имя интерфейса</p> <p><b>vlan</b> отображает динамические записи MAC-адресов в указанной VLAN</p> <p><b>vlan-id</b> указывает номер VLAN. Диапазон допустимых значений 1–4094</p> <p><b>static</b> отображает только статические записи MAC-адресов, добавленные администратором</p> |

## 9.5 Удаление динамических MAC-адресов

Таблицу изученных коммутатором MAC-адресов в некоторых случаях необходимо очистить. Это может быть полезно при разрешении проблем со связностью или при



изменении топологии сети. Используйте следующую команду в привилегированном режиме:

| Команда   | Описание  |
|---|---|
| <pre>clear mac address-table dynamic [address mac-addr   interface interface-id   vlan vlan-id]</pre> | <p>Удаление динамических записей MAC-адресов</p> <p><b>dynamic</b> означает динамические MAC-адреса</p> <p><b>mac-addr</b> указывает конкретный MAC-адрес для удаления из таблицы. Если присутствует этот параметр, коммутатор удалит только запись с указанным MAC-адресом</p> <p><b>interface-id</b> указывает, что следует удалить адреса, изученные данным интерфейсом</p> <p><b>vlan-id</b> указывает номер VLAN, все записи динамических MAC-адресов которой следует удалить. Диапазон допустимых значений 1–4094</p> |

## 10. Агрегация каналов

### 10.1 Введение

Агрегация каналов, также называемая транкингом, является дополнительной функцией, доступной на коммутаторе Ethernet, и используется при создании моста второго уровня. Агрегация позволяет логически объединить несколько портов в один канал. Поскольку при объединении становится доступной полная полоса пропускания каждого физического канала, неэффективная маршрутизация трафика не тратит полосу пропускания впустую. В результате весь кластер используется более эффективно. Агрегация каналов обеспечивает более высокую совокупную пропускную способность для серверов с большим трафиком и возможность перенаправления в случае отказа одного порта или кабеля.

Поддерживаемые функции

➤ **Статическое управление агрегацией портов:**

возможность связывания физического порта с логическим портом независимо от того, могут ли они фактически связаться с логическим портом.

➤ **Управление агрегацией с динамическим согласованием LACP:**

когда физический порт настраивается на привязку к логическому порту, эта возможность доступна только портам с LACP-согласованием. Другие порты не могут быть объединены в логический порт.

➤ **Балансировка потоков данных агрегированных портов:**

после создания агрегации данные потока агрегированного порта будут распределены на каждый физический порт, входящий в группу.

Задачи настройки агрегации портов



- Настройка логического канала, используемого для агрегации
- Агрегация физических портов
- Выбор режима балансировки нагрузки агрегированных портов
- Отслеживание состояния агрегации

## 10.2 Настройка логического канала, используемого для агрегации

Прежде чем связывать физические порты вместе, вам следует создать логический порт. Он используется для управления каналом, образованным связанными физическими портами. Для создания порта выполните следующую команду:

| Команда                                    | Описание                           |
|--|------------------------------------|
| <b>interface port-aggregator <i>id</i></b> | Создает логический канал агрегации |

## 10.3 Агрегация физических портов

Чтобы объединить несколько физических портов в логический канал, вы можете использовать для согласования статическую агрегацию или протокол LACP.

В случае использования статической агрегации требуется, чтобы физический порт был активен и атрибуты VLAN на агрегированном и физическом порту совпадали. Только после этого физический порт будет включен в логический канал, независимо от того, соответствует ли текущий порт условиям агрегации и соответствует ли им порт, который связан с физическим портом.

Предварительные условия для агрегации портов.

- Порт должен быть в состоянии link-up и работать в полнодуплексном режиме.
- Во время настройки агрегации скорость всех физических портов должна быть одинаковой. То есть, если уже есть один успешно агрегированный физический порт, то скорость второго должна быть такой же. Также атрибуты VLAN всех физических портов должны быть идентичны атрибутам порта агрегации.

LACP предоставляет два метода агрегирования: активный и пассивный. В активном режиме коммутатор активно инициирует процесс согласования агрегации, а в пассивном – пассивно принимает процесс согласования. Если оба порта используют пассивный метод, агрегация не удастся. Это связано с тем, что обе стороны будут ждать, пока другая сторона начнет процесс переговоров по агрегированию.

Атрибуты VALN: PVID, транк, разрешенный диапазон VLAN и диапазон VLAN для пересылки нетегированных фреймов.

Используйте следующую команду для выполнения агрегации физических портов:



| Команда   | Описание  |
|---|---|
| <b>aggregator-group</b> <i>agg-id</i> <b>mode</b> {lscp   static} | Настраивает параметры агрегации для физического порта |

## 10.4 Выбор режима балансировки нагрузки агрегированных портов

Вы можете выбрать метод распределения нагрузки, чтобы все порты могли совместно использовать трафик данных после агрегирования. Коммутатор может обеспечить до шести стратегий балансировки нагрузки:

### ➤ **src-mac**

Совместное использование трафика данных в соответствии с MAC-адресом источника, то есть сообщения с одинаковыми атрибутами MAC-адреса.

### ➤ **dst-mac**

Совместное использование трафика данных в соответствии с MAC-адресом назначения, то есть сообщения с одинаковыми атрибутами MAC-адреса.

### ➤ **both-mac**

Разделение трафика данных в соответствии с MAC-адресами источника и назначения, то есть сообщения с одинаковыми атрибутами MAC-адреса.

### ➤ **src-ip**

Разделение трафика данных в соответствии с исходным IP-адресом, то есть сообщения с одинаковыми атрибутами IP-адреса.

### ➤ **dst-ip**

Разделение трафика данных в соответствии с IP-адресом назначения, то есть сообщения с одинаковыми атрибутами IP-адреса.

### ➤ **both-ip**

Разделение трафика данных в соответствии с IP-адресами назначения и источника, то есть сообщения с одинаковыми атрибутами IP-адреса.

Используйте следующую команду для настройки метода балансировки нагрузки

| Команда                                     | Описание                                 |
|---|--|
| <b>aggregator-group</b> <b>load-balance</b> | Настраивает метод распределения нагрузки |



Команда недоступна на коммутаторе, который не поддерживает методы балансировки нагрузки или поддерживает только один метод. При вводе команды



коммутатор выбирает только поддерживаемые им самим стратегии балансировки нагрузки.

## 10.5 Отслеживание состояния агрегации

Используйте следующую команду для мониторинга состояния агрегации портов в режиме EXEC:

| Команда                                  | Описание                              |
|--|---------------------------------------|
| <b>show aggregator-group</b> <i>[id]</i> | Отображает состояния агрегации портов |

## 11. Настройка GVRP

### 11.1 Введение

GVRP (GARP VLAN Registration Protocol) – это приложение GARP, которое обеспечивает оптимизацию VLAN, совместимую с IEEE 802.1Q, и динамическое создание VLAN на магистральных (trunk) портах 802.1Q. С помощью GVRP коммутатор может обмениваться информацией о конфигурации VLAN с другими GVRP-коммутаторами, отсекал ненужный широковещательный и неизвестный одноадресный трафик, а также динамически создавать и управлять сетями VLAN на коммутаторах, которые подключены через магистральные порты 802.1Q.

Задачи настройки GVRP

- Глобальное включение/отключение GVRP
- Включение/отключение GVRP на интерфейсе
- Мониторинг и обслуживание GVRP

### 11.2 Глобальное включение/отключение GVRP

Выполните следующую настройку в режиме глобальной конфигурации:

| Команда          | Описание                          |
|------------------|-----------------------------------|
| <b>[no] gvrp</b> | Включить/отключить GVRP глобально |

По умолчанию функция отключена.



## 11.3 Включение/отключение GVRP на интерфейсе

Выполните следующую настройку в режиме настройки интерфейса:

| Команда          | Описание                          |
|------------------|-----------------------------------|
| <b>[no] gvrp</b> | Включает/отключает интерфейс GVRP |

Чтобы порт стал активным участником GVRP, сначала необходимо включить GVRP глобально, при этом порт должен быть магистральным портом 802.1Q.

По умолчанию функция включена.

## 11.4 Мониторинг и обслуживание GVRP

Выполните следующие операции в режиме EXEC:

| Команда   | Описание  |
|---|---|
| <b>show gvrp statistics [interface port_list]</b> | Отображает статистику GVRP  |
| <b>show gvrp status</b>                           | Отображает информацию о глобальном состоянии GVRP   |
| <b>[no] debug gvrp [packet   event]</b>           | Включает/отключает отображение отладочной информации о GVRP на устройстве<br><b>packet</b> – включает отладочную информацию о пакетах GVRP, предоставляя подробности о пакетах, передаваемых и получаемых устройством<br><b>event</b> – включает отладочную информацию о событиях GVRP, оповещая о начатых или завершенных действиях сетевого устройства, таких как регистрация или удаление VLAN |

### ➤ Отображение статистики GVRP

```
Switch# show gvrp statistics interface Ethernet0/1
```

```
GVRP statistics on port Ethernet0/1
```

```
GVRP Status: Enabled
```

```
GVRP Failed Registrations: 0
```

```
GVRP Last Pdu Origin: 0000.0000.0000
```

```
GVRP Registration Type: Normal
```



➤ **Отображение информации о глобальном состоянии GVRP**

```
Switch# show gvrp status
```

```
GVRP is enabled!
```

## 11.5 Пример настройки

Подключение к сети происходит следующим образом. Чтобы сделать информацию о конфигурации VLAN коммутатора А и коммутатора В идентичной, вы можете включить GVRP на коммутаторе А и коммутаторе В. Конфигурация выглядит следующим образом:

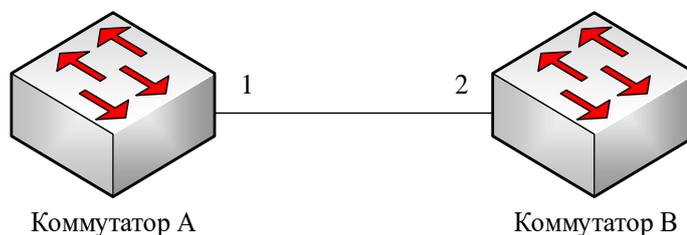


Рисунок 16 – Коммутаторы GVRP

1) Настройте порт 1, через который коммутатор А подключается к коммутатору В в качестве транкового:

```
Switch_config_g0/1# switchport mode trunk
```

2) Включите глобальный GVRP коммутатора А:

```
Switch_config# gvrp
```

3) Включите GVRP интерфейса 1 коммутатора А:

```
Switch_config_g0/1# gvrp
```

4) Настройте VLAN 10, VLAN 20 и VLAN30 на коммутаторе А:

```
Switch_config# vlan 10
```

```
Switch_config# vlan 20
```

```
Switch_config# vlan 30
```

5) Настройте порт 2, через который коммутатор В подключается к коммутатору А в качестве транкового:

```
Switch_config_g0/2# switchport mode trunk
```

6) Включите глобальный GVRP коммутатора В:

```
Switch_config# gvrp
```

7) Включите GVRP интерфейса 2 коммутатора В:



```
Switch_config_g0/2# gvrp
```

8) Настройте VLAN 40, VLAN 50 and VLAN 60 на коммутаторе B:

```
Switch_config# vlan 40
```

```
Switch_config# vlan 50
```

```
Switch_config# vlan 60
```

После завершения настройки информация о конфигурации VLAN будет отображаться соответственно на коммутаторе A и коммутаторе B, то есть VLAN 10, VLAN 20, VLAN 30, VLAN 40, VLAN 50 и VLAN 60 на обоих коммутаторах.

## 12. IGMP Snooping

### 12.1 Введение

Задача IGMP Snooping – поддерживать связи между VLAN и групповым адресом и обновлять их одновременно с изменениями многоадресной рассылки, позволяя коммутаторам второго уровня пересылать данные в соответствии со структурой топологии многоадресной группы.

Основные функции IGMP Snooping следующие:

- прослушивание сообщений IGMP;
- ведение таблицы соответствия между VLAN и групповыми адресами;
- синхронизация состояния между IGMP-сущностями хоста и маршрутизатора для предотвращения избыточного широковещательного трафика.



IGMP Snooping выполняет вышеуказанные функции, прослушивая запросы и отчетные сообщения, отправляемые по протоколу IGMP. Этот механизм может функционировать корректно только при условии, что он подключен к мультикастовому маршрутизатору. Другими словами, коммутатор должен периодически получать IGMP-запросы от маршрутизатора. Для правильной работы IGMP Snooping необходимо установить таймер истечения срока действия данных маршрутизатора (router age timer) на значение, большее, чем период отправки групповых запросов маршрутизатором, с которым связан IGMP Snooping. Вы можете проверить информацию о многоадресном маршрутизаторе в каждой VLAN, запустив команду **show ip IGMP Snooping**.

Задачи настройки

- Включение/отключение IGMP Snooping для VLAN
- Добавление/удаление статического мультикастового адреса VLAN
- Настройка немедленного выхода VLAN из группы



- Настройка фильтрации многоадресных сообщений без зарегистрированного адреса назначения
- Настройка таймера Router Age
- Настройка таймера Response Time
- Настройка генератора IGMP-запросов
- Мониторинг и поддержка IGMP Snooping
- Пример настройки IGMP Snooping

## 12.2 Включение/отключение IGMP Snooping для VLAN

Выполните следующие команды в режиме глобальной конфигурации:

| Команда                                   | Описание                               |
|---|--|
| <b>ip igmp-snooping [vlan vlan_id]</b>    | Включает IGMP Snooping для VLAN        |
| <b>no ip igmp-snooping [vlan vlan_id]</b> | Восстанавливает настройки по умолчанию |

Если VLAN не указана, все виртуальные сети в системе, включая созданные позже, можно включить или отключить.

В конфигурации по умолчанию включено отслеживание IGMP всех VLAN, также, как это делается при помощи команды **ip igmp-snooping**.



IGMP-Snooping может работать в 16 VLAN.

Чтобы включить IGMP Snooping, например, только в VLAN 3, необходимо сначала отключить эту функцию для всех VLAN при помощи команды **no ip igmp-snooping**, а затем запустить команду **ip igmp-snooping vlan 3** и сохранить конфигурацию.

## 12.3 Добавление/удаление статического мультикастового адреса VLAN

Хосты, не поддерживающие IGMP, могут получать соответствующие сообщения многоадресной рассылки, используя статический мультикастовый адрес. Выполните следующие команды в режиме глобальной конфигурации:



| Команда   | Описание  |
|---|---|
| <b>ip igmp-snooping vlan <i>vlan_id</i> static A.B.C.D interface <i>intf</i></b>    | Добавляет статический мультикастовый адрес VLAN |
| <b>no ip igmp-snooping vlan <i>vlan_id</i> static A.B.C.D interface <i>intf</i></b> | Удаляет статический мультикастовый адрес VLAN   |

## 12.4 Настройка немедленного выхода VLAN из группы

Если настроена функция немедленного выхода, коммутатор может удалить VLAN ID из списка VLAN многоадресной группы после того, как получит leave-сообщение. Таким образом, коммутатору не требуется включать таймер для ожидания подключения других хостов к многоадресной рассылке. Если другие хосты в той же VLAN принадлежат к той же группе и их пользователи не хотят покинуть группу, это может повлиять на многоадресную связь этих пользователей. В таком случае функцию немедленного выхода включать не следует. Выполните следующие команды в режиме глобальной конфигурации:

| Команда  | Описание   |
|--|--|
| <b>ip igmp-snooping vlan <i>vlan_id</i> immediate-leave</b>    | Настраивает функцию немедленного выхода VLAN из группы                             |
| <b>no ip igmp-snooping vlan <i>vlan_id</i> immediate-leave</b> | Устанавливает значение по умолчанию для функции немедленного выхода VLAN из группы |

По умолчанию данная функция отключена.

## 12.5 Настройка фильтрации многоадресных сообщений без зарегистрированного адреса назначения

Если цель многоадресного сообщения не найдена (DLF – адрес назначения не зарегистрирован в микросхеме коммутатора посредством IGMP Snooping), методом обработки по умолчанию является отправка сообщения на все порты VLAN. Путем настройки вы можете изменить метод обработки, и все многоадресные сообщения, адреса назначения которых не зарегистрированы ни на одном порту, будут удалены.



| Команда                             | Описание   |
|-------------------------------------|--|
| <b>ip igmp-snooping dlf-drop</b>    | Отбрасывает многоадресное сообщение, пункт назначения которого не найден |
| <b>no ip igmp-snooping dlf-drop</b> | Возобновляет конфигурацию по умолчанию (многоадресную рассылку)          |



- Атрибут настраивается для всех VLAN.
- Для коммутатора методом обработки сообщений этого типа по умолчанию является пересылка (сообщение этого типа будет транслироваться внутри VLAN).

## 12.6 Настройка таймера Router Age

Таймер срока действия данных маршрутизатора используется для отслеживания существования в сети IGMP-запросчика. Запрашивающие устройства IGMP поддерживают адреса многоадресной рассылки, отправляя сообщение запроса. Отслеживание работает посредством связи между IGMP-запросчиком и хостом.

Выполните следующие команды в режиме глобальной конфигурации:

| Команда   | Описание                              |
|---|---------------------------------------|
| <b>ip igmp-snooping timer router-age <i>timer_value</i></b> | Настраивает значение таймера          |
| <b>no ip igmp-snooping timer router-age</b>                 | Восстанавливает значение по умолчанию |



Корректная установка значения зависит от настройки IGMP-запросчика и его таймера запросов (*querier-timer*). Таймер Router Age не может быть установлен на время, меньшее, чем время периода запроса. Рекомендуется установить значение таймера на время, в три раза превышающее период запроса.

Значение по умолчанию для таймера Router Age – 260 секунд.



## 12.7 Настройка таймера Response Time

Таймер времени ответа – это верхний предел времени, в течение которого хост отправляет отчет после того, как IGMP-запросчик отправит свое сообщение. Если сообщение отчета не получено по истечении времени таймера, коммутатор удалит этот мультикастовый адрес.

Выполните следующие команды в режиме глобальной конфигурации:

| Команда   | Описание  |
|---|---|
| <b>ip igmp-snooping timer response-time</b><br><i>timer_value</i> | Настраивает значение времени ответа IGMP-Snooping                 |
| <b>no ip igmp-snooping timer response-time</b>                    | Возвращает значение по умолчанию для времени ответа IGMP-Snooping |



Значение таймера не может быть слишком маленьким. В противном случае многоадресная связь будет нестабильной.

По умолчанию значение Response Time IGMP Snooping составляет 10 секунд.

## 12.8 Настройка генератора запросов IGMP Snooping

Если в VLAN, где активировано отслеживание IGMP, не существует маршрутизатора многоадресной рассылки, можно использовать функцию запросчика IGMP Snooping, чтобы имитировать маршрутизатор с его регулярной отправкой IGMP-запросов. Функция является глобальной, то есть ее можно включить или отключить в VLAN, где глобально включено отслеживание IGMP.

Если маршрутизатора многоадресной рассылки не существует в VLAN, и поток многоадресной рассылки не требует маршрутизации, функция автоматического запроса на коммутаторе может быть активирована посредством IGMP Snooping, что обеспечит корректную работу отслеживания.

Выполните следующую команду в режиме глобальной конфигурации:

| Команда   | Описание  |
|---|---|
| <b>[no] ip igmp-snooping querier</b><br><b>[address [ip_addr]</b> | Настраивает генератор запросов IGMP-Snooping. Необязательный параметр <b>address</b> – это IP-адрес источника сообщений запроса |

Изначально функция **ip igmp-snooping querier** выключена. Исходный IP-адрес фиктивного сообщения IGMP-запроса по умолчанию – 10.0.0.200.



Если функция запроса включена, она отключается, когда в VLAN появляется многоадресный маршрутизатор; функция может автоматически активироваться по истечении времени ожидания многоадресного маршрутизатора.

## 12.9 Мониторинг и поддержка IGMP Snooping

В режиме управления выполните следующие операции:

| Команда   | Описание  |
|---|---|
| <b>show ip igmp-snooping</b>  | Отображает информацию о конфигурации IGMP Snooping  |
| <b>show ip igmp-snooping timers</b>                                 | Отображает информацию о временных параметрах IGMP Snooping  |
| <b>show ip igmp-snooping groups</b>                                 | Отображает информацию о группах многоадресной рассылки, контролируемых при помощи IGMP Snooping   |
| <b>show ip igmp-snooping statistics</b>                             | Отображает статистическую информацию IGMP Snooping  |
| <b>[no] debug ip igmp-snooping [packet   timer   event   error]</b> | Включает и отключает отладочные сообщения, связанные с протоколом IGMP Snooping. С помощью указания параметров можно выбирать, какие конкретные аспекты необходимо отслеживать с помощью отладочных сообщений. Команда <b>[no] debug ip igmp-snooping</b> позволяет включать или выключать отладочный режим для этих аспектов протокола в зависимости от потребности пользователя |

### ➤ Отображение информации VLAN о работе IGMP Snooping:

```
switch# show ip igmp-snooping
igmp-snooping response time: 10 s
vlan 1
```



-----

running

Router: 90.0.0.120(F0/2)

➤ **Отображение информации о группах многоадресной рассылки:**

switch# show ip igmp-snooping groups

| Vlan Source | Group | Type | Port(s) |
|-------------|-------|------|---------|
|-------------|-------|------|---------|

-----

|           |           |      |      |
|-----------|-----------|------|------|
| 1 0.0.0.0 | 234.5.6.6 | IGMP | F0/2 |
|-----------|-----------|------|------|

|           |                 |      |      |
|-----------|-----------------|------|------|
| 1 0.0.0.0 | 239.255.255.250 | IGMP | F0/2 |
|-----------|-----------------|------|------|

➤ **Отображение информации о таймерах IGMP Snooping:**

switch# show ip igmp-snooping timers

vlan 1 router age: 251

# Указывает значение таймера Router Age.

vlan 1 multicast address 0100.5e00.0809 response time: 1

# Указывает период с момента получения последнего группового запроса до текущего времени; если ни один хост на порту не ответит по истечении времени таймера, порт будет удален.

➤ **Отображение статистики IGMP Snooping:**

switch# show ip igmp-snooping statistics

vlan 1

-----

v1\_packets: 0

#Количество пакетов IGMP v1

v2\_packets: 6

# Количество пакетов IGMP v2

v3\_packets: 0

# Количество пакетов IGMP v3

general\_query\_packets: 5

# Количество общих запросов

special\_query\_packets: 0

# Количество специальных запросов



```
join_packets: 6
# Количество отчетных сообщений
leave_packets: 0
# Количество сообщений о выходе из группы
send_query_packets: 0
# Резервированные опции статистики
err_packets: 0
# Количество пакетов с ошибками
```

➤ **Отладочная информация IGMP Snooping:**

```
switch# debug ip igmp-snooping packet
rx: s_ip:90.0.0.3, d_ip:224.0.8.9
# Адреса источника и назначения
    type:16(V2-Report), max resp:00, group address:224.0.8.9
    # Тип и содержание пакета
rx: s_ip:90.0.0.90, d_ip:224.0.0.1
    type:11(Query), max resp:64, group address:0.0.0.0
rx: s_ip:90.0.0.3, d_ip:224.0.8.9
    type:16(V2-Report), max resp:00, group address:224.0.8.9
rx: s_ip:90.0.0.3, d_ip:224.0.0.2
    type:17(V2-Leave), max resp:00, group address:224.0.8.9
rx: s_ip:90.0.0.90, d_ip:224.0.8.9
    type:11(Query), max resp:0a, group address:224.0.8.9
```

➤ **Отладочная информация о таймерах IGMP Snooping:**

```
switch# debug ip igmp-snooping timer
tm: vlan 1 igmp router age expiry at port 2(F0/2)
tm: multicast item 0.0.0.0->224.0.8.9(0100.5e00.0809) response time expiry at port F0/4
```



## 12.10 Пример настройки IGMP Snooping

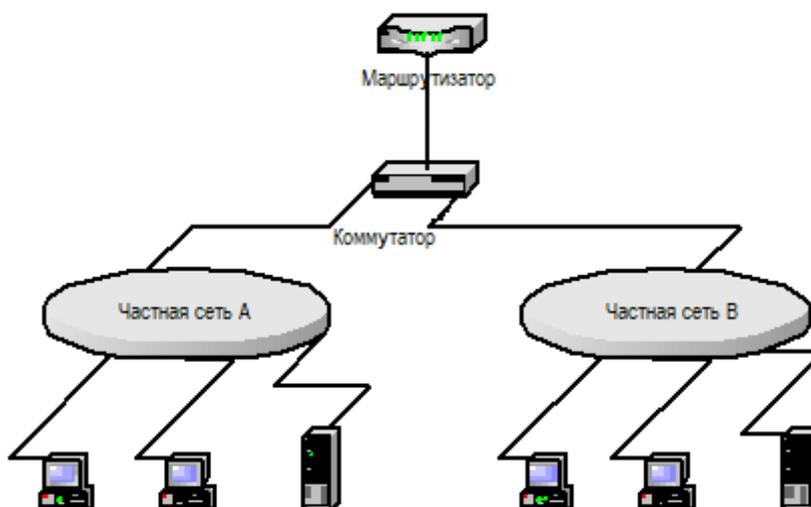


Рисунок 17 – Топология сети

Настройка коммутатора

1. Включите IGMP Snooping для VLAN 1, соединяющей частную сеть А.  
Switch\_config# ip igmp-snooping vlan 1
2. Включите IGMP Snooping для VLAN 2, соединяющей частную сеть В.  
Switch\_config# ip igmp-snooping vlan 2

## 13. Настройка 802.1x.

Задачи настройки

- Настройка аутентификации 802.1x на основе портов
- Настройка многопортовой аутентификации 802.1x
- Настройка максимального количества запросов аутентификации ID 802.1x
- Настройка повторной аутентификации 802.1x
- Настройка частоты передачи сообщений 802.1x
- Настройка привязки пользователя 802.1x
- Настройка метода аутентификации 802.1x для порта
- Выбор типа аутентификации 802.1x для порта
- Настройка учета 802.1x
- Настройка гостевой VLAN 802.1x



- Запрет использования нескольких сетевых карт
- Восстановление настроек 802.1x по умолчанию
- Мониторинг конфигурации и состояния аутентификации 802.1x

## 13.1 Настройка аутентификации 802.1x на основе портов

802.1x определяет три метода управления портом: обязательное одобрение аутентификации, обязательное отклонение аутентификации и запуск аутентификации 802.1x.

Обязательное одобрение означает, что порт уже прошел аутентификацию. Она больше не требуется порту, и через него все пользователи могут осуществлять доступ. Метод аутентификации определяется портом по умолчанию. Обязательное отклонение означает, что аутентификация порта не проходит независимо от того, какой метод применяется. Ни один пользователь не может осуществлять доступ к данным через такой порт.

Запуск аутентификации 802.1x означает, что порт должен использовать данный протокол аутентификации и будет применяться его к пользователям, имеющим доступ к порту. Прошедшие аутентификацию пользователи получают доступ к данным через порт. Для этого режима необходимо настроить метод аутентификации AAA.

Перед настройкой 802.1x выполните следующую команду, чтобы включить протокол:

| Команда             | Описание                 |
|---------------------|--------------------------|
| <b>dot1x enable</b> | Включение функции 802.1x |

Выполните следующую команду, чтобы запустить аутентификацию 802.1x:

| Команда  | Описание   |
|--|--|
| <b>dot1x port-control auto</b>   | Настройка на порту метода управления протоколом 802.1x |
| <b>aaa authentication dot1x {default   list name} method1 [method2...]</b> | Настройка аутентификации AAA 802.1x                    |

Запустите одну из следующих команд в режиме настройки порта, чтобы выбрать метод управления 802.1x:

| Команда                        | Описание                                      |
|--------------------------------|---|
| <b>dot1x port-control auto</b> | Включает метод аутентификации 802.1x на порту |



|  |   |
|--|---|
| <b>dot1x port-control force-authorized</b>   | Утверждает обязательную аутентификацию на порту |
| <b>dot1x port-control force-unauthorized</b> | Отклоняет обязательную аутентификацию на порту  |

## 13.2 Настройка мульти-аутентификации 802.1x

Протокол 802.1x предназначен для аутентификации пользователя с одного хоста. В этом случае коммутатор позволяет только одному пользователю пройти аутентификацию и получить контроль доступа. Другие пользователи не могут пройти аутентификацию и получить доступ, пока предыдущий не завершит сеанс. Если порт соединяет несколько хостов через коммутационные устройства, которые не поддерживают 802.1x, вы можете запустить функцию доступа множества портов, чтобы обеспечить доступ пользователям с разных хостов.

После настройки порта на аутентификацию множества хостов коммутатор начнет аутентифицировать различных пользователей. В результате подтверждения аутентификации хосту будет разрешен доступ через коммутатор (для управления используется MAC-адрес хоста). Теоретически 802.1x не может ограничивать количество пользователей. Поскольку коммутатор управляет аутентификацией пользователя через его MAC-адрес, количество пользователей будет ограничено размером таблицы MAC-адресов коммутатора.

Запустите следующие команды в режиме настройки интерфейса, чтобы активировать мульти-аутентификацию 802.1x:

| Команда                                    | Описание   |
|--|--|
| <b>dot1x authentication multiple-hosts</b> | Включение режима аутентификации множества хостов |

## 13.3 Настройка максимального количества запросов аутентификации ID 802.1x

Когда протокол 802.1x запускается впервые или выполняется повторно, он отправляет запрос аутентификации ID гостевым хостам. Если сообщение с запросом отбрасывается или задерживается из-за проблем с сетью, оно будет отправлено снова. Если сообщение отправляется повторно определенное количество раз, 802.1x прекращает его отправку, и аутентификация ID завершается неудачей.



Вы можете настроить максимальное количество запросов аутентификации ID в соответствии с конкретными сетевыми условиями, гарантируя, что клиенты будут успешно аутентифицированы сервером.

Запустите следующую команду в режиме настройки интерфейса, чтобы задать максимальное количество запросов аутентификации ID:

| Команда                    | Описание  |
|----------------------------|---|
| <b>dot1x max-req count</b> | Настройка максимального количества запросов аутентификации ID |

## 13.4 Настройка повторной аутентификации 802.1x

В целях безопасности рекомендуется периодически повторять процедуру проверки подлинности успешно вошедшего пользователя.

В этом случае необходимо включить функцию повторной аутентификации. После запуска данной функции запрос аутентификации будет периодически отправляться на хост.

Выполните следующие команды, чтобы настроить функцию повторной аутентификации:

| Команда                                 | Описание  |
|---|---|
| <b>dot1x re-authentication</b>          | Включает функцию повторной аутентификации   |
| <b>dot1x timeout re-authperiod time</b> | Настраивает временной интервал повторной аутентификации                                   |
| <b>dot1x reauth-max count</b>           | Устанавливает количество дополнительных попыток в случае неудачи повторной аутентификации |

## 13.5 Настройка частоты передачи сообщений 802.1x

Во время процесса аутентификации между хостом (клиентом или соискателем) и сервером аутентификации происходит обмен текстовыми сообщениями EAP (расширяемый протокол аутентификации). Изменяя частоту передачи, можно управлять ответом хоста, что помогает избежать тайм-аутов, разрывов соединений и других проблем, которые могут возникнуть из-за неподходящих временных диапазонов обмена сообщениями.

Для настройки частоты передачи запустите следующую команду:



| Команда                             | Описание                                    |
|-------------------------------------|---|
| <b>dot1x timeout tx-period time</b> | Установка частоты передачи сообщений 802.1x |

## 13.6 Настройка привязки пользователя 802.1x

При выполнении аутентификации 802.1x вы можете привязать пользователя к определенному порту, чтобы обеспечить безопасность доступа. Выполните следующую команду в режиме настройки интерфейса, чтобы запустить привязку пользователя 802.1x:

| Команда                       | Описание                      |
|-------------------------------|-------------------------------|
| <b>dot1x user-permit xxxz</b> | Привязка пользователя к порту |

## 13.7 Настройка метода аутентификации 802.1x для порта

Аутентификация 802.1x может выполняться разными методами на разных портах. В конфигурации по умолчанию аутентификация 802.1x использует метод **default**.

Запустите следующую команду в режиме настройки интерфейса, чтобы указать метод аутентификации 802.1x:

| Команда                                | Описание                               |
|--|--|
| <b>dot1x authentication method ууу</b> | Настройка метода аутентификации 802.1x |

## 13.8 Выбор типа аутентификации 802.1x для порта

Вы можете выбрать тип аутентификации 802.1x. Тип определяет, использует ли AAA аутентификацию CHAP или EAP. Аутентификация EAP поддерживает режим MD5-challenge и режим EAP-TLS. Когда используется аутентификация CHAP, вызов (challenge), необходимый для проверки пользователя согласно MD5, генерируется локально. В случае применения аутентификации EAP вызов генерируется на сервере аутентификации. Каждый порт принимает только один тип аутентификации. Тип аутентификации глобальной конфигурации принимается по умолчанию. После того, как для порта установлен свой тип аутентификации в режиме настройки интерфейса, порт будет использовать его, если вы не запустите команду **no**, чтобы восстановить значение по умолчанию.

EAP-TLS использует электронный сертификат в качестве гарантии аутентификации и соответствует правилам установления связи в Translation Layer Security (TLS). Таким образом гарантируется высокая безопасность.



Запустите следующую команду в режиме глобальной конфигурации, чтобы назначить тип аутентификации:

| Команда                               | Описание           |
|---------------------------------------|--------------------|
| <b>dot1x authen-type {chap   eap}</b> | Выбор CHAP или EAP |

Также выполните следующую команду в режиме настройки интерфейса:

| Команда                                       | Описание   |
|---|--|
| <b>dot1x authentication type {chap   eap}</b> | Выбрать для порта CHAP, EAP или тип, настроенный в глобальной конфигурации |

## 13.9 Настройка учета 802.1x

Аутентификация и учет 802.1x могут выполняться одновременно. Механизм работы следующий: после подтверждения аутентификации dot1x определите, включена ли функция учета на интерфейсе аутентификации; если функция учета включена, отправьте запрос на учет через интерфейс AAA; когда модуль AAA возвращает сообщение об успешном ответе на запрос, интерфейс AAA сможет пересылать тексты.

После начала учёта данных, dot1x периодически отправляет сообщения обновления на сервер через интерфейс AAA для получения правильной информации об учёте. В зависимости от конфигурации AAA, AAA-модуль определяет, стоит ли отправлять это обновляющее сообщение.

В то же время вам необходимо включить функцию повторной аутентификации dot1x, чтобы коммутатор мог определить, когда клиент работает некорректно.

Выполните следующие команды в режиме настройки интерфейса, чтобы включить учет dot1x и настроить метод учета:

| Команда                                      | Описание   |
|--|--|
| <b>dot1x accounting enable</b>               | Включение функции учета dot1x                                  |
| <b>dot1x accounting method {method name}</b> | Настройка метода учёта. Значение по умолчанию – <b>default</b> |

## 13.10 Настройка гостевой VLAN 802.1x

Гостевая VLAN предоставляет соответствующим портам некоторые права доступа (например, загрузку клиентского программного обеспечения), когда клиент не отвечает. Гостевой может быть любая настроенная виртуальная сеть в системе. Если настроенная гостевая VLAN не соответствует необходимым условиям, порты не смогут в ней работать.



В случае неудачной аутентификации право доступа к гостевой VLAN отсутствует.

Запустите следующую команду в режиме глобальной конфигурации, чтобы разрешить гостевую виртуальную сеть:

| Команда                 | Описание                               |
|-------------------------|--|
| <b>dot1x guest-vlan</b> | Включение гостевой VLAN на всех портах |

Если для каждого порта изначально не настроен идентификатор гостевой VLAN (ID=0), она не сможет работать, даже если функция включена в глобальном режиме. Для успешной работы гостевой VLAN требуется прямо указать ее идентификатор в режиме настройки интерфейса. Для этого запустите следующую команду:

| Команда                    | Описание   |
|----------------------------|--|
| <b>dot1x guest-vlan id</b> | Указать ID гостевой VLAN. Допустимый диапазон 1 – 4094 |

## 13.11 Запрет клиенту использования нескольких сетевых карт

Запретите соискателю использование нескольких сетевых адаптеров, чтобы предотвратить работу агентов. Запустите следующую команду в режиме настройки порта:

| Команда                                   | Описание   |
|---|--|
| <b>dot1x forbid multi-network-adapter</b> | Запретить соискателю использование нескольких сетевых карт |

## 13.12 Восстановление настроек 802.1x по умолчанию

Выполните следующую команду, чтобы восстановить всю глобальную конфигурацию до значений по умолчанию:

| Команда              | Описание                                    |
|----------------------|---|
| <b>dot1x default</b> | Восстановление настроек 802.1x по умолчанию |



## 13.13 Мониторинг конфигурации и состояния аутентификации 802.1x

Чтобы отслеживать конфигурацию и состояние аутентификации 802.1x и решить, какой параметр 802.1x необходимо настроить, выполните следующую команду в режиме управления:

| Команда                                   | Описание   |
|---|--|
| <b>show dot1x</b> { <i>interface...</i> } | Показать настройки и состояние аутентификации 802.1x |

## 13.14 Пример настройки

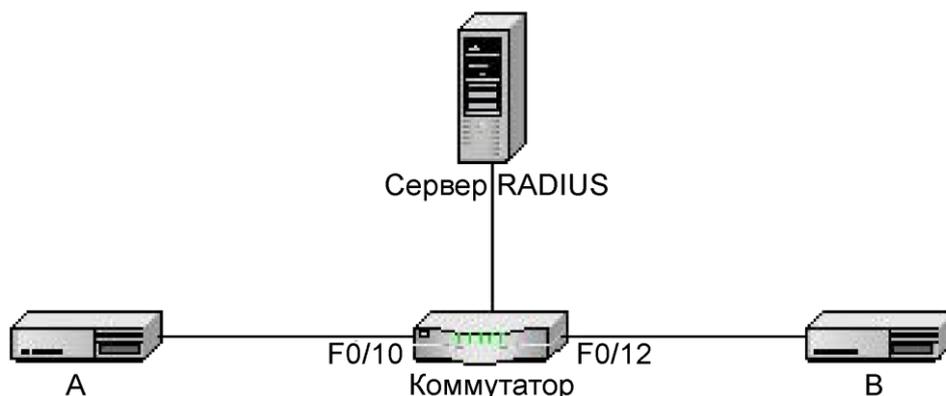


Рисунок 18 – Схема аутентификации 802.1x

Хост А подключается к порту F0/10 коммутатора. Хост В подключается к порту F0/12. IP-адрес RADIUS-сервера – 192.168.20.2. Ключ RADIUS – TST. Порт F0/10 поддерживает удаленную аутентификацию RADIUS, привязку пользователя и повторную аутентификацию. Порт F0/12 поддерживает локальную аутентификацию типа EAP, мульти-аутентификацию и гостевую VLAN.

### ➤ Общая настройка

```
username switch password 0 TST
username TST password 0 TST
aaa authentication dot1x TST-F0/10 radius
aaa authentication dot1x TST-F0/12 local
interface VLAN1
ip address 192.168.20.24 255.255.255.0
```



```
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813
```

```
radius-server key TST
```

### ➤ Настройка порта F0/10

```
interface FastEthernet0/10
```

```
dot1x port-control auto
```

```
dot1x authentication method TST-F0/10
```

```
dot1x user-permit radius-TST
```

### ➤ Настройка порта F0/12

```
interface FastEthernet0/12
```

```
dot1x multiple-hosts
```

```
dot1x port-control auto
```

```
dot1x authentication method TST-F0/12
```

```
dot1x authentication type eap
```

## 14. Настройка MAC ACL

### 14.1 Создание списка управления доступом

Прежде чем применять к порту список управления доступом на основе MAC-адресов (MAC ACL), его необходимо создать. После создания этого списка, вы входите в специальный режим конфигурации, в котором можно настроить каждый элемент списка.

Войдите в привилегированный режим и выполните следующие действия, чтобы добавить или удалить список доступа основе MAC-адресов:

| Команда                          | Описание   |
|----------------------------------|--|
| <b>config</b>                    | Вход в режим глобальной конфигурации                               |
| <b>[no] mac access-list name</b> | Добавление или удаление MAC ACL<br><b>name</b> означает имя списка |

### 14.2 Настройка элементов списка

Вы можете использовать команду **permit** или **deny** для настройки разрешающих и запрещающих элементов списка MAC-адресов. В списке могут быть настроены несколько разрешающих или запрещающих элементов. Маска настроенных элементов должна быть



одинаковой. В противном случае конфигурация может оказаться нерабочей (см. следующий пример). Один и тот же элемент может быть настроен для одного MAC-адреса только один раз.

Войдите в режим настройки MAC ACL и выполните следующие операции, чтобы настроить элементы списка:

| Команда   | Описание   |
|---|--|
| <code>[no] {deny   permit} {any   host src-mac-addr} {any   host dst-mac-addr} [ethertype]</code> | Добавить/удалить элемент списка. Вы можете повторно запустить команду, чтобы добавить или удалить несколько элементов<br><b>any</b> означает, что любой MAC-адрес может быть совместим<br><b>src-mac-addr</b> означает исходный MAC-адрес<br><b>dst-mac-addr</b> означает целевой MAC-адрес<br><b>ethertype</b> означает тип сопоставленного пакета Ethernet |
| <code>exit</code>   | Выйти из режима настройки MAC ACL и вернуться в режим глобальной конфигурации  |
| <code>exit</code>   | Вернуться в режим управления   |
| <code>write</code>  | Сохранить настройки  |

### ➤ Пример настройки MAC ACL

```
Switch_config# mac acce 1
```

```
Switch-config-macl# permit host 1.1.1 any
```

```
Switch-config-macl# permit host 2.2.2 any
```

# Вышеуказанная конфигурация предназначена для сравнения исходного MAC-адреса, маска та же. Настройка выполнена успешно.

```
Switch_config# mac acce 1
```

```
Switch-config-macl# permit host 1.1.1 any
```

```
Switch-config-macl# permit any host 1.1.2
```

```
Switch-config-macl# 2024-11-19 18:54:25 rule conflict, all the rule in the acl should match!
```

Первая строка в приведенной выше конфигурации предназначена для сравнения исходных MAC-адресов, а вторая – для сравнения целевых. Следовательно, маска отличается. Настройка не выполняется.



## 14.3 Применение списка

Созданный MAC ACL можно применить к любому физическому порту. К порту можно применить только один список. Один и тот же список можно применить к нескольким портам. Войдите в привилегированный режим и выполните следующие команды:

| Команда                           | Описание   |
|-----------------------------------|--|
| <b>config</b>                     | Вход в режим глобальной конфигурации                                       |
| <b>interface f0/1</b>             | Вход в режим настройки выбранного интерфейса                               |
| <b>[no] mac access-group name</b> | Применить/отменить MAC ACL для текущего порта<br><b>name</b> – имя MAC ACL |
| <b>exit</b>                       | Вернуться в режим глобальной конфигурации                                  |
| <b>exit</b>                       | Вернуться в режим управления   |
| <b>write</b>                      | Сохранить настройки  |

## 15. Настройка IP ACL

### 15.1 Фильтрация IP-пакетов

Фильтрация сообщений помогает управлять движением пакетов в сети, позволяя ограничивать передачу данных и использование сети определенными пользователями или устройствами. Для определения, допустимы ли или нет сетевые пакеты через определенный интерфейс, данный маршрутизирующий коммутатор предоставляет функцию списка контроля доступа (ACL). Этот список можно использовать для таких целей, как:

- контроль передачи пакетов через интерфейс;
- контроль доступа к виртуальным терминалам;
- ограничение обновлений маршрута.

Данный раздел описывает, как создавать списки IP-доступа и как их использовать для управления потоком данных в сети.

Список контроля IP-доступа – это упорядоченный набор условий разрешения или запрета для определенных IP-адресов. Программное обеспечение данного коммутатора проверяет адреса по одному в соответствии с правилами, заданными в списке доступа. Первое совпадение определяет, принимается ли адрес или отклоняется. После первого совпадения программное обеспечение завершает проверку по заданным правилам. Порядок условий имеет важное значение. Если ни одно правило не совпадает, адрес отклоняется. Для использования списка доступа необходимо вначале его создать, указав его имя и условия, а затем применить к выбранному интерфейсу.



## 15.2 Создание стандартного и расширяемого IP ACL

Используйте строку символов для создания списка управления IP-доступом.



Стандартный и расширяемый список доступа не могут иметь одинаковые имена.

Запустите следующую команду в режиме глобальной конфигурации, чтобы создать стандартный IP ACL:

| Команда  | Описание   |
|--|--|
| <b>ip access-list standard</b> <i>name</i>   | Создает стандартный список доступа<br><b>name</b> означает имя списка  |
| <b>deny</b> <i>source</i> [ <i>source-mask</i> ]   <b>any</b><br>или:<br><b>permit</b> <i>source</i> [ <i>source-mask</i> ]   <b>any</b> | Указывает одно или несколько условий разрешения/запрета в режиме настройки стандартного списка доступа. Параметр <b>permit</b> или <b>deny</b> определяет, будет ли пакет одобрен или отклонен |
| <b>Exit</b>  | Выход из режима настройки списка доступа   |

Запустите следующую команду в режиме глобальной конфигурации, чтобы создать расширяемый список доступа:

| Команда   | Описание  |
|---|---|
| <b>ip access-list extended</b> <i>name</i>  | Создает расширяемый список доступа<br><b>name</b> означает имя списка   |
| { <b>deny</b>   <b>permit</b> } <i>protocol source source-mask destination destination-mask</i> [ <b>precedence precedence</b> ] [ <b>tos tos</b> ] { <b>deny</b>   <b>permit</b> } <i>protocol any any</i> | Обозначает одно или несколько условий разрешения/запрета в режиме настройки расширяемого списка доступа. Параметр <b>permit</b> или <b>deny</b> определяет, будет ли пакет одобрен или отклонен<br><br><b>precedence</b> означает приоритет IP-пакета<br><b>tos</b> означает тип услуги.<br>Если список настраивается для физического порта, и используется протокол TCP или UDP, то нужно выбрать один или несколько портов из определенного диапазона (см. раздел «Примеры применения расширяемого списка доступа») |



|      |  |
|------|--|
| Exit | Выход из режима настройки списка доступа |
|------|--|

После первоначального создания IP ACL любую часть, добавленную позже, можно поместить в конец списка. То есть вы не можете изменить существующую команду, однако можно использовать команды **no permit** и **no deny** для удаления элементов из списка.



При создании списка доступа в конце его автоматически добавляется неявное правило «запретить все». Если при создании списка не указана маска для IP-адреса хоста, то по умолчанию используется маска 255.255.255.255.

После создания списка доступа, его необходимо применить к маршруту или интерфейсу, чтобы он начал работать и влиять на трафик в сети.

## 15.3 Применение IP ACL

После создания списка доступа можно применить его к одному или нескольким интерфейсам.

Запустите следующую команду в режиме настройки интерфейса:

| Команда                                       | Описание                              |
|---|---------------------------------------|
| <b>ip access-group</b> <i>name</i> {in   out} | Применяет список доступа к интерфейсу |

Список управления доступом можно использовать на входном или выходном интерфейсе. После получения пакета адрес его источника будет проверен в соответствии со стандартным списком, примененным к выходному интерфейсу. Для расширяемого списка маршрутизирующий коммутатор также проверяет адрес назначения. Если список разрешает адрес назначения, система продолжит обработку пакета, если запрещает – система отбросит пакет, а затем вернет ICMP-сообщение о недоступности хоста.

Если указанный список управления доступом не существует, прохождение всех пакетов разрешено.

## 15.4 Примеры применения расширяемого списка доступа

➤ Применение к физическому интерфейсу с поддержкой TCP/UDP

Формат настройки следующий:

**{deny | permit}** {tcp | udp}

*source source-mask* [{src\_portrange begin-port end-port} | [{gt | lt} port ]]

*destination destination-mask* [{dst\_portrange begin-port end-port} | [{gt | lt} port]]

[**precedence precedence**] [**tos tos**]



Настраивая список доступа с использованием диапазона портов необходимо учитывать требования этого метода к ресурсам системы:

1) Если вы настраиваете ACL, указывая диапазон портов как на стороне отправителя, так и на стороне получателя, это может потребовать больших ресурсов и привести к неудачной конфигурации. В таком случае рекомендуется указать диапазон портов на одной стороне и конкретный порт на другой стороне.

2) Фильтрация по диапазону портов может потребовать значительных ресурсов, и, если ее использовать слишком часто, это может привести к ухудшению производительности других программ, которые используют ACL.

➤ В следующем примере первая строка позволяет любому новому TCP подключиться к порту SMTP хоста 130.2.1.2:

```
ip access-list extended aaa
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface g0/1
ip access-group aaa
```

## 16. QoS

### 16.1 Основные понятия

В обычных условиях коммутатор функционирует в режиме «максимального усилия» (best-effort), при котором он обрабатывает разные потоки данных одинаково и старается доставить все потоки. Поэтому, если возникает перегрузка, все потоки имеют одинаковый шанс быть отброшенными. Однако в реальных сетях разные потоки имеют различное значение, и функция качества обслуживания (QoS) коммутатора может обеспечивать различные услуги разным потокам в зависимости от их значимости. Важные потоки получают более высокий уровень обслуживания.

Для классификации важности сетевых потоков существуют два основных способа:

- В заголовке кадра 802.1Q есть два байта, и 3 бита используются для обозначения приоритета пакета. Существует 8 уровней приоритета, где 0 означает самый низкий приоритет, а 7 – самый высокий.
- Поле DSCP (Differentiated Services Code Point) в заголовке IP-пакета использует нижние 6 битов в области TOS (Type of Service) заголовка IP.

В реальных сетевых приложениях граничный коммутатор назначает разные приоритеты разным потокам данных в зависимости от их важности, а затем предоставляет разные услуги этим потокам на основе их приоритетов. Это способ реализации QoS между конечными устройствами.

Кроме того, вы также можете настроить коммутатор в сети так, чтобы он обрабатывал определенные пакеты с определенными атрибутами (на основе MAC-уровня или информации L3 в пакетах) особым образом. Эти виды поведения называются «одним прыжком» (one-leaf behaviors).



Функция QoS коммутатора оптимизирует использование ограниченной пропускной способности, что значительно повышает общую производительность сети.

## 16.2 Модель QoS между терминалами

Модель описывает набор возможностей QoS между конечными устройствами, то есть возможности сети передавать определенные услуги сетевой связи от одного терминала к другому. Программное обеспечение QoS поддерживает два типа моделей обслуживания: обслуживание с максимальными усилиями и дифференцированное обслуживание.

➤ Обслуживание с максимальными усилиями – это единая модель обслуживания. В этой модели приложение может отправлять любой объем данных в любое необходимое время без применения разрешений или предварительного уведомления сети. Что касается обслуживания с максимальными усилиями, если это разрешено, сеть может передавать данные без каких-либо гарантий надежности, времени задержки или пропускной способности. QoS коммутатора, на котором реализована обслуживание с максимальными усилиями, по своей природе является услугой, выполняющейся по принципу «первым пришел – первым обслужен» (FCFS).

➤ Что касается дифференцированного обслуживания, то если в сети должна передаваться специальная услуга, каждый пакет должен быть указан соответствующим тегом QoS. Это обозначение может быть реализовано в различных режимах, например, использование установки статуса приоритета IP в пакете IP-данных. Коммутатор использует это правило QoS для проведения классификации и создания интеллектуальной очереди. QoS коммутатора обеспечивает строгий приоритет (SP), взвешенный циклический перебор (WRR), циклический перебор с дефицитом (DRR) и принцип «первым пришел – первым обслужен» (FCFS).

## 16.3 Алгоритмы очереди QoS

Каждый алгоритм очереди является важной основой для реализации QoS. QoS коммутатора обеспечивает следующие алгоритмы: строгий приоритет (SP), взвешенный циклический перебор (WRR), циклический перебор с дефицитом (DRR) и принцип «первым пришел – первым обслужен» (FCFS).

### ➤ Строгий приоритет

Этот алгоритм означает, что сначала предоставляется услуга потоку с наивысшим приоритетом, после чего следует услуга для потока с приоритетом, следующим за наивысшим. Этот алгоритм обеспечивает сравнительно хорошее обслуживание потоков с относительно высоким приоритетом, но его недостаток также очевиден: потоки с низким приоритетом не могут получить обслуживание и в итоге отбрасываются.



#### ➤ Взвешенный циклический перебор

Взвешенный циклический перебор (WRR) – эффективное решение проблемы строгого приоритета (SP), при котором очереди с низким приоритетом всегда затухают. WRR – это алгоритм, который выделяет каждой приоритетной очереди определенную полосу пропускания и обеспечивает обслуживание каждой приоритетной очереди в порядке от высокого приоритета к низкому. После того как очередь с наивысшим приоритетом заняла всю свою полосу пропускания, система автоматически предоставляет обслуживание очередям со следующим по величине приоритетом.

#### ➤ Первым пришел – первым обслужен

Алгоритм очереди «первым пришел — первым обслужен», сокращенно FCFS, обслуживает пакеты в соответствии с последовательностью их поступления на коммутатор, соответственно, первый прибывший пакет будет обслужен первым.

## 16.4 Настройка QoS

В обычных условиях коммутатор старается доставить каждый пакет, и при перегрузке все пакеты имеют одинаковый шанс быть отброшенными. Однако в реальности разные пакеты имеют разную важность, и более важные из них должны получать более качественное обслуживание. QoS – это механизм, который обеспечивает различные приоритетные услуги для пакетов с разной важностью, что позволяет сети работать более эффективно и с высокой производительностью.

Данная глава рассматривает, как настраивать QoS на коммутаторе, чтобы обеспечить наиболее эффективное управление приоритетами пакетов в сети.

Задачи настройки

- Настройка очереди глобальных приоритетов CoS
- Настройка полосы пропускания для приоритетной очереди CoS
- Настройка политики планирования приоритетных очередей CoS
- Настройка стандарта планирования для приоритетных очередей CoS
- Установка значения CoS по умолчанию для порта
- Настройка приоритетной очереди CoS для порта
- Создание карты политики QoS
- Настройка описания карты политики QoS
- Настройка сопоставления потока данных с картой политики QoS
- Настройка действий для потока данных в рамках управления политикой QoS
- Применение политики QoS к порту
- Отображение карты политики QoS
- Установка ограничения скорости на порту



### 16.4.1 Настройка очереди глобальных приоритетов CoS

Задача установки очереди приоритетов QoS состоит в том, чтобы сопоставить 8 значений CoS, определенных стандартом IEEE802.1p, с очередями приоритетов в коммутаторе. Коммутаторы этой серии имеют 8 приоритетных очередей. В зависимости от очередей коммутатор будет использовать разные политики планирования для реализации QoS.

Если очередь приоритетов CoS установлена в глобальном режиме, это повлияет на ее отображение на всех портах. Если приоритетные очереди установлены на порту L2, они смогут работать только на этом порту L2.

Войдите в режим управления и выполните одну за другой следующие команды, чтобы установить глобальную приоритетную очередь CoS:

| Команда                                    | Описание  |
|--|---|
| <b>configure</b>                           | Вход в режим глобальной конфигурации  |
| <b>[no] cos map quid cos1...cosn (1–8)</b> | Устанавливает очередь приоритетов CoS<br><b>quid</b> обозначает идентификатор приоритетной очереди CoS.<br><b>cos1...cosn</b> означает значение CoS, определенное стандартом IEEE802.1p |
| <b>exit</b>                                | Возвращение в режим EXEC  |
| <b>write</b>                               | Сохранение настроек   |

### 16.4.2 Настройка полосы пропускания для приоритетной очереди CoS

Полоса пропускания приоритетной очереди CoS означает коэффициент распределения пропускной способности для каждой приоритетной очереди, который устанавливается, когда для политики планирования очереди задано значение WRR или DRR. Всего эта серия коммутаторов имеет 8 очередей приоритетов.

Если команда запущена, это повлияет на пропускную способность для всех приоритетных очередей на всех интерфейсах. Настройка проверяется только в том случае, если для режима планирования очереди установлено значение WRR/DRR. В этом случае команда определяет значение веса пропускной способности очереди приоритетов CoS.

Выполните следующие команды одну за другой, чтобы установить пропускную способность для очереди приоритетов CoS:

| Команда       | Описание                             |
|---------------|--------------------------------------|
| <b>config</b> | Вход в режим глобальной конфигурации |



|  |   |
|--|---|
| <b>[no] scheduler weight bandwidth</b><br><i>weight1...weightn (1–8)</i> | Устанавливает пропускную способность для очереди приоритетов CoS<br><br><i>weight1...weightn</i> обозначает веса 8 очередей приоритетов CoS WRR/DRR |
| <b>exit</b>  | Возвращение в режим EXEC  |
| <b>write</b>   | Сохранение настроек   |

### 16.4.3 Настройка политики планирования приоритетных очередей CoS

Коммутатор имеет множество исходящих очередей на каждом своем порту. Данная серия коммутаторов поддерживает 8 приоритетных очередей. Исходящие очереди могут использовать следующие четыре режима планирования:

- SP (строгий приоритет) – это алгоритм, в котором пересылка пакетов в очереди с низким приоритетом возможна только тогда, когда очередь с высоким приоритетом равна нулю. Если в очереди с высоким приоритетом есть пакеты, они будут пересылаться безоговорочно.
- FCFS (первым пришел – первым обслужен) это алгоритм, который обеспечивает обслуживание пакетов в соответствии с последовательностью их поступления на коммутатор. Первый прибывший пакет обслуживается в первую очередь.
- WRR (взвешенный циклический перебор) – это алгоритм, который выделяет каждой приоритетной очереди определенную полосу пропускания и обеспечивает обслуживание каждой приоритетной очереди в соответствии с ее весом, от высокого приоритета к низкому. Единицей измерения полосы пропускания в этом режиме является пакет.
- DRR (циклический перебор с дефицитом) – этот метод также использует круговое распределение, но с учетом «дефицита». Каждому потоку назначается квота (или «дефицит»), которая может накапливаться, если поток не использует всю свою квоту в текущем цикле. Это позволяет потокам, которые не использовали свою долю в предыдущих циклах, получить дополнительные ресурсы в следующих. Единицей измерения полосы пропускания в этом режиме является байт.

После выполнения этой команды режим планирования потоков трафика принимает указанное значение. Войдите в режим управления и установите политику планирования обработки приоритетных очередей CoS:

| Команда          | Описание                             |
|------------------|--------------------------------------|
| <b>configure</b> | Вход в режим глобальной конфигурации |



|  |   |
|--|---|
| <code>[no] scheduler policy { sp   fcfs   wrr   drr }</code> | Устанавливает политику планирования обработки приоритетных очередей CoS |
| <code>exit</code>  | Возвращение в режим EXEC  |
| <code>write</code>   | Сохранение настроек   |

## 16.4.4 Настройка стандарта планирования для приоритетных очередей CoS

Показатель планирования приоритетной очереди – это стандарт масштаба соотношения распределения пропускной способности различных приоритетных очередей, когда политика планирования настроена на WRR/DRR. Основные стандарты следующие:

**packet-count:** означает, что занимаемая полоса пропускания выражается числом пакетов;

**byte-count:** означает, что занимаемая полоса пропускания выражается размером пакета;

**latency:** означает, что занимаемая полоса пропускания выражается временным сегментом.

Данная серия коммутаторов поддерживает стандарты packet-count для WRR и byte-count для DRR.

## 16.4.5 Установка значения CoS по умолчанию для порта

Если порт коммутатора получает кадр данных без тега, он добавит к кадру свой приоритет CoS по умолчанию. Установка значения CoS по умолчанию для порта – это определение приоритета, который будет присвоен непометенным данным при их получении на этом порту.

Войдите в режим управления и выполните следующие команды, чтобы установить значение CoS по умолчанию для порта:

| Команда                                 | Описание  |
|---|---|
| <code>configure</code>                  | Вход в режим глобальной конфигурации  |
| <code>interface g0/1</code>             | Вход в режим настройки выбранного интерфейса  |
| <code>[no] cos default cos (0–7)</code> | Устанавливает значение CoS для полученных нетегированных кадров<br><i>cos</i> означает соответствующее значение CoS |
| <code>exit</code>                       | Возвращение в режим глобальной конфигурации   |
| <code>exit</code>                       | Возвращение в режим EXEC  |



|              |                     |
|--------------|---------------------|
| <b>write</b> | Сохранение настроек |
|--------------|---------------------|

### 16.4.6 Настройка приоритетной очереди CoS для порта

Если приоритетная очередь настроена на порту L2, она будет использоваться этим портом; в противном случае вам следует выполнить настройку глобальной очереди приоритетов CoS.

Войдите в режим управления и выполните следующие команды, чтобы установить настройки по умолчанию для очереди CoS на порту:

| Команда                                    | Описание   |
|--|--|
| <b>configure</b>                           | Вход в режим глобальной конфигурации   |
| <b>interface g0/1</b>                      | Вход в режим настройки выбранного интерфейса   |
| <b>[no] cos map quid cos1...cosn (1–8)</b> | Настраивает приоритетную очередь CoS<br><b>quid</b> обозначает идентификатор приоритетной очереди CoS<br><b>cos1...cosn</b> – значение CoS, определенное стандартом IEEE802.1p |
| <b>exit</b>                                | Возвращение в режим глобальной конфигурации  |
| <b>exit</b>                                | Возвращение в режим EXEC   |
| <b>write</b>                               | Сохранение настроек  |

### 16.4.7 Создание карты политики QoS

Классификация потока означает идентификацию класса пакетов с определенными атрибутами путем применения определенных правил и выполнение определенных действий в отношении этих пакетов.

Списки доступа по IP и MAC, которые используются для сопоставления с потоками данных, могут быть настроены только с одним правилом. Если вы попытаетесь добавить больше правил, настройка не сработает. Когда действие в правиле разрешает трафик (permit), это правило помогает различать потоки данных. Если же действие запрещает трафик (deny), то такое правило не выполняет никакой функции. Идентификатор порта в IP ACL должен иметь определенное значение и не может быть диапазоном.

Вы можете настроить политику QoS, установив все параметры политики, то есть описание, классификацию и действие, или один-два из них. Также можно изменить политику путем настройки отдельных параметров, как описано далее.



Войдите в привилегированный режим, а затем выполните следующие команды, чтобы создать новую карту политики QoS:

| Команда   | Описание  |
|---|---|
| <b>configure</b>  | Вход в режим глобальной конфигурации  |
| <b>[no]policy-map name</b>  | Вход в режим настройки политики QoS<br><b>name</b> означает имя политики  |
| <b>description description-text</b>   | Создает описание политики QoS<br><b>description-text</b> означает текст, описывающий политику   |
| <b>[no] classify {ip access-list-name   dscp dscp-value   mac mac-access-name   vlan vlan-id   cos cos-value   any}</b> | Настраивает классификацию пакетов<br><b>access-list-name</b> – имя IP ACL<br><b>dscp</b> – поле diffserv в IP-пакете<br><b>mac-access-name</b> – имя MAC ACL<br><b>vlan-id</b> – идентификатор сопоставленной VLAN<br><b>cos</b> – сопоставленное значение CoS<br><b>any</b> – сопоставление любого потока данных с правилом  |
| <b>action {bandwidth max-band   cos cos-value   dscp dscp-value   redirect interface-id   drop   stat   monitor}</b>    | Настраивает политику, применяемую к соответствующему потоку данных<br><b>max-band</b> обозначает максимальную полосу пропускания, допустимую для потока данных<br><b>cos-value</b> означает изменение поля CoS пакетов соответствующего потока на указанное значение<br><b>dscp-value</b> означает изменение поля DSCP пакетов соответствующего потока на указанное значение<br><b>interface-id</b> означает перенаправление потока на указанный выходной порт<br><b>drop</b> означает, что все пакеты, соответствующие настройкам, будут отбрасываться<br><b>stat</b> означает, что коммутатор собирает статистику соответствующих потоков |



|             |  |
|-------------|--|
|             | <b>monitor</b> означает передачу пакета на зеркальный порт |
| <b>exit</b> | Возвращение в режим глобальной конфигурации                |
| <b>exit</b> | Возвращение в режим EXEC                                   |

## 16.4.8 Настройка описания карты политики QoS

Войдите в режим управления и выполните следующие команды, чтобы задать описание карты политики QoS. Это заменит предыдущие настройки.

| Команда                             | Описание  |
|-------------------------------------|---|
| <b>configure</b>                    | Вход в режим глобальной конфигурации  |
| <b>[no]policy-map name</b>          | Вход в режим настройки политики QoS<br><b>name</b> означает имя политики                      |
| <b>description description-text</b> | Создает описание политики QoS<br><b>description-text</b> означает текст, описывающий политику |
| <b>exit</b>                         | Возвращение в режим глобальной конфигурации   |
| <b>exit</b>                         | Возвращение в режим EXEC  |

## 16.4.9 Настройка сопоставления потока данных с картой политики QoS

Правила классификации для потока данных определяются в соответствии с требованиями администратора. Эти правила могут быть простыми, например, идентификация потоков с разными приоритетами на основе поля ToS в заголовке IP-пакета, или сложными, когда пакеты классифицируются на основе различной информации о комплексном уровне связи, сетевом уровне и транспортном уровне (например, MAC-адрес, исходный IP-адрес, целевой IP-адрес или идентификатор порта приложения). Обычно стандарт классификации ограничивается заголовком инкапсулированного пакета, но иногда в качестве критерия классификации используется содержание пакета.

Войдите в режим управления, настройте потоки данных для сопоставления политике и замените ими предыдущие настройки, выполнив следующие действия:

| Команда | Описание |
|---------|----------|
|         |          |



|   |  |
|---|--|
| <b>configure</b>  | Вход в режим глобальной конфигурации   |
| <b>[no]policy-map name</b>  | Вход в режим настройки политики QoS<br><b>name</b> означает имя политики   |
| <b>[no] classify {ip access-list-name   dscp dscp-value   mac mac-access-name   vlan vlan-id   cos cos-value   any}</b> | Настраивает классификацию пакетов<br><b>access-list-name</b> – имя IP ACL<br><b>dscp</b> – поле diffserv в IP-пакете<br><b>mac-access-name</b> – имя MAC ACL<br><b>vlan-id</b> – идентификатор сопоставленной VLAN<br><b>cos</b> – сопоставленное значение CoS<br><b>any</b> – сопоставление любого потока данных с правилом |
| <b>exit</b>   | Возвращение в режим глобальной конфигурации  |
| <b>exit</b>   | Возвращение в режим EXEC   |

## 16.4.10 Настройка действий для потока данных в рамках управления политикой QoS

Команда **action** определяет, какие действия должны выполняться для потока данных в соответствии с правилами фильтрации, такие как ограничение пропускной способности, отбрасывание данных, их обновление и т. д.

Войдите в режим управления и выполните следующие команды, чтобы установить необходимые действия для политики, сопоставляющейся с потоком данных. Эти действия заменят предыдущие настройки.

| Команда  | Описание   |
|--|--|
| <b>configure</b>   | Вход в режим глобальной конфигурации                                     |
| <b>[no]policy-map name</b>   | Вход в режим настройки политики QoS<br><b>name</b> означает имя политики |
| <b>action {bandwidth max-band   cos cos-value   dscp dscp-value   redirect interface-id   drop   stat   monitor}</b> | Настраивает политику, применяемую к соответствующему потоку данных       |



|             |  |
|-------------|--|
|             | <p><b>max-band</b> обозначает максимальную полосу пропускания, допустимую для потока данных</p> <p><b>cos-value</b> означает изменение поля CoS пакетов соответствующего потока на указанное значение</p> <p><b>dscp-value</b> означает изменение поля DSCP пакетов соответствующего потока на указанное значение</p> <p><b>interface-id</b> означает перенаправление потока на указанный выходной порт</p> <p><b>drop</b> означает, что все пакеты, соответствующие настройкам, будут отбрасываться</p> <p><b>stat</b> означает, что коммутатор собирает статистику соответствующих потоков</p> <p><b>monitor</b> означает передачу пакета на зеркальный порт</p> |
| <b>exit</b> | Возвращение в режим глобальной конфигурации  |
| <b>exit</b> | Возвращение в режим EXEC   |

## 16.4.11 Применение политики QoS к порту

Политика QoS может быть применена к порту. Допускается применение как нескольких политик к одному порту, так и одной политике к нескольким портам. При этом политики, примененные ранее, имеют больший приоритет перед теми, которые применены позже. Если пакету назначены две политики, и действия в них противоречат друг другу, то применяются действия из первой сопоставленной политики. После применения политики QoS к порту, коммутатор автоматически добавляет правило блокировки для предотвращения прохождения других потоков данных, которым не разрешено проходить через этот порт. Когда все политики на порту удаляются, коммутатор автоматически удаляет с порта и правило блокировки по умолчанию.

Войдите в режим управления и выполните следующие команды, чтобы применить политику QoS.

| Команда          | Описание                             |
|------------------|--------------------------------------|
| <b>configure</b> | Вход в режим глобальной конфигурации |



|  |   |
|--|---|
| <b>interface g0/1</b>                          | Вход в режим настройки выбранного интерфейса  |
| <b>[no] qos policy name {ingress   egress}</b> | Применяет политику QoS к порту<br><b>name</b> – имя карты политики QoS<br><b>ingress</b> означает оказывать влияние на входящие потоки.<br><b>egress</b> означает оказывать влияние на исходящие потоки |
| <b>exit</b>                                    | Возвращение в режим глобальной конфигурации   |
| <b>exit</b>                                    | Возвращение в режим EXEC  |

## 16.4.12 Отображение карты политики QoS

Вы можете запустить команду **show**, чтобы отобразить все или определенные карты политик QoS.

Выполните следующую команду в режиме управления, чтобы отобразить таблицу сопоставления:

| Команда                                  | Описание   |
|--|--|
| <b>show policy-map [policy-map-name]</b> | Отображает все или указанные карты политик QoS<br><b>policy-map-name</b> – имя таблицы сопоставления QoS |

## 16.4.13 Установка ограничения скорости на порту

Посредством конфигурации можно ограничить скорости потока на входе и выходе.

Войдите в привилегированный режим и выполните следующие команды, чтобы ограничить скорость порта:

| Команда               | Описание                                     |
|-----------------------|--|
| <b>configure</b>      | Вход в режим глобальной конфигурации         |
| <b>interface g0/1</b> | Вход в режим настройки выбранного интерфейса |



|  |   |
|--|---|
| <p>[no] <b>switchport rate-limit band (1–1000)</b><br/>       {ingress   egress}</p> | <p>Настраивает ограничение скорости для порта</p> <p><b>band</b> – значение, определяющее максимальную пропускную способность</p> <p><b>ingress</b> указывает, что ограничение скорости применяется к входящему трафику</p> <p><b>egress</b> указывает, что ограничение скорости применяется к исходящему трафику</p> |
| <p><b>exit</b></p>   | <p>Возвращение в режим глобальной конфигурации</p>  |
| <p><b>exit</b></p>   | <p>Возвращение в режим EXEC</p>   |

## 16.5 Пример настройки QoS

После того, как вы настроили на порту политику, меняющую значение CoS пакета на 2, и применили ее, вам необходимо настроить еще одну политику, разрешающую прохождение всех потоков данных, иначе они будут заблокированы. Смотрите следующий пример:

```
ip access-list extended ipacl
permit ip 192.168.20.2 255.255.255.255 192.168.20.210 255.255.255.255
policy-map any
classify any
policy-map pmap
classify ip ipacl
action cos 2
interface GigaEthernet0/2
qos policy pmap ingress
qos policy any ingress
# Обратите внимание на порядок применения двух политик.
```

## 17. Туннель протокола второго уровня

### 17.1 Введение



Туннель протокола второго уровня позволяет пользователям, чьи терминалы подключены к коммутатору, прозрачно передавать пакеты протокола L2 в своих собственных сетях через коммутатор без воздействия соответствующего L2-модуля этого коммутатора. Коммутатор здесь – всего лишь прозрачная среда передачи для пользователей.

## 17.2 Настройка туннеля

Выполните следующие команды, чтобы настроить функцию туннеля L2:

| Команда                             | Описание  |
|-------------------------------------|---|
| <b>configure</b>                    | Вход в режим глобальной конфигурации  |
| <b>interface &lt;intf_name&gt;</b>  | Вход в режим настройки интерфейса. Только порты коммутатора поддерживают туннель L2 (включая физические порты и порты агрегации)  |
| <b>[no] l2protocol-tunnel [stp]</b> | Указывает протокол L2, который используется для включения функции туннеля на этом порту коммутатора<br><br>В настоящее время поддерживается только туннельная функция протокола STP |
| <b>[CTRL] + Z</b>                   | Возвращение в режим EXEC  |
| <b>write</b>                        | Сохранение настроек   |

## 17.3 Пример настройки туннеля

Сетевое оборудование подключено следующим образом:

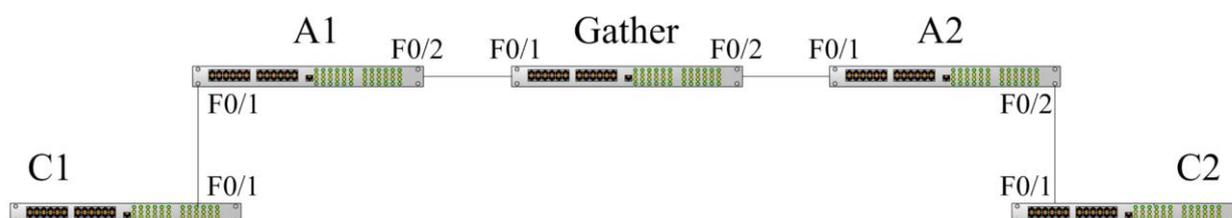


Рисунок 19 – Топология сети

A1/A2/Gather принадлежит базовой сети. C1/C2 обозначает два коммутатора, расположенные в двух филиалах заказчика. Клиент хочет, чтобы две сети управлялись как независимые, то есть базовая сеть является для этого клиента прозрачным каналом



передачи. Чтобы реализовать прозрачную передачу STP, необходимо выполнить следующие настройки на каждом коммутаторе:

1. Установите порт f0/2 коммутатора A1, порт f0/1 коммутатора Gather и порт f0/1 коммутатора A2 в режим trunk соответственно.
2. Настройте порт f0/1 коммутатора A1 и порт f0/2 коммутатора A2 как порты доступа, а затем включите функцию туннелирования протокола STP на двух портах.

## 18. AAA

### 18.1 Введение

Контроль доступа – это способ управления доступом к сети и службам. Службы сетевой безопасности аутентификации, авторизации и учета (AAA) предоставляют основную структуру, с помощью которой контроль доступа настраивается на маршрутизаторе или специальном сервере.

#### 18.1.1 Служба безопасности AAA

AAA – это архитектурный каркас для согласованной настройки набора из трех независимых функций безопасности. AAA предлагает модульный способ предоставления следующих услуг:

##### ➤ Аутентификация

Это метод идентификации пользователей, включая запрос имени пользователя/пароля и шифрование в соответствии с выбранным протоколом безопасности.

Аутентификация – это метод идентификации личности пользователей до того, как они получат доступ к сети и воспользуются сетевыми услугами. Аутентификацию AAA можно настроить с помощью определения списка методов аутентификации и последующего применения этого списка на всех интерфейсах. Список методов определяет тип аутентификации и порядок ее выполнения. Перед выполнением любой определенной список методов аутентификации должен быть применен к определенному интерфейсу. Единственным исключением является список по умолчанию (который называется default). Если других списков методов аутентификации нет, на всех интерфейсах автоматически будет применен метод по умолчанию. Если метод для отдельного интерфейса определен, он заменит значение по умолчанию. Чтобы узнать, как настроить различные методы, см. раздел «Настройка аутентификации».

##### ➤ Авторизация

Это метод управления удаленным доступом для ограничения разрешений пользователя, включая однократную авторизацию или авторизацию для каждой службы, список и профиль учетных записей для каждого пользователя, поддержку групп пользователей и поддержку IP, IPX, ARA и Telnet.

Авторизация AAA осуществляется через группу функций, в которых пользователь авторизуется с некоторыми разрешениями. Во-первых, функции в этой группе будут



сравниваться с информацией о конкретном пользователе в базе данных, затем результат сравнения будет возвращен в AAA для подтверждения фактических разрешений этого пользователя. Эта база данных может находиться на локальном сервере авторизации или на маршрутизаторе, к которому осуществляется доступ, а также на удаленном сервере Radius/TACACS+. Сервер Radius или TACACS+ проводит авторизацию пользователя через связанный с пользователем одноранговый атрибут-значение. Значение атрибута (AV) определяет доступные разрешения. Все методы авторизации определяются через AAA. Как и при аутентификации, сначала будет определен список методов авторизации, а затем этот список будет применяться ко всем типам интерфейсов. О том, как выполнить настройку авторизации, см. в разделе «Настройка авторизации».

#### ➤ Учет

Это метод сбора информации о пользователе и отправки информации на сервер безопасности. Собранную информацию можно использовать для открытия учетной записи, проведения аудита и формирования списков отчетов, таких как идентификатор пользователя, время начала/окончания сеанса, команды выполнения и количество пакетов или байтов.

Функция учета может отслеживать сервисы, к которым обращаются пользователи, и в то же время отслеживать количество потребляемых сервисом сетевых ресурсов. Когда учет AAA активирован, сервер доступа может сообщать о действиях пользователя серверу TACACS+ или Radius в форме учетных записей. Каждая запись содержит узел AV, который хранится на сервере безопасности. Данные могут быть использованы для управления сетью, анализа клиента или аудита. Все методы учета указываются через AAA. Подобно аутентификации и авторизации, методы учета сначала должны быть определены в именованном списке, а затем применены к различным интерфейсам. О том, как выполнить настройку, см. в разделе «Настройка учета».

### 18.1.2 Преимущества использования AAA

AAA дает следующие преимущества:

- повышенную гибкость и контроль конфигурации доступа;
- масштабируемость;
- стандартные методы аутентификации, такие как RADIUS, TACACS+;
- несколько систем резервного копирования.

### 18.1.3 Принципы AAA

AAA предназначается для того, чтобы вы могли динамически настраивать нужный тип аутентификации и авторизации для каждой линии (для каждого пользователя) или для каждой услуги (например, IP, IPX или VPDN). Вы определяете нужный тип аутентификации и авторизации, создавая списки методов, а затем применяя эти списки методов к определенным службам или интерфейсам.



### 18.1.4 Список методов AAA

Список методов – это последовательная запись, определяющая методы, используемые для аутентификации пользователя. Списки методов позволяют вам назначить один или несколько протоколов безопасности, которые будут применяться для аутентификации, обеспечивая при этом резервную систему на случай, если исходный метод не сработает. Программное обеспечение коммутатора использует первый из перечисленных методов и, если этот метод не отвечает, выбирается следующий метод в списке. Данный процесс продолжается до тех пор, пока не будет установлена успешная связь или список методов не будет исчерпан и аутентификация завершится ошибкой.

Важно отметить, что программное обеспечение коммутатора пытается выполнить аутентификацию с помощью следующего из перечисленных методов аутентификации только в том случае, если предыдущий метод не дает ответа. Если аутентификация завершается ошибкой в какой-либо момент этого цикла – это означает, что сервер безопасности или локальная база данных имен пользователей отвечает отказом в доступе пользователя. В таком случае процесс аутентификации останавливается, и никакие другие методы не применяются.

На следующем рисунке показана типичная конфигурация сети AAA, включающая четыре сервера безопасности: R1 и R2 – серверы RADIUS, а T1 и T2 – серверы TACACS+.

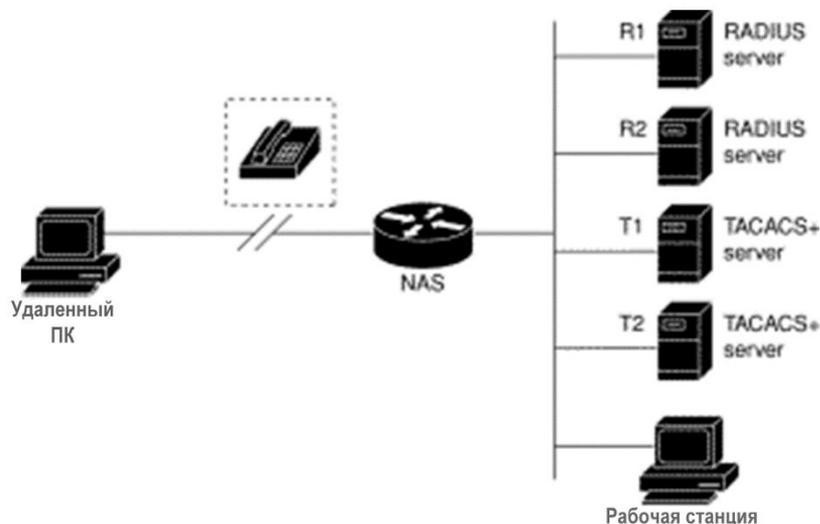


Рисунок 20 – Типовая конфигурация AAA

Предположим, что системный администратор определил список методов, в котором сначала будет обращаться к R1 за информацией об аутентификации, затем к R2, T1, T2 и, наконец, к локальной базе данных имен пользователей на самом сервере доступа. Когда удаленный пользователь пытается подключиться к сети, сервер сетевого доступа сначала запрашивает информацию об аутентификации у R1. Если R1 аутентифицирует пользователя, он отправляет ответ PASS на сервер сетевого доступа, и пользователю разрешается доступ к сети. Если R1 возвращает ответ FAIL, пользователю отказывается в доступе, и сеанс завершается. Если R1 не отвечает, сервер сетевого доступа обрабатывает это как ERROR и запрашивает информацию об аутентификации у R2. Этот механизм



продолжает обрабатываться для оставшихся назначенных методов, пока пользователь не будет либо аутентифицирован, либо отклонен, либо пока не завершится сеанс. Если все методы аутентификации возвращают ошибки, сервер сетевого доступа обработает сеанс как сбой и завершит его.

Ответ FAIL существенно отличается от ERROR. FAIL означает, что для прохождения успешной аутентификации пользователь не соответствует критериям, содержащимся в применяемой базе данных. ERROR означает, что сервер безопасности не ответил на запрос аутентификации. Из-за этого попытка аутентификации не была предпринята. Только при обнаружении ERROR AAA выберет следующий метод, определенный в назначенном списке.

### 18.1.5 Процесс настройки AAA

Сначала необходимо определить, какое решение безопасности вы хотите внедрить. Вам нужно оценить риски безопасности в конкретной сети и выбрать подходящие средства для предотвращения несанкционированного проникновения и атак. Прежде чем настраивать AAA, необходимо знать базовую процедуру настройки. Чтобы провести настройку на маршрутизаторе или серверах доступа, выполните следующие действия:

- если вы решили использовать сервер безопасности, сначала настройте параметры протокола безопасности, такие как RADIUS, TACACS+ или Kerberos;
- определите списки методов для аутентификации с помощью команды **aaa authentication**;
- при необходимости примените списки методов к конкретному интерфейсу или линии;
- (необязательно) настройте авторизацию с помощью команды **aaa authorization**;
- (необязательно) настройте учет с помощью команды **aaa accounting**.

## 18.2 Настройка аутентификации

Задачи настройки

- Настройка аутентификации при входе с помощью AAA
- Аутентификация на привилегированном уровне
- Настройка баннеров сообщений для аутентификации AAA
- Изменение текста приглашения ввода имени пользователя
- Изменение текста приглашения ввода пароля пользователя
- Создание аутентификации на основе имени пользователя
- Создание пароля enable

Чтобы настроить аутентификацию AAA, выполните следующие процессы:



1. Если вы решили использовать для аутентификации отдельный сервер, настройте параметры протокола безопасности, такие как RADIUS, TACACS+ или Kerberos.
2. Определите списки методов для аутентификации с помощью команды **aaa authentication**.
3. Примените списки методов к определенному интерфейсу или линии, если необходимо.

## 18.2.1 Настройка аутентификации при входе с помощью AAA

Службы безопасности AAA упрощают различные методы аутентификации при входе в систему. Используйте команду **aaa authentication login**, чтобы включить аутентификацию AAA независимо от того, какой из поддерживаемых методов аутентификации при входе вы решите использовать. С помощью команды **aaa authentication login** вы настраиваете один или несколько списков методов аутентификации, которые пробуются при входе в систему. После настройки методов вы можете применить их, запустив **login authentication**. Выполните следующие команды в режиме глобальной конфигурации:

| Команда  | Описание   |
|--|--|
| <b>aaa authentication login</b> {default   list-name} method1 [method2...] | Включает AAA глобально   |
| <b>line</b> {console   vty} line-number [ending-line-number]               | Вход в режим настройки линии                                   |
| <b>login authentication</b> {default   list-name}                          | Применяет список проверки подлинности к линии или набору линий |

**list-name** – это строка символов, используемая для наименования списка, который вы создаете. Аргумент **method** означает фактический метод аутентификации. Дополнительные методы аутентификации используются только в том случае, если предыдущий метод возвращает ошибку (error), а не в случае неудачи (fail). Если необходимо, чтобы аутентификация проходила успешно, даже если все методы возвращают ошибку, нужно указать **none** в качестве последнего метода в командной строке. Это предоставляет возможность разрешить аутентификацию в случае проблем и неисправностей с другими методами проверки подлинности.

Параметр **default** может создать список аутентификации по умолчанию, который будет автоматически применяться ко всем интерфейсам. Например, чтобы указать, что аутентификация должна пройти успешно, даже если сервер TACACS+ возвращает ошибку, введите следующую команду:

```
aaa authentication login default group radius
```



Поскольку ключевое слово **none** позволяет успешно пройти аутентификацию любому пользователю, вошедшему в систему, его следует использовать только в качестве резервного метода аутентификации.

---

В следующей таблице перечислены поддерживаемые методы аутентификации при входе:



| Ключевое слово    | Описание  |
|-------------------|---|
| enable            | Для аутентификации используется пароль enable                             |
| group <i>name</i> | Для аутентификации используется определенная группа серверов              |
| group radius      | Для аутентификации используется RADIUS                                    |
| line              | Для аутентификации используется пароль линии                              |
| local             | Для аутентификации используется локальная база данных имен пользователей  |
| local-case        | Использует аутентификацию локального имени пользователя с учетом регистра |
| none              | Проходит аутентификацию без каких-либо условий                            |

### 1. Аутентификация с использованием пароля уровня enable

Используйте команду **aaa authentication** с ключевым словом **enable**, чтобы указать пароль enable в качестве метода аутентификации при входе в систему. Например, чтобы указать пароль enable в качестве метода аутентификации, когда не задан другой список методов, введите следующую команду:

```
aaa authentication login default enable
```

### 2. Аутентификация с использованием пароля линии

Используйте команду **aaa authentication** с ключевым словом **line**, чтобы указать пароль конкретной линии/порта в качестве метода аутентификации. Например, чтобы указать пароль линии в качестве метода аутентификации пользователя при входе в систему, когда не задан другой список методов, введите следующую команду:

```
aaa authentication login default line
```

Прежде чем вы сможете использовать линейный пароль в качестве метода аутентификации, вам необходимо определить этот пароль.

### 3. Аутентификация с использованием локального пароля

Используйте команду **aaa authentication** с ключевым словом **local**, чтобы указать, что маршрутизатор или сервер доступа будут использовать локальную базу данных имен пользователей для аутентификации. Например, чтобы указать локальную базу данных имен пользователей в качестве метода аутентификации пользователя при входе в систему, если не задан другой список методов, введите следующую команду:

```
aaa authentication login default local
```

### 4. Аутентификация с помощью группы RADIUS

Используйте команду **aaa authentication** с ключевыми словами **group radius**, чтобы указать RADIUS в качестве метода аутентификации. Например, чтобы указать RADIUS в качестве



метода аутентификации пользователя при входе в систему, когда не задан другой список методов, введите следующую команду:

```
aaa authentication login default group radius
```

Прежде чем вы сможете использовать RADIUS в качестве метода аутентификации, необходимо включить связь с сервером безопасности RADIUS. Дополнительные сведения об установлении связи с сервером RADIUS см. в разделе «Настройка RADIUS».

## 18.2.2 Аутентификация на привилегированном уровне

Используйте команду **aaa authentication enable default**, чтобы создать серию методов аутентификации, которые используются для определения того, может ли пользователь получить доступ к привилегированному командному режиму уровня EXEC. Вы можете указать до четырех методов аутентификации. Дополнительные методы аутентификации используются только в том случае, если предыдущий метод возвращает «error», а не «fail». Чтобы указать, что аутентификация должна пройти успешно, даже если все методы возвращают ошибку, укажите **none** в качестве последнего метода в командной строке. Используйте следующую команду в режиме глобальной конфигурации:

| Команда   | Описание   |
|---|--|
| <b>aaa authentication enable default</b> <i>method1</i> [ <i>method2...</i> ] | Включает проверку идентификатора пользователя и пароля для пользователей, запрашивающих привилегированный уровень EXEC |

Аргумент **method** относится к фактическому списку методов, которые пробует алгоритм аутентификации, в введенной последовательности.

В следующей таблице содержатся ключевые слова, связанные с поддерживаемыми методами аутентификации при входе в привилегированный режим:

| Ключевое слово    | Описание   |
|-------------------|--|
| enable            | Для аутентификации используется пароль enable                |
| group <i>name</i> | Для аутентификации используется определенная группа серверов |
| group radius      | Для аутентификации используется RADIUS                       |
| line              | Для аутентификации используется линейный пароль              |
| none              | Проходит аутентификацию без каких-либо условий               |



### 18.2.3 Настройка баннеров сообщений для аутентификации AAA

AAA поддерживает использование настраиваемых, персонализированных баннеров входа и неудачного входа. Вы можете настроить баннеры для сообщений, которые будут отображаться, когда пользователь входит в систему для аутентификации с помощью AAA и когда по какой-либо причине аутентификация не удалась.

#### ➤ Настройка баннера входа

Чтобы настроить баннер, который будет отображаться при каждом входе пользователя в систему (заменяя сообщение по умолчанию), используйте следующую команду в режиме глобальной конфигурации:

| Команда  | Описание   |
|--|--|
| <b>aaa authentication banner delimiter text-string delimiter</b> | Используется для настройки персонального баннера, который будет отображаться при входе пользователей на устройство |

#### ➤ Настройка баннера неудачного входа в систему

Чтобы настроить сообщение, которое будет отображаться при неудачной попытке входа пользователя в систему (заменяющее сообщение по умолчанию), используйте следующую команду в режиме глобальной конфигурации:

| Команда  | Описание   |
|--|--|
| <b>aaa authentication fail-message delimiter text-string delimiter</b> | Используется для настройки персонального баннера, который будет отображаться при неудачной попытке входа пользователей на устройство |

#### ➤ Методические рекомендации

При создании баннера необходимо настроить разделитель, а затем ввести саму текстовую строку. Разделитель уведомляет о том, что следующая текстовая строка будет отображаться в качестве баннера. Разделитель повторно появляется в конце строки текстовых символов, указывая на то, что сообщение баннера завершено. Символом-разделителем может быть любой отдельный символ из расширенного набора символов ASCII, но после определения в качестве разделителя этот символ нельзя использовать в текстовой строке, составляющей баннер.



### 18.2.4 Изменение текста приглашения ввода имени пользователя

Чтобы изменить текст приглашения ввода имени пользователя по умолчанию, запустите **aaa authentication username-prompt**. Вы можете запустить использовать форму **no** данной команды, чтобы восстановить стандартный запрос «Username:».

Команда **aaa authentication username-prompt** не изменяет никакие пригласительные диалоговые окна, предоставляемые удаленным сервером безопасности, например, RADIUS. Выполните следующую команду в режиме глобальной конфигурации:

| Команда   | Описание  |
|---|---|
| <b>aaa authentication username-prompt text-string</b> | Текстовая строка, которая будет отображаться при запросе на ввод имени пользователя |

### 18.2.5 Изменение текста приглашения ввода пароля пользователя

Чтобы изменить текст, отображаемый при запросе пароля, используйте команду **aaa authentication password-prompt**. Чтобы вернуться к тексту запроса пароля по умолчанию, используйте форму **no** этой команды. Вы можете запустить **no aaa authentication username-prompt**, чтобы восстановить стандартный запрос на ввод пароля «Password:».

Команда **aaa authentication password-prompt** не изменяет никакие пригласительные диалоговые окна, предоставляемые удаленным сервером безопасности, например, RADIUS. Выполните следующую команду в режиме глобальной конфигурации:

| Команда   | Описание  |
|---|---|
| <b>aaa authentication password-prompt text-string</b> | Текстовая строка, которая будет отображаться, когда пользователю предлагается ввести пароль |

### 18.2.6 Создание аутентификации на основе имени пользователя

Вы можете создать систему аутентификации на основе имени пользователя, которая будет полезна в следующих ситуациях:

для предоставления зашифрованной системы аутентификации в стиле TACACS для сетей, которые не поддерживают TACACS;

для предоставления входа в особых случаях: например, проверка списка доступа, отсутствие проверки пароля, автоматическое выполнение команд при входе, ситуации «no escape».

Для создания аутентификации по имени пользователя используйте следующие команды в режиме глобальной конфигурации, в зависимости от того, что необходимо для конфигурации вашей системы:



**username** *name* {**nopassword** | **password** *password* | **password** *encryption-type* *encrypted-password*}

**username** *name* [**autocommand** *command*]

**username** *name* [**callback-dialstring** *telephone-number*]

**username** *name* [**callback-rotary** *rotary-group-number*]

**username** *name* [**callback-line** [**tty** | **aux**] *line-number* [*ending-line-number*]]

**username** *name* [**noescape**] [**nohangup**]

**username** *name* [**privilege** *level*]

**username** *name* [**user-maxlinks** *number*]

**no username** *name*

Для удаления имени пользователя применяется форма **no** этой команды.

### 18.2.7 Создание пароля enable

Чтобы установить локальный пароль для управления доступом с различными уровнями привилегий, выполните команду **enable password** в режиме глобальной конфигурации. Вы можете указать тип шифрования, зашифрованный пароль и уровень привилегий. Для удаления или отмены настройки пароля enable, используйте команду **no enable password** с указанием уровня привилегий, если необходимо.

**enable password** {[*encryption-type*] *encrypted-password*} [**level** *level*]

**no enable password** [**level** *level*]

### 18.2.8 Пример настройки аутентификации AAA

Пример аутентификации RADIUS

В следующем примере показано, как настроить коммутатор для аутентификации и авторизации с использованием RADIUS:

```
aaa authentication login radius-login group radius local
```

```
aaa authorization network radius-network group radius
```

```
line vty 3
```

```
login authentication radius-login
```

Значение каждой командной строки показано ниже:

- Команда **aaa authentication login radius-login group radius local** настраивает коммутатор на использование RADIUS для аутентификации при запросе входа в систему. Если RADIUS возвращает ошибку, пользователь аутентифицируется с использованием локальной базы данных.



- Команда **aaa authorization network radius-network group radius** запрашивает у RADIUS сетевую авторизацию, назначение адресов и другие списки доступа.
- Команда **login authentication radius-login** включает список методов входа в систему для линии 3.

## 18.3 Настройка авторизации

Чтобы настроить авторизацию AAA, выполните следующие процедуры:

1. Если вы решили использовать отдельный сервер, настройте параметры протокола безопасности, например, RADIUS, TACACS+ или Kerberos.
2. Запустите **aaa authorization**, чтобы определить список методов авторизации.
3. При необходимости примените список методов авторизации к конкретному интерфейсу или линии 3.

### 18.3.1 Настройка авторизации EXEC с помощью AAA

Используйте команду **aaa authorization exec** для проверки прав пользователя на выполнение оболочки EXEC. Этот механизм позволяет определить, разрешено ли пользователю запускать командный интерфейс. В процессе авторизации могут быть возвращены данные профиля пользователя, включая информацию об автоматических командах, которые должны выполняться при входе. После настройки списков методов авторизации вы можете применить эти списки, запустив **login authentication**. Выполните следующие команды в режиме глобальной конфигурации:

| Команда   | Описание   |
|---|--|
| <b>aaa authorization exec</b> {default   <i>list-name</i> }<br><i>method1</i> [ <i>method2</i> ...] | Создает общий список авторизации   |
| <b>line</b> [console   vty] <i>line-number</i> [ <i>ending-line-number</i> ]                        | Вход в режим настройки линии   |
| <b>login authentication</b> {default   <i>list-name</i> }   | Применяет список авторизации к линии или набору линий (в режиме настройки линии) |

**list-name** – это строка символов, используемая для именованя создаваемого вами списка. Ключевое слово **method** используется для обозначения реального метода авторизации. Только когда ранее использованный метод возвращает error, можно использовать другие методы. Если авторизация не удалась и предыдущий метод возвратил fail, другие методы использоваться не будут. Если требуется, чтобы вход в оболочку EXEC был произведен даже



тогда, когда все методы возвращают ошибку, назначьте **none** в качестве последнего метода авторизации в командной строке.

Параметр **default** указывает список авторизации по умолчанию, который будет автоматически применяться ко всем интерфейсам. Например, вы можете запустить следующую команду, чтобы указать RADIUS в качестве метода авторизации по умолчанию для EXEC:

```
aaa authorization exec default group radius
```



Если список методов не определен, локальная служба авторизации будет недоступна и авторизация будет разрешена.

В следующей таблице перечислены поддерживаемые в настоящее время методы авторизации EXEC:

| Ключевое слово    | Описание   |
|-------------------|--|
| group <i>WORD</i> | Использует определенную группу серверов для выполнения авторизации                         |
| group radius      | Использует авторизацию RADIUS  |
| local             | Использует локальную базу данных для выполнения авторизации                                |
| if-authenticated  | Автоматически авторизует аутентифицированного пользователя со всеми необходимыми функциями |
| none              | Проходит авторизацию без каких-либо условий  |

### 18.3.2 Пример авторизации AAA

В следующем примере показано, как выполнить локальную авторизацию EXEC.

```
aaa authentication login default local
```

```
aaa authorization exec default local
```

```
!
```

```
username exec1 password 0 abc privilege
```

```
username exec2 password 0 abc privilege 10
```

```
username exec3 nopassword
```

```
username exec4 password 0 abc user-maxlinks 10
```

```
username exec5 password 0 abc autocommand telnet 172.16.20.1
```

```
!
```

Ниже показано значение каждой командной строки:

- Команда **aaa authentication login default local** используется для определения списка методов аутентификации по умолчанию, который будет автоматически применяться ко всем серверам аутентификации при входе.



- Команда **aaa authorization exec default local** используется для определения списка методов авторизации EXEC по умолчанию, который будет автоматически применяться ко всем пользователям, которым требуется вход в оболочку EXEC.
- Имя пользователя – `exec1`, открытый пароль для входа – `abc`, уровень привилегий EXEC – 15 (наивысший уровень). То есть, когда пользователь `exec1`, чей уровень привилегий равен 15, входит в командную оболочку `exec`, все команды могут быть набраны и выполнены.
- Имя пользователя – `exec2`, открытый пароль для входа – `abc`, уровень привилегий EXEC – 10. То есть, когда пользователь `exec2`, уровень привилегий которого равен 10, входит в оболочку EXEC, могут быть набраны и выполнены команды с уровнем привилегий ниже 10.
- Имя пользователя – `exec3`, пароль для входа не требуется.
- Имя пользователя – `exec4`, открытый пароль для входа – `abc`, максимальное количество сессий пользователя – 10.
- Имя пользователя – `exec5`, открытый пароль для входа – `abc`, сразу при входе в оболочку EXEC выполняется команда `telnet 172.16.20.1`.

## 18.4 Настройка учета

Чтобы настроить учет AAA, выполните следующие процедуры:

1. Если вы решили использовать для учета отдельный сервер, настройте параметры протокола безопасности, например, RADIUS, TACACS+ или Kerberos.
2. Настройте списки методов учета при помощи команды **aaa accounting**.
3. При необходимости примените список методов к конкретному интерфейсу или линии.

### 18.4.1 Настройка учета подключений с помощью AAA

Чтобы включить учет AAA, запустите команду **aaa accounting**. Чтобы создать список методов для предоставления учетной информации обо всех исходящих соединениях, выполненных с сервера сетевого доступа, используйте команду **aaa accounting connection**.

| Команда   | Описание                              |
|---|---------------------------------------|
| <b>aaa accounting connection</b> { <b>default</b>   <i>list-name</i> } {{{ <b>start-stop</b>   <b>stop-only</b> } <b>group</b> <i>groupname</i> }   <b>none</b> } | Устанавливает глобальный список учета |

**list-name** – это символьная строка имени создаваемого вами списка.

В следующей таблице перечислены поддерживаемые в настоящее время методы учета подключений:



| Ключевое слово    | Описание   |
|-------------------|--|
| group <i>WORD</i> | Для проведения учета используется определенная группа серверов                   |
| group radius      | Для учета используется RADIUS  |
| none              | Отключает службы учета для указанной линии или интерфейса                        |
| stop-only         | Включает учет только при завершении соединения                                   |
| start-stop        | Включает учет как при начале соединения (start), так и при его завершении (stop) |

## 18.4.2 Настройка сетевого учета с помощью AAA

Чтобы создать список методов для предоставления учетной информации для сеансов SLIP, PPP, NCP и ARAP, используйте команду **aaa accounting network** в режиме глобальной конфигурации.

| Команда   | Описание                              |
|---|---------------------------------------|
| <b>aaa accounting network</b> {default   <i>list-name</i> } {{{start-stop   stop-only} group <i>groupname</i> }   none} | Устанавливает глобальный список учета |

**list-name** – это символьная строка имени создаваемого вами списка.

В следующей таблице перечислены поддерживаемые в настоящее время методы сетевого учета:

| Ключевое слово    | Описание  |
|-------------------|---|
| group <i>WORD</i> | Для проведения учета используется определенная группа серверов                      |
| group radius      | Для учета используется RADIUS   |
| none              | Отключает службы учета для указанной линии или интерфейса                           |
| stop-only         | Включает учет только при завершении сетевой сессии                                  |
| start-stop        | Включает учет как при начале сетевой сессии (start), так и при ее завершении (stop) |



### 18.4.3 Настройка обновления учета через AAA

Чтобы включить отправку периодических промежуточных записей учета на сервер, используйте команду **aaa accounting update** в режиме глобальной конфигурации. Чтобы отключить промежуточные обновления учета, используйте форму **no** этой команды.

| Команда  | Описание                      |
|--|-------------------------------|
| <b>aaa accounting update [newinfo] [periodic number]</b> | Включает обновление учета AAA |

Если используется ключевое слово **newinfo**, временная учетная запись будет отправлена на сервер учета, когда появится новая учетная информация, которую необходимо сообщить. Например, после согласования IPSP с IP-адресом удаленного терминала временная учетная запись, включая IP-адрес удаленного терминала, будет отправлена на сервер учета.

При использовании ключевого слова **periodic** временная учетная запись будет отправляться периодически. Период определяется числовым параметром. Временная учетная запись включает всю учетную информацию, имевшуюся до ее отправки.

Когда вы используете оба параметра (**newinfo** и **periodic**), происходит следующее:

- Для всех пользователей, которые уже находятся в системе, будут продолжать отправляться промежуточные учетные записи через заданные интервалы времени (параметр **periodic**).
- Для новых пользователей, которые подключаются к системе, учетные записи будут отправляться сразу, как только появится новая информация о них (параметр **newinfo**).

### 18.4.4 Ограничение учета пользователей без имени

Чтобы предотвратить отправку AAA записей об учетных событиях, если имя пользователя отсутствует или равно пустому значению (null), выполните следующую команду в режиме глобальной конфигурации:

**aaa accounting suppress null-username**

Чтобы разрешить отправку записей для пользователей с нулевым именем, используйте форму **no** этой команды.

## 19. RADIUS

В этой главе описывается безопасная система удаленной аутентификации пользователей RADIUS, определяется ее работа, а также подходящие и неподходящие сетевые среды для использования данной технологии; объясняется, как настроить RADIUS с помощью набора команд аутентификации, авторизации и учета (AAA).



## 19.1 Введение

### 19.1.1 Описание RADIUS

RADIUS (Remote Authentication Dial-In User Service) – это распределенная клиент-серверная система, защищающая сети от несанкционированного доступа. Клиенты RADIUS работают на удаленных устройствах и отправляют запросы аутентификации на центральный сервер, который содержит всю информацию об аутентификации пользователей и доступе к сетевым службам. Служба RADIUS выполняется в различных сетевых средах, требующих высокого уровня безопасности при сохранении сетевого доступа для удаленных пользователей.

Используйте RADIUS в следующих сетевых средах, требующих безопасности доступа:

- Сети с серверами доступа от разных поставщиков, каждый из которых поддерживает RADIUS. Например, серверы доступа от нескольких поставщиков используют единую базу данных безопасности на основе сервера RADIUS. В сети на основе IP с различными серверами доступа удаленные пользователи аутентифицируются через сервер RADIUS, который оптимизирован для работы с системой безопасности Kerberos.
- Сети, в которых пользователь должен иметь доступ только к одной услуге. Используя RADIUS, вы можете контролировать доступ пользователей к одному хосту, к одной утилите, такой как Telnet, или к одному протоколу, такому как протокол двухточечной связи (PPP). Например, когда пользователь входит в систему, RADIUS определяет, что этот пользователь имеет право запускать PPP с использованием IP-адреса 10.2.3.4, и реализуется определенный список управления доступом.
- Сети, требующие учета ресурсов. Вы можете использовать учет RADIUS независимо от аутентификации или авторизации RADIUS. Функции учета RADIUS позволяют отправлять данные в начале и в конце сеанса, указывая количество ресурсов (таких как время, пакеты, байты и т. д.), использованных во время сеанса. Поставщик услуг Интернета (ISP) может использовать бесплатную версию программного обеспечения для контроля доступа и учета RADIUS для реализации требований в области безопасности и выставления счетов.

RADIUS не совместим с определенными сетевыми условиями:

- Среда мультипротокольного доступа. RADIUS не поддерживает следующие протоколы:
  - удаленный доступ AppleTalk (ARA);
  - протокол управления кадрами NetBIOS (NBFCP).
- Интерфейс асинхронных служб NetWare (NASI).
- Соединения X.25 PAD.
- В условиях работы «коммутатор-коммутатор» RADIUS не обеспечивает двустороннюю аутентификацию.
- Сети, использующие различные услуги. RADIUS обычно привязывает пользователя к одной модели обслуживания.



### 19.1.2 Принцип работы

Когда пользователь пытается войти и аутентифицироваться на сервере доступа с помощью RADIUS, выполняются следующие действия:

1. Пользователю предлагается ввести имя пользователя и пароль.
2. Имя пользователя и зашифрованный пароль отправляются по сети на сервер RADIUS.
3. Пользователь получает один из следующих ответов от сервера RADIUS:

**ACCEPT:** пользователь аутентифицирован.

**REJECT:** пользователь не аутентифицирован и ему предлагается повторно ввести имя пользователя и пароль, или доступ запрещен.

**CHALLENGE:** сервером RADIUS выдается запрос для сбора дополнительных данных от пользователя.

**CHANGE PASSWORD:** сервер RADIUS отправляет пользователю запрос на выбор нового пароля.

Ответ ACCEPT или REJECT связан с дополнительными данными, которые используются для EXEC или сетевой авторизации. Вы должны сначала пройти аутентификацию RADIUS, прежде чем использовать авторизацию RADIUS. Дополнительные данные, включенные в пакеты ACCEPT или REJECT, содержат следующее:

- а) службы, к которым пользователь может получить доступ, включая Telnet, rlogin или локальные транспортные соединения (LAT), а также службы PPP, Serial Line Internet Protocol (SLIP) или EXEC;
- б) параметры подключения, включая IP-адрес хоста или клиента, список доступа и таймауты пользователя.

## 19.2 Настройка RADIUS

Чтобы настроить RADIUS на удаленном устройстве или сервере доступа, вы должны выполнить следующие действия:

- Используйте команду **aaa authentication** в режиме глобальной конфигурации для определения списков методов аутентификации RADIUS. Дополнительные сведения об использовании команды см. в разделе «Настройка аутентификации».
- Используйте линейные и интерфейсные команды, чтобы разрешить использование определенных списков методов. Дополнительные сведения см. в разделе «Настройка аутентификации».

Следующие действия при настройке являются необязательными:

- При необходимости запустите команду **aaa authorization** в режиме глобальной конфигурации, чтобы авторизовать запрос пользователя на обслуживание. Дополнительные сведения об использовании команды см. в разделе «Настройка авторизации».



- При необходимости запустите **aaa accounting record** в режиме глобальной конфигурации для отслеживания и документирования действий пользователей на устройстве.

## Задачи настройки RADIUS

- Настройка связи с сервером RADIUS
- Настройка коммутатора под атрибуты RADIUS, специфичные для поставщика
- Назначение RADIUS для аутентификации
- Назначение RADIUS для авторизации
- Назначение RADIUS для учета

### 19.2.1 Настройка связи коммутатора с сервером RADIUS

Хост RADIUS обычно представляет собой многопользовательскую систему с программным обеспечением сервера RADIUS от Livingston, Merit, Microsoft или другого поставщика программного обеспечения. Сервер RADIUS и коммутатор используют общую секретную текстовую строку для шифрования паролей и обмена ответами. Чтобы настроить RADIUS для использования команд безопасности AAA, необходимо указать хост, на котором запущена служба сервера RADIUS, и секретную текстовую строку (ключ), которую он использует совместно с маршрутизатором.

Чтобы настроить взаимодействие с RADIUS-сервером для каждого сервера, используйте следующую команду в режиме глобальной конфигурации:

| Команда  | Описание  |
|--|---|
| <b>radius-server host</b> <i>ip-address</i> [ <b>auth-port</b> <i>port-number</i> ][ <b>acct-port</b> <i>port-number</i> ] | Задаёт IP-адрес или имя хоста удаленного узла RADIUS-сервера и назначает номера целевых портов для аутентификации и учета |
| <b>radius-server key</b> <i>string</i>   | Задаёт общую текстовую строку секретного ключа, используемую маршрутизатором и RADIUS-сервером                            |

Чтобы настроить глобальные коммуникационные параметры между маршрутизатором и RADIUS-сервером, используйте следующие команды в режиме глобальной конфигурации:

| Команда  | Описание  |
|--|---|
| <b>radius-server retransmit</b> <i>retries</i> | Указывает, сколько раз коммутатор передает серверу каждый запрос RADIUS, прежде чем прекратить запросы (по умолчанию – 2) |



|  |   |
|--|---|
| <b>radius-server timeout</b> <i>seconds</i>  | Указывает, в течение скольких секунд коммутатор ожидает ответа на запрос RADIUS, прежде чем повторно передать запрос                                      |
| <b>radius-server deadtime</b> <i>minutes</i> | Устанавливает время (в минутах), в течение которого устройство не будет пытаться повторно связаться с удаленным RADIUS-сервером после его сбоя или отказа |

## 19.2.2 Настройка коммутатора под атрибуты RADIUS, специфичные для поставщика

Проект стандарта Internet Engineering Task Force (IETF) определяет метод передачи информации о поставщике между сервером доступа к сети и сервером RADIUS с использованием атрибута поставщика (атрибут 26). Атрибуты, специфичные для поставщика (VSA), позволяют поставщикам поддерживать свои собственные расширенные функции, не подходящие для общего использования. Дополнительные сведения об идентификаторах поставщиков и VSA см. в документе RFC 2138, Remote Authentication Dial-In User Service (RADIUS). Чтобы настроить сервер доступа к сети для распознавания и использования VSA, используйте следующую команду в режиме глобальной конфигурации:

| Команда  | Описание   |
|--|--|
| <b>radius-server vsa send</b> [authentication] | Позволяет серверу доступа к сети распознавать и использовать VSA в соответствии с атрибутом 26 RADIUS IETF |

## 19.2.3 Назначение RADIUS для аутентификации

После определения сервера RADIUS и определения ключа аутентификации RADIUS необходимо определить списки методов для аутентификации RADIUS. Поскольку аутентификация RADIUS инициируется с помощью AAA, вы должны ввести команду **aaa authentication**, указав RADIUS в качестве метода аутентификации. Дополнительные сведения см. в разделе «Настройка аутентификации».

## 19.2.4 Назначение RADIUS для авторизации

Авторизация AAA позволяет установить параметры, ограничивающие доступ пользователя к сети. Авторизация с использованием RADIUS обеспечивает один метод управления удаленным доступом, включая однократную авторизацию или авторизацию для каждой службы, список и профиль учетных записей для каждого пользователя, поддержку групп пользователей и поддержку IP, IPX, ARA и Telnet. Поскольку авторизация RADIUS



инициируется с помощью AAA, вы должны выполнить команду **aaa authorization**, указав RADIUS в качестве метода авторизации. Подробнее см. в разделе «Настройка авторизации».

### 19.2.5 Назначение RADIUS для учета

Функция учета AAA позволяет отслеживать, к каким услугам пользователи обращаются, а также объем потребляемых ими сетевых ресурсов. Поскольку учет RADIUS инициируется с помощью AAA, вы должны выполнить команду **aaa accounting**, указав RADIUS в качестве метода учета. Дополнительные сведения см. в разделе «Настройка учета».

## 19.3 Примеры настройки RADIUS

### 19.3.1 Пример аутентификации RADIUS

В следующем примере показано, как настроить коммутатор для аутентификации и авторизации с использованием RADIUS:

```
aaa authentication login use-radius group radius local
```

Эта команда настраивает удаленное устройство на использование RADIUS для аутентификации при подсказке входа в систему. Если RADIUS возвращает ошибку, пользователь аутентифицируется с использованием локальной базы данных. В этом примере `use-radius` – это имя списка методов, в котором указывается группа серверов RADIUS, а затем – локальная аутентификация.

### 19.3.2 Применение RADIUS в AAA

В следующем примере показана общая настройка с использованием RADIUS и набора команд AAA:

```
radius-server host 1.2.3.4  
radius-server key myRaDiUSpassWoRd  
username root password AlongPassword  
aaa authentication login admins group radius local  
line vty 1 16  
login authentication admins
```

Значение команд показано ниже:

Команда **radius-server host** используется для указания IP-адреса сервера RADIUS.

Команда **radius-server key** используется для указания общего ключа между сервером доступа к сети и сервером RADIUS.

Команда **aaa authentication login admins group radius local** определяет список методов аутентификации «admins», который указывает на аутентификацию RADIUS, а затем (если сервер RADIUS не отвечает) будет использоваться локальная аутентификация на последовательных линиях с использованием PPP.



Команда **login authentication admins** используются для обозначения применения списка методов «admins» во время входа в систему.

## 20. Веб-аутентификация

В разделе описывается концепция веб-аутентификации, а также ее настройка и использование.

### 20.1 Введение

#### 20.1.1 Описание

Веб-аутентификация коммутатора представляет собой режим управления соединением, как PPPoE и 802.1x. При использовании веб-аутентификации операции входа и выхода могут быть успешно выполнены посредством взаимодействия браузера и встроенного порталного сервера коммутатора. Во время операций входа и выхода не требуется никакое другое клиентское программное обеспечение.

#### 1. Роли устройств

Роли, которые сетевые устройства выполняют во время веб-аутентификации, показаны на рисунке 21:

- **Клиент** – это пользовательский компьютер, который получает доступ к сети через коммутатор. Пользовательский компьютер должен иметь настроенный сетевой браузер, функцию DHCP-клиента и возможность создания DNS-запросов.
- **Сервер DHCP** – это устройство, предназначенное для распределения IP-адресов между пользователями.
- **Сервер AAA** – это устройство, предназначенное для сохранения информации о правах пользователей и ведения журналов сессий пользователей, включая время начала и окончания сеанса.
- **Коммутатор** – это коммутатор с веб-аутентификацией. Он предназначен для управления правами доступа пользователей и работает как агент между пользователями и AAA-сервером.

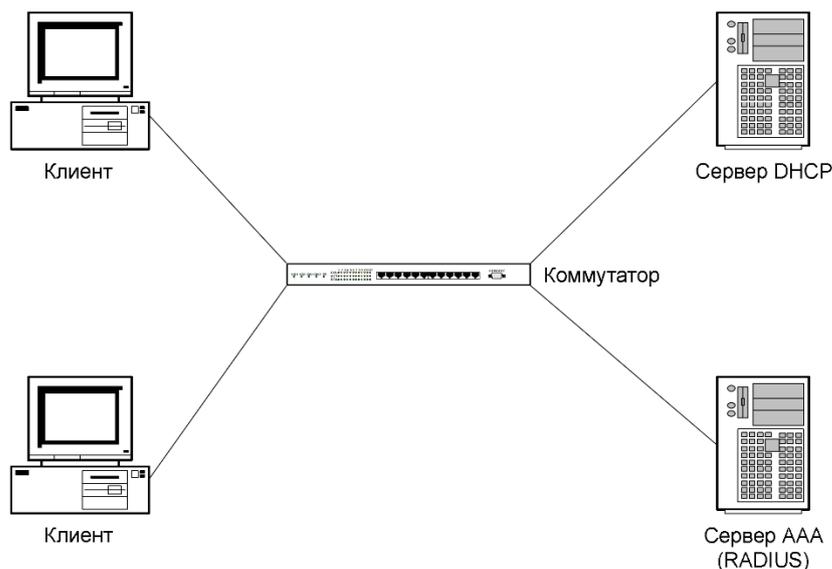


Рисунок 21 – Топология сети для веб-аутентификации

## 2. Поток данных аутентификации

В соответствии с различными стратегиями конфигурации поток данных веб-аутентификации коммутатора может относиться к таким протоколам, как DHCP и DNS. Типовой поток показан на рисунке 22. Алгоритм процедуры обычно следующий:

- 1) DHCP-сервер отправляет запрос подтверждения пользователю через коммутатор после того, как пользователь инициирует процесс распределения DHCP-адресов. Затем коммутатор идентифицирует и регистрирует пользователя.
- 2) Пользователь заходит на любой веб-сайт через браузер (введите доменное имя, а не IP-адрес в адресной строке браузера), что активирует DNS-запрос пользовательского компьютера.
- 3) DNS-сервер возвращает пользователю ответ на запрос. Коммутатор перехватывает это сообщение и изменяет разрешенный адрес на адрес своего встроенного portalного сервера.
- 4) Процесс подтверждения DHCP продолжается после того, как браузер захватывает разрешение DNS. Получив запрос, коммутатор возвращает страницу аутентификации в соответствии с различными методами.
- 5) Пользователь отправляет запрос на аутентификацию; коммутатор аутентифицирует пользователя через сервер AAA после получения информации, отправленной пользователем. Если аутентификация прошла успешно, сервер AAA будет уведомлен о начале пользовательской сессии. Коммутатор предоставляет пользователю право доступа к сети и возвращает ему страницу с сообщением об успешной аутентификации; в то же время коммутатор также возвращает страницу подтверждения активности, которая периодически отправляет коммутатору уведомление о том, что пользователь находится в сети.



- 6) Пользователь через браузер отправляет коммутатору запрос на выход из системы. В ответ коммутатор уведомляет сервер AAA об окончании сессии и отзывает у пользователя право доступа к сети.
- 7) После успешной аутентификации пользователя коммутатор отслеживает его активность в сети до тех пор, пока пользователь не выполнит выход. Если в течение заданного времени коммутатор не получает уведомление о том, что пользователь все еще онлайн, он считает, что пользователь вышел из системы ненормально, уведомляет сервер AAA об окончании сессии и отзывает у пользователя право доступа к сети.

Вышеуказанные шаги могут немного отличаться в зависимости от стратегий конфигурации и действий пользователя. Например, если пользователь напрямую обращается к серверу портала коммутатора до того, как аутентификация будет одобрена, процессы, связанные с DNS, не будут включены.

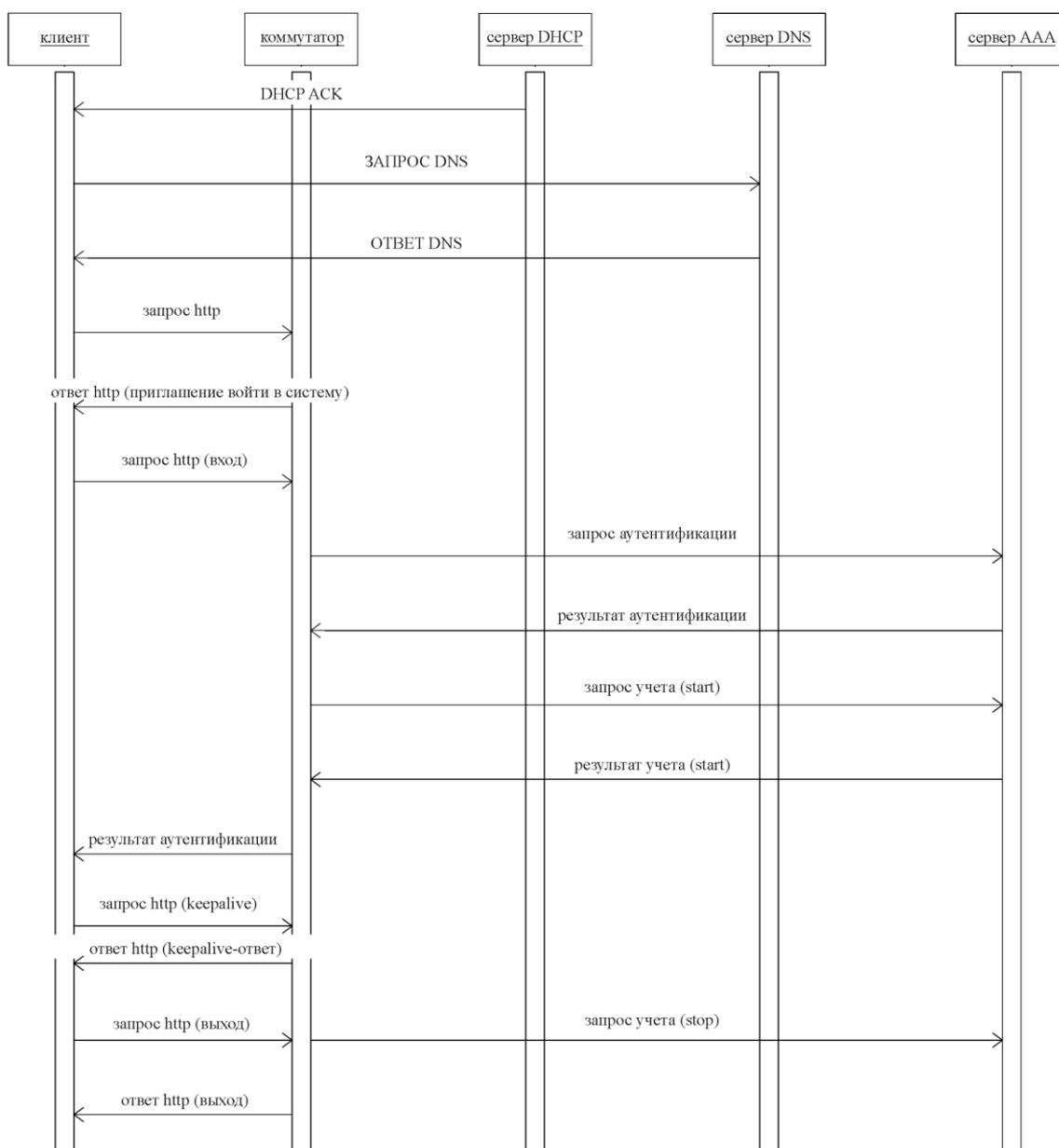


Рисунок 22 – Обмен сообщениями при веб-аутентификации



## 20.1.2 Подготовка к настройке

### 1. Планирование режима аутентификации

Для управления доступом пользователя предусмотрено два режима аутентификации:

Режим аутентификации по имени пользователя/паролю: в этом режиме коммутатор идентифицирует пользователя по имени и паролю и уведомляет сервер AAA о начале пользовательского сеанса. При входе пользователю необходимо ввести свое имя и пароль через браузер.

Режим аутентификации по VLAN ID: в этом режиме коммутатор идентифицирует пользователя по идентификатору VLAN, к которому тот принадлежит, и уведомляет сервер AAA о начале пользовательского сеанса в соответствии с идентификатором VLAN. пользователю требуется только подтвердить соответствующие операции на веб-странице перед доступом к сети.

Различные стратегии работы предполагают использование различных режимов аутентификации. Поддерживаемое максимальное количество пользователей, которые одновременно получают доступ к сети, зависит от выбранного режима. Для аутентификации по имени пользователя/паролю коммутатор поддерживает настолько большое одновременное количество пользователей, насколько позволяет его производительность. Для режима аутентификации по VLAN ID максимальное количество одновременно получающих доступ пользователей равно количеству VLAN, поддерживаемых коммутатором.

### 2. Планирование топологии сети

Коммутатор использует интерфейс маршрутизации в качестве единицы для установки атрибута аутентификации. Если функция веб-аутентификации включена на интерфейсе маршрутизации, сетевой доступ через него полностью контролируется веб-аутентификацией. Серверы DHCP, DNS и AAA должны подключаться к коммутатору через интерфейс с отключенной функцией веб-аутентификации. На рисунке 23 показана типовая рабочая топология сети.

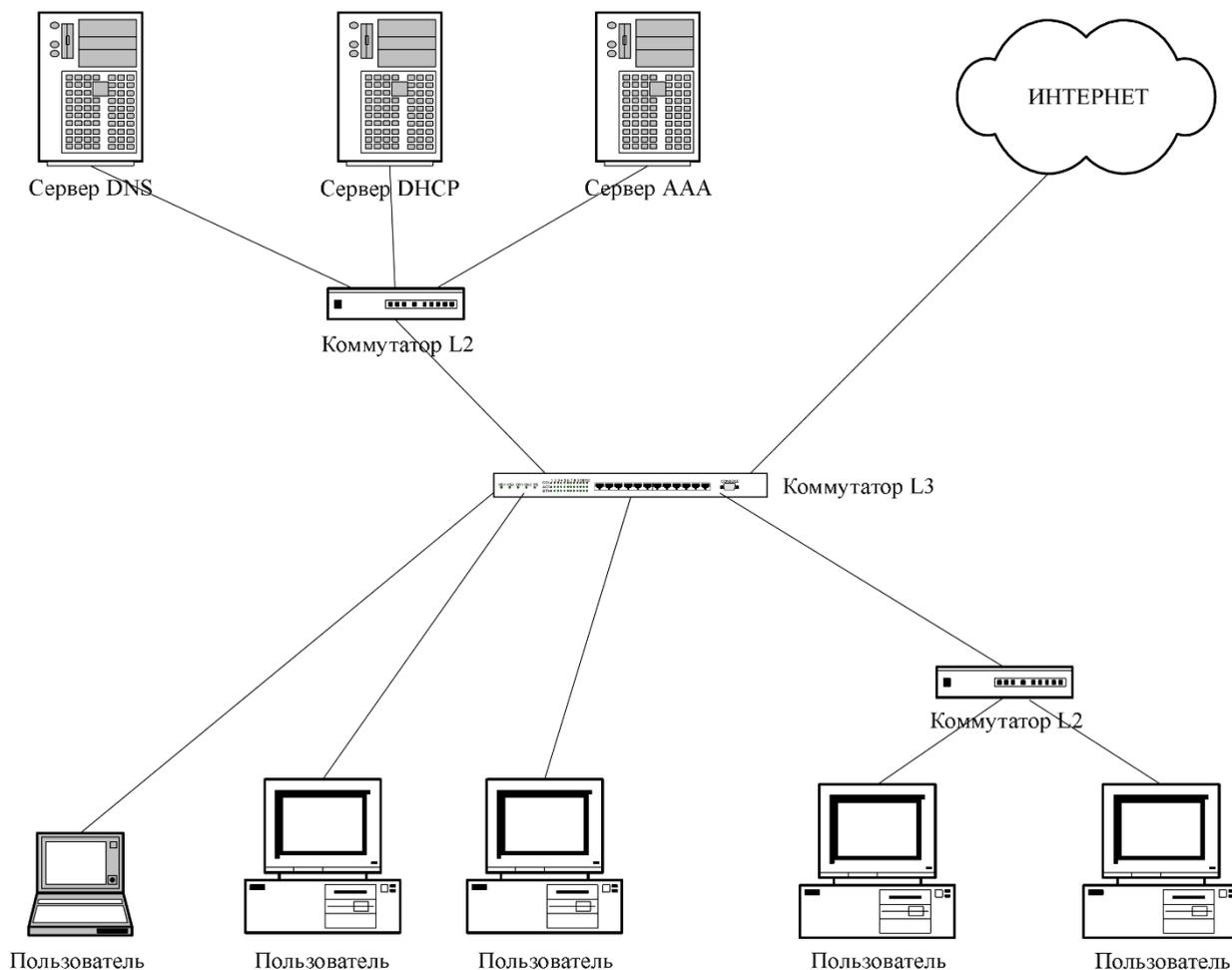


Рисунок 23 – Сетевая топология

## 20.2 Настройка веб-аутентификации

### 20.2.1 Глобальная конфигурация

#### 1. Настройка адреса сервера портала

Выполните следующую команду в режиме глобальной конфигурации, чтобы настроить адрес порталного сервера:

| Команда                               | Описание                           |
|---------------------------------------|------------------------------------|
| <b>web-auth portal-server A.B.C.D</b> | Задаёт IP-адрес порталного сервера |

#### 2. Настройка длительности аутентификации



Параметр **authtime** определяет максимальное время аутентификации пользователя. Если аутентификация не одобрена в течение максимального времени, коммутатор завершает процедуру.

Выполните следующую команду в режиме глобальной конфигурации, чтобы настроить длительность аутентификации (единица измерения – секунда):

| Команда                                   | Описание  |
|---|---|
| <b>web-auth authtime &lt;60-65535&gt;</b> | Указывает максимальную длительность процесса аутентификации |

### 3. Настройка периода передачи онлайн-уведомления

С помощью онлайн-уведомления, отправляемого браузером, коммутатор проверяет, находится ли пользователь в сети.

Выполните следующую команду в режиме глобальной конфигурации, чтобы настроить период передачи (единица измерения – секунда):

| Команда                                     | Описание                                       |
|---|--|
| <b>web-auth keep-alive &lt;60-65535&gt;</b> | Указывает периода передачи сообщения keepalive |

### 4. Настройка времени удержания

Если коммутатор не получает онлайн-уведомление пользователя от браузера в течение установленного периода времени, коммутатор считает, что пользователь вышел из системы, и сеанс завершен некорректно.

Выполните следующую команду в режиме глобальной конфигурации, чтобы настроить продолжительность сеанса после прекращения получения сообщений keepalive от пользователя:

| Команда                                   | Описание                  |
|---|---------------------------|
| <b>web-auth holdtime &lt;60-65535&gt;</b> | Указывает время удержания |

### 5. Настройка пароля для аутентификации на основе VLAN ID

Когда режим аутентификации установлен на VLAN ID, коммутатор принимает **vlan n** в качестве имени пользователя, где **n** представляет соответствующий порядковый номер VLAN. Все пользователи используют один и тот же пароль.

Выполните следующую команду в режиме глобальной конфигурации, чтобы настроить пароль для аутентификации на основе VLAN ID:



| Команда                              | Описание  |
|--------------------------------------|---|
| <b>web-auth vlan-password</b> <WORD> | Настраивает пароль для аутентификации на основе VLAN ID |

## 20.2.2 Настройка интерфейса

### 1. Настройка режима аутентификации

Коммутатор обеспечивает два режима аутентификации: имя пользователя/пароль и VLAN ID.

Выполните следующую команду в режиме настройки интерфейса, чтобы указать режим аутентификации:

| Команда                             | Описание                         |
|-------------------------------------|----------------------------------|
| <b>web-auth mode user   vlan-id</b> | Настраивает режим аутентификации |

### 2. Настройка методов аутентификации

К каждому интерфейсу могут применяться различные методы аутентификации. По умолчанию ко всем интерфейсам применяется список методов с именем **default**.

Выполните следующую команду в режиме настройки интерфейса, чтобы указать метод аутентификации:

| Команда                             | Описание                         |
|-------------------------------------|----------------------------------|
| <b>web-auth authentication</b> WORD | Настраивает метод аутентификации |

### 3. Настройка методов учета

К каждому интерфейсу могут применяться различные методы учета. По умолчанию ко всем интерфейсам применяется список методов с именем **default**.

Выполните следующую команду в режиме настройки интерфейса, чтобы указать метод учета:

| Команда                         | Описание                |
|---------------------------------|-------------------------|
| <b>web-auth accounting</b> WORD | Настраивает метод учета |



### 20.2.3 Включение веб-аутентификации

Если глобальная конфигурация и конфигурация интерфейса удовлетворяют требованиям, вы можете включить веб-аутентификацию на выбранном порту маршрутизации.

Выполните следующую команду в режиме настройки интерфейса, чтобы включить веб-аутентификацию:

| Команда                | Описание                    |
|------------------------|-----------------------------|
| <b>web-auth enable</b> | Включает веб-аутентификацию |

## 20.3 Мониторинг и поддержка веб-аутентификации

### 20.3.1 Проверка глобальной конфигурации

Запустите следующую команду в привилегированном режиме, чтобы проверить глобальную конфигурацию:

| Команда              | Описание                           |
|----------------------|------------------------------------|
| <b>show web-auth</b> | Отображает глобальную конфигурацию |

### 20.3.2 Проверка конфигурации интерфейса

Запустите следующую команду в режиме настройки интерфейса, чтобы проверить конфигурацию порта:

| Команда   | Описание                           |
|---|------------------------------------|
| <b>show web-auth interface [vlan   supervlan] &lt;vlan-id&gt;</b> | Отображает конфигурацию интерфейса |

### 20.3.3 Проверка состояния пользователей

Запустите следующую команду в привилегированном режиме, чтобы просмотреть подключенных пользователей:

| Команда                   | Описание                                      |
|---------------------------|---|
| <b>show web-auth user</b> | Отображает информацию о текущих пользователях |



## 20.3.4 Принудительное отключение пользователей

Запустите следующую команду в режиме глобальной конфигурации, чтобы принудительно отключить пользователя:

| Команда                                     | Описание                             |
|---|--------------------------------------|
| <b>web-auth kick-out user-ip ip-address</b> | Принудительно отключает пользователя |

## 20.4 Пример настройки веб-аутентификации

Топология сети изображена на следующем рисунке:

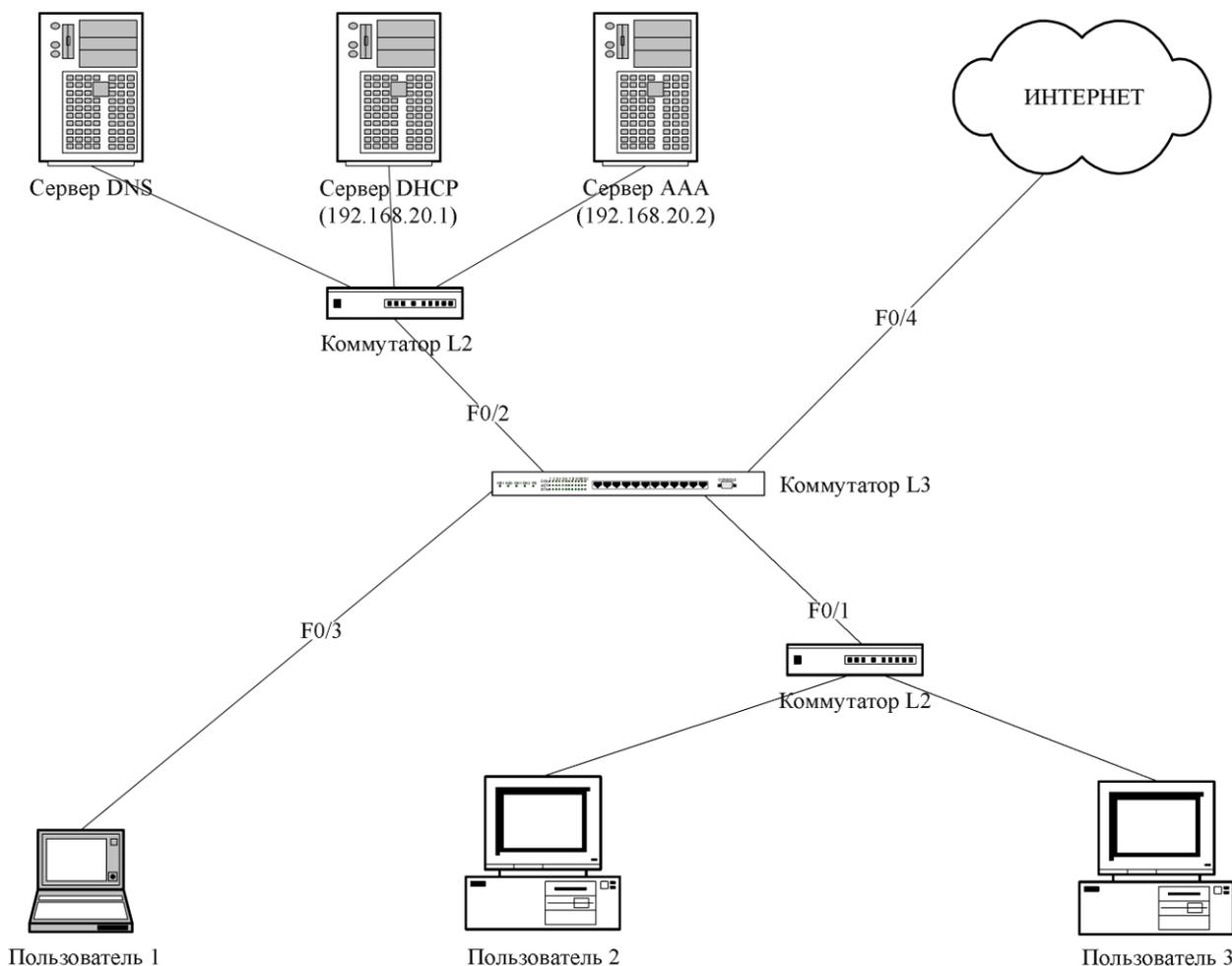


Рисунок 24 – Топология сети

### ➤ Глобальная конфигурация

```
aaa authentication login auth-weba radius
aaa accounting network acct-weba start-stop radius
```



```
!  
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813  
radius-server key 405.10  
!  
ip dhcpd enable  
ip http server  
!  
vlan 1-4  
!  
web-auth portal-server 192.168.20.41  
web-auth holdtime 3600  
web-auth authtime 600  
web-auth keep-alive 180
```

➤ **Настройка интерфейсов второго уровня**

```
interface FastEthernet0/1  
switchport pvid 1  
!  
interface FastEthernet0/2  
switchport pvid 2  
!  
interface FastEthernet0/3  
switchport pvid 3  
!  
interface FastEthernet0/4  
switchport pvid 4
```

➤ **Настройка интерфейсов маршрутизации**

```
interface VLAN1  
no ip directed-broadcast  
ip helper-address 192.168.20.1  
web-auth accounting acct-weba  
web-auth authentication auth-weba
```



```
web-auth mode vlan-id
web-auth enable
!
interface VLAN2
ip address 192.168.20.41 255.255.255.0
no ip directed-broadcast
!
interface VLAN3
no ip directed-broadcast
ip helper-address 192.168.20.1
web-auth accounting acct-weba
web-auth authentication auth-weba
web-auth mode user
web-auth enable
!
interface VLAN4
no ip directed-broadcast
!
```

## 21. DHCP Snooping

DHCP Snooping предназначен для предотвращения действий поддельных DHCP-серверов, которые могут предоставлять DHCP-сервис, путем анализа DHCP-пакетов и поддержания связи между MAC- и IP-адресами. Это механизм, который следит за DHCP-пакетами в сети. Он определяет, какие устройства в сети могут предоставлять DHCP-сервис и сохраняет соответствие между MAC- и IP-адресами. Кроме того, на основе этой связи адресов, коммутаторы L2 могут выполнять функции Dynamic ARP Inspection (DAI) и IP Source Guard для повышения безопасности сети. Если пакеты не соответствуют этой связи между MAC и IP, то они фильтруются, что помогает предотвратить сетевые атаки со стороны несанкционированных пользователей.

Задачи настройки

- Включение/выключение функции DHCP Snooping
- Включение DHCP Snooping в VLAN
- Настройка интерфейса в качестве доверенного порта DHCP
- Включение DAI в VLAN
- Настройка интерфейса в качестве доверенного порта ARP



- Включение мониторинга исходного IP-адреса в VLAN
- Настройка интерфейса, доверенного для мониторинга исходного IP-адреса
- Настройка TFTP-сервера для резервного копирования привязок адресов
- Настройка имени файла для резервного копирования привязок адресов
- Настройка интервала резервного копирования привязок адресов
- Настройка или добавление привязки вручную
- Мониторинг и поддержка DHCP Snooping
- Пример настройки DHCP Snooping

## 21.1 Включение/выключение функции DHCP Snooping

Выполните следующие команды в режиме глобальной конфигурации:

| Команда                          | Описание                               |
|----------------------------------|--|
| <b>ip dhcp-relay snooping</b>    | Включает DHCP Snooping                 |
| <b>no ip dhcp-relay snooping</b> | Восстанавливает настройки по умолчанию |

Эта команда используется для включения отслеживания DHCP в режиме глобальной конфигурации. После выполнения этой команды коммутатор должен отслеживать все пакеты DHCP и формировать соответствующие отношения привязки.



Если клиент получает от коммутатора адрес до выполнения этой команды, коммутатор не сможет добавить соответствующее отношение привязки.

## 21.2 Включение DHCP Snooping в VLAN

Если в VLAN включено отслеживание DHCP, пакеты DHCP, полученные от всех недоверенных физических портов в VLAN, будут проверяться. Ответные сообщения DHCP, полученные от недоверенных физических портов в VLAN, будут отброшены, что не позволит поддельному или неправильно настроенному DHCP-серверу предоставлять услуги распределения адресов. Что запросов DHCP от недоверенных портов, если поле аппаратного адреса в пакете запроса не соответствует MAC-адресу этого пакета, пакет запрос считается поддельным и используемым в качестве пакета для атаки DHCP DoS. Коммутатор отбросит такой пакет.

Выполните следующие команды в режиме глобальной конфигурации:



| Команда  | Описание                       |
|--|--------------------------------|
| <b>ip dhcp-relay snooping vlan <i>vlan_id</i></b>    | Включает DHCP Snooping в VLAN  |
| <b>no ip dhcp-relay snooping vlan <i>vlan_id</i></b> | Отключает DHCP Snooping в VLAN |

## 21.3 Настройка интерфейса в качестве доверенного порта DHCP

Если интерфейс настроен в качестве доверенного порта DHCP, пакеты DHCP, полученные от этого интерфейса, не будут проверяться.

Выполните следующие команды в режиме настройки интерфейса:

| Команда                       | Описание  |
|-------------------------------|---|
| <b>dhcp snooping trust</b>    | Настройка интерфейса в качестве доверенного порта DHCP  |
| <b>no dhcp snooping trust</b> | Возвращение интерфейса в режим недоверенного порта DHCP |

По умолчанию интерфейс является недоверенным.

## 21.4 Включение DAI в VLAN

Когда динамический мониторинг ARP (DAI) проводится на всех физических портах VLAN, полученный пакет ARP будет отклонен, если исходный MAC-адрес и исходный IP-адрес этого пакета не совпадают с настроенным соотношением привязки MAC-IP. Отношения привязки на интерфейсе могут быть динамически связаны с помощью DHCP или настроены вручную. Если ни один MAC-адрес не привязан к IP-адресу на физическом интерфейсе, коммутатор отклоняет пересылку всех пакетов ARP.

| Команда  | Описание   |
|--|--|
| <b>ip arp inspection vlan <i>vlanid</i></b>    | Включает динамический мониторинг ARP на всех недоверенных портах в VLAN  |
| <b>no ip arp inspection vlan <i>vlanid</i></b> | Отключает динамический мониторинг ARP на всех недоверенных портах в VLAN |



## 21.5 Настройка интерфейса в качестве доверенного порта ARP

Функция DAI не работает на доверенных интерфейсах. По умолчанию интерфейсы являются недоверенными.

Выполните следующие команды в режиме настройки интерфейса:

| Команда                        | Описание  |
|--------------------------------|---|
| <b>arp inspection trust</b>    | Настройка интерфейса в качестве доверенного порта ARP |
| <b>no arp inspection trust</b> | Восстановление настройки по умолчанию                 |

## 21.6 Включение мониторинга исходного IP-адреса в VLAN

После включения мониторинга IP-адреса источника в VLAN IP-пакеты, полученные от всех физических портов в VLAN, будут отклонены, если их MAC- и IP-адреса источника не совпадают с настроенным соотношением привязки MAC-IP. Отношения привязки на интерфейсе могут быть динамически связаны с помощью DHCP или настроены вручную. Если ни один MAC-адрес не привязан к IP-адресу на физическом интерфейсе, коммутатор отклоняет пересылку всех IP-пакетов, полученных от физического интерфейса.

Выполните следующие команды в режиме глобальной конфигурации:

| Команда                                       | Описание  |
|---|---|
| <b>ip verify source vlan <i>vlanid</i></b>    | Включает проверку IP-адреса источника на всех недоверенных интерфейсах в VLAN |
| <b>no ip verify source vlan <i>vlanid</i></b> | Отключает проверку IP-адреса источника на всех интерфейсах VLAN               |



Если пакет DHCP (также IP-пакет) получен, он будет перенаправлен, поскольку настроено глобальное отслеживание.

## 21.7 Настройка интерфейса, доверенного для мониторинга исходного IP-адреса



Функция определения исходного адреса не будет включена для доверенного интерфейса.

Выполните следующие команды в режиме настройки интерфейса:

| Команда                   | Описание   |
|---------------------------|--|
| <b>ip-source trust</b>    | Настройка интерфейса, которому доверяет мониторинг IP-адреса источника |
| <b>no ip-source trust</b> | Восстановление настройки по умолчанию                                  |

## 21.8 Настройка TFTP-сервера для резервного копирования привязок адресов

После сохранения конфигурации коммутатора и его перезагрузки ранее настроенные привязки портов больше не существуют. В этом случае, если включена функция мониторинга исходного IP-адреса, коммутатор не сможет пересылать IP-сообщения, так как не найдет соответствующую привязку. Если настроить TFTP-сервер для резервного копирования связей интерфейсов, связи будут скопированы на сервер через протокол TFTP. После перезагрузки коммутатор автоматически загрузит список связей с TFTP-сервера, обеспечивая нормальное функционирование сети.

Выполните следующие команды в режиме глобальной конфигурации:

| Команда  | Описание   |
|--|--|
| <b>ip dhcp-relay snooping database-agent ip-address</b>    | Настраивает IP-адрес TFTP-сервера, который должен резервировать привязки интерфейсов |
| <b>no ip dhcp-relay snooping database-agent ip-address</b> | Отменяет использование TFTP-сервера для резервного копирования привязок интерфейсов  |



## 21.9 Настройка имени файла для резервного копирования привязок адресов

При резервном копировании отношений привязки интерфейсов файл с соответствующим именем будет сохранен на TFTP-сервере. Таким образом, разные коммутаторы могут создавать резервные копии своих собственных привязок на одном и том же TFTP-сервере.

Выполните следующие команды в режиме глобальной конфигурации:

| Команда                                    | Описание   |
|--|--|
| <b>ip dhcp-relay snooping db-file name</b> | Настраивает имя файла для резервной копии привязки интерфейсов |
| <b>no ip dhcp-relay snooping db-file</b>   | Удаляет имя файла  |

## 21.10 Настройка интервала резервного копирования привязок адресов

Отношения привязки MAC-IP на интерфейсах изменяются динамически. Следовательно, необходимо проверять, обновляются ли отношения привязки через определенный интервал. Если таблица обновляется (добавляются или удаляются записи привязки), необходимо снова создать резервную копию. Временной интервал по умолчанию составляет 30 минут.

Выполните следующие команды в режиме глобальной конфигурации:

| Команда                                 | Описание   |
|---|--|
| <b>ip dhcp-relay snooping write num</b> | Настраивает интервал проверки резервной копии привязки интерфейсов. Единица измерения – минута |
| <b>no ip dhcp-relay snooping write</b>  | Возвращает интервал проверки привязки интерфейса к настройкам по умолчанию                     |

## 21.11 Ручная настройка привязки интерфейса

Если хосты не получают адреса через DHCP, вы можете добавить элементы привязки на интерфейс коммутатора, чтобы разрешить хосту доступ к сети.

Обратите внимание, что элементы привязки, настроенные вручную, имеют более высокий приоритет, чем элементы привязки, настроенные динамически. Если элемент привязки,



настроенный вручную, и элемент привязки, настроенный динамически, имеют один и тот же MAC-адрес, элемент, настроенный вручную, заменит собой динамически настроенный элемент. Элемент привязки интерфейса принимает MAC-адрес в качестве уникального индекса.

Выполните следующие команды в режиме глобальной конфигурации:

| Команда  | Описание                                |
|--|---|
| <b>ip source binding MAC IP interface name</b> | Настраивает привязку интерфейса вручную |
| <b>no ip source binding MAC IP</b>             | Отменяет элемент привязки интерфейса    |

## 21.12 Мониторинг и поддержка DHCP Snooping

Выполните следующие команды в режиме управления:

| Команда  | Описание   |
|--|--|
| <b>show ip dhcp-relay snooping</b>                           | Отображает информацию о конфигурации DHCP Snooping   |
| <b>show ip dhcp-relay snooping binding</b>                   | Отображает действующие элементы адресной привязки на интерфейсе  |
| <b>show ip dhcp-relay snooping binding all</b>               | Отображает все элементы привязки, созданные DHCP Snooping  |
| <b>[no] debug ip dhcp-relay [snooping   binding   event]</b> | Используется для управления отладочной информацией, связанной с ретрансляцией DHCP на коммутаторе, и может быть настроена для отслеживания конкретных событий или аспектов этой ретрансляции |

Отображение информации о настройках DHCP Snooping:

```
switch# show ip dhcp-relay snooping
```

```
ip dhcp-relay snooping vlan 3
```

```
ip arp inspection vlan 3
```

```
DHCP Snooping trust interface:
```

```
FastEthernet0/1
```

```
ARP Inspect interface:
```



FastEthernet0/11

Отображение информации о привязках DHCP Snooping на интерфейсе:

```
switch# show ip dhcp-relay snooping binding
```

| Hardware Address  | IP Address  | remainder time | Type    | VLAN | interface       |
|-------------------|-------------|----------------|---------|------|-----------------|
| 00-e0-0f-26-23-89 | 192.2.2.101 | 86400          | DHCP_SN | 3    | FastEthernet0/3 |

Отображение информации обо всех привязках DHCP Snooping:

```
switch# show ip dhcp-relay snooping binding all
```

| Hardware Address  | IP Address  | remainder time | Type    | VLAN | interface       |
|-------------------|-------------|----------------|---------|------|-----------------|
| 00-e0-0f-32-1c-59 | 192.2.2.1   | infinite       | MANUAL  | 1    | FastEthernet0/2 |
| 00-e0-0f-26-23-89 | 192.2.2.101 | 86400          | DHCP_SN | 3    | FastEthernet0/3 |

Отладочная информация DHCP Snooping:

```
switch# debug ip DHCP Snooping packet
```

```
DHCPR: receive l2 packet from vlan 3, diID: 3
```

```
DHCPR: DHCP packet len 277
```

```
DHCPR: add binding on interface FastEthernet0/3
```

```
DHCPR: send packet continue
```

```
DHCPR: receive l2 packet from vlan 3, diID: 1
```

```
DHCPR: DHCP packet len 300
```

```
DHCPR: send packet continue
```

```
DHCPR: receive l2 packet from vlan 3, diID: 3
```

```
DHCPR: DHCP packet len 289
```

```
DHCPR: send packet continue
```

```
DHCPR: receive l2 packet from vlan 3, diID: 1
```

```
DHCPR: DHCP packet len 300
```

```
DHCPR: update binding on interface FastEthernet0/3
```

```
DHCPR: IP address: 192.2.2.101, lease time 86400 seconds
```

```
DHCPR: send packet continue
```

## 21.13 Пример настройки DHCP Snooping

Топология сети показана на следующем рисунке:

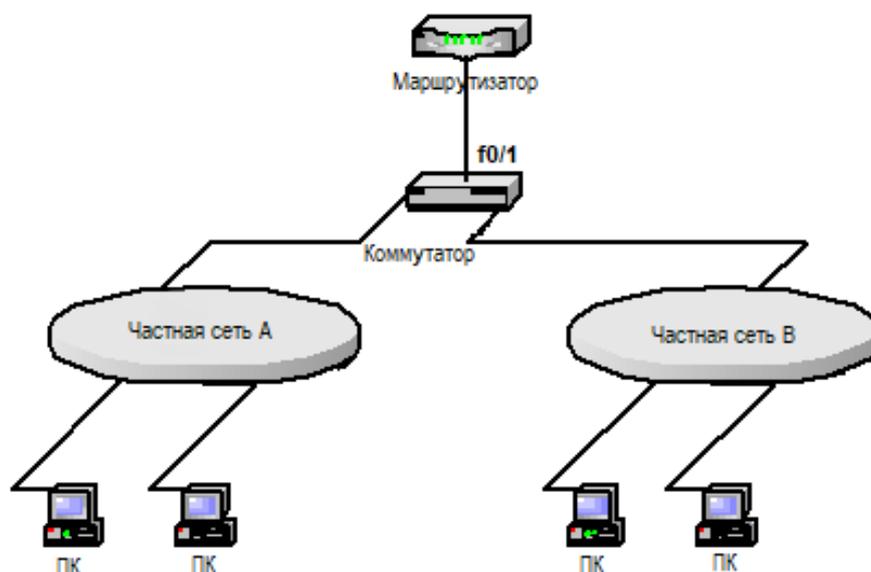


Рисунок 25 – Топология сети

Настройка коммутатора

1. Включите DHCP Snooping в VLAN 1, которая объединяет частную сеть А:

```
Switch_config# ip dhcp-relay snooping
```

```
Switch_config# ip dhcp-relay snooping vlan 1
```

2. Включите DHCP Snooping в VLAN 2, которая объединяет частную сеть В:

```
Switch_config# ip dhcp-relay snooping
```

```
Switch_config# ip dhcp-relay snooping vlan 2
```

3. Укажите доверенный интерфейс, который соединен с DHCP-сервером:

```
Switch_config_g0/1# dhcp snooping trust
```

## 22. LLDP

### 22.1 Введение

LLDP (Link Layer Discovery Protocol) является протоколом, который позволяет устройствам в сети обмениваться информацией о своем состоянии. Каждый агент LLDP передает информацию о себе через свои соединения и может получать информацию о состоянии соседних устройств. Однако агент LLDP не может запрашивать информацию у соседей.

Во время обмена сообщениями передача и прием данных происходят независимо друг от друга, что позволяет настраивать только передачу, только прием или оба процесса одновременно.



LLDP является полезным инструментом для управления сетью, предоставляя администраторам точные данные о топологии сети, трафике и другую информацию для диагностики проблем.

Задачи настройки

- Включение/отключение LLDP
- Настройка времени удержания
- Настройка таймера
- Настройка реинициализации
- Настройка TLV для отправки
- Настройка режима передачи или приема
- Отображение информации LLDP
- Удаление информации LLDP
- Отображение отладочной информации

## 22.2 Включение/отключение LLDP

LLDP по умолчанию отключен. Для включения протокола выполните следующую команду в режиме глобальной конфигурации:

| Команда         | Описание      |
|-----------------|---------------|
| <b>lldp run</b> | Включает LLDP |

Выполните следующую команду, чтобы отключить LLDP:

| Команда            | Описание       |
|--------------------|----------------|
| <b>no lldp run</b> | Выключает LLDP |

## 22.3 Настройка времени удержания

Вы можете контролировать время ожидания передачи сообщения LLDP, изменяя время удержания. Для этого запустите следующую команду в режиме глобальной конфигурации:

| Команда                          | Описание   |
|----------------------------------|--|
| <b>lldp holdtime <i>time</i></b> | Настраивает время ожидания LLDP. Диапазон от: 0 до 65535, по умолчанию 120 с |



|                         |  |
|-------------------------|--|
| <b>no lldp holdtime</b> | Восстанавливает время ожидания по умолчанию, то есть 120 с |
|-------------------------|--|

## 22.4 Настройка таймера

Вы можете контролировать интервал передачи сообщения коммутатором, настроив таймер LLDP. Для этого запустите следующую команду в режиме глобальной конфигурации:

| Команда                | Описание  |
|------------------------|---|
| <b>lldp timer time</b> | Настраивает интервал передачи сообщений LLDP. Значение варьируется от 5 до 65534. Время по умолчанию – 30 с |
| <b>no lldp timer</b>   | Возобновляет интервал по умолчанию, то есть 30 с  |

## 22.5 Настройка реинициализации

Информация LLDP автоматически отправляется при изменении состояния и значения одного или нескольких информационных элементов (управляемых объектов) в локальной системе и истечении таймера передачи. Поскольку одно изменение информации требует передачи кадров LLDP, непрерывная серия изменений может инициировать передачу множества кадров LLDP, так как в каждом кадре сообщается только об одном изменении. Чтобы избежать этой ситуации, управление сетью определяет время ожидания между двумя последовательными передачами кадров LLDP. Вы можете контролировать интервал между непрерывными передачами двух сообщений, настроив повторную инициализацию LLDP.

Запустите следующую команду в режиме глобальной конфигурации, чтобы настроить повторную инициализацию LLDP:

| Команда                 | Описание  |
|-------------------------|---|
| <b>lldp reinit time</b> | Устанавливает интервал непрерывной передачи сообщений. Значение варьируется от 2 до 5. Значение интервала по умолчанию составляет 2 с |
| <b>no lldp reinit</b>   | Восстанавливает интервал непрерывной передачи сообщений по умолчанию (2 с)  |



## 22.6 Настройка TLV для отправки

По умолчанию передаются все TLV. Вы можете выбрать только те, который необходимо отправлять в соответствии с требованиями вашей сети.

Выполните следующие команды в режиме глобальной конфигурации, чтобы добавить или удалить TLV LLDP:

| Команда                                   | Описание  |
|---|---|
| <b>lldp tlv-select</b> <i>tlv-type</i>    | Добавление TLV соответствующего типа. Можно указать следующие типы TLV:<br><b>macphy-config</b> – состояние и конфигурация интерфейсов<br><b>management-address</b> – адрес управления<br><b>port-description</b> – описание порта<br><b>port-vlan</b> – информация о VLAN, ассоциированной с портом<br><b>system-capabilities</b> – производительность системы<br><b>system-description</b> – описание системы<br><b>system-name</b> – имя системы |
| <b>no lldp tlv-select</b> <i>tlv-type</i> | Удаление TLV соответствующего типа  |

## 22.7 Настройка режима передачи или приема

LLDP может работать в трех режимах: только передача, только прием и передача и прием.

По умолчанию LLDP работает в режиме передачи и приема. Вы можете изменить рабочий режим LLDP с помощью следующих команд в режиме настройки интерфейса:

| Команда                   | Описание   |
|---------------------------|--|
| <b>[no] lldp transmit</b> | Включает/отключает для порта режим «только передачи» |
| <b>[no] lldp receive</b>  | Включает/отключает для порта режим «только прием»    |

## 22.8 Отображение информации LLDP

Вы можете просмотреть информацию о соседнем устройстве, статистике или состоянии порта, полученную модулем LLDP, с помощью команд **show**.

Выполните следующие команды в режиме глобальной конфигурации или EXEC:



| Команда  | Описание   |
|--|--|
| <b>show lldp errors</b>                          | Отображает информацию об ошибках модуля LLDP                                     |
| <b>show lldp interface <i>interface-name</i></b> | Отображает информацию о состоянии порта, то есть режиме передачи и режиме приема |
| <b>show lldp neighbors</b>                       | Отображает общую информацию о соседе   |
| <b>show lldp neighbors detail</b>                | Отображает детальную информацию о соседе   |
| <b>show lldp traffic</b>                         | Отображает всю полученную и переданную статистическую информацию                 |

## 22.9 Удаление информации LLDP

Вы можете удалить полученные списки соседних устройств и всю статистическую информацию, выполнив следующие команды в режиме EXEC:

| Команда                    | Описание   |
|----------------------------|--|
| <b>clear lldp counters</b> | Удаляет все статистические данные                        |
| <b>clear lldp table</b>    | Удаляет всю полученную информацию о соседних устройствах |

Отображение отладочной информации

Для простого мониторинга модуля LLDP выполните следующие команды в режиме EXEC:

| Команда                   | Описание  |
|---------------------------|---|
| <b>debug lldp errors</b>  | Выводит отладочную информацию об ошибках LLDP           |
| <b>debug lldp events</b>  | Выводит отладочную информацию о событиях LLDP           |
| <b>debug lldp packets</b> | Выводит отладочную информацию о передаче сообщений LLDP |
| <b>debug lldp states</b>  | Выводит отладочную информацию о состоянии порта LLDP    |



## 23. Протоколы защиты кольцевых соединений Ethernet

### 23.1 Введение

#### 23.1.1 Обзор протоколов

Протокол защиты кольцевых соединений, или кольцевого резервирования – это особый тип протокола канального уровня, специально разработанный для построения кольцевой топологии Ethernet. Он может отключить один канал в полной кольцевой топологии, предотвращая формирование широковещательного шторма в случае закливания потока данных. При прерывании связи по одному каналу, протокол немедленно возобновляет работу другого, который был ранее отключен. Таким образом, узлы в кольцевой сети могут продолжить взаимодействовать друг с другом.

Протокол может передавать пакеты данных на правильный канал, контролируя устаревание таблицы MAC-адресов коммутатора при изменении топологии. Обычно время устаревания MAC-адреса в таблице составляет 300 секунд. Протокол защиты кольца Ethernet может значительно сократить время, в течение которого MAC-адреса остаются в таблице, что позволяет быстрее обновлять информацию о подключенных устройствах при изменениях в сети.

Протоколы кольцевой защиты и STP используются для управления топологией на канальном уровне. STP подходит для всех видов сложных сетей, которые передают изменение топологии сети с шагом за шагом. Протокол защиты кольца применяется в кольцевой топологии и использует механизм распространения оповещений для передачи изменений топологии сети. Таким образом, сходимость такого протокола в кольцевой сети лучше, чем STP. В хорошо построенной сети он может возобновить сетевое соединение менее чем за 50 мс.



Протокол защиты кольца позволяет одному коммутатору выполнять роль центрального узла для нескольких физических кольцевых сетей, создавая соединение между ними, называемое тангенциальным кольцом. Однако этот протокол не может поддерживать тангенциальные кольца, если они используют общие соединения.

Данная серия коммутаторов поддерживает два типа протокола кольцевой защиты:

- EAPS (Ethernet Automatic Protection Switching), основанный на RFC-3619
- ERPS (Ethernet Ring Protection Switching)

#### 23.1.2 Базовые сведения о настройке кольцевого резервирования

Перед настройкой протокола кольцевой защиты на Ethernet-коммутаторе обратите внимание на следующие положения:



- Одной из важных функций протокола защиты кольца является остановка широковещательного шторма, поэтому, пожалуйста, убедитесь, что перед повторным подключением кольцевого соединения все его узлы корректно настроены. Например, при настройке EAPS сначала необходимо сконфигурировать главный узел и все промежуточные узлы, а затем подключить сетевой кабель ко вторичному порту главного узла. При настройке ERPS важно оставить хотя бы одно соединение отключенным до завершения конфигурации всех узлов кольцевой сети. Если сеть будет подключена до завершения настройки, это может легко привести к возникновению широковещательного шторма.
- EAPS и ERPS являются протоколами с обратимой защитой. Это значит, что если происходит сбой на порту, а затем соединение восстанавливается, протокол автоматически вернется к состоянию, в котором он находился до сбоя.
- EAPS и ERPS могут быть настроены на одном и том же коммутаторе одновременно, но они должны использоваться для управления разными кольцевыми сетями. То есть, EAPS и ERPS несовместимы и не могут работать одновременно в одной и той же кольцевой сети.
- Протоколы кольцевого резервирования могут работать вместе с SSTP и RSTP одновременно, а также в случае, если STP отключен. Уже настроенный порт кольца не будет принимать участия в расчете STP.
- В зависимости от версии программного обеспечения некоторые коммутаторы данной серии поддерживают только EAPS. Некоторые не поддерживают одновременную работу EAPS и STP.
- Если протокол защиты кольца работает без отключения STP, мы рекомендуем настроить функцию передачи BPDU связующего дерева, таким образом, чтобы запретить всем узлам кольца пересылать BPDU и влиять на производительность сети.
- Протоколы защиты кольца не работают одновременно с MSTP. В случае настройки EAPS или ERPS MSTP не может быть перезапущен.
- Протокол защиты кольца позволяет настраивать коммутатор для работы с несколькими кольцевыми сетями. Однако он не поддерживает более сложные конфигурации кольцевых сетей, которые включают общие каналы.



## 23.2 EAPS

### 23.2.1 Основные понятия

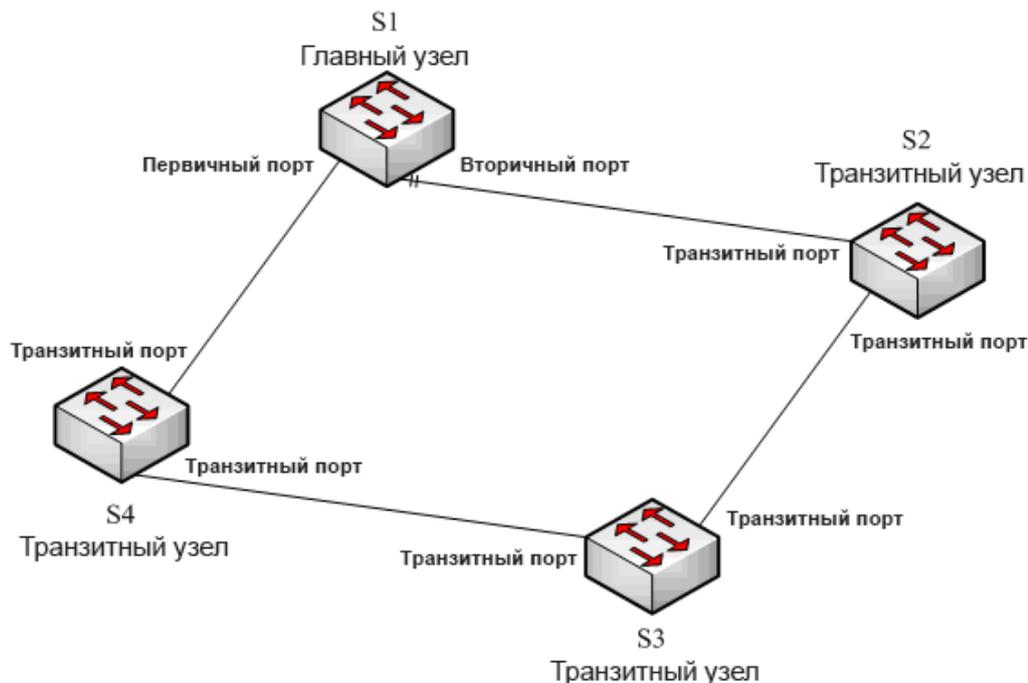


Рисунок 26 – Ethernet-кольцо EAPS

### 23.2.2 Роли кольцевых узлов

Каждый коммутатор в кольце Ethernet является узлом этого кольца. Кольцевые узлы подразделяются на главные и транзитные. Только один коммутатор в кольце Ethernet может служить просто главным узлом, а остальные коммутаторы работают как транзитные узлы.

#### ➤ Главный (мастер) узел

Он точно знает, замкнута ли топология кольца, устраняет петлю, управляет другими коммутаторами для обновления информации о топологии.

#### ➤ Транзитный узел

Он только проверяет состояние локального порта кольца и уведомляет главный узел о неисправном канале.

Роль каждого узла может быть указана пользователем посредством настройки. Дело в том, что каждому коммутатору в одном кольце можно назначить только один тип узла. На рисунке 26 коммутатор S1 является главным узлом кольцевой сети, а коммутаторы S2, S3 и S4 – транзитными узлами.



### 23.2.3 Роли кольцевых портов

EAPS требует, чтобы каждый коммутатор имел два порта для подключения к кольцевой сети. Каждый порт кольцевой сети также необходимо указать в конфигурации. Протокол поддерживает несколько ролей порта.

#### ➤ Первичный (основной) порт

Основной порт можно настроить только на главном узле. Главный узел передает информацию о кольце (пакеты Ring detection) через основной порт.

#### ➤ Вторичный порт

Вторичный порт можно настроить только на главном узле. Главный узел получает пакеты Ring detection от вторичного порта и оценивает целостность топологии кольцевой сети. В замкнутой топологии главный узел блокирует пакеты данных на вторичном порту и предотвращает возникновение петли; после прерывания соединения в кольцевой сети главный узел откроет вторичный порт для пересылки пакетов данных.

#### ➤ Транзитный порт

Транзитный порт можно настроить только на транзитном узле. Оба порта, через которые транзитный узел подключается к кольцевой сети, являются транзитными портами.

Для каждого порта кольцевой сети можно назначить только одну роль после настройки роли узла коммутатора и управляющей VLAN. Как показано на рисунке 26, порт, через который главный узел S1 соединяется с транзитным узлом S4, является первичным портом, порт, через который S1 соединяется с S2, является вторичным портом, а порты, через которые другие коммутаторы подключаются к кольцевой сети, являются транзитными.



Чтобы настроить один и тот же коммутатор для работы с несколькими кольцами, необходимо подключать разные кольца через разные физические порты.

### 23.2.4 Управляющая VLAN и VLAN для передачи данных

Частная управляющая VLAN используется между главным и транзитным узлом для передачи пакетов протокола. Эта управляющая VLAN указывается пользователем в настройках. Также пользователь добавляет в нее кольцевые порты, что гарантирует нормальную пересылку пакетов протокола. Как правило, каждый порт кольцевой сети находится в управляющей VLAN в состоянии пересылки, а порты, не принадлежащие кольцевой сети, не могут пересылать пакеты управляющей VLAN.



Вы можете указать разные управляющие VLAN для каждого кольца на коммутаторе. Управляющая VLAN используется только для пересылки управляющих пакетов кольцевой сети, а не для связи L2/L3. Например, если установлен порт VLAN, соответствующий управляющей VLAN, IP-адрес порта VLAN не может быть проверен через другие устройства.



Все VLAN, за исключением управляющей, являются VLAN данных, которые используются для передачи пакетов обычных услуг или пакетов управления. Пересылкой пакетов данных VLAN на кольцевом порту управляет протокол кольцевого резервирования; состояние пересылки некоего порта контролируется при помощи STP.



VLAN для передачи данных можно использовать для обычной связи L2/L3. Например, вы можете выбрать порт VLAN, соответствующий VLAN данных, и настроить протоколы динамической маршрутизации.

### 23.2.5 Символ замкнутой кольцевой сети

И главный, и транзитный узел могут показать, замкнута ли текущая кольцевая сеть, с помощью символа состояния «COMPLETE». На главном узле это происходит только тогда, когда все каналы кольцевой сети находятся в норме, первичный порт находится в состоянии пересылки, а вторичный – в состоянии блокировки. На транзитном узле – только тогда, когда его два транзитных порта находятся в состоянии пересылки.

Символ состояния кольцевой сети помогает пользователю оценивать исправность топологии.

### 23.2.6 Типы пакетов EAPS

Пакеты EAPS можно разделить на следующие типы, как показано в таблице 10:

Таблица 10 – Типы пакетов EAPS

| Тип пакета          | Описание   |
|---------------------|--|
| (HEALTH)            | Обнаружение петель (здоровье системы). Пакет передается главным узлом, чтобы определить, замкнута ли топология кольцевой сети                    |
| LINK-DOWN           | Указывает, что в кольце происходит прерывание соединения. Пакеты такого типа передаются транзитным узлом   |
| RING-DOWN-FLUSH-FDB | Пакет передается главным узлом после обнаружения прерывания кольцевой сети и в нем отображается таблица устаревания MAC-адресов транзитного узла |
| RING-UP-FLUSH-FDB   | Пакет передается главным узлом при восстановлении связи после прерывания кольцевой сети, и в нем   |



|  |   |
|--|---|
|  | отображается таблица устаревания MAC-адресов транзитного узла |
|--|---|

## 23.2.7 Механизм работы EAPS

### 23.2.7.1 Работа главного узла

Главный узел передает пакеты HEALTH в управляющую VLAN через основной порт с определенным интервалом. В случае нормальной связи пакеты HEALTH проходят через все остальные узлы кольцевой сети и, наконец, достигают вторичного порта главного узла.

В исходном состоянии вторичный порт блокирует все сети VLAN для передачи данных. При непрерывном получении пакетов HEALTH вторичный порт продолжает блокировать VLAN данных, предотвращая образование петли. Если вторичный порт не получает пакеты HEALTH от основного порта в течение определенного времени (которое можно настроить), он будет считать, что кольцевая сеть вышла из строя. Затем главный узел снимает блокировку VLAN данных на вторичном порту, признает локальную таблицу MAC-адресов устаревшей и передает пакеты RING-DOWN-FLUSH-FDB для уведомления других узлов.

Если главный узел получает пакеты HEALTH на вторичном порту, открытом для VLAN данных, кольцевая сеть восстанавливается. В этом случае главный узел немедленно блокирует VLAN данных на вторичном порту, обновляет информацию о локальной топологии и сообщает другим узлам об устаревании таблицы MAC-адресов посредством пакетов RING-UP-FLUSH-FDB.

Вы можете настроить параметры «Hello-time» и «Fail-time» с целью изменения интервала передачи пакетов HEALTH через основной порт и временного ограничения, в течение которого вторичный порт ожидает получения пакетов HEALTH.

### 23.2.7.2 Уведомление о нерабочем канале транзитного узла

После того, как транзитный порт транзитного узла выйдет из строя, пакет LINK-DOWN будет немедленно передан другим транзитным портом для уведомления остальных узлов. В обычной ситуации пакет проходит через другие транзитные узлы и, наконец, достигает порта главного узла.

После того как главный узел получает пакет LINK-DOWN, он считает, что кольцевая сеть неисправна. В этом случае главный узел снимает блокировку VLAN данных на своем вторичном порту, признает локальную таблицу MAC-адресов устаревшей, передает пакет RING-DOWN-FLUSH-FDB и уведомляет другие узлы.

### 23.2.7.3 Возобновление соединения транзитного узла

После возобновления работы транзитного порта он не сразу передает пакеты данных VLAN, а переходит в состояние, предшествующее пересылке (Pre-Forwarding). В этом состоянии транзитный порт передает и принимает только пакеты управления из управляющей VLAN.



Если в кольцевой сети имеется только один нерабочий транзитный порт, то, когда он переходит в состояние Pre-Forwarding, вторичный порт главного узла может снова получить пакет HEALTH от основного порта. В этом случае главный узел снова блокирует VLAN данных на вторичном порту и передает уведомление об устаревании таблицы адресов другим узлам. После того, как узел с транзитным портом в состоянии Pre-Forwarding получит уведомление об устаревании таблицы адресов, он сначала переведет порт в состояние обычной передачи данных, а затем удалит устаревшую локальную таблицу MAC-адресов.

Если транзитный узел не получает уведомление об устаревании таблицы адресов от главного узла и считает, что связь с главным узлом уже недействительна, он автоматически переводит порт Pre-Forwarding в состояние обычной передачи.

Вы можете настроить соответствующие временные параметры режима Pre-Forwarding, чтобы изменить интервал, в течение которого транзитный порт продолжает работу в данном режиме.

## 23.2.8 Настройка EAPS

### 23.2.8.1 Введение

Перед настройкой EAPS внимательно прочтите следующие пункты:

- EAPS можно настроить одновременно с ERPS или SSTP/RSTP, но не с MSTP.
- Настройка управляющей VLAN в кольцевой сети не приводит к автоматическому созданию соответствующей системной VLAN. Вам нужно вручную создать системную VLAN, используя команду глобальной конфигурации.
- Порт каждого кольца может пересылать пакеты из управляющей VLAN кольца, в то время как другие порты, даже в режиме Trunk, пакеты из управляющей VLAN пересылать не могут.
- По умолчанию время сбоя (Fail-time) главного узла в три раза дольше, чем время приветствия (Hello-time), поэтому задержка пакетов не приводит к нарушению работы кольца. После изменения времени приветствия необходимо соответствующим образом изменить время сбоя.
- По умолчанию время Pre-Forwarding транзитного узла в три раза превышает время приветствия главного узла, чтобы гарантировать, что главный узел сможет обнаружить восстановление кольцевой сети до того, как транзитный порт войдет в режим передачи данных. Если время приветствия, настроенное на главном узле, превышает время Pre-Forwarding транзитного узла, легко генерируется петля и запускается широковещательный шторм.
- В зависимости от версии программного обеспечения узлы кольца, настроенные на некоторых коммутаторах данной серии, по умолчанию работают в режиме распределенного управления, что позволяет добиться превосходной производительности конвергенции. Рабочий режим протокола защиты кольца можно изменить с помощью команд настройки узла **distributed-mode** и **centralized-mode**.
- Физический интерфейс и логический интерфейс агрегации можно настроить в качестве кольцевого порта. Если на физическом интерфейсе уже включены функции агрегации,



802.1X или Port Security, этот физический интерфейс больше нельзя настроить в качестве кольцевого.

Задачи настройки

- Настройка главного узла
- Настройка транзитного узла
- Настройка кольцевого порта
- Просмотр состояния протокола

### 23.2.8.2 Настройка главного узла

Настройте коммутатор в качестве главного узла кольцевой сети, выполнив следующие действия:

| Команда   | Описание   |
|---|--|
| Switch# <b>configure</b>                        | Вход в режим глобальной конфигурации   |
| Switch_config# <b>no spanning-tree</b>          | Выключает запущенный протокол связующего дерева  |
| Switch_config# <b>ether-ring id</b>             | Устанавливает узел и входит в режим настройки узла<br><b>id</b> : идентификатор экземпляра   |
| Switch_config_ring# <b>control-vlan vlan-id</b> | Настраивает управляющую VLAN.<br><b>vlan-id</b> : идентификатор управляющей VLAN   |
| Switch_config_ring# <b>master-node</b>          | Указывает, что узел является главным   |
| Switch_config_ring# <b>hello-time value</b>     | Этот шаг необязателен. Настраивает интервал передачи главным узлом пакетов HEALTH<br><b>value</b> : значение времени в диапазоне от 1 до 10 секунд, значение по умолчанию – 1 секунда                        |
| Switch_config_ring# <b>fail-time value</b>      | Этот шаг необязателен. Настраивает время, в течение которого вторичный порт будет ожидать пакетов HEALTH<br><b>value</b> : значение времени в диапазоне от 3 до 30 секунд, значение по умолчанию – 3 секунды |



|   |   |
|---|---|
| Switch_config_ring# <b>distributed-mode</b> | Этот шаг необязателен. Настраивает режим распределенного управления для протокола защиты кольца   |
| Switch_config_ring# <b>centralized-mode</b> | Этот шаг необязателен. Настраивает режим централизованного управления для протокола защиты кольца |
| Switch_config_ring# <b>exit</b>             | Сохранение текущих настроек и выход из режима настройки узла                                      |
| Switch_config# <b>vlan vlan-id</b>          | Устанавливает соответствующую управляющую VLAN  |



Команда **no ether-ring id** используется для удаления настроек узла и кольцевого порта.

### 23.2.8.3 Настройка транзитного узла

Для настройки коммутатора в качестве транзитного узла кольцевой сети, выполните следующие действия:

| Команда  | Описание   |
|--|--|
| Switch# <b>configure</b>                         | Вход в режим глобальной конфигурации   |
| Switch_config# <b>no spanning-tree</b>           | Выключает запущенный протокол связующего дерева  |
| Switch_config# <b>spanning-tree bpduterminal</b> | Запрещает коммутатору пересылать BPDU STP  |
| Switch_config# <b>ether-ring id</b>              | Устанавливает узел и входит в режим настройки узла<br><b>id</b> : идентификатор экземпляра |
| Switch_config_ring# <b>control-vlan vlan-id</b>  | Настраивает управляющую VLAN.<br><b>vlan-id</b> : идентификатор управляющей VLAN           |
| Switch_config_ring# <b>transit-node</b>          | Указывает, что узел является транзитным  |



|  |  |
|--|--|
| Switch_config_ring# <b>pre-forward-time</b> <i>value</i> | Этот шаг необязателен. Настраивает время поддержания состояния Pre-Forwarding на транзитном порту<br><br><b>value:</b> значение времени в диапазоне от 3 до 30 секунд, значение по умолчанию – 3 секунды |
| Switch_config_ring# <b>exit</b>                          | Сохранение текущих настроек и выход из режима настройки узла   |
| Switch_config# <b>vlan</b> <i>vlan-id</i>                | Устанавливает соответствующую управляющую VLAN   |

### 23.2.8.4 Настройка кольцевого порта

Чтобы настроить порт коммутатора в качестве порта кольца Ethernet, выполните следующие действия:

| Команда   | Описание  |
|---|---|
| Switch# <b>configure</b>  | Вход в режим глобальной конфигурации  |
| Switch_config# <b>interface</b> <i>intf-name</i>  | Вход в режим настройки интерфейса<br><b>intf-name:</b> имя интерфейса             |
| Switch_config_intf# <b>ether-ring</b> <i>id</i> <b>primary-port</b> { <b>secondary-port</b>   <b>transit-port</b> } | Настраивает тип кольцевого порта<br><b>id:</b> идентификатор узла кольца Ethernet |
| Switch_config_intf# <b>exit</b>   | Выход из режима настройки интерфейса  |



Команда **no ether-ring id primary-port {secondary-port | transit-port}** может использоваться для отмены настроек кольцевого порта.

### 23.2.8.5 Просмотр состояния протокола

Выполните следующую команду, чтобы просмотреть состояние кольцевого протокола:

| Команда                   | Описание   |
|---------------------------|--|
| <b>show ether-ring id</b> | Отображает сводную информацию о кольцевом протоколе и портах кольца Ethernet |



|   |  |
|---|--|
|   | <b>id:</b> идентификатор кольца Ethernet                                       |
| <b>show ether-ring id detail</b>              | Отображает подробную информацию о кольцевом протоколе и портах кольца Ethernet |
| <b>show ether-ring id interface intf-name</b> | Отображает состояние кольцевого порта  |

## 23.2.9 Пример настройки EAPS

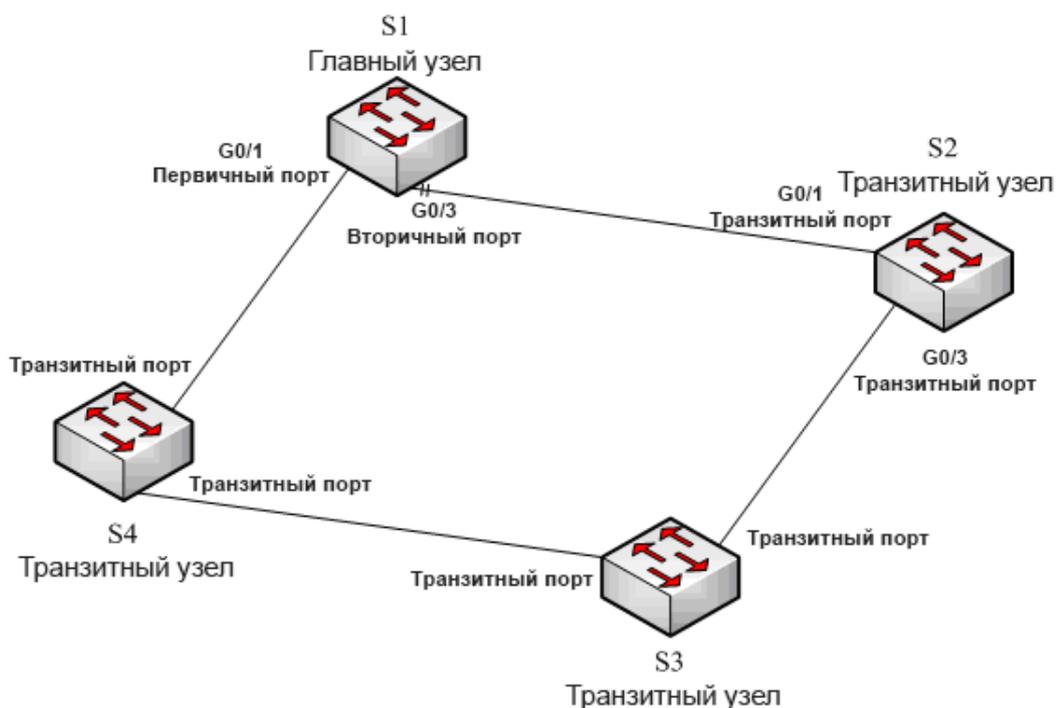


Рисунок 27 – Кольцо EAPS

Как показано на рисунке 27, главный узел S1 и транзитный узел S2 настроены следующим образом. Что касается настроек остальных узлов, то они аналогичны настройкам S2.

### ➤ Настройка коммутатора S1:

Выключение STP и настройка узла кольцевой топологии:

```
S1_config# no spanning-tree
```

```
S1_config# ether-ring 1
```

```
S1_config_ring1# control-vlan 2
```

```
S1_config_ring1# master-node
```

Следующие команды используются для установки параметров, связанных со временем:

```
S1_config_ring1# hello-time 2
```



```
S1_config_ring1# fail-time 6
```

Выход из режима настройки узла:

```
S1_config_ring1# exit
```

Настройка первичного и вторичного портов:

```
S1_config# interface gigaEthernet 0/1
```

```
S1_config_g0/1# ether-ring 1 primary-port
```

```
S1_config_g0/1# exit
```

```
S1_config# interface gigaEthernet 0/3
```

```
S1_config_g0/3# ether-ring 1 secondary-port
```

```
S1_config_g0/3# exit
```

Настройка управляющей VLAN:

```
S1_config# vlan 2
```

```
S1_config_vlan2# exit
```

```
S1_config# interface range g0/1 , 3
```

```
S1_config_if_range# switchport mode trunk
```

```
S1_config_if_range# exit
```

➤ **Настройка коммутатора S2:**

```
S1_config# no spanning-tree
```

```
S1_config# ether-ring 1
```

```
S1_config_ring1# control-vlan 2
```

```
S1_config_ring1# transit-node
```

```
S1_config_ring1# pre-forward-time 8
```

```
S1_config_ring1# exit
```

```
S1_config# interface gigaEthernet 0/1
```

```
S1_config_g0/1# ether-ring 1 transit-port
```

```
S1_config_g0/1# exit
```

```
S1_config# interface gigaEthernet 0/3
```

```
S1_config_g0/3# ether-ring 1 transit-port
```

```
S1_config_g0/3# exit
```

```
S1_config# vlan 2
```

```
S1_config_vlan2# exit
```

```
S1_config# interface range gigaEthernet 0/1 , 3
```

```
S1_config_if_range# switchport mode trunk
```



S1\_config\_if\_range# exit

## 23.3 ERPS

### 23.3.1 Основные понятия

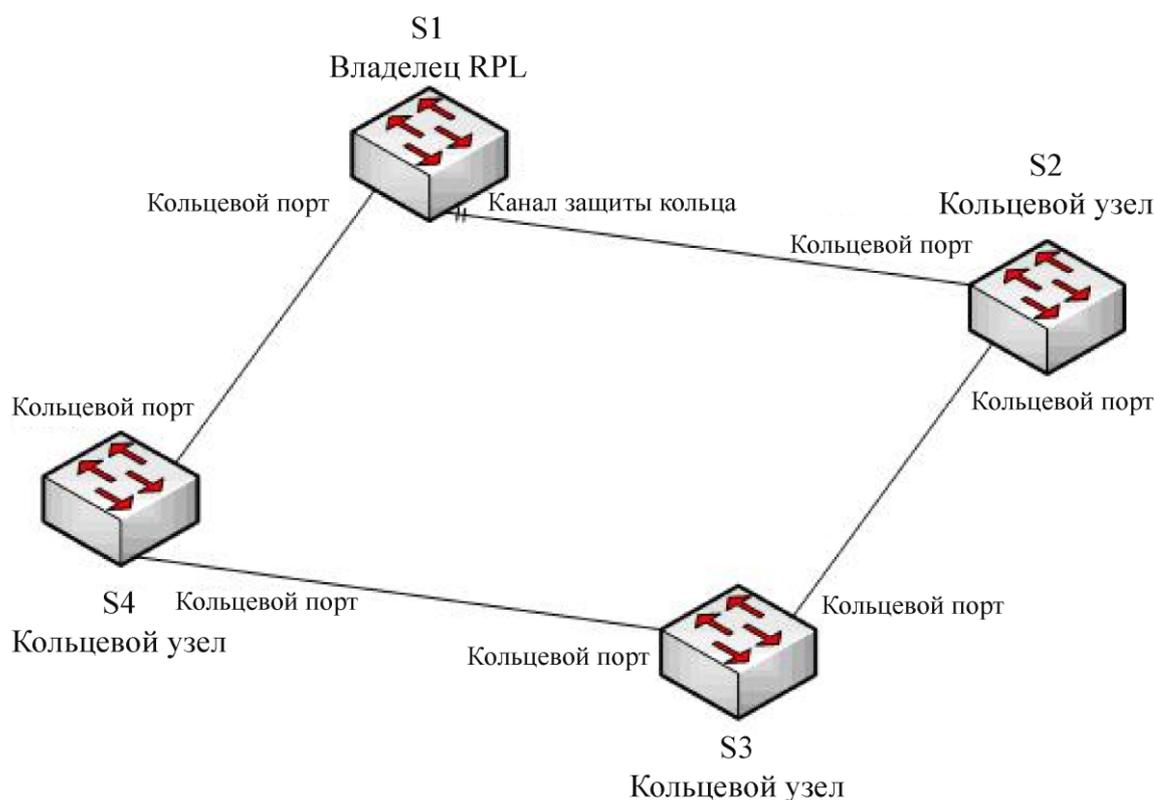


Рисунок 28 – Кольцо ERPS

#### 23.3.1.1 Роли кольцевых узлов

Каждый коммутатор в Ethernet-кольце является узлом этого кольца. Узлы в Ethernet-кольце можно разделить на две категории: владельцы RPL (канала защиты кольца) и обычные узлы. В кольце только один коммутатор может быть владельцем канала защиты, а остальные коммутаторы работают как обычные узлы.

Тип узла в ERPS не требует специальной настройки. По умолчанию все устройства в Ethernet-кольце автоматически определяют узел с самым высоким приоритетом и назначают его владельцем RPL. Один из портов этого узла автоматически становится каналом защиты кольца (RPL).

Если порт одного устройства настроен на работу в режиме RPL с помощью команды, приоритет этого устройства автоматически изменится. Это сделано для того, чтобы это устройство могло стать узлом защиты в сети.



Владелец RPL выполняет те же функции, что и обычный узел. Он следит за состоянием портов локального Ethernet-кольца и отправляет уведомления в случае неисправности соединения. Однако есть одно важное отличие: владелец RPL в обычном режиме блокирует канал защиты кольца, в то время как обычный узел этого не делает.



- Владелец RPL существенно отличается от главного узла EAPS по функциональности: он не будет ни проверять целостность кольца Ethernet, ни контролировать старение MAC-адресов других узлов.
- Если включен автоматический механизм обнаружения в Ethernet-кольце, порт устройства настраивается на режим RPL с помощью специальной команды. Это означает, что для этого устройства устанавливается самое меньшее значение приоритета. Если значение приоритета других устройств такое же, необходимо выбрать владельца RPL вручную.

### 23.3.1.2 Роли кольцевых портов

Система ERPS требует, чтобы каждый узел имел два порта для подключения к Ethernet-кольцу, и эти порты называются кольцевыми портами. Кроме того, в каждом Ethernet-кольце есть кольцевой порт, который выполняет роль RPL.

В обычном режиме все порты Ethernet-кольца, кроме порта RPL, находятся в состоянии передачи данных, а порт RPL блокируется, чтобы избежать заикливания. Если связь в Ethernet-кольце нарушается, владелец RPL отменяет блокировку этого порта, чтобы восстановить сетевое соединение.

На коммутаторе можно настроить только один RPL-порт.



- ERPS поддерживает логический порт агрегации в качестве кольцевого порта.
- Чтобы настроить один и тот же коммутатор для работы с несколькими кольцами, необходимо подключать разные кольца через разные физические порты.

### 23.3.1.3 Управляющая VLAN и VLAN данных

ERPS не требует различия между управляющей VLAN и VLAN данных.

Когда ERPS работает вместе с EAPS, состояние кольцевого порта ERPS влияет на все VLAN, которые подключены к этому порту.

Если ERPS и EAPS настроены одновременно, состояние кольцевого порта ERPS также будет влиять на все VLAN данных EAPS, которые используют этот порт.



ERPS всегда отправляет свои пакеты в стандартную VLAN порта. Поэтому необходимо заранее убедиться, что VLAN по умолчанию у всех портов одинаковая.

#### 23.3.1.4 Автоматическое обнаружение и проверка согласованности кольцевого порта

В ERPS механизм автоматического обнаружения используется для выбора узла кольца Ethernet в качестве узла защиты. По сравнению с EAPS, автоматическое обнаружение значительно упрощает развертывание устройств Ethernet-кольца.

Механизм автоматического обнаружения использует значение приоритета и MAC-адрес для идентификации узла кольца. Чем меньше значение приоритета и MAC-адрес, тем выше приоритет.

После запуска процесса автоматического обнаружения устройство начинает отправлять пакеты обнаружения на кольцевой порт. Эти пакеты содержат локальную информацию о устройстве. Когда устройство получает внешний пакет обнаружения, оно должно сравнить информацию в этом пакете со своей локальной информацией и определить, является ли она более приоритетной. Если информация в пакете более приоритетна, устройство не будет выполнять роль владельца RPL. Если устройство не получит более приоритетный пакет до завершения процесса обнаружения, оно само станет владельцем RPL.

Команда **discovery time** используется для настройки времени работы потока обнаружения, а команда **discovery disable** может быть использована для отключения автоматического обнаружения.

Механизм автоматического обнаружения одновременно используется для проверки целостности кольцевого порта, чтобы предотвратить влияние неверных или пропущенных настроек, а также неправильного подключения сетевого кабеля на работу протокола.

ERPS гарантирует, что пакеты обнаружения отправляются только на кольцевые порты, и эти пакеты содержат идентификатор Ethernet-кольца. Если порт P устройства получает пакет обнаружения с идентификатором ID1, то в следующих двух случаях будет считаться, что у порта P возникла ошибка согласованности, и он будет переведен в состояние Error-Disable (отключение из-за ошибки):

- порт P уже настроен как порт кольца, но его идентификатор не равен ID1;
- порт P не был настроен как порт кольца, но на устройстве уже есть два других настроенных порта, и у них обоих идентификаторы ID1.

В режиме глобальной конфигурации команда **no erps inconsistency-check** может использоваться для запрета проверки согласованности кольцевого порта, а команда **error-disable-recovery** – для настройки времени восстановления порта после ошибки.

#### 23.3.1.5 Типы пакетов ERPS

Пакеты ERPS можно классифицировать по следующим типам, как показано в таблице 11:

Таблица 11 – Типы пакетов ERPS



| Тип пакета                      | Описание   |
|---------------------------------|--|
| Signal Fail (SF)                | Узел кольца (включая владельца RPL) уведомляет другие узлы после того, как локальный канал связи оказывается недоступным |
| No Request (NR)                 | Узел кольца уведомляет другие узлы после того, как обнаруживает, что все локальные каналы связи восстановлены            |
| No Request, RPL Blocked (NR-RB) | Владелец RPL уведомляет другие узлы о восстановлении прежнего канала связи и блокировке защитного канала RPL.            |

## 23.3.2 Механизм защиты кольца ERPS

### 23.3.2.1 Стабильное состояние

В стабильном состоянии узел кольцевой защиты блокирует порт RPL и передает пакеты NR-RB через настроенный промежуток времени.

Все обычные узлы, которые получают пакеты NR-RB, устанавливают свои локальные кольцевые порты в состояние передачи данных. В стабильном состоянии обычные узлы не передают пакеты протокола.

Вы можете запустить команду **send-time**, чтобы изменить время цикла передачи пакетов NR-RB узлом защиты.

### 23.3.2.2 Обработка неисправного локального канала связи

После того как кольцевой узел обнаруживает недействительную локальную связь, он сначала снимает блокировку с резервных локальных портов (включая порт RPL и обычные кольцевые порты, которые не находятся в состоянии пересылки). Затем узел начинает отправлять пакеты протокола SF и обновляет таблицу локальных MAC-адресов.

Другие узлы, получающие пакеты SF, сначала останавливают передачу локальных пакетов, а затем отменяют состояние блокировки своих резервных локальных портов и обновляют таблицы MAC-адресов.

Узел с недействительной связью отправляет пакеты SF через определенные промежутки времени. Если в процессе работы порт другого узла восстанавливается, узел переведет порт в состояние пересылки после получения пакетов SF.



### 23.3.2.3 Обработка восстановления локального канала связи

Когда кольцевой узел обнаруживает, что локальный кольцевой порт восстановился, он держит порт заблокированным для передачи данных и начинает постоянно отправлять пакеты NR.

Если при передаче пакетов NR узел получает пакеты SF от других узлов, это означает, что в сети все еще существует недействительное соединение. Тогда локальный узел прекратит передачу пакетов NR и восстановит состояние пересылки.

Если локальный узел не получает новые пакеты SF, он запускает таймер ожидания восстановления (WTR) после того, как владелец RPL получит пакеты NR. Когда время WTR истечет, владелец RPL снова заблокирует порт RPL, отправит пакеты NR-RB и обновит таблицу MAC-адресов. Таким образом, сеть вернется к первоначальному стабильному состоянию.

### 23.3.2.4 Восстановление кольца ERPS

Владелец RPL осуществляет восстановление кольца с помощью таймера ожидания восстановления (WTR). Этот таймер помогает избежать частых переключений защиты на Ethernet-кольце. После получения владельцем RPL сообщений NR от других узлов запускается WTR. До истечения времени WTR владелец RPL сохраняет состояние передачи данных порта RPL и не отправляет уведомления о восстановлении кольца. Если владелец RPL снова получает сообщения SF, это означает, что Ethernet-кольцо еще не полностью восстановлено, и в этом случае WTR останавливается.

Когда время WTR истечет, владелец RPL снова блокирует порт RPL.

## 23.3.3 Настройка ERPS

### 23.3.3.1 Введение

Перед настройкой ERPS внимательно прочтите следующие пункты:

- ERPS можно настроить одновременно с EAPS или SSTP/RSTP, но не с MSTP.
- VLAN по умолчанию для каждого кольцевого порта должна быть настроена согласованно, чтобы пакеты ERPS могли нормально пересылаться.
- Когда ERPS и EAPS работают одновременно, VLAN по умолчанию кольцевого порта ERPS должна отличаться от управляющей VLAN EAPS. Пакеты ERPS не могут быть перенаправлены в управляющую VLAN EAPS.
- Один порт не может одновременно использоваться как кольцевой порт и ERPS, и EAPS.
- ERPS может использовать физический порт или порт агрегации в качестве кольцевого порта. Однако физический порт, на котором настроена агрегация каналов, 802.1X или Port Security, не может быть настроен в качестве кольцевого порта ERPS.
- По умолчанию ERPS выбирает владельца RPL через механизм автоматического обнаружения; этот механизм может быть запрещен с помощью команды **discovery disable** в режиме настройки ERPS. Если автоматическое обнаружение запрещено, убедитесь, что



RPL настроен и отображается на кольце Ethernet; в противном случае может возникнуть широковещательный шторм.

➤ Чтобы гарантировать восстановление кольцевого порта ERPS после отключения из-за ошибки, выполните команду **error-disable-recovery** в режиме глобальной конфигурации и укажите время, по истечении которого работа порта должна быть восстановлена.

## Задачи настройки

- Настройка кольцевого узла
- Настройка кольцевого порта
- Просмотр состояния протокола защиты кольца

### 23.3.3.2 Настройка кольцевого узла

В режиме глобальной конфигурации выполните следующие команды, чтобы настроить коммутатор в качестве узла ERPS:

| Команда   | Описание   |
|---|--|
| Switch_config# <b>error-disable-recovery</b> <i>value</i> | Настраивает время автоматического восстановления порта после ошибки  |
| Switch_config# <b>erps</b> <i>id</i>                      | Назначает коммутатор на роль кольцевого узла ERPS и входит в режим настройки узла<br><b>id</b> : идентификатор кольца Ethernet, который находится в диапазоне от 0 до 7                                    |
| Switch_config# <b>discovery</b> [enable   disable]        | Включает или отключает механизм обнаружения  |
| Switch_config# <b>discovery time</b> <i>value</i>         | Устанавливает время выполнения для автоматического обнаружения ERPS<br><b>value</b> : указывает время работы автоматического обнаружения, которое варьируется от 15 до 300 секунд (по умолчанию 30 секунд) |
| Switch_config# <b>discovery interval</b> <i>value</i>     | Устанавливает интервал передачи пакетов обнаружения.<br>Диапазон значений: 1–20 секунд (по умолчанию 2 секунды)  |



|  |   |
|--|---|
| Switch_config# <b>priority</b> <i>value</i>        | Устанавливает приоритет локального узла. Это значение используется для выбора владельца RPL в механизме обнаружения<br><br><b>value</b> : значение должно находиться в диапазоне от 0 до 61440 и быть целым числом, умноженным на 4096. Значение по умолчанию –32768  |
| Switch_config_ring# <b>wtr-time</b> <i>value</i>   | Устанавливает время ожидания таймера WTR<br><br>Диапазон значений: 10–720 секунд (по умолчанию 300 секунд)  |
| Switch_config_ring# <b>guard-time</b> <i>value</i> | Настраивает время тайм-аута таймера Guard. Когда порт восстанавливается из недопустимого состояния, таймеру Guard запрещается обрабатывать полученные пакеты протоколов, чтобы избежать генерации неточных протоколов устаревшими пакетами.<br><br><b>value</b> : единица измерения составляет 10 мс, значение находится в диапазоне от 1 до 200 (значение по умолчанию составляет 50 мс) |
| Switch_config_ring# <b>send-time</b> <i>value</i>  | Устанавливает интервал передачи пакетов протокола.<br><br><b>value</b> : диапазон от 1 до 10 (по умолчанию 5 секунд)  |
| Switch_config_ring# <b>exit</b>                    | Выход из режима настройки узла и запуск узла  |



Команда **no erps id** используется для удаления настроек узла и кольцевого порта.

### 23.3.3.3 Настройка кольцевого порта

Чтобы настроить порт коммутатора в качестве кольцевого порта ERPS, выполните следующие действия:

| Команда | Описание |
|---------|----------|
|---------|----------|



|  |   |
|--|---|
| Switch_config# <b>interface</b> <i>intf-name</i> | Вход в режим настройки интерфейса<br><b>intf-name</b> : имя интерфейса  |
| Switch_config_intf# <b>erps id ring-port</b>     | Назначает порт на роль обычного кольцевого порта выбранного узла.<br><b>id</b> : идентификатор кольца Ethernet  |
| Switch_config_intf# <b>erps id rpl</b>           | Назначает порт на роль порта RPL выбранного узла. В случае, если включено автоматическое обнаружение, функция команды аналогична изменению значения приоритета на 10<br><b>id</b> : идентификатор кольца Ethernet |
| Switch_config_intf# <b>exit</b>                  | Выход из режима настройки интерфейса  |



- Команда **no erps id rpl** используется для настройки порта RPL в качестве обычного кольцевого.
- Команда **no erps id ring-port** используется для удаления любого кольцевого порта, как обычного, так и RPL.
- В случае, если кольцевые узлы еще не настроены глобально, для их создания одновременно используются как команда **erps id ring-port**, так и **rpl**.

### 23.3.3.4 Просмотр состояния протокола

Выполните следующую команду, чтобы просмотреть состояние ERPS:

| Команда  | Описание  |
|--|---|
| <b>show erps id</b>                            | Отображает сводную информацию о кольцевом протоколе и портах кольца Ethernet<br><b>id</b> : идентификатор кольца Ethernet |
| <b>show erps id detail</b>                     | Отображает подробную информацию о кольцевом протоколе и его портах  |
| <b>show erps id interface</b> <i>intf-name</i> | Отображает состояние кольцевого порта   |



## 23.3.4 Примеры настройки ERPS

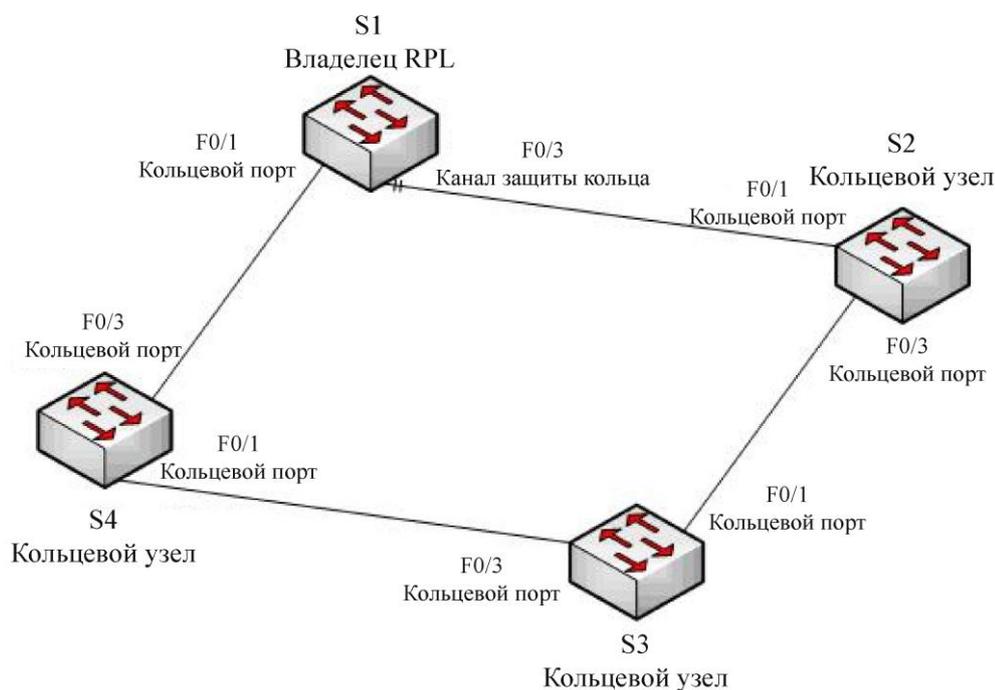


Рисунок 29 – Топология кольца ERPS

### 23.3.4.1 Фиксированные настройки RPL

В данном примере показаны настройки узла RPL (S1) и обычного узла (S2), изображенных на рисунке 29.

#### ➤ Настройка коммутатора S1

Для установки времени восстановления порта, отключенного из-за ошибки, используются следующие команды:

```
Switch# config
Switch_config# error-disable-recovery 30
```

Для настройки узла кольца используется следующая команда:

```
Switch_config# erps 1
```

Для настройки параметров, связанных со временем, используются следующие команды:

```
Switch_config_ring1# wtr-time 15
Switch_config_ring1# send-time 5
Switch_config_ring1# exit
```

Для настройки обычного кольцевого порта используются следующие команды:

```
Switch_config# interface f0/1
```



```
Switch_config_f0/1# erps 1 ring-port
```

Для настройки порта RPL используются следующие команды:

```
Switch_config_f0/1# interface f0/3
```

```
Switch_config_f0/3# erps 1 rpl
```

### ➤ Настройка коммутатора S2

```
Switch_config# erps 1
```

```
Switch_config_ring1# send-time 5
```

```
Switch_config_ring1# exit
```

```
Switch_config_if_range# interface range fastethernet 0/1 , 3
```

```
Switch_config_if_range# erps 1 ring-port
```

```
Switch_config_if_range# exit
```

### 23.3.4.2 Простые настройки для применения автоматического обнаружения

Все коммутаторы, изображенные на рисунке 29, настраиваются следующим образом:

```
Switch_config# error-disable-recovery 30
```

```
Switch_config# interface range fastethernet 0/1 , 3
```

```
Switch_config_if_range# erps 1 ring-port
```

```
Switch_config_if_range# exit
```

Для просмотра состояния ERPS используется следующая команда:

```
Switch# show erps
```

## 24. Протоколы маршрутизации

### 24.1 RIP

#### 24.1.1 Введение

RIP (Routing Information Protocol) – это относительно старый, но все еще широко используемый протокол внутреннего шлюза (IGP), который в основном применяется в небольших однотипных сетях. RIP – это традиционный протокол векторной маршрутизации, описанный в RFC 1058.

RIP обменивается информацией о маршрутизации посредством широковещательной передачи пакетов UDP. Маршрутизирующий коммутатор обновляет информацию о маршрутах каждые 30 секунд. Если в течение 180 секунд не было получено никакой обновленной информации от соседнего маршрутизатора, его маршруты будут помечены в таблице маршрутизации как неиспользуемые. И если в течение следующих 120 секунд



обновленная информация по-прежнему не поступит, эти маршруты будут удалены из таблицы маршрутизации.

Число переходов (хопов) используется протоколом RIP для балансировки веса различных маршрутов. Подсчет переходов относится к количеству пройденных пакетами маршрутизаторов на пути от источника к пункту назначения. Метрика маршрута в сети, подключенной напрямую, равна 0, метрика маршрута, сеть которого недостижима, равна 16. Поскольку метрика маршрута, используемая RIP, находится в относительно небольшом диапазоне, она неприменима к крупномасштабной сети.

Если маршрутизатор имеет маршрут по умолчанию, RIP объявит маршрут к псевдо-сети со специальным адресом 0.0.0.0. На самом деле сети 0.0.0.0 не существует, она используется только для реализации функции маршрута по умолчанию в RIP. Если RIP изучил маршрут по умолчанию или у маршрутизатора настроен шлюз по умолчанию со стандартными настройками, маршрутизатор объявит сеть по умолчанию.

RIP отправит обновления на интерфейс назначенной сети. Если сеть самого интерфейса не назначена, то сеть потом не будет анонсирована ни в одном обновлении RIP.

RIP-2 в устройствах данной серии поддерживает Route Summary, CIDR, VLSM, а также аутентификацию Plaintext и MD5

Для настройки RIP необходимо выполнить следующие задачи. Задача по активации RIP является обязательной, остальные выполняются по мере необходимости:

- Запуск RIP
- Включение одноадресной рассылки сообщений об обновлении маршрута RIP
- Изменение метрики маршрута
- Настройка таймеров
- Указание номера версии RIP
- Активация аутентификации RIP
- Запрет суммирования маршрутов
- Запрет аутентификации исходного IP-адреса
- Настройка максимального количества маршрутов
- Активация или запрет режима расщепления горизонта
- Мониторинг и поддержка RIP

### 24.1.2 Запуск RIP

Чтобы активировать RIP, выполните следующую команду в режиме глобальной конфигурации:

| Команда | Описание |
|---------|----------|
|---------|----------|



|  |  |
|--|--|
| <b>router rip</b>  | Активация процесса маршрутизации RIP и вход в режим настройки маршрутизатора |
| <b>network</b> <i>network-number</i> < <i>network-mask</i> > | Указывает номер сети, связанный с процессом маршрутизации RIP                |

### 24.1.3 Включение одноадресной рассылки сообщений об обновлении маршрута RIP

RIP – это протокол широковещательного типа. Обновление маршрутов можно настроить так, чтобы они достигали сети, работающей по протоколу без широковещания. Для этого маршрутизатор должен быть настроен таким образом, чтобы обеспечить обмен информацией с нужным устройством.

Выполните следующую команду в режиме настройки маршрутизатора:

| Команда                           | Описание  |
|-----------------------------------|---|
| <b>neighbor</b> <i>ip-address</i> | Определяет соседний коммутатор для обмена с ним информацией о маршрутизации |

Кроме того, если вы хотите контролировать, какие интерфейсы могут использоваться для обмена информацией о маршрутизации, можно выполнить команду **ip rip passive** для обозначения одного или нескольких интерфейсов, которым будет запрещена отправка обновления маршрутов.

### 24.1.4 Изменение метрики маршрута

Эта настройка используется для изменения метрик маршрутов, которые передаются через определенный интерфейс. Например, можно увеличить метрику для определенных маршрутов, чтобы они стали менее предпочтительными, или уменьшить метрику для улучшения маршрутизации. Выполните следующую команду в режиме настройки маршрутизатора:

| Команда  | Описание   |
|--|--|
| <b>offset-list</b> { <i>interface-type number</i>   *} { <b>in</b>   <b>out</b> } <i>access-list-name offset</i> | Изменяет метрику маршрута<br><b>interface-type number</b>   *: указывает интерфейс, к которому применяется команда. Можно указать конкретный интерфейс или использовать символ *, чтобы применить настройку ко всем интерфейсам<br><b>in</b>   <b>out</b> : определяет направление, в котором будет применяться изменение метрики. <b>in</b> |



|  |  |
|--|--|
|  | <p>означает, что метрика будет изменена для входящих маршрутов, а <b>out</b> – для исходящих</p> <p><b>access-list-name:</b> указывает имя списка доступа (access list), который определяет, какие маршруты будут затронуты изменением метрики</p> <p><b>offset:</b> указывает значение, на которое будет изменена метрика маршрутов, соответствующих указанному списку доступа. Это значение может быть положительным или отрицательным</p> |
|--|--|

## 24.1.5 Настройка таймеров

Протоколы маршрутизации используют несколько таймеров, которые определяют частоту отправки обновлений маршрутов, время, через которое маршрутизатор станет недействительным и другие параметры. Вы можете регулировать эти таймеры, чтобы производительность протоколов маршрутизации более соответствовала требованиям сети.

Также можно регулировать протокол маршрутизации, чтобы ускорить время конвергенции всех видов вычислений IP-маршрутизации, быстро выполнить копирование на резервный маршрутизатор для минимизации времени восстановления после сбоя. Для настройки таймеров используйте следующие команды режиме настройки маршрутизатора:

| Команда                      | Описание  |
|------------------------------|---|
| <b>timers holddown value</b> | Время, необходимое для удаления определенного маршрута из таблицы маршрутизации |
| <b>timers expire value</b>   | Время, в течение которого маршрут объявляется недействительным                  |
| <b>timers update value</b>   | Интервал времени между отправкой обновлений маршрутизации                       |

## 24.1.6 Указание номера версии RIP

RIP-2 маршрутизатора данной серии поддерживает аутентификацию, управление паролями, сводку маршрутов, CIDR и VLSM.

По умолчанию маршрутизатор может получать обновления RIP-1 и RIP-2, а отправлять – только обновления RIP-1. Маршрутизатор можно настроить на получение и отправку только обновлений RIP-1 или на получение и отправку только обновлений RIP-2. Для этого в режиме настройки маршрутизатора необходимо выполнить следующую команду:





| Команда                | Описание  |
|------------------------|---|
| <b>version {1   2}</b> | Настройка маршрутизатора для отправки и получения обновлений только RIP-1 или RIP-2 |

Эта команда управляет поведением RIP по умолчанию. Также можно настроить определенный интерфейс, чтобы изменить это поведение. Для этого необходимо использовать следующие команды в режиме настройки интерфейса:

| Команда                                  | Описание  |
|--|---|
| <b>ip rip send version 1</b>             | Настраивает интерфейс для отправки только пакетов RIP-1 |
| <b>ip rip send version 2</b>             | Настраивает интерфейс для отправки только пакетов RIP-2 |
| <b>ip rip send version compatibility</b> | Отправка сообщений обновления RIP-2 путем широковещания |

Выполните следующие команды в режиме настройки интерфейса, чтобы указать, будет ли интерфейс получать пакеты RIP-1 или RIP-2:

| Команда                           | Описание   |
|-----------------------------------|--|
| <b>ip rip receive version 1</b>   | Настройка интерфейса для получения только пакетов RIP-1  |
| <b>ip rip receive version 2</b>   | Настройка интерфейса для получения только пакетов RIP-2  |
| <b>ip rip receive version 1 2</b> | Настройка интерфейса для получения пакетов RIP-1 и RIP-2 |

## 24.1.7 Активация аутентификации RIP

RIP-1 не поддерживает аутентификацию, ее можно активировать на интерфейсе в режиме RIP-2. На активированном интерфейсе предусмотрено два типа аутентификации: простой текст и MD5. Каждый пакет RIP-2 по умолчанию использует аутентификацию простым способом.



Из соображений безопасности не рекомендуется использовать аутентификацию в виде открытого текста, поскольку ключ аутентификации без шифрования пересылается в каждую группу RIP-2. Если безопасность не учитывается (например,



хост с ошибочной конфигурацией не может участвовать в маршруте), аутентификация с открытым текстом допустима.

Чтобы настроить аутентификацию RIP с открытым текстом, выполните следующие действия в режиме настройки интерфейса:

| Команда                              | Описание  |
|--------------------------------------|---|
| <b>ip rip authentication simple</b>  | Настраивает интерфейс с аутентификацией в виде открытого текста |
| <b>ip rip password <i>string</i></b> | Настраивает ключ аутентификации в виде открытого текста         |

Чтобы настроить аутентификацию RIP при помощи MD5, выполните следующие действия в режиме настройки интерфейса:

| Команда  | Описание   |
|--|--|
| <b>ip rip authentication message-digest</b>            | Настраивает интерфейс с аутентификацией MD5                        |
| <b>ip rip message-digest-key <i>key-ID md5 key</i></b> | Настраивает ключ аутентификации MD5 и идентификатор аутентификации |

### 24.1.8 Запрет суммирования маршрутов

По умолчанию протокол RIP-2 автоматически суммирует маршруты при пересечении границ сети, чтобы уменьшить объем информации. Это означает, что маршруты объединяются в более крупные блоки при передаче за пределы классифицированной сети. Функция автоматического сбора маршрутов RIP-1 всегда активирована.

Однако, если у вас есть отдельная подсеть, чьи маршруты вы не хотите объединять в более крупный блок при пересечении границы сетей, вам нужно запретить автоматическое суммирование.

В режиме настройки маршрутизатора выполните следующую команду:

| Команда                | Описание                              |
|------------------------|---------------------------------------|
| <b>no auto-summary</b> | Запрещает автоматическое суммирование |



### 24.1.9 Запрет аутентификации исходного IP-адреса

По умолчанию маршрутизатор проверяет подлинность IP-адреса источника полученного обновления маршрута. Если этот адрес недопустим, обновление маршрутизатора будет отклонено.

Если у вас есть маршрутизатор и вы надеетесь получить от него обновление, но вы не настроили соответствующую информацию о сети или соседнем узле на приемнике, эту функцию следует запретить. Однако в обычной практике эту команду использовать не рекомендуется.

| Команда                          | Описание   |
|----------------------------------|--|
| <b>no validate-update-source</b> | Запрещает аутентифицировать исходный IP-адрес входящего обновления RIP |

### 24.1.10 Настройка максимального количества маршрутов

По умолчанию локальная таблица маршрутизации RIP содержит до 1024 маршрутов. Когда количество маршрутов превышает максимальное значение, новые маршруты в таблицу маршрутизации добавляться не смогут, и система уведомит об этом. Выполните следующую команду в режиме настройки маршрутизатора, чтобы указать максимальное количество маршрутов для локальной таблицы маршрутизации RIP:

| Команда                            | Описание  |
|------------------------------------|---|
| <b>maximum-count</b> <i>number</i> | Настраивает максимальное количество маршрутов для локальной таблицы маршрутизации RIP |

Активация или запрет режима расщепления горизонта

В обычных условиях маршрутизатор, подключенный к IP-сети и использующий протокол дистанционно-векторной маршрутизации, будет использовать расщепление горизонта для оптимизации коммуникации между несколькими маршрутизаторами, особенно когда образуется петля.

Расщепленный горизонт препятствует передаче информации о маршруте обратно по тому интерфейсу, с которого эта информация была получена. Однако, при работе с нешироковещательными сетями, например, Frame Relay (FR), применение данной функции может обернуться сложностями, поэтому во многих случаях рекомендуется ее отключить.

Также стоит упомянуть, что, если интерфейс настроен с дополнительным IP-адресом, и при этом включено расщепление горизонта, исходный IP-адрес обновления маршрута может не включать все вторичные IP-адреса. В каждом обновлении маршрутизации исходный IP-адрес будет включать только один номер сети, если, конечно, расщепление горизонта не отключено.



Чтобы активировать или запретить расщепление горизонта, в режиме настройки интерфейса необходимо выполнить следующие команды:



| Команда                        | Описание                         |
|--------------------------------|----------------------------------|
| <b>ip rip split-horizon</b>    | Активирует расщепление горизонта |
| <b>no ip rip split-horizon</b> | Запрещает расщепление горизонта  |

По умолчанию для интерфейса «точка-точка» активируется расщепленный горизонт; для интерфейса «точка-множество точек» расщепление горизонта запрещено.



Обычно рекомендуется оставить состояние по умолчанию неизменным, если только вы не уверены, что ваше приложение не сможет правильно объявить маршрут, пока вы не измените настройки. Всегда помните: если расщепление горизонта запрещено на последовательном интерфейсе (и интерфейс подключен к сети с коммутацией пакетов), вам необходимо запретить расщепление горизонта для всех маршрутизаторов соответствующей группы многоадресной рассылки в этой сети.

## 24.1.11 Мониторинг и поддержка RIP

При мониторинге RIP может отображаться сетевая статистика, такая как: конфигурация параметров протокола RIP, использование сети, отслеживание сетевых коммуникаций в реальном времени и т. д. Эта помогает оценивать использование сетевых ресурсов, а также решать сетевые проблемы и узнавать о доступности сетевых узлов.

Выполните следующие команды в режиме управления, чтобы отобразить статистику маршрутизации:

| Команда                     | Описание  |
|-----------------------------|---|
| <b>show ip rip</b>          | Отображает текущее состояние всех процессов RIP       |
| <b>show ip rip database</b> | Отображает все маршруты RIP                           |
| <b>show ip rip protocol</b> | Отображает всю необходимую информацию о протоколе RIP |

В режиме управления также доступна отладочная информация RIP:

| Команда | Описание |
|---------|----------|
|---------|----------|



|                                    |   |
|------------------------------------|---|
| <code>debug ip rip database</code> | Отслеживает информацию о процедуре маршрутизации RIP, такую как вставка в таблицу маршрутизации, удаление из таблицы маршрутизации, изменение маршрутов и т. д. |
| <code>debug ip rip protocol</code> | Отслеживает сообщения протокола RIP   |

### 24.1.12 Пример настройки RIP

Два коммутатора, А и В, настраиваются следующим образом:

#### Коммутатор А:

```
interface vlan 11
ip address 192.168.20.81 255.255.255.0
!
interface loopback 0
ip address 10.1.1.1 255.0.0.0
!
router rip
network 192.168.20.0
network 10.0.0.0
!
```

#### Коммутатор В:

```
interface vlan 11
ip address 192.168.20.82 255.255.255.0
interface loopback 0
ip address 20.1.1.1 255.0.0.0
!
router rip
network 192.168.20.0
network 20.0.0.0
!
```



## 24.2 BEIGRP

### 24.2.1 Введение

Технология, используемая динамическим протоколом BEIGRP, аналогична протоколу дистанционно-векторной маршрутизации:

- маршрутизатор принимает решения о маршрутизации только на основе информации, предоставленной напрямую подключенными соседями;
- маршрутизатор предоставляет информацию о маршрутизации, которую он использует, только напрямую подключенным соседям.

Тем не менее, BEIGRP имеет некоторые базовые отличия от протокола дистанционно-векторной маршрутизации, что дает ему больше преимуществ:

- BEIGRP сохраняет в таблице топологии все маршруты от всех соседей, а не только лучшие на данный момент маршруты;
- BEIGRP способен отправлять запросы соседям, когда не может получить доступ к месту назначения и нет альтернативных маршрутов, поэтому скорость конвергенции BEIGRP может конкурировать с лучшими протоколами состояния канала.

Алгоритм диффузного обновления (DUAL) – важная функция, дающая BEIGRP преимущество перед другими традиционными дистанционно-векторными протоколами. Функция всегда активно работает и опрашивает соседей, когда не может получить доступ к месту назначения и нет альтернативных маршрутов (возможная замена). Поскольку процесс конвергенции является активным, а не негативным (ожидание тайм-аута маршрутизаторов), скорость конвергенции BEIGRP очень высока.

BEIGRP – это специальный протокол маршрутизации, разработанный для адаптации к требованиям EIGRP и непосредственно основанный на IP. BEIGRP выполняет следующие требования:

- появление новых соседей и исчезновение старых автоматически определяется при помощи Hello-сообщений;
- передача данных надежна;
- протокол позволяет передавать данные в режимах одноадресной и многоадресной передачи;
- протокол передачи сам может адаптироваться к изменению сетевых условий и реакции соседей;
- BEIGRP может ограничить процент занятости полосы пропускания в соответствии с требованиями.

Для настройки BEIGRP необходимо выполнить задачи, среди которых обязательной является активация протокола, а остальные можно выполнять в соответствии с требованиями.

- Активация протокола BEIGRP
- Настройка процента используемой пропускной способности



- Настройка арифметического коэффициента суммарного расстояния BEIGRP
- Использование смещения для настройки суммарного расстояния
- Отключение автоматического суммирования
- Импортинг других маршрутов в процесс BEIGRP
- Настройка таймеров BEIGRP
- Отключение расщепления горизонта
- Мониторинг и поддержка BEIGRP

## 24.2.2 Активация протокола BEIGRP

Для создания процесса BEIGRP необходимо выполнить следующие команды:

| Команда   | Описание  |
|---|---|
| <b>router beigrp</b> <i>as-number</i>                       | Добавляет процесс BEIGRP в режиме глобальной конфигурации                       |
| <b>network</b> <i>network-number</i><br><i>network-mask</i> | Добавляет адреса к указанному процессу BEIGRP в режиме настройки маршрутизатора |

После завершения вышеуказанной настройки BEIGRP начнет работать на всех интерфейсах, принадлежащих этому адресу, обнаружит новых соседей через «Hello» и осуществит первоначальное взаимодействие по маршрутизации через «Update».

## 24.2.3 Настройка процента используемой пропускной способности

По умолчанию BEIGRP может занимать не более 50 % пропускной способности. Вы можете выполнить следующую команду в режиме настройки интерфейса VLAN, чтобы указать полосу пропускания, которая будет доступна для BEIGRP:

| Команда   | Описание   |
|---|--|
| <b>ip beigrp bandwidth-percent</b> <i>percent</i> | Настраивает максимальный процент полосы пропускания, используемый сообщениями BEIGRP |

## 24.2.4 Настройка арифметического коэффициента суммарного расстояния BEIGRP

В определенных ситуациях может потребоваться корректировка арифметического коэффициента суммарного расстояния BEIGRP, что, в конечном итоге, влияет на политику маршрутизации. Хотя арифметический коэффициент BEIGRP по умолчанию удовлетворяет требованиям большинства сетей, при определенных условиях его все же может



потребуется скорректировать. Эта настройка может привести к большим изменениям во всей сети, поэтому выполнять ее необходимо с осторожностью.

Используйте следующую команду в режиме настройки маршрутизатора:

| Команда                                     | Описание  |
|---|---|
| <b>metric weights</b> <i>k1 k2 k3 k4 k5</i> | Настройка арифметического коэффициента суммарного расстояния BEIGRP |

## 24.2.5 Использование смещения для настройки суммарного расстояния

С помощью таблицы смещения можно умышленно изменять суммарное расстояние для всех входящих и исходящих маршрутов в соответствии с заданными требованиями. Это делается для определенных маршрутов, удовлетворяющих определенным условиям. Цель такого подхода – влияние на итоговую маршрутизацию, чтобы она соответствовала нашим ожиданиям. На этапе настройки пользователь может выбирать между списком доступа или применяемым интерфейсом в списке смещения, в зависимости от своих потребностей, чтобы конкретно указать, для каких маршрутов следует применять операцию смещения.

Выполните следующую команду:

| Команда  | Описание                   |
|--|----------------------------|
| <b>offset</b> { <i>type number   *</i> } { <i>in   out</i> }<br><i>access-list-name offset</i> | Применяет таблицу смещения |

## 24.2.6 Отключение автосуммирования

Автоматический сбор маршрутных данных BEIGRP отличается от других протоколов динамической маршрутизации. Он соответствует следующим правилам:

- Если имеется несколько подсетей, и хотя бы одна из них зарегистрирована в системе маршрутизации BEIGRP, то маршрутизатор создаст общий маршрут, который будет представлять всю сеть.
- Созданный обобщенный маршрут BEIGRP направлен на интерфейс Null0 и имеет минимальную дистанцию среди всех подсетей. Этот обобщенный маршрут также добавляется в основную таблицу IP-маршрутизации. Его административная дистанция составляет 5, и её нельзя изменить.
- Когда информация об обновлениях отправляется соседним маршрутизаторам в разных основных IP-сетях, подсети, связанные с обобщенным маршрутом по правилам 1 и 2, больше не передаются. Вместо этого отправляется только сам обобщенный маршрут.
- Подсети, которые не входят ни в одну из сетей, определенных в процессе BEIGRP, не будут собираться или учитываться.



В некоторых условиях может понадобиться сообщать соседним маршрутизаторам о каждом отдельном маршруте. В этом случае нужно выполнить следующую команду:

| Команда                | Описание                   |
|------------------------|----------------------------|
| <b>no auto-summary</b> | Отключает автосуммирование |

### 24.2.7 Настройка обобщения маршрутов

Когда автоматическое обобщение маршрутов не подходит для ваших условий, вы можете вручную настроить обобщение маршрутов на каждом интерфейсе, где работает BEIGRP, указав, какие сети должны использовать обобщение. Такие интерфейсы не будут отправлять подробную информацию о маршрутах для указанных сетей. Остальные интерфейсы при этом не затрагиваются.

Операции обобщения маршрутов подчиняются следующим правилам:

Когда вы настраиваете обобщение маршрутов на интерфейсе, создается обобщенный маршрут для указанной сети, если хотя бы одна подсеть этой сети есть в таблице BEIGRP.

Этот обобщенный маршрут направляется на интерфейс Null0 и имеет наименьшую стоимость среди всех подсетей. Он также добавляется в основную таблицу маршрутизации IP и имеет фиксированное значение административной дистанции 5 (это значение нельзя изменить).

Когда информация о маршрутах отправляется с интерфейса, на котором настроено обобщение, подробные маршруты для этой сети не будут отправляться. При этом информация о других маршрутах останется без изменений.

| Команда   | Описание   |
|---|--|
| <b>ip beigrp summary-address</b> <i>ip-address</i><br><i>address mask</i> | Настраивает суммирование маршрутов на интерфейсе |

### 24.2.8 Импортрование других маршрутов в процесс BEIGRP

Когда протокол BEIGRP пересылает маршруты других типов, соблюдаются следующие правила:

- Нет необходимости настраивать параметры с помощью команды **default-metric** при перераспределении статических и прямо подключенных маршрутов. Соответствующий параметр (например, пропускная способность, задержка, надежность, нагрузка и MTU) получается из соответствующих настроек интерфейса.
- Нет необходимости настраивать параметры с помощью команды **default-metric** при перераспределении маршрутов другого процесса BEIGRP. Соответствующий параметр получается из исходного процесса.



- Необходимо настроить параметры с помощью команды `default-metric` при импортировании маршрутов из других протоколов (например, RIP, OSPF). Команда устанавливает значение, которое определяет, как маршруты будут передаваться. Без этого значения передача маршрутов не будет работать.

В маршрутизаторе, использующем одновременно BEIGRP и RIP, необходимо настроить параметры с помощью следующих команд, если нужно получить маршруты из протокола RIP в протокол BEIGRP:

| Команда   | Описание   |
|---|--|
| <code>default-metric bandwidth delay reliability loading mtu</code> | Настраивает векторное расстояние по умолчанию для переадресации маршрута |
| <code>redistribute protocol [process] [route-map name]</code>       | Перераспределяет маршруты в протокол BEIGRP                              |

## 24.2.9 Настройка дополнительных параметров BEIGRP

Чтобы адаптироваться к различным сетевым средам и сделать BEIGRP более эффективным и полнофункциональным, может потребоваться настроить следующие параметры:

- временной интервал BEIGRP для отправки сообщений «Hello» и таймаут времени устаревания информации о соседних устройствах;
- расщепление горизонта

1. Настройка временного интервала BEIGRP для отправки сообщений Hello и таймаута времени устаревания информации о соседних устройствах

Алгоритм отправки сообщений Hello выполняет три функции, обеспечивающие правильную работу BEIGRP:

- обнаруживает доступных новых соседей. Обнаружение происходит автоматически и не требует ручной настройки;
- проверяет конфигурацию соседей и разрешает связь только с соседями, настроенными в совместимом режиме;
- продолжает поддерживать доступность соседей и обнаруживает их исчезновение.

Маршрутизатор отправляет многоадресный пакет Hello на все интерфейсы, на которых работает BEIGRP. Все маршрутизаторы, поддерживающие BEIGRP, входят в эти группы многоадресной рассылки, чтобы они могли обнаружить всех соседей.

Протокол Hello использует два таймера для обнаружения исчезновения соседей: интервал приветствия определяет частоту отправки сообщений приветствия BEIGRP на интерфейс маршрутизатора, а таймер удержания определяет интервал времени, в течение которого маршрутизатор должен ждать данные связи от соседнего устройства до объявления о его



исчезновении. Каждый раз, когда маршрутизатор получает пакет BEIGRP от соседнего узла, он сбрасывает таймер удержания.

Для разных типов сети и разной пропускной способности будет использоваться разное значение таймера приветствия по умолчанию.

Таблица 12 – Значение таймеров по умолчанию

| Инкапсуляция типа интерфейса |       | Таймер приветствия (секунды) | Таймер удержания (секунды) |
|------------------------------|-------|------------------------------|----------------------------|
| Интерфейс LAN                | Любой | 5                            | 15                         |

Разница в значении таймера по умолчанию в протоколе Hello может привести к тому, что соседи BEIGRP, подключенные к разным IP-подсетям, будут использовать разные таймеры приветствия и удержания. Для решения этой проблемы каждый маршрутизатор указывает свой собственный таймер Hold в Hello-пакете, и каждый маршрутизатор BEIGRP использует этот указанный таймер от соседей для определения времени ожидания данного соседа. Это может привести к появлению разных таймеров обнаружения ошибок соседей в разных частях одной и той же сети WAN. Но в некоторых случаях значения таймеров по умолчанию не подходят, поэтому если вы хотите настроить интервал отправки сообщений Hello, используйте следующую команду:

| Команда                                 | Описание   |
|---|--|
| <b>ip beigrp hello-interval seconds</b> | Регулирует временной интервал отправки сообщения Hello для выбранного интерфейса |

Если вы хотите настроить время ожидания соседа, используйте следующую команду:

| Команда                            | Описание  |
|------------------------------------|---|
| <b>ip beigrp hold-time seconds</b> | Регулирует временной интервал, по истечении которого соседний узел объявляется несуществующим |

## 2. Отключение расщепления горизонта

В обычных условиях целесообразно использовать функцию расщепления горизонта. Это предотвратит передачу информации о маршрутизации обратно на ее исходный интерфейс, чтобы избежать заикливания маршрута. Но при определенных обстоятельствах это неоптимальный выбор, в таком случае можно использовать следующую команду, чтобы отключить данную функцию:



| Команда                           | Описание                        |
|-----------------------------------|---------------------------------|
| <b>no ip beigrp split-horizon</b> | Отключает расщепления горизонта |

### 24.2.10 Мониторинг и поддержка BEIGRP

Чтобы очистить информацию об окружении, включая все соседние узлы, используйте следующую команду:

| Команда                                      | Описание                     |
|--|------------------------------|
| <b>clear ip beigrp neighbors [interface]</b> | Удаляет информацию о соседях |

Чтобы отобразить различную статистическую информацию BEIGRP, выполните следующие команды:

| Команда  | Описание                            |
|--|-------------------------------------|
| <b>show ip beigrp interface [interface] [as-number]</b>                  | Отображает информацию об интерфейсе |
| <b>show ip beigrp neighbors [as-number]   interface]</b>                 | Отображает информацию о соседях     |
| <b>show ip beigrp topology [as-number   all-link   summary   active]</b> | Отображает информацию о топологии   |

### 24.2.11 Пример настройки BEIGRP

В этом примере мы настраиваем обобщенный маршрут для сети 10.0.0.0/8 на VLAN 11. Это означает, что все подсети этой сети не будут отправляться соседним маршрутизаторам. Также в этом примере отключается автоматическое обобщение в процессе BEIGRP.

```
interface vlan 11
ip beigrp summary-address 1 10.0.0.0 255.0.0.0
!
router beigrp 1
network 172.16.0.0 255.255.0.0
no auto-summary
```

## 24.3 OSPF



### 24.3.1 Введение

OSPF – это протокол динамической маршрутизации внутреннего шлюза (IGP), основанный на технологии отслеживания состояния канала. Он предназначен для маршрутизации IP-трафика внутри сети, поддерживает информацию о подсетях IP и внешних маршрутах, а также обеспечивает аутентификацию сообщений и поддерживает многоадресную рассылку.

Реализация OSPF коммутаторов данной серии соответствует спецификации OSPF V2 (относится к RFC2328). Некоторые ключевые моменты реализации перечислены ниже:

**Тупиковая зона** – поддержка тупиковой зоны (Stub Area), что означает, что внутри этой области используются особые правила маршрутизации.

**Перераспределение маршрутов** – возможность передачи маршрутов, полученных одним маршрутизационным протоколом, другому. Например, маршруты, изученные OSPF, могут быть переданы протоколу RIP, и наоборот. Это также работает между разными автономными системами и другими протоколами, такими как BGP.

**Аутентификация** – поддержка методов аутентификации, включая Plaintext и MD5, для обеспечения безопасности при обмене данными между соседними маршрутизаторами в одной области.

**Параметры интерфейса маршрутизатора** – возможность настройки различных параметров интерфейса, таких как стоимость исходящего соединения, интервал повторной отправки, задержка передачи, приоритет маршрутизатора, интервал передачи Hello-сообщений и пароль аутентификации.

**Виртуальный канал** – поддерживается Virtual link

**Зона NSSA** – это отсылка к RFC 1587 и связанным с ним особенностям области NSSA (Not So Stubby Area) в OSPF.

**OSPF по запросу** – упоминается RFC 1793, может быть полезен в сценариях, таких как VPN-соединения, где соединение устанавливается только по мере необходимости, или в сетях с переменной загрузкой.

OSPF требует обмена данными маршрутизации между всеми маршрутизаторами ABR и ASBR в домене. Чтобы упростить настройку, можно позволить им всем работать с параметрами по умолчанию (без аутентификации и т. д.), но, если вы хотите изменить некоторые параметры, необходимо убедиться, что одинаковые изменения проведены на всех маршрутизаторах.

Чтобы настроить OSPF, выполните следующие задачи. Помимо необходимости активации OSPF, все остальные настройки не являются обязательными.

- Запуск OSPF
- Настройка параметров интерфейса OSPF
- Настройка OSPF в разных физических сетях
- Настройка домена OSPF
- Настройка зоны NSSA



- Настройка суммирования маршрутов в домене OSPF
- Настройка сбора данных пересылающим маршрутизатором
- Создание маршрута по умолчанию
- Выбор идентификатора маршрутизатора через интерфейс Loopback
- Настройка административной дистанции OSPF
- Настройка таймера расчета маршрута
- Мониторинг и поддержка OSPF

## 24.3.2 Запуск OSPF

Как и другие протоколы маршрутизации, активация OSPF требует создания процесса маршрутизации, выделения диапазона IP-адресов, связанного с исполняемым процессом, выделения идентификатора области, связанного с диапазоном IP-адресов. В режиме глобальной конфигурации используйте следующие команды:

| Команда   | Описание   |
|---|--|
| <b>router ospf</b> <i>process-id</i>            | Активирует протокол маршрутизации OSPF и входит в режим настройки маршрутизатора |
| <b>network</b> <i>address mask area area-id</i> | Настраивает интерфейс(ы), на которых работает OSPF, и идентификатор зоны         |

## 24.3.3 Настройка параметров интерфейса OSPF

Во время настройки OSPF разрешено изменять параметры, относящиеся к интерфейсу, в соответствии с требованиями. Нет необходимости изменять какой-либо параметр, но идентичность параметров должна быть гарантирована на всех маршрутизаторах в подключенной сети.

В режиме настройки интерфейса используйте следующие команды:

| Команда   | Описание   |
|---|--|
| <b>ip ospf cost</b> <i>cost</i>                   | Настраивает метрику интерфейса OSPF для пересылки пакетов  |
| <b>ip ospf retransmit-interval</b> <i>seconds</i> | Устанавливает интервал повторной передачи LSA между соседями, принадлежащими одному и тому же интерфейсу OSPF (в секундах) |
| <b>ip ospf transmit-delay</b> <i>seconds</i>      | Настраивает расчетное время передачи LSA на интерфейсе OSPF (в секундах)   |



|  |   |
|--|---|
| <b>ip ospf priority</b> <i>number</i>                  | Настраивает приоритет маршрутизатора, необходимый для выбора DR   |
| <b>ip ospf hello-interval</b> <i>seconds</i>           | Настраивает временной интервал для отправки пакета приветствия через интерфейс OSPF   |
| <b>ip ospf dead-interval</b> <i>seconds</i>            | Настраивает время ожидания ответа соседнего узла (в секундах). Если маршрутизатор не получает пакет Hello от соседа в течение определенного интервала времени, он считает, что соседний маршрутизатор выключен  |
| <b>ip ospf authentication-key</b> <i>key</i>           | Используется для установки простого текстового ключа аутентификации для OSPF на конкретном интерфейсе. Только маршрутизаторы, знающие этот пароль, могут установить соседство и обмениваться маршрутной информацией   |
| <b>ip ospf message-digest-key</b> <i>keyid md5 key</i> | Настраивает аутентификацию MD5  |
| <b>ip ospf passive</b>                                 | Устанавливает интерфейс OSPF в пассивный режим. Когда интерфейс находится в пассивном режиме, он не будет отправлять OSPF Hello-пакеты и, следовательно, не участвует в процессе обнаружения и обмена OSPF маршрутной информацией   |
| <b>ip ospf passive</b>                                 | Используется для настройки интерфейса маршрутизатора в режиме «пассивного» OSPF. Это означает, что OSPF не будет отправлять или принимать OSPF-обновления (hello-пакеты) на этом интерфейсе, но маршрутизатор все равно будет рассматривать этот интерфейс как часть OSPF-области |

## 24.3.4 Настройка OSPF в разных физических сетях

OSPF разделяет физическую среду сети на следующие три категории:

- широковещательная сеть (Ethernet, Token Ring, FDDI);
- нешироковещательная сеть с множественным доступом (SMDS, Frame Relay, X.25);
- сеть «точка-точка» (HDLC, PPP).

Сети X.25 и Frame Relay предоставляют дополнительные возможности широковещательной передачи. OSPF можно настроить для работы в широковещательных сетях с помощью мар-



команд. Информацию о команде **map** см. в описании команд x.25 и Frame Relay в Справочнике команд WAN.

Независимо от типа физической среды сети, вы можете настроить свою сеть как ширококвещательную или как нешироковещательную сеть с множественным доступом (NBMA). Это позволяет гибко настраивать сеть, например, можно преобразовать физическую сеть с ширококвещательной рассылкой в сеть без нее, а также наоборот. Это также упрощает настройку соседей в сети.

Настройка сети OSPF с типом NBMA может быть сложной, особенно если вы пытаетесь имитировать поведение ширококвещательной сети. В случае, если у вас есть несколько маршрутизаторов, которые должны обмениваться маршрутной информацией, но они не могут автоматически обнаружить друг друга, вам нужно будет вручную настраивать соседство.

Использование виртуальных соединений может помочь соединить разрозненные области OSPF, но это не является практическим решением для обычных маршрутизаторов, которые не имеют физического соединения. Вместо этого, для экономии ресурсов и упрощения настройки, вы можете рассмотреть возможность настройки сети как «точка-множество точек». Это позволит маршрутизаторам обмениваться маршрутной информацией без необходимости ручной настройки каждого соединения, что делает конфигурацию более эффективной и менее затратной.

Интерфейс OSPF «точка-множество точек» может быть определен как несколько сетевых интерфейсов «точка-точка», которые создают несколько маршрутов к хостам. Сеть OSPF «точка-множество точек» имеет следующие преимущества перед сетями NBMA и «точка-точка»:

- Сеть «точка-множество точек» легко настраивается, она не требует специальной настройки соседнего узла, использует только один IP-адрес и не создает DR.
- Поскольку для такой сети не требуется построения полносвязной топологии, это обходится дешевле.
- Такая сеть более надежна. Даже если виртуальные каналы выходят из строя, соединение все равно сохраняется.

В режиме настройке интерфейса укажите тип сети OSPF с помощью следующей команды:

| Команда  | Описание                  |
|--|---------------------------|
| <code>ip ospf network {broadcast   non-broadcast   {point-to-multipoint [non-broadcast]}}</code> | Настраивает тип сети OSPF |

### 24.3.5 Настройка области OSPF

Настраиваемые параметры области OSPF включают в себя: аутентификацию, назначение тупиковой зоны, назначение метрики для суммарного маршрута по умолчанию. Аутентификация использует защиту на основе паролей.



Тупиковые зоны (Stub Area) – это те области, в которых не распределяются внешние маршруты. Вместо этого ABR генерирует внешний маршрут по умолчанию для связи с тупиковой зоной, позволяющий ей выйти во внешнюю сеть автономной системы. Чтобы использовать функции поддержки тупиковой зоны OSPF, следует применить в ней маршрут по умолчанию. Чтобы дополнительно уменьшить количество LSA, отправляемых в тупиковую зону, можно запретить сборку маршрутов ABR, чтобы уменьшить отправку в нее сводных LSA (тип 3).

В режиме настройки маршрутизатора используйте следующие команды для определения параметров области:

| Команда   | Описание   |
|---|--|
| <b>area area-id authentication simple</b>         | Активирует аутентификацию в домене OSPF                          |
| <b>area area-id authentication message-digest</b> | Позволяет OSPF использовать MD5 для аутентификации               |
| <b>area area-id stub [no-summary]</b>             | Определяет тупиковую зону  |
| <b>area area-id default-cost cost</b>             | Устанавливает метрику для маршрута по умолчанию в тупиковой зоне |

### 24.3.6 Настройка суммирования маршрутов в области OSPF

Эта функция позволяет маршрутизатору ABR передавать суммарный маршрут другим зонам. В OSPF ABR передает информацию о каждой сети в другие зоны. Однако, если номера сетей можно сгруппировать по определенному методу, и они идут подряд, целесообразно настроить ABR для передачи другим областям суммарного маршрута. Он может охватывать все сети в определенном диапазоне.

В режиме настройки маршрутизатора используйте следующую команду для определения диапазонов адресов:

| Команда                                | Описание   |
|--|--|
| <b>area area-id range address mask</b> | Определяет диапазон адресов для суммирования маршрутов |

### 24.3.7 Настройка сбора данных пересылающим маршрутизатором

Когда маршруты распределяются из других областей в OSPF, они передаются с помощью различных типов LSA. Например, маршруты, полученные из других протоколов маршрутизации, могут быть объявлены с использованием Type 5 LSA (External LSA).



Для оптимизации использования ресурсов и уменьшения размера базы данных состояния каналов OSPF, можно настроить агрегирование маршрутов. Это позволяет объединить несколько маршрутов в один, что снижает количество записей в базе данных OSPF и упрощает управление маршрутизацией.

В режиме конфигурации маршрутизатора используйте следующую команду для настройки сбора данных о маршрутах:

| Команда   | Описание   |
|---|--|
| <b>summary-address</b> <i>prefix mask</i> [not advertise] | Описывает адрес и маску, охватывающую распространяемый маршрут. Транслируется только один обобщенный маршрут |

### 24.3.8 Создание маршрута по умолчанию

ASBR (Autonomous System Boundary Router) – это маршрутизатор, который соединяет OSPF с другими протоколами маршрутизации. Чтобы ASBR мог передавать маршруты в область OSPF, он может генерировать маршрут по умолчанию, который обеспечивает доступ к внешним сетям.

Когда вы настраиваете маршрутизатор для распределения маршрутов в область OSPF, этот маршрутизатор становится ASBR, если он импортирует маршруты из других протоколов. Однако не все ASBR автоматически генерируют маршрут по умолчанию в OSPF, и это поведение зависит от конфигурации.

В режиме настройки маршрутизатора используйте следующую команду, чтобы ASBR мог создавать маршрут по умолчанию:

| Команда  | Описание   |
|--|--|
| <b>default-information originate</b> [always] [route-map <i>map-name</i> ] | Указывает маршрутизатору ASBR создавать маршрут по умолчанию |

### 24.3.9 Выбор идентификатора маршрутизатора через интерфейс Loopback

Интерфейс обратной связи (Loopback) представляет собой виртуальный интерфейс на маршрутизаторе. Он создается программно и не имеет ассоциированных с ним физических аппаратных устройств. Этот интерфейс имеет особое значение в протоколе OSPF.

OSPF использует наибольший IP-адрес, настроенный на интерфейсе, в качестве идентификатора маршрутизатора. Если интерфейс, подключенный к этому IP-адресу, перейдет в состояние ВЫКЛЮЧЕНО или этот IP-адрес будет удален, процесс OSPF перезапустится для расчета нового идентификатора маршрутизатора и повторной отправки информации о маршрутизации со всех интерфейсов.



Если один интерфейс Loopback настроен с IP-адресом, то маршрутизатор использует этот IP-адрес в качестве идентификатора маршрутизатора, поскольку интерфейс обратной связи никогда не отключается, и это делает таблицу маршрутизации более стабильной.

Маршрутизатор предпочтительно использует интерфейс обратной связи в качестве идентификатора маршрутизатора, при этом выбирает самый большой IP-адрес среди всех Loopback-интерфейсов. Если интерфейс обратной связи отсутствует, используется наибольший IP-адрес маршрутизатора. Вы не можете указать OSPF использовать какой-либо специальный интерфейс.

В режиме глобальной конфигурации используйте следующую команду для настройки IP-интерфейса Loopback:

| Команда                           | Описание   |
|-----------------------------------|--|
| <b>interface loopback 0</b>       | Создает интерфейс Loopback и входит в режим настройки интерфейса |
| <b>ip address ip-address mask</b> | Выделяет IP-адрес для интерфейса                                 |

## 24.3.10 Настройка административной дистанции OSPF

Административная дистанция определяет уровень надежности источника информации о маршрутах, такого как маршрутизатор или группа маршрутизаторов. Общими словами, административная дистанция – это целое число от 0 до 255, и чем выше значение, тем ниже уровень надежности. Если административная дистанция равна 255, то источник информации о маршруте не считается надежным и его следует игнорировать.

В OSPF используются три типа административной дистанции: для маршрутов внутри области (intra-area), для маршрутов к другим зонам (inter-area) и для маршрутов, распространяемых из других автономных систем (external). Значение административной дистанции по умолчанию для каждого типа маршрута равно 110.

В режиме настройки маршрутизатора используйте следующую команду для установки значения административной дистанции OSPF:

| Команда   | Описание  |
|---|---|
| <b>distance ospf [intra-area dist1] [inter-area dist2] [external dist3]</b> | Изменяет значение административной дистанции для внутреннего, междоменного и внешнего маршрута OSPF |

## 24.3.11 Настройка таймера расчета маршрута

Вы можете настроить временную задержку между моментом получения OSPF информации о топологических изменениях и началом расчета таблицы маршрутизации по алгоритму



SPF. Также можно настроить интервал между двумя последовательными расчетами SPF. В режиме настройки маршрутизатора используйте следующие команды:

| Команда                              | Описание   |
|--------------------------------------|--|
| <b>timers delay</b> <i>delaytime</i> | Устанавливает задержку начала расчета маршрута после получения данных                    |
| <b>timers hold</b> <i>holdtime</i>   | Устанавливает минимальный временной интервал между двумя последовательными расчетами SPF |

## 24.3.12 Мониторинг и поддержка OSPF

Команда **show** позволяет отображать статистическую информацию о сети, такую как содержимое таблицы IP-маршрутизации, кэша и базы данных. Эта информация может помочь оценить использование сетевых ресурсов и решить возникшую сетевую проблему. Вы можете проверить доступность сетевых узлов, узнать маршруты, по которым пакеты данных проходят через сеть.

Используйте следующие команды для отображения статистики маршрутизации:

| Команда  | Описание  |
|--|---|
| <b>show ip ospf</b> [ <i>process-id</i> ]  | Отображает общую информацию о процессе маршрутизации OSPF |
| <b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b><br><b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>router</b> ] [ <i>link-state-id</i> ]<br><b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>router</b> ] [ <b>self-originate</b> ]<br><b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>router</b> ] [ <b>adv-router</b> ] [ <i>ip-address</i> ]<br><b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>network</b> ] [ <i>link-state-id</i> ]<br><b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>summary</b> ] [ <i>link-state-id</i> ]<br><b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>asbr-summary</b> ] [ <i>link-state-id</i> ]<br><b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>external</b> ] [ <i>link-state-id</i> ]<br><b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>database-summary</b> ] | Отображает соответствующую информацию базы данных OSPF    |



|   |  |
|---|--|
| <b>show ip ospf border-routers</b>  | Отображает записи таблицы внутренней маршрутизации ABR и ASBR  |
| <b>show ip ospf interface</b>   | Отображает информацию об интерфейсе OSPF   |
| <b>show ip ospf neighbor</b>  | Отображает информацию о соседях OSPF в соответствии с интерфейсом  |
| <b>debug ip ospf adj</b>  | Отслеживает информацию об установлении коммуникации соседних узлов OSPF  |
| <b>debug ip ospf events</b>   | Отслеживает информацию о событиях, связанных с OSPF, таких как изменения состояния интерфейсов, обмен OSPF-пакетами и т.д. |
| <b>debug ip ospf flood</b>  | Отслеживает процесс заполнения базы данных OSPF  |
| <b>debug ip ospf lsa-generation</b>   | Отслеживает генерацию LSA OSPF   |
| <b>debug ip ospf packet</b>   | Отслеживает сообщения OSPF   |
| <b>debug ip ospf retransmission</b>   | Отслеживает повторную передачу сообщений OSPF  |
| <b>debug ip ospf spf</b><br><b>debug ip ospf spf intra</b><br><b>debug ip ospf spf inter</b><br><b>debug ip ospf spf external</b> | Отслеживает информацию о маршрутных расчетах SPF   |
| <b>debug ip ospf tree</b>   | Отслеживает создание дерева SPF  |

## 24.3.13 Примеры настройки OSPF

### 24.3.13.1 Пример конфигурации VLSM

OSPF и статические маршруты поддерживают маску подсети с переменной длиной (VLSM). Благодаря VLSM разные маски на разных интерфейсах могут использовать один и тот же сетевой номер. Таким образом, сохраняется IP-адрес и эффективно используется адресное пространство.



В следующем примере используется 30-значная маска подсети. 2-значное адресное пространство зарезервировано для адреса хоста последовательного порта. Для последовательного соединения точка-точка достаточно двух адресов хоста.

```
interface vlan 10
```

```
ip address 131.107.1.1 255.255.255.0
```

! 8 бит адресного пространства хоста зарезервировано для Ethernet

```
interface vlan 11
```

```
ip address 131.107.254.1 255.255.255.252
```

! 2 бита адресного пространства зарезервировано для последовательных линий

```
router ospf 107
```

! Маршрутизатор настроен для OSPF и назначена AS 107

```
network 131.107.0.0 0.0.255.255 area 0.0.0.0
```

! Указана сеть, напрямую подключенную к маршрутизатору

### 24.3.13.2 Примеры настройки маршрута OSPF и распределения маршрутов

OSPF требует обмена информацией между внутренними коммутаторами, ABR и ASBR. В минимальной конфигурации коммутатор на основе OSPF может работать с настройками параметров по умолчанию. Требование аутентификации отсутствует.

Ниже приведены три примера конфигурации. В первом примере показаны основные команды OSPF. Во втором показано, как настроить внутренние коммутаторы маршрутизации ABR и ASBR в автономной системе. В третьем примере используются все виды инструментов OSPF.

#### 1. Пример базовой конфигурации OSPF

В следующем примере показано, как настроить простой OSPF. Активируйте процесс маршрутизации 90; подключите интерфейс Ethernet 0 к области 0.0.0.0. Одновременно отправьте RIP в OSPF или OSPF в RIP.

```
interface vlan 10
```

```
ip address 130.130.1.1 255.255.255.0
```

```
ip ospf cost 1
```

!

```
interface vlan 10
```

```
ip address 130.130.1.1 255.255.255.0
```

!

```
router ospf 90
```

```
network 130.130.0.0 255.255.0.0 area 0
```



```
redistribute rip
!  
router rip  
network 130.130.0.0  
redistribute ospf 90
```

## 2. Пример базовой конфигурации внутреннего маршрутного коммутатора; ABR и ASBR

В следующем примере четыре идентификатора областей распределены по четырем диапазонам IP-адресов. Активируется процесс маршрутизации 109. Четыре области – это область 10.9.50.0, область 0, область 2 и область 3. Маски областей 10.9.50.0, 2 и 3 обозначены диапазоном адресов. Область 0 включает все сети.

```
router ospf 109  
network 131.108.20.0 255.255.255.0 area 10.9.50.0  
network 131.108.0.0 255.255.0.0 area 2  
network 131.109.10.0 255.255.255.0 area 3  
network 0.0.0.0 0.0.0.0 area 0  
!  
! Интерфейс VLAN 10 находится в области 10.9.50.0:  
interface vlan 10  
ip address 131.108.20.5 255.255.255.0  
!  
! Интерфейс VLAN 11 находится в области 2:  
interface vlan 11  
ip address 131.108.1.5 255.255.255.0  
!  
! Интерфейс VLAN 12 находится в области 2:  
interface vlan 12  
ip address 131.108.2.5 255.255.255.0  
!  
! Интерфейс VLAN 13 находится в области 3:  
interface vlan 13  
ip address 131.109.10.5 255.255.255.0  
!  
! Интерфейс VLAN 14 находится в области 0:
```



```
interface vlan 14
ip address 131.109.1.1 255.255.255.0
```

!

! Интерфейс VLAN 100 находится в области 0:

```
interface vlan 100
ip address 10.1.0.1 255.255.0.0
```

Функция команд настройки сетевой области **network area** имеет свой порядок, поэтому важна последовательность команд. Коммутатор сопоставляет пару IP-адрес/маска в соответствии с установленным порядком.

Проверьте первую сетевую область. Подсеть интерфейса 131.108.20.0, настроенная для идентификатора области 10.9.50.0, соответствует подсети 131.108.20.0. Таким образом, этот интерфейс находится в области 10.9.50.0.

Во второй области, если применить тот же процесс анализа к другим интерфейсам, можно увидеть, что интерфейс VLAN 11 с адресом 131.108.1.5 соответствует области 2. Аналогично, интерфейс VLAN 12 с адресом 131.108.2.5 также относится к области 2.

Продолжая сопоставление других сетевых областей, мы видим, что интерфейс VLAN 13 с адресом 131.109.10.5 подключен к области 3.

Обратите внимание, что последняя команда для сетевой области (0.0.0.0) является исключением: она означает, что все оставшиеся интерфейсы, которые не были явно указаны в предыдущих командах, будут подключены к области 0. В данном случае это интерфейсы VLAN 14 и VLAN 100, которые имеют адреса 131.109.1.1 и 10.1.0.1 соответственно.

### 3. Сложная конфигурация внутренних коммутаторов ABR и ASBR

В этом примере показано, как настроить несколько коммутаторов в одной автономной системе OSPF. На следующем рисунке показана топология сети, рассматриваемая в данном примере.

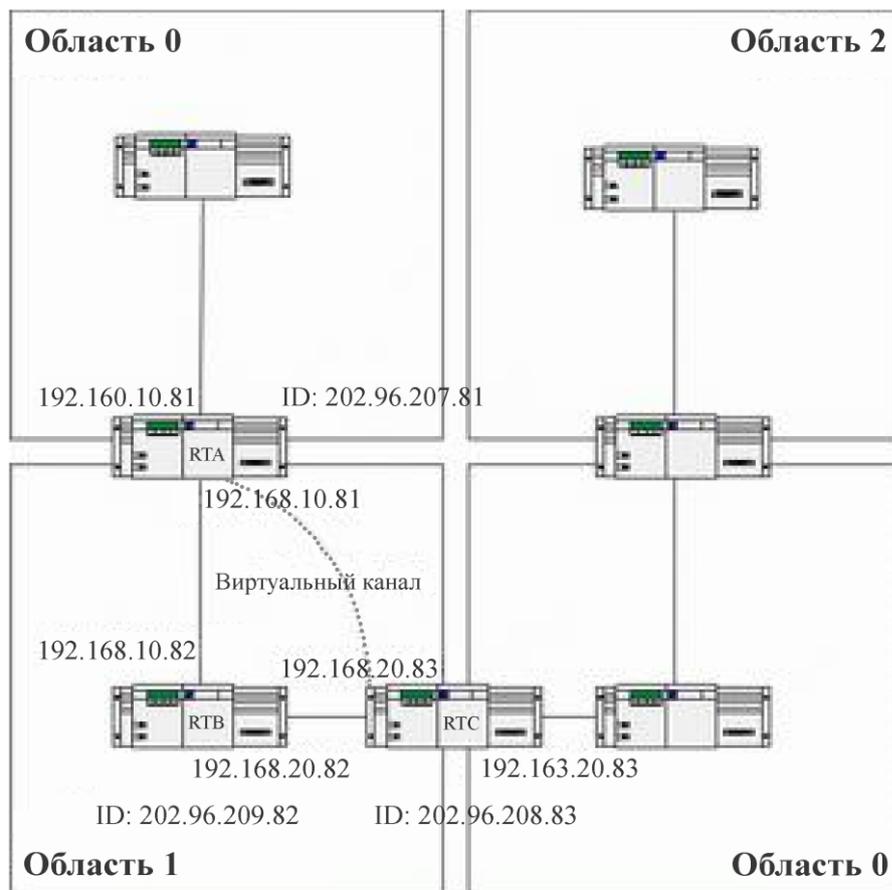


Рисунок 30 – Топология сети

Настройте коммутаторы в соответствии с приведенным рисунком.

RTA:

```
interface loopback 0
ip address 202.96.207.81 255.255.255.0
!
interface vlan 10
ip address 192.168.10.81 255.255.255.0
!
interface vlan 10
ip address 192.160.10.81 255.255.255.0
!
router ospf 192
network 192.168.10.0 255.255.255.0 area 1
network 192.160.10.0 255.255.255.0 area 0
```



```
!  
RTB:  
interface loopback 0  
ip address 202.96.209.82 255.255.255.252  
!  
interface vlan 10  
ip address 192.168.10.82 255.255.255.0  
!  
interface vlan 11  
ip address 192.168.20.82 255.255.255.0  
!  
router ospf 192  
network 192.168.20.0 255.255.255.0 area 1  
network 192.168.10.0 255.255.255.0 area 1  
!  
RTC:  
interface loopback 0  
ip address 202.96.208.83 255.255.255.252  
!  
interface vlan 10  
ip address 192.163.20.83 255.255.255.0  
!  
interface vlan 11  
ip address 192.168.20.83 255.255.255.0  
!  
router ospf 192  
network 192.168.20.0 255.255.255.0 area 1  
network 192.163.20.0 255.255.255.0 area 0  
!
```

### 24.3.13.3 Пример комплексной настройки OSPF на коммутаторе ABR

В следующем примере описывается настройка граничного маршрутизатора ABR.

- Настройка базового OSPF



- Распределение маршрутов

На следующем рисунке показан диапазон адресов и распределение зон.

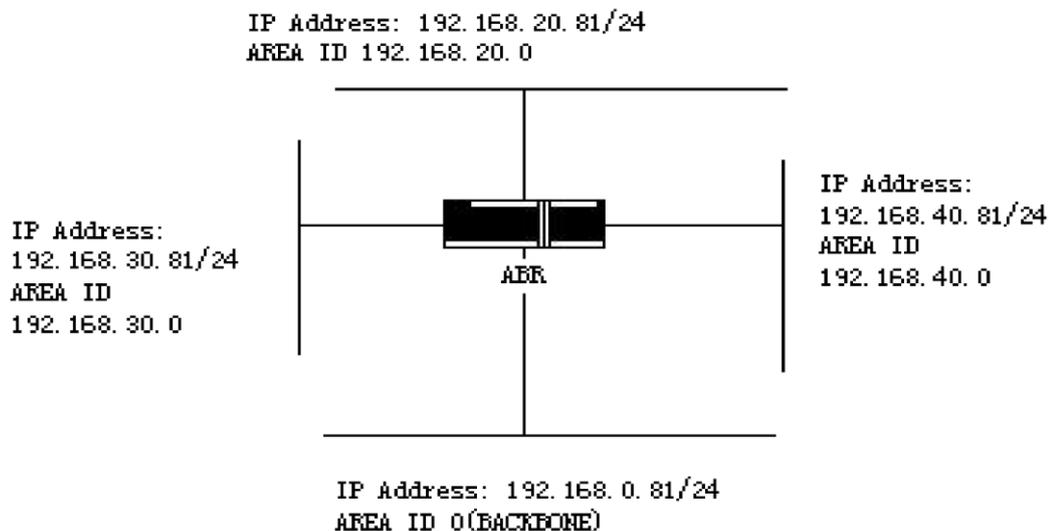


Рисунок 31 – Области OSPF

Ниже приведены основные задачи настройки:

- 1) Настройка диапазона адресов для Ethernet от 0 до 3
- 2) Активация OSPF на каждом интерфейсе
- 3) Установка пароля аутентификации для каждой области и сети
- 4) Установка значения состояния канала и других параметров интерфейса



Используйте отдельную команду **area** для настройки параметров аутентификации и тупиковой зоны соответственно.

- Задайте магистральную (backbone) область area 0.

Задачи настройки, связанные с распределением, перечислены ниже.

- Распределите маршруты IGRP и маршруты RIP для ввода настроек параметров OSPF (включая тип метрики, метрику, тег и подсеть).
- Распределите маршруты IGRP и OSPF в RIP.

Ниже приведен пример конфигурации OSPF.

```
interface vlan 10
ip address 192.168.20.81 255.255.255.0
ip ospf password GHGHHGHG
ip ospf cost 10
```



```
!  
interface vlan 11  
ip address 192.168.30.81 255.255.255.0  
ip ospf password ijklmnop  
ip ospf cost 20  
ip ospf retransmit-interval 10  
ip ospf transmit-delay 2  
ip ospf priority 4  
!  
interface vlan 12  
ip address 192.168.40.81 255.255.255.0  
ip ospf password abcdefgh  
ip ospf cost 10  
!  
interface vlan 13  
ip address 192.168.0.81 255.255.255.0  
ip ospf password ijklmnop  
ip ospf cost 20  
ip ospf dead-interval 80  
!  
router ospf 192  
network 192.168.0.0 255.255.255.0 area 0  
network 192.168.20.0 255.255.255.0 area 192.168.20.0  
network 192.168.30.0 255.255.255.0 area 192.168.30.0  
network 192.168.40.0 255.255.255.0 area 192.168.40.0  
area 0 authentication simple  
area 192.168.20.0 stub  
area 192.168.20.0 authentication simple  
area 192.168.20.0 default-cost 20  
area 192.168.20.0 authentication simple  
area 192.168.20.0 range 36.0.0.0 255.0.0.0  
area 192.168.30.0 range 192.42.110.0 255.255.255.0  
area 0 range 130.0.0.0 255.0.0.0
```



```
area 0 range 141.0.0.0 255.0.0.0
redistribute rip
RIP is in network 192.168.30.0.
router rip
network 192.168.30.0
redistribute ospf 192
!
```

## 24.4 BGP

### 24.4.1 Введение

В этой главе описывается, как настроить протокол граничного шлюза BGP. Это протокол внешнего шлюза (EGP), определенный в RFC1163, 1267 и 1771. Он позволяет установить механизм выбора маршрута между различными автономными системами и гарантировать обмен информацией о маршрутизации без образования петель.

#### 24.4.1.1 Описание

В BGP каждый маршрут включает в себя номер сети, список автономных систем, которые этот маршрут проходит (так называемый AS-путь), и другие атрибуты. Программное обеспечение данного маршрутизатора поддерживает BGPv4, определенный в RFC1771. Основная функция BGP – обмен информацией о доступности сети с другими системами BGP, включая информацию о AS-пути. Эта информация может использоваться для построения графа связи между автономными системами (AS), что позволяет избегать петель в маршрутизации, а также для реализации политики маршрутизации на уровне AS с использованием графа связи между AS. BGP v4 поддерживает бесклассовый междоменный маршрутизатор (CIDR), что позволяет сократить размер таблицы маршрутизации за счет создания суммарных маршрутов, объединяемых в «суперсеть». CIDR отменяет ограничения, связанные с классовой адресацией, позволяя использовать адреса и подсети с произвольной длиной префикса, а также поддерживает широковещательную трансляцию IP-префиксов. Маршруты CIDR могут передаваться через различные протоколы маршрутизации, такие как OSPF, Enhanced IGRP, ISIS-IP и RIP2.

Важное различие между внешней и внутренней маршрутизацией заключается в том, что маршрутизатор внешнего шлюза имеет более широкие возможности контроля. Для управления маршрутами в BGP предусмотрено несколько дополнительных методов:

- Фильтрация маршрутов. Для отбора маршрутов можно использовать различные параметры, такие как списки доступа на основе соседей, списки AS-путей (aspath-list), списки префиксов (prefix-list), а также списки доступа на основе интерфейсов и префиксов. Также можно управлять выбором следующего шага (nexthop) для маршрутов.
- Изменение атрибутов маршрутов. С помощью карты маршрутизации можно изменять атрибуты маршрутов BGP, такие как MED, локальный приоритет, вес и другие атрибуты.



- Интеграция с протоколами динамической маршрутизации внутри сети (например, OSPF, RIP). Можно осуществлять автоматическую генерацию информации о маршрутизации BGP через перераспределение маршрутов из внутренних протоколов. Также в BGP можно вручную настраивать сети и агрегировать маршруты. При генерации маршрутов BGP можно использовать **route-map** для настройки их атрибутов.
- Управление приоритетом маршрутов BGP. Можно использовать команду **distance** для настройки административной дистанции маршрутов в системе.

#### 24.4.1.2 Выбор пути

Процесс принятия решения происходит на основе сравнения значений атрибутов маршрута. Если в одной сети имеется несколько маршрутов, BGP выбирает лучший маршрут к месту назначения.

- Если следующий транзитный участок не может быть достигнут, то рассматривается оптимальный маршрут.
- Если маршрут является внутренним (то есть он объявлен внутри одной автономной системы), и синхронизация активирована, то BGP не будет рассматривать этот маршрут как оптимальный, если он не присутствует в IGP.
- Выбирается маршрут с наибольшим весом.
- Если у каждого маршрута одинаковый вес, предпочтительным считается маршрут с наивысшим локальным приоритетом.
- Если у каждого маршрута одинаковый локальный приоритет, выбирается маршрут, сгенерированный локальным маршрутизатором. Это может быть маршрут, созданный с помощью команды **network aggregate** или путем перераспределения маршрутов IGP.
- Если локальные приоритеты одинаковы и нет маршрутов, сгенерированных локальным маршрутизатором, то выбирается маршрут с кратчайшим AS-путем.
- Если длины AS-пути одинаковы, выбирается маршрут с наименьшим значением атрибута «origin» (IGP < EGP < INCOMPLETE).
- Если значения атрибута «origin» совпадают, выбирается маршрут с наименьшим значением MED. Если не активирована функция **bgp always-compare-med**, это сравнение может быть выполнено только между маршрутами от одной и той же соседней AS.
- Если каждый маршрут имеет одно и то же значение MED, предпочтение отдается внешнему маршруту (EBGP) перед внутренним (IBGP). Внутри конфедерации автономной системы все маршруты считаются внутренними, но предпочтение отдается конфедерации EBGP, а не IBGP.

Если у каждого маршрута одинаковые характеристики соединения, выбирается маршрут с меньшим идентификатором маршрутизатора (router-id).



## 24.4.2 Настройка BGP

Настройку BGP можно разделить на базовую и расширенную. Первые две задачи базовой настройки необходимы для работы BGP. Остальные, как и все задачи расширенной настройки, не являются обязательными.

### 24.4.2.1 Базовая настройка

#### 1. Активация выбора маршрута BGP

Запустите следующие команды в режиме глобальной конфигурации, чтобы активировать выбор маршрута BGP:

| Команда  | Описание  |
|--|---|
| <b>router bgp</b> <i>autonomous-system</i>   | В режиме настройки маршрутизатора активирует процесс выбора маршрута BGP    |
| <b>network</b> <i>network-number</i>   <i>masklen</i> [ <b>route-map</b> <i>route-map-name</i> ] | Помечает сеть как локальную автономную систему и добавляет ее в таблицу BGP |



В отличие от протоколов внутренней маршрутизации (например, RIP), где команда **network** определяет, куда отправлять обновления, в BGP эта команда используется для импорта маршрутов в таблицу BGP. Ограничение на использование команды **network** устанавливается ресурсами маршрутизатора, такими как выделенная оперативная память (RAM). При необходимости можно использовать команду **redistribute** для достижения того же эффекта.

#### 2. Настройка параметров соседнего устройства

Настройка соседства BGP необходима для обмена данными о маршрутах с внешней сетевой средой. BGP поддерживает два вида соседей: внутренние (IBGP) и внешние (EBGP). Внутренние соседи находятся в одной AS, а внешние – в разных. Обычно внешние соседи смежны и используют одну и ту же подсеть, в то время как внутренние могут находиться в любой части одной и той же AS.

Чтобы указать соседнее устройство BGP, выполните следующие команды:

| Команда  | Описание                       |
|--|--------------------------------|
| <b>neighbor</b> { <i>ip-address</i> } <b>remote-as</b> <i>number</i> | Определяет соседнее устройство |

#### 3. Мягкая реконфигурация BGP

Обычно BGP-соседи обмениваются всеми доступными маршрутами при установлении соединения, а затем – только обновленными маршрутами. Если внесены изменения в



настроенную политику маршрутизации, для применения этих изменений к полученным маршрутам необходимо очистить сеанс BGP.

Однако очистка сеанса может отключить высокоскоростной кэш и серьезно подорвать работу сети. Рекомендуется использовать функцию мягкой реконфигурации, поскольку она помогает настраивать и активировать политику без очистки сеансов BGP. В настоящее время функция мягкой реконфигурации может быть применена к каждому соседу. Когда функция применяется к входящему обновлению, сгенерированному соседями, она называется входящей мягкой реконфигурацией. Когда функция используется для отправки исходящего обновления соседу, она называется исходящей мягкой реконфигурацией. После запуска входящей мягкой реконфигурации проверяются новые входные политики. После запуска исходящей мягкой реконфигурации проверяются новые локальные выходные политики без сброса сеанса BGP.

Чтобы сгенерировать входящее обновление без сброса сеанса BGP, маршрутизатор сеанса должен восстановить полученное входящее обновление без изменений. Получено или отклонено входящее обновление текущей входящей политикой – не имеет значения. В этом случае память будет сильно загружена. Исходящая реконфигурация не требует дополнительных затрат памяти, поэтому она всегда эффективна. Вы можете запустить исходящую мягкую реконфигурацию на стороне соседа, чтобы проверить новую локальную входящую политику.

Чтобы разрешить входящую мягкую реконфигурацию, вам необходимо настроить BGP для восстановления всех полученных обновлений маршрутизации. Исходящая мягкая реконфигурация не требует предварительной настройки.

Выполните следующую команду для настройки мягкой реконфигурации BGP:

| Команда   | Описание                           |
|---|------------------------------------|
| <b>neighbor {ip-address} soft-reconfiguration [inbound]</b> | Включает мягкую реконфигурацию BGP |

#### 4. Сброс соединения BGP

Как только два маршрутизатора определены как BGP-соседи, они создают соединение BGP и обмениваются информацией о маршрутизации. Если политика маршрутизации BGP или другие настройки были изменены, вам следует сбросить соединение, чтобы изменения вступили в силу. Для этого используйте одну из следующих команд:

| Команда                     | Описание                            |
|-----------------------------|-------------------------------------|
| <b>clear ip bgp *</b>       | Сбрасывает все соединения BGP       |
| <b>clear ip bgp address</b> | Сбрасывает указанное соединение BGP |



## 5. Настройка синхронизации между BGP и IGP

Если вы разрешаете другой AS передавать данные в третью AS через вашу AS, то очень важна синхронизация между состоянием внутренней маршрутизации вашей AS и информацией о маршрутизации, которую она передает другим AS. Например, если ваш протокол BGP начинает передавать маршруты до того, как все маршрутизаторы в вашей AS узнают об этих маршрутах через внутренний протокол маршрутизации (IGP), то некоторые маршрутизаторы в вашей AS могут получить информацию о маршрутах, которые им неизвестны.

Чтобы избежать подобных ситуаций, BGP должен дожидаться, пока все маршрутизаторы, работающие с IGP, узнают о новых маршрутах. Это называется синхронизацией между BGP и IGP, и эта синхронизация активирована по умолчанию.

Однако в некоторых ситуациях синхронизация не является необходимой. Например, если вы не разрешаете другим AS передавать данные через вашу AS, или если все маршрутизаторы в вашей AS используют BGP, вы можете отключить функцию синхронизации. Отключение этой функции позволит вам использовать меньше маршрутов в вашем IGP и обеспечит более быструю сходимость BGP.

Для отмены синхронизации используйте следующую команду:

| Команда                   | Описание                               |
|---------------------------|--|
| <b>no synchronization</b> | Отменяет синхронизацию между BGP и IGP |

При отмене синхронизации следует использовать команду **clear ip bgp**, чтобы очистить диалог BGP. Пример синхронизации BGP приведен в конце данного раздела.

Обычно не требуется перераспределять все маршруты в вашем внутреннем протоколе маршрутизации (IGP). Как правило перераспределяют один или два маршрута и обозначают их как внешние маршруты в вашем IGP или заставляют сеанс BGP генерировать AS-маршрут по умолчанию. Перераспределяются только маршруты, полученные через EBGP.

Вместо импорта вашего IGP в BGP используйте команду конфигурации **network**, чтобы перечислить сети в вашей автономной системе. Эти сети называются локальными сетями и позволяют BGP иметь атрибут «origin» от IGP. Они должны присутствовать в основной таблице IP-маршрутизации и могут быть непосредственно подключенными маршрутами, статическими маршрутами или маршрутами, известными через IGP.

Будьте осторожны при перераспределении маршрутов между BGP и IGP, потому что эти маршруты могут быть внедрены другими маршрутизаторами через BGP. Это может привести к ситуации, когда BGP внедряет информацию в IGP, а затем отправляет обратно информацию в BGP. И наоборот.

## 6. Настройка веса маршрута BGP

Значение, или вес маршрута BGP – это номер, установленный для управления процессом выбора маршрута. Значение является локальным для маршрутизатора. Оно варьируется от



0 до 65535. Маршрут BGP, сгенерированный локально, имеет по умолчанию значение 32768, маршрут, полученный от соседа, имеет значение 0. Администратор может реализовать политику маршрутизации путем изменения значения маршрута.

Для установки веса маршрута BGP используйте следующую команду:

| Команда   | Описание                           |
|---|------------------------------------|
| <b>neighbor</b> {ip-address} <b>weight</b> weight | Назначает вес для маршрутов соседа |

Кроме того, вы можете изменить вес маршрута через карту маршрутизации при помощи команды **route-map**.

## 7. Настройка фильтрации маршрутов BGP на основе соседа

В реализации программного обеспечения маршрутизатора BGP существует 4 метода фильтрации маршрутов BGP назначенных соседей:

➤ Используйте фильтр на основе списка Aspath при помощи команды глобальной конфигурации **ip aspath-list** и команды **neighbour filter-list**.

| Команда   | Описание                                     |
|---|--|
| <b>ip as-path access-list</b> aspaths-list-name {permit   deny} as-regular-expression | Определяет список доступа, относящийся к BGP |
| <b>router bgp</b> autonomous-system   | Вход в режим настройки маршрутизатора        |
| <b>neighbor</b> {ip-address } <b>filter-list</b> aspath-list-name {in   out}          | Устанавливает фильтр BGP                     |

➤ Используйте один из ранее созданных списков доступа при помощи команды глобальной конфигурации **ip access-list** и команды **neighbour distribute-list**.

| Команда   | Описание                              |
|---|---------------------------------------|
| <b>ip access-list standard</b> access-list-name                                 | Определяет список доступа             |
| <b>router bgp</b> autonomous-system   | Вход в режим настройки маршрутизатора |
| <b>neighbor</b> {ip-address} <b>distribute-list</b> access-list-name {in   out} | Устанавливает фильтр BGP              |

➤ Используйте фильтр на основе префиксов при помощи команды глобальной конфигурации **ip prefix-list** и команды **neighbour prefix-list**.



| Команда   | Описание                              |
|---|---------------------------------------|
| <b>ip prefix-list</b> <i>prefix-list-name</i> { <b>permit</b>   <b>deny</b> }<br>A.B.C.D/n ge x le y        | Определяет список префиксов           |
| <b>router bgp</b> <i>autonomous-system</i>  | Вход в режим настройки маршрутизатора |
| <b>neighbor</b> { <i>ip-address</i> } <b>prefix-list</b> <i>prefix-list-name</i> { <b>in</b>   <b>out</b> } | Устанавливает фильтр BGP              |

➤ Используйте карту маршрутизации при помощи команды глобальной конфигурации **route-map** и команды **neighbour route-map**.

Использование маршрутной карты не только фильтрует маршруты, но и изменяет их атрибуты. Более подробно эти настройки будут описаны в следующих главах.

## 8. Настройка фильтрации маршрутов BGP на основе интерфейса

Настроить фильтрацию маршрутов BGP на основе интерфейса можно с помощью списка доступа и списка префиксов. Можно фильтровать сетевой номер и адрес шлюза маршрутов. Можно указать опцию «**access-list**» для использования списка доступа для фильтрации сетевого номера маршрутов, указать опцию «**prefix-list**» для использования списка префиксов для фильтрации сетевого номера маршрутов, указать опцию «**gateway**» для использования списка доступа для фильтрации атрибута «**next-hop**» маршрутов. Также можно фильтровать и сетевой номер, и атрибут «**next-hop**» маршрутов одновременно, но опцию «**access-list**» нельзя использовать вместе с опцией «**prefix-list**». Опция «**\***» может фильтровать маршруты на всех интерфейсах.

Чтобы настроить фильтрацию маршрутов BGP на основе интерфейса, необходимо в режиме настройки BGP выполнить следующие действия:

| Команда  | Описание                                    |
|--|---|
| <b>filter</b> <i>interface</i> { <b>in</b>   <b>out</b> } ( <b>access-list</b> <i>access-list-name</i> ) ( <b>prefix-list</b> <i>prefix-list-name</i> ) ( <b>gateway</b> <i>access-list-name</i> ) | Фильтрует маршруты BGP на основе интерфейса |

## 9. Отключение обработки следующего перехода при обновлении BGP

В BGP каждая обновленная информация о маршруте включает атрибут «**next-hop**», который указывает на следующий маршрутизатор, к которому должен быть отправлен трафик для достижения определенного префикса.

Вы можете настроить маршрутизатор на игнорирование этого атрибута при получении обновления от соседнего BGP. Это может быть полезно в нешироковещательной сети (например, FR или X.25). В таких сетях соседи могут не иметь прямого доступа ко всем



другим соседям в одной и той же IP-подсети. Существует два способа отмены обработки «next-hop»:

- использование локального IP-адреса текущего соединения BGP, чтобы заменить адрес следующего перехода исходящего маршрута;
- использование карты маршрутизации, чтобы указать адрес следующего перехода для входящих или исходящих маршрутов (см. описание расширенных настроек).

В режиме настройки маршрутизатора выполните следующую команду, чтобы отключить обработку атрибута «next-hop»:

| Команда                                    | Описание   |
|--|--|
| <b>neighbor {ip-address} next-hop-self</b> | Отключает обработку следующего перехода при выполнении обновления BGP соседа |

Данная команда позволяет настроить маршрутизатор так, чтобы он сообщал, что сам является следующим узлом для определенного маршрута. Это значит, что другие соседи BGP будут пересылать пакеты для этой сети через текущий маршрутизатор. Такой подход полезен в средах, где не производится ширококвещательной передачи, так как между текущим маршрутизатором и указанным соседом существует путь. Однако в условиях ширококвещательной сети такая настройка может привести к ненужным дополнительным переходам между узлами.

## 24.4.2.2 Расширенная настройка

1. Фильтрация и изменение обновлений маршрутов при помощи карты маршрутизации.

Вы можете использовать карту маршрутизации для фильтрации обновления маршрута и изменения атрибутов параметров в зависимости каждого соседа. Карта может применяться как к входящему обновлению, так и к исходящему. При отправке или принятии обновления могут обрабатываться только маршруты, соответствующие карте маршрутизации.

Карта маршрутизации поддерживает входящие и исходящие обновления в соответствии с атрибутами, такими как путь AS, комьюнити и номер сети. Сопоставление в соответствии с путем AS требует использования команды **aspath-list**; сопоставление на основе комьюнити требует использования команды **community-list**, сопоставление на основе сети требует использования команды **ip access-list**.

Чтобы настроить карту маршрутизации для фильтрации и изменения обновления маршрутов выполните следующую команду режиме настройки BGP:

| Команда  | Описание   |
|--|--|
| <b>neighbor {ip-address} route-map route-map-name {in   out}</b> | Применение карты маршрутизации на входящих или исходящих маршрутах |



## 2. Настройка агрегированных адресов

Для того чтобы уменьшить размер таблицы маршрутизации, используемой в BGP, можно создавать агрегированные маршруты, которые объединяют несколько меньших маршрутов в один. Это можно сделать, либо путем перераспределения агрегированных маршрутов в BGP, либо с использованием условных атрибутов агрегации. Если в таблице маршрутизации BGP уже есть более детальные записи, то можно добавить в нее агрегированный адрес. Таким образом оптимизируется размер таблицы.

Для создание агрегированного адреса используйте следующие команды:

| Команда   | Описание   |
|---|--|
| <b>aggregate network/len</b>                        | Создает агрегированный адрес в таблице маршрутизации BGP                                     |
| <b>aggregate network/len summary-only</b>           | Только общий адрес широковещательной рассылки  |
| <b>aggregate network/len attribute-map map-name</b> | Генерирует агрегированный адрес в соответствии с условиями, указанными в карте маршрутизации |

## 3. Настройка атрибута BGP-комьюнити

Политика маршрутизации, поддерживаемая BGP, базируется на одном из трех значений информации о маршрутизации:

- сетевой номер маршрута;
- значение атрибута «as\_path» маршрутов;
- значение атрибута «community» маршрутов.

Разделение маршрутов на группы посредством атрибута «community» и применение политики маршрутизации на их основе упрощает настройку управления информацией маршрутизации.

Комьюнити (сообщество) – группа маршрутов с общими атрибутами; каждый маршрут может принадлежать нескольким группам. Администраторы AS могут определить, какой группе принадлежит данный маршрут.

Атрибут «community» – это необязательный и передаваемый глобальный атрибут в диапазоне от 1 до 4 294 967 200. В BGP существуют определенные комьюнити, которые предназначены для тегирования маршрутов и помогают в управлении, используя различные подходы к объявлению маршрутов:

**no-export** – не объявляет маршрут одноранговому узлу EBGP, включая узлы внутри конфедерации автономной системы;

**no-advertise** – не объявляет маршрут никому из одноранговых узлов;

**local-as** – не объявляет маршрут за пределами автономной системы.



В процессе работы BGP маршрутизаторы могут управлять атрибутами «community» для маршрутов на разных этапах – при создании, получении или пересылке. Это позволяет администраторам сети группировать маршруты и применять к ним определенные политики. Например, маршрутизатор может добавить атрибут «community» к маршруту, чтобы указать, что этот маршрут следует обрабатывать особым образом.

Когда маршруты агрегируются, то есть несколько более узких маршрутов объединяются в один более широкий, агрегированный маршрут может включать атрибуты «community» от всех исходных маршрутов. Это позволяет сохранить информацию о том, как эти маршруты должны обрабатываться в сети, даже после их объединения.

По умолчанию атрибуты «community» соседям не отправляются. Используйте следующую команду, чтобы указать отправку атрибута определенному соседу:

| Команда  | Описание  |
|--|---|
| <b>neighbor</b> {ip-address} <b>send-community</b> | Активирует отправку соседу атрибута «community» |

Чтобы настроить атрибут «community» для маршрутизатора, необходимо выполнить следующие действия:

| Команда   | Описание   |
|---|--|
| <b>route-map</b> map-name sequence-number {deny   permit}                 | Настраивает карту маршрутизации                              |
| <b>set community</b> community-value                                      | Устанавливает значение атрибута «community»                  |
| <b>router bgp</b> autonomous-system                                       | Вход в режим настройки маршрутизатора                        |
| <b>neighbor</b> {ip-address} <b>route-map</b> access-list-name {in   out} | Применяет карту маршрутов к входящим или исходящим маршрутам |

Чтобы отфильтровать информацию о маршрутизации на основе атрибутов «community», необходимо выполнить следующие действия:

| Команда   | Описание                        |
|---|---------------------------------|
| <b>ip community-list</b> {expanded   standard} community-list-name {permit   deny} community-expression | Определяет список комьюнити     |
| <b>route-map</b> map-name sequence-number {deny   permit}   | Настраивает карту маршрутизации |



|   |                                       |
|---|---------------------------------------|
| <b>match community</b> <i>community-list-name</i>   | Настраивает правила сопоставления     |
| <b>router bgp</b> <i>autonomous-system</i>  | Вход в режим настройки маршрутизатора |
| <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>route-map</b> <i>route-map-name</i> { <b>in</b>   <b>out</b> } | Применяет карту маршрутизации         |

#### 4. Настройка конфедерации автономной системы

Способ уменьшить количество IBGP-соединений – разделить AS на несколько суб-AS, а затем сформировать из них конфедерацию. С внешней точки зрения конфедерация выглядит как AS. В конфедерации каждая суб-AS внутри является полносвязной и имеет соединения с другими суб-AS в той же конфедерации. Даже если между узлами разных суб-AS существуют сеансы EBGP, они все равно могут обмениваться информацией о выборе маршрутизации, как узлы IBGP, сохраняя информацию о следующем переходе, MED и локальном приоритете.

Чтобы настроить конфедерацию автономной системы BGP, необходимо указать ее идентификатор. Идентификатор конфедерации – это номер AS. С внешней точки зрения конфедерация аналогична отдельной AS, которая в качестве номера имеет ID конфедерации.

Используйте следующую команду, чтобы настроить идентификатор конфедерации автономной системы:

| Команда  | Описание                    |
|--|-----------------------------|
| <b>bgp confederation identifier</b> <i>autonomous-system</i> | Настраивает ID конфедерации |

Чтобы указать автономные системы, принадлежащие конфедерации, используйте следующую команду:

| Команда   | Описание   |
|---|--|
| <b>bgp confederation peers</b> <i>autonomous-system</i><br>[ <i>autonomous-system ...</i> ] | Указывает номер автономной системы, принадлежащей конфедерации |

#### 5. Настройка маршрутного рефлексора

Другой способ уменьшить количество соединений IBGP вместо настройки конфедерации автономной системы – настроить рефлексор, или отражатель маршрутов.

Внутренние узлы рефлексора маршрута делятся на две группы: клиентские узлы и все остальные маршрутизаторы (неклиентские узлы). Рефлексор отражает маршруты между двумя группами; он и его одноранговые клиентские узлы образуют кластер. Неклиентские



одноранговые узлы обязаны быть подключенными к полносвязной сети, а клиентские – не обязаны. Клиенты в кластере не взаимодействуют с узлами IBGP за пределами кластера.

Когда отражатель получает информацию о маршрутизации, он выполняет следующие задачи:

- трансляция маршрутов от внешнего узла BGP всем клиентским и неклиентским узлам;
- трансляция маршрутов от неклиентских узлов всем клиентам;
- трансляция маршрутов от клиентов всем клиентам и неклиентским узлам. Таким образом, клиентские узлы не обязательно должны быть подключены к полносвязной сети.

Используйте следующую команду, чтобы настроить локальный маршрутизатор как рефлектор и назначить соседей в качестве его клиентов:

| Команда   | Описание  |
|---|---|
| <b>neighbor {ip-address} route-reflector-client</b> | Настраивает локальный маршрутизатор как рефлектор и назначает соседей в качестве его клиентов |

Автономная система может иметь несколько маршрутных рефлекторов для более эффективной маршрутизации данных. Рефлекторы обрабатывают информацию о маршрутизации аналогично тому, как это делают спикеры IBGP. Обычно группа клиентов имеет только один рефлектор, и определяется его идентификатором (router ID). Для повышения надежности и предотвращения отказов одиночных узлов в сети, группа может иметь более одного маршрутного рефлектора. В этом случае каждый маршрутный рефлектор в группе должен быть настроен с 4-битным идентификатором кластера (cluster ID), чтобы однозначно идентифицировать информацию о маршрутах внутри этой группы. Все отражатели маршрутов, принадлежащие одному кластеру, должны быть полносвязными и иметь одинаковый набор клиентских и неклиентских одноранговых узлов.

Если в группе имеется более одного маршрутного отражателя, выполните следующую команду для настройки идентификатора кластера:

| Команда                          | Описание                           |
|----------------------------------|------------------------------------|
| <b>bgp cluster-id cluster-id</b> | Настраивает идентификатор кластера |

## 6. Отключение однорангового узла

В режиме настройки BGP используйте следующую команду, чтобы отключить BGP-соседа:

| Команда                               | Описание                       |
|---------------------------------------|--------------------------------|
| <b>neighbor {ip-address} shutdown</b> | Завершает работу соседнего BGP |



Используйте следующую команду, чтобы включить ранее отключенного BGP-соседа:

| Команда                                  | Описание                        |
|--|---------------------------------|
| <b>no neighbor {ip-address} shutdown</b> | Активирует работу соседнего BGP |

## 7. Настройка внешнего узла с несколькими переходами

По умолчанию внешние одноранговые узлы должны находиться в сети с прямым подключением. Когда прямое физическое соединение невозможно или нежелательно, для настройки внешнего узла с несколькими переходами необходимо выполнить следующую настройку:

| Команда  | Описание   |
|--|--|
| <b>neighbor {ip-address} ebgp-multihop ttl</b> | Настройка внешнего узла с несколькими переходами в качестве BGP-соседа |

## 8. Настройка административной дистанции маршрутов BGP

Административная дистанция, или расстояние управления – это метрика, используемая в сетевой инфраструктуре для определения надежности или предпочтительности разных протоколов маршрутизации. Меньшее значение этой метрики указывает на более предпочтительный или надежный маршрут. Этот параметр помогает при определении наилучшего маршрута для передачи данных в сложных сетевых конфигурациях с несколькими возможными маршрутами.

BGP использует три различных расстояния управления: внешнее, внутреннее и локальное. Маршрутам, полученным от внешнего BGP, будет назначено внешнее расстояние; маршруты, полученные из внутреннего BGP, будут иметь внутреннее расстояние, локальным маршрутам назначается локальное расстояние. Используйте следующую команду для настройки административной дистанции маршрутов BGP:

| Команда  | Описание                               |
|--|--|
| <b>distance bgp {external-distance   internal-distance   local-distance}</b> | Настраивает административную дистанцию |

Изменение расстояний при настройке административной дистанции маршрута BGP опасно и обычно не рекомендуется. Внешнее расстояние должно быть короче, чем расстояние любого другого протокола динамической маршрутизации, а внутреннее расстояние должно быть длиннее, чем расстояние любого другого протокола динамической маршрутизации.



## 9. Настройка таймера BGP

Используйте следующую команду, чтобы настроить таймеры поддержки активности и времени удержания BGP:

| Команда   | Описание   |
|---|--|
| <b>neighbor</b> { <i>ip-address</i>   <i>peer group-name</i> }<br><b>timers</b> <i>keepalive holdtime</i> | Установка интервала таймера «поддержки активности» и «времени удержания» (отсчитывается в секундах) для назначенного узла или сообщества узлов |

Используйте команду **no neighbour timers**, чтобы сбросить интервал таймера соседа или однорангового сообщества BGP до значения по умолчанию.

## 10. Сравнение MED маршрутов от разных AS

MED (Multi-Exit Discriminator) – это параметр, который следует учитывать при выборе наилучшего маршрута из нескольких путей. Предпочтительнее рассматривать маршрут с более низким значением MED, чем с более высоким.

По умолчанию в процессе выбора лучшего маршрута сравнение MED происходит только между маршрутами из одной и той же AS. Вы можете разрешить сравнение MED при выборе маршрутизации, независимо от того, из какой AS исходят маршруты. Для этого используйте следующую команду:

| Команда                       | Описание  |
|-------------------------------|---|
| <b>bgp always-compare-med</b> | Позволяет выполнять сравнение MED между маршрутами из разных AS |

## 24.4.3 Мониторинг и поддержка BGP

Администратор может просмотреть или удалить таблицу маршрутизации BGP или содержимое других баз данных. Также может быть отображена подробная статистическая информация.

### 1. Удаление таблицы маршрутизации BGP и базы данных

Выполните следующие команды в режиме управления для очистки высокоскоростного кэша, таблицы или базы данных BGP:

| Команда                       | Описание  |
|-------------------------------|---|
| <b>clear ip bgp *</b>         | Удаляет все соединения BGP                            |
| <b>clear ip bgp as-number</b> | Удаляет соединения BGP назначенной автономной системы |



|   |  |
|---|--|
| <code>clear ip bgp address</code>                 | Удаляет соединения BGP назначенного соседа                     |
| <code>clear ip bgp address soft {in   out}</code> | Удаляет входящую или исходящую базу данных назначенного соседа |
| <code>clear ip bgp aggregates</code>              | Удаляет маршруты, созданные в процессе агрегации               |
| <code>clear ip bgp networks</code>                | Удаляет маршруты, созданные командой <b>network</b>            |
| <code>clear ip bgp redistribute</code>            | Удаляет маршруты, созданные в процессе передачи данных         |

## 2. Отображение таблицы маршрутизации и данных статистики

Приведенные ниже команды позволяют отобразить подробную статистическую информацию о таблице маршрутизации BGP или базе данных. Предоставленная информация может помочь в оценке использования ресурсов и решении сетевых проблем.

| Команда   | Описание  |
|---|---|
| <code>show ip bgp</code>  | Отображает таблицу маршрутизации BGP в системе                        |
| <code>show ip bgp prefix</code>   | Отображает маршруты, соответствующие указанному префиксу              |
| <code>show ip bgp community value</code>  | Отображает статистическую информацию сообщества                       |
| <code>show ip bgp regexp regular-expression</code>  | Отображает маршруты, соответствующие указанному регулярному выражению |
| <code>show ip bgp network</code>  | Отображает указанный маршрут BGP                                      |
| <code>show ip bgp neighbors address</code>  | Отображает информацию о соединениях TCP и BGP назначенного соседа     |
| <code>show ip bgp neighbors [address] [received-routes   routes   advertised-routes]</code> | Отображает маршруты, полученные от определенного соседа BGP           |
| <code>show ip bgp paths</code>  | Отображает всю информацию базы данных о путях BGP                     |



|                            |  |
|----------------------------|--|
| <b>show ip bgp summary</b> | Отображает состояния всех соединений BGP |
|----------------------------|--|

### 3. Отслеживание информации BGP

Вы можете наблюдать за установлением соединения BGP и маршрутизацией передачи/приема, отслеживая информацию BGP. Это помогает выявлять неполадки и устранять проблемы. Команды для вывода отладочной информации BGP показаны в следующей таблице:

| Команда                       | Описание                            |
|-------------------------------|-------------------------------------|
| <b>debug ip bgp</b>           | Отслеживает общую информацию BGP    |
| <b>debug ip bgp all</b>       | Отслеживает всю информацию BGP      |
| <b>debug ip bgp fsm</b>       | Отслеживает изменения состояний BGP |
| <b>debug ip bgp keepalive</b> | Отслеживает пакеты KeepAlive        |
| <b>debug ip bgp open</b>      | Отслеживает пакеты OPEN             |
| <b>debug ip bgp update</b>    | Отслеживает пакеты UPDATE           |

## 24.4.4 Примеры настройки BGP

### 24.4.4.1 Примеры использования карты маршрутизации

В следующем примере показано, как использовать карту маршрутизации для изменения атрибута входящего маршрута от соседа. Установите метрику всех маршрутов, приходящих от соседа 140.222.1.1 и соответствующих требованиям списка доступа ASPATH «aaa», равной 200; значение локального приоритета – 250. Такие маршруты будут приняты, все остальные будут отклонены.

```
router bgp 100
neighbor 140.222.1.1 route-map fix-weight in
neighbor 140.222.1.1 remote-as 1
!
route-map fix-weight permit 10
match as-path aaa
set local-preference 250
set weight 200
!
```



```
ip as-path access-list aaa permit ^690$
```

```
ip as-path access-list aaa permit ^1800
```

В следующем примере первая запись маршрутной карты «freddy» установит метрику MED равной 127 для всех маршрутов, исходящих из автономной системы, у которых AS\_PATH начинается с 690. Вторая запись позволяет передавать маршруты, которые не соответствуют вышеуказанным условиям, соседу 1.1.1.1.

```
router bgp 100
neighbor 1.1.1.1 route-map freddy out
!
ip as-path access-list abc permit ^690_
ip as-path access-list xyz permit .*
!
route-map freddy permit 10
match as-path abc
set metric 127
!
route-map freddy permit 20
match as-path xyz
```

В следующем примере показано, как использовать **route-map** для изменения маршрутов при их перераспределении:

```
router bgp 100
redistribute rip 1 route-map rip2bgp
!
route-map rip2bgp
match ip address rip
set local-preference 25
set metric 127
set weight 30000
set ip next-hop 192.92.68.24
set origin igp
!
ip access-list standard rip
permit 131.108.0.0 255.255.0.0
```



```
permit 160.89.0.0 255.255.0.0  
permit 198.112.0.0 255.255.128.0
```

#### 24.4.4.2 Пример конфигурации соседей

В следующем примере маршрутизатор BGP принадлежит AS109 и создает две сети. У данного роутера 3 соседа: первый сосед внешний (в разных AS); второй – внутренний (с тем же номером AS). Третий – внешний.

```
router bgp 109  
network 131.108.0.0  
network 192.31.7.0  
neighbor 131.108.200.1 remote-as 167  
neighbor 131.108.234.2 remote-as 109  
neighbor 150.136.64.19 remote-as 99
```

#### 24.4.4.3 Пример фильтрации маршрутов BGP на основе соседей

Маршруты, проходящие через AS\_PATH, указанный в списке доступа «test1», будут иметь значение метрики 100. Только маршруты, проходящие через AS\_PATH, указанный в списке доступа «test2», будут отправлены по направлению к 193.1.12.10, и аналогично, только те маршруты, которые проходят через список доступа «test3», будут приняты от 193.1.12.10:

```
router bgp 200  
neighbor 193.1.12.10 remote-as 100  
neighbor 193.1.12.10 filter-list test1 in weight 100  
neighbor 193.1.12.10 filter-list test2 out  
neighbor 193.1.12.10 filter-list test3 in  
!  
ip as-path access-list test1 permit ^109  
ip as-path access-list test2 permit ^200$  
ip as-path access-list test2 permit ^100$  
ip as-path access-list test3 deny ^690$  
ip as-path access-list test3 permit .*
```

#### 24.4.4.4 Примеры фильтрации маршрутов BGP на основе интерфейса

Ниже приведен пример настройки фильтрации маршрутов на основе интерфейса. В данной конфигурации при помощи списка доступа «acl» фильтруются маршруты, проходящие через интерфейс vlan1:



```
router bgp 122
filter vlan1 in access-list acl
```

В следующем примере используется список доступа «filter-network» для фильтрации сетевых номеров маршрутов, а также используется список доступа «filter-gateway» для фильтрации адресов шлюзов маршрутов, проходящих через интерфейс vlan1.

```
router bgp 100
filter vlan1 in access-list filter-network gateway filter-gateway
```

В следующем примере используется список префиксов «filter-prefix» для фильтрации сетевых номеров маршрутов. Одновременно применяется список доступа «filter-gateway» для фильтрации адресов шлюзов маршрутов, проходящих через все интерфейсы.

```
router bgp 100
filter * in prefix-list filter-prefix gateway filter-gateway
```

#### 24.4.4.5 Примеры использования списка префиксов для настройки фильтрации маршрутов

В следующем примере маршрут по умолчанию 0.0.0.0/0 запрещен.

```
ip prefix-list abc deny 0.0.0.0/0
```

В следующем примере BGP разрешает маршруты, соответствующие префиксу 35.0.0.0/8:

```
ip prefix-list abc permit 35.0.0.0/8
```

В следующем примере процесс BGP принимает только префиксы длиной от /8 до /24:

```
router bgp 1
network 101.20.20.0
filter * in prefix max24
!
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
!
```

В следующей конфигурации маршрутизатор фильтрует маршруты со всех интерфейсов, принимая только маршруты с префиксом от 8 до 24:

```
router bgp 12
filter * in prefix-list max24
```



```
!  
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24  
!
```

В следующем примере BGP разрешает маршруты с длиной префикса не более 24 в сети 192/8:

```
ip prefix-list abc permit 192.0.0.0/8 le 24
```

В следующем примере BGP запрещает маршруты с длиной префикса более 25 в сети 192/8:

```
ip prefix-list abc deny 192.0.0.0/8 ge 25
```

В следующем примере BGP разрешает маршруты с длиной префикса более 8, но менее 24 во всем адресном пространстве:

```
ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

В следующем примере BGP запрещает все маршруты с длиной префикса более 25 во всем адресном пространстве:

```
ip prefix-list abc deny 0.0.0.0/0 ge 25
```

В этом примере запрещены маршруты из сети 10/8, поскольку если маска в сети класса А 10.0.0.0/8 меньше или равна 32 битам, все маршруты из этой сети будут запрещены:

```
ip prefix-list abc deny 10.0.0.0/8 le 32
```

В следующем примере BGP запрещает маршруты с длиной маски более 25 в сети 204.70.1.24:

```
ip prefix-list abc deny 204.70.1.0/24 ge 25
```

В следующем примере BGP разрешает все маршруты:

```
ip prefix-list abc permit any
```

#### 24.4.4.6 Примеры агрегации маршрутов BGP

Пример ниже иллюстрирует, как создавать агрегированные маршруты в BGP. Это можно сделать путем перераспределения маршрутов или с использованием условной функции агрегации маршрутов.



В следующем примере команда **redistribute static** используется для перераспределения агрегированного маршрута 193.\*.\*.\*:

```
ip route 193.0.0.0 255.0.0.0 null 0
```

!

```
router bgp 100
```

```
redistribute static
```

Если в таблице маршрутизации есть хотя бы один маршрут в пределах назначенного диапазона, следующая конфигурация создаст маршрут агрегации в таблице маршрутизации BGP. Маршрут агрегации будет считаться исходящим от вашей AS и иметь атрибут «atomic», чтобы указать на возможность потери информации.

```
router bgp 100
```

```
aggregate 193.0.0.0/8
```

В следующем примере создается агрегированный маршрут 193...\* и запрещается передавать более конкретные маршруты всем соседям:

```
router bgp 100
```

```
aggregate 193.0.0.0/8 summary-only
```

#### 24.4.4.7 Пример настройки маршрутного рефлексора

Ниже приведен пример конфигурации отражателя маршрута. RTA, RTB, RTC, RTE принадлежат одной автономной системе AS200, RTA служит рефлексором, RTB и RTC являются его клиентами, а RTE – обычным соседом IBGP. RTD принадлежит AS100 и создает соединение EBGP с RTA. Конфигурация показана на следующем рисунке:

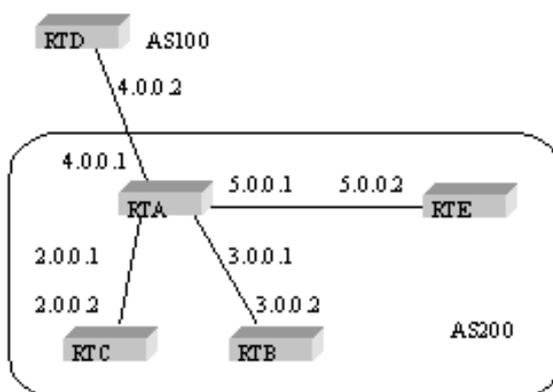


Рисунок 32 – Топология сети BGP

#### ➤ Настройка RTA:

```
interface vlan2
```

```
ip address 2.0.0.1 255.0.0.0
```

!



```
interface vlan3
ip address 3.0.0.1 255.0.0.0
!
interface vlan4
ip address 4.0.0.1 255.0.0.0
!
interface vlan5
ip address 5.0.0.1 255.0.0.0
!
router bgp 200
neighbor 2.0.0.1 remote-as 200 /*RTC IBGP*/
neighbor 2.0.0.1 route-reflector-client
neighbor 3.0.0.1 remote-as 200 /*RTB IBGP*/
neighbor 3.0.0.1 route-reflector-client
neighbor 5.0.0.1 remote-as 200 /*RTE IBGP*/
neighbor 4.0.0.2 remote-as 100 /*RTD EBGP*/
network 11.0.0.0/8
!
ip route 11.0.0.0 255.0.0.0 2.0.0.12
```

➤ **Настройка RTB:**

```
interface vlan3
ip address 3.0.0.2 255.0.0.0
!
router bgp 200
neighbor 3.0.0.1 remote-as 200 /*RTA IBGP*/
network 13.0.0.0/8
!
ip route 13.0.0.0 255.0.0.0 3.0.0.12
```

➤ **Настройка RTC:**

```
interface vlan2
ip address 2.0.0.2 255.0.0.0
!
```



```
router bgp 200
neighbor 2.0.0.1 remote-as 200 /*RTA IBGP*/
network 12.0.0.0/8
!
ip route 12.0.0.0 255.0.0.0 2.0.0.12
```

➤ **Настройка RTD:**

```
interface vlan4
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
neighbor 4.0.0.1 remote-as 200 /*RTA EBGP*/
network 14.0.0.0/8
!
ip route 14.0.0.0 255.0.0.0 4.0.0.12
```

➤ **Настройка RTE:**

```
interface vlan5
ip address 5.0.0.2 255.0.0.0
!
router bgp 200
neighbor 5.0.0.1 remote-as 200 /*RTA IBGP*/
network 15.0.0.0/8
!
ip route 15.0.0.0 255.0.0.0 5.0.0.12
```

#### 24.4.4.8 Пример конфедерации BGP

Ниже приведена топология конфедерации автономных систем. RTA, RTB, RTC создают соединения IBGP и принадлежат частной автономной системе 65010; RTE принадлежит другой частной автономной системе 65020; RTE и RTA устанавливают внутреннее EBGP-соединение конфедерации; AS65010 и AS65020 составляют конфедерацию AS200; RTD принадлежит автономной системе AS100, RTD устанавливает соединение EBGP с автономной системой 200 через RTA.

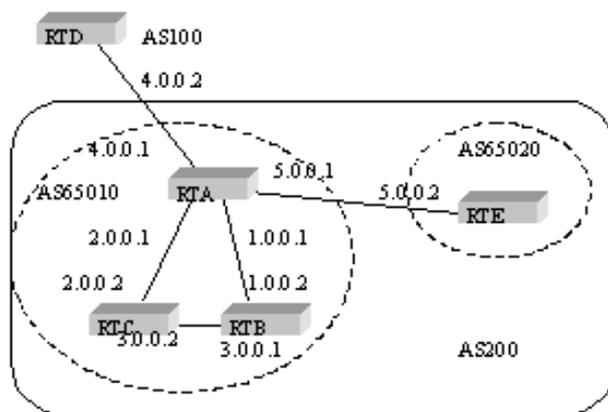


Рисунок 33 – Конфедерация BGP

➤ **Настройка RTA:**

```
interface vlan1
ip address 1.0.0.1 255.0.0.0
!
interface vlan2
ip address 2.0.0.1 255.0.0.0
!
interface vlan4
ip address 4.0.0.1 255.0.0.0
!
interface vlan5
ip address 5.0.0.1 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 1.0.0.2 remote-as 65010 /*RTB IBGP*/
neighbor 2.0.0.2 remote-as 65010 /*RTC IBGP*/
neighbor 5.0.0.2 remote-as 65020 /*RTE EBGP*/
neighbor 4.0.0.2 remote-as 100 /*RTD EBGP*/
```

➤ **Настройка RTB:**

```
interface vlan1
ip address 1.0.0.2 255.0.0.0
```



```
!  
interface vlan3  
ip address 3.0.0.1 255.0.0.0  
!  
router bgp 65010  
bgp confederation identifier 200  
bgp confederation peers 65020  
neighbor 1.0.0.1 remote-as 65010 /*RTA IBGP*/  
neighbor 3.0.0.2 remote-as 65010 /*RTC IBGP*/
```

➤ **Настройка RTC:**

```
interface vlan2  
ip address 2.0.0.2 255.0.0.0  
!  
interface vlan3  
ip address 3.0.0.2 255.0.0.0  
!  
router bgp 65010  
bgp confederation identifier 200  
bgp confederation peers 65020  
neighbor 2.0.0.1 remote-as 65010 /*RTA IBGP*/  
neighbor 3.0.0.1 remote-as 65010 /*RTB IBGP*/
```

➤ **Настройка RTD:**

```
interface vlan4  
ip address 4.0.0.2 255.0.0.0  
!  
router bgp 100  
neighbor 4.0.0.1 remote-as 200 /*RTA EBGP*/
```

➤ **Настройка RTE:**

```
interface vlan5  
ip address 5.0.0.2 255.0.0.0
```



```
!  
router bgp 65020  
  bgp confederation identifier 200  
  bgp confederation peers 65010  
  neighbor 5.0.0.1 remote-as 65010 /*RTA EBGP*/
```

#### 24.4.4.9 Примеры карты маршрутизации с атрибутом группы BGP

В этом разделе приведены три примера использования маршрутных карт с атрибутом BGP-комьюнити.

В первом примере настройка **route-map set-community** применяется к исходящему обновлению соседа 171.69.232.50. Установите специальный атрибут «community» со значением «no-export» для маршрутов, соответствующих списку доступа «aaa», в то время как другие маршруты будут транслироваться обычным образом. Этот специальный атрибут автоматически не позволит узлам BGP в AS200 объявлять маршрут за пределами своей автономной системы.

```
router bgp 100  
  neighbor 171.69.232.50 remote-as 200  
  neighbor 171.69.232.50 send-community  
  neighbor 171.69.232.50 route-map set-community out  
!  
route-map set-community 10 permit  
  match ip address aaa  
  set community no-export  
!  
route-map set-community 20 permit
```

Во втором примере **route-map set-community** используется для обновления исходящих маршрутов соседа 171.69.232.90. Все маршруты, исходящие из AS70, будут добавлять значение 200 в атрибут комьюнити 200. Остальные маршруты будут объявляться обычным образом.

```
route-map bgp 200  
  neighbor 171.69.232.90 remote-as 100  
  neighbor 171.69.232.90 send-community  
  neighbor 171.69.232.90 route-map set-community out  
!  
route-map set-community 10 permit
```



```
match as-path test1
set community-additive 200 200
!
route-map set-community 20 permit
match as-path test2
!
ip as-path access-list test1 permit 70$
ip as-path access-list test2 permit .*
```

В третьем примере выборочно установите MED и значение локального приоритета маршрутов от соседа 171.69.232.55 в соответствии со значением атрибута комьюнити. Всем маршрутизаторам, соответствующим списку сообщества com1, будет присвоен номер MED 8000, это может включать маршруты со значением комьюнити 100, 200, 300 или 900, 901. Эти маршруты могут иметь другие значения атрибутов.

Для всех маршрутов, соответствующих списку комьюнити com2, будет установлено значение локального приоритета 500.

Всем остальным маршрутам будет присвоено значение локального приоритета 50. Таким образом, все остальные маршруты соседа 171.69.232.55 будут иметь приоритет 50.

```
router bgp 200
neighbor 171.69.232.55 remote-as 100
neighbor 171.69.232.55 route-map filter-on-community in
!
route-map filter-on-community 10 permit
match community com1
set metric 8000
!
route-map filter-on-community 20 permit
match community com2
set local-preference 500
!
route-map filter-on-community 30 permit
set local-preference 50
!
ip community-list standard com1 permit 100 200 300
ip community-list standard com1 permit 900 901
```



```
!  
ip community-list standard com2 permit 88  
ip community-list standard com2 permit 90  
!
```

## 25. Многоадресная рассылка

### 25.1 Введение

В данном разделе описывается, как настроить протокол многоадресной маршрутизации. Традиционная IP-передача позволяет одному хосту взаимодействовать только с одним хостом (одноадресная связь) или со всеми хостами (широковещательная связь). Технология многоадресной рассылки позволяет одному хосту отправлять сообщения нескольким хостам. Эти хосты называются членами группы.

Адрес назначения сообщения, отправленного члену группы, представляет собой адрес класса D (224.0.0.0–239.255.255.255). Многоадресное сообщение передается как UDP. Он не обеспечивает надежную передачу и контроль ошибок, как TCP.

В схеме многоадресной рассылки всегда присутствуют отправитель и получатель. Отправитель может отправить многоадресное сообщение, не присоединяясь к группе. Однако получатель должен присоединиться к группе, прежде чем он сможет получать адресованные ей сообщения.

Отношения между членами группы динамичны. Организатор может присоединиться к группе или покинуть ее в любое время. Ограничений по местонахождению и количеству участников группы нет. При необходимости хост может быть членом нескольких групп. Следовательно, состояние группы и количество ее членов меняется со временем.

Маршрутизатор может поддерживать таблицу маршрутизации для пересылки многоадресных сообщений, выполняя протокол многоадресной маршрутизации, такой как PIM-DM и PIM-SM. Маршрутизатор изучает состояние членов группы в сегменте сети с прямым подключением через IGMP-отчеты. Хост может присоединиться к назначенной группе IGMP, отправив IGMP-сообщение.

Технология многоадресной IP-адресации подходит для мультимедийных схем типа «один-ко-множеству».

### 25.2 Реализация многоадресной маршрутизации

В программном обеспечении коммутатора многоадресная маршрутизация следует следующим правилам:

- IGMP работает между маршрутизатором и хостом в локальной сети и используется для отслеживания отношений между членами группы.



- OLNK – это статическая многоадресная технология, которая используется в простой топологии. Она реализует многоадресную пересылку и эффективно экономит ресурсы ЦП и пропускную способность.
- PIM-DM, PIM-SM и DVMRP – протоколы динамической многоадресной маршрутизации. Они работают между коммутаторами и реализуют многоадресную пересылку путем создания таблицы многоадресной маршрутизации.

На рисунке 34 показаны протоколы, используемые в приложениях многоадресной IP-адресации:

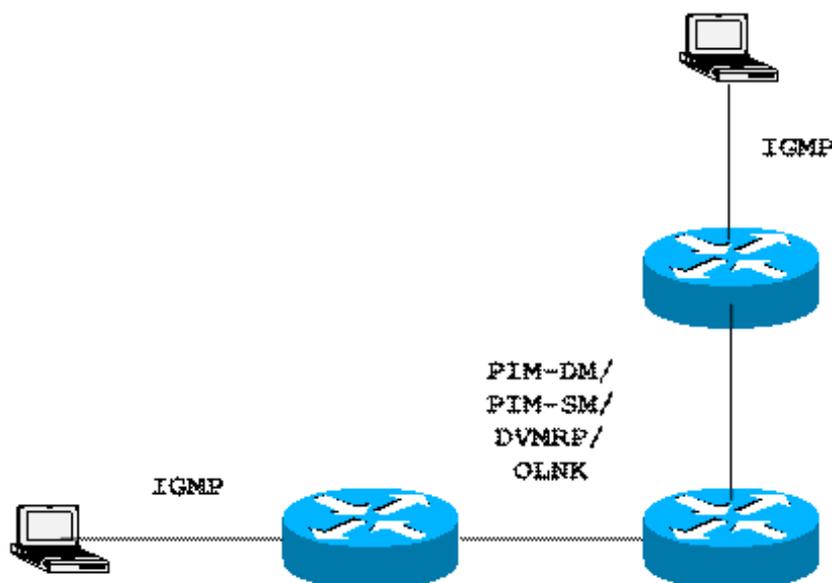


Рисунок 34 – Многоадресные протоколы

## 25.3 Задачи настройки многоадресной маршрутизации

### 25.3.1 Задачи основной настройки многоадресной рассылки

- Запуск многоадресной маршрутизации (обязательно)
- Настройка порога TTL (необязательно)
- Настройка быстрой многоадресной передачи (необязательно)
- Настройка статического многоадресного маршрута (необязательно)
- Настройка границы многоадресной передачи (необязательно)
- Настройка помощника многоадресной рассылки (необязательно)
- Настройка тупикового многоадресного маршрута (необязательно)
- Мониторинг и поддержка многоадресного маршрута (необязательно)

### 25.3.2 Задачи настройки IGMP

- Изменение текущей версии IGMP



- Настройка интервала запросов IGMP
- Настройка интервала проверки запросчика IGMP
- Настройка максимального времени ответа IGMP
- Настройка интервала опроса последнего члена группы IGMP
- Статическая конфигурация IGMP
- Настройка списка немедленного выхода из группы IGMP

### 25.3.3 Задачи настройки PIM-DM

- Настройка таймера
- Обозначение версии PIM-DM
- Настройка обновления состояния
- Настройка списка фильтрации
- Установка приоритета DR
- Очистка (S, G)-информации

### 25.3.4 Задачи настройки PIM-SM

- Настройка статической точки встречи (RP)
- Настройка резервного маршрутизатора загрузки (BSR)
- Настройка резервной RP
- Отображение многоадресной маршрутизации PIM-SM
- Очистка многоадресных маршрутов, изученных PIM-SM

### 25.3.5 Задачи настройки DVMRP

- Настройка сводного маршрута
- Настройка обязательного конечного узла порта
- Настройка фильтра маршрутов
- Отображение одноадресного маршрута DVMRP
- Отображение многоадресного маршрута DVMRP
- Очистка многоадресных маршрутов, изученных DVMRP

## 25.4 Основные настройки многоадресной маршрутизации



### 25.4.1 Запуск многоадресной маршрутизации

Чтобы разрешить программному обеспечению коммутатора пересылать многоадресные сообщения, необходимо запустить многоадресную маршрутизацию. Выполните следующую команду в режиме глобальной конфигурации, чтобы запустить пересылку многоадресных сообщений:

| Команда                     | Описание                              |
|-----------------------------|---------------------------------------|
| <b>ip multicast-routing</b> | Запускает многоадресную маршрутизацию |

### 25.4.2 Запуск функции многоадресной рассылки на порту

Когда на порту работает протокол многоадресной маршрутизации, активируется IGMP. Протоколы многоадресной маршрутизации включают OLNK, PIM-DM, PIM-SM и DVMRP. На одном порту может работать только один протокол. Когда маршрутизатор соединяет несколько доменов многоадресной рассылки, на разных портах могут работать разные многоадресные протоколы.

Тем не менее, программное обеспечение коммутатора может работать как пограничный маршрутизатор многоадресной рассылки (MBR). Если возможно, не запускайте одновременно несколько протоколов многоадресной маршрутизации на одном коммутаторе, поскольку это может серьезно повлиять на работу некоторых из них. Например, при одновременном запуске PIM-DM (поддерживает только записи (S, G)) и BIDIR PIM-SM (поддерживает только записи (\*, G)) возможны конфликты и несогласованность данных. Также может произойти повторное построение деревьев, что приведет к неэффективному использованию сетевых ресурсов и увеличению задержек в доставке информации.

#### 25.4.2.1 Запуск OLNK

Выполните следующую команду в режиме настройки интерфейса, чтобы запустить многоадресную маршрутизацию на порту:

| Команда        | Описание                              |
|----------------|---------------------------------------|
| <b>ip olnk</b> | Запускает многоадресную маршрутизацию |

#### 25.4.2.2 Запуск PIM-DM

Выполните следующую команду в режиме настройки интерфейса чтобы запустить PIM-DM на порту:

| Команда | Описание |
|---------|----------|
|---------|----------|



|                  |   |
|------------------|---|
| <b>ip pim-dm</b> | Активирует «плотный» режим многоадресной маршрутизации PIM-DM на интерфейсе |
|------------------|---|

### 25.4.2.3 Запуск PIM-SM

Выполните следующую команду в режиме настройки интерфейса чтобы запустить PIM-SM на порту:

| Команда          | Описание  |
|------------------|---|
| <b>ip pim-sm</b> | Активирует «разреженный» режим многоадресной маршрутизации PIM-SM на интерфейсе |

### 25.4.2.4 Настройка порога TTL

Запустите команду **ip multicast ttl-threshold**, чтобы настроить порог TTL многоадресного сообщения, которому разрешено проходить через порт. Запустите команду **no ip multicast ttl-threshold**, чтобы использовать пороговое значение по умолчанию 1.

| Команда  | Описание                       |
|--|--------------------------------|
| <b>ip multicast ttl-threshold <i>ttl-value</i></b> | Настраивает порог TTL на порту |

#### ➤ Пример

В следующем примере показана настройка порога TTL для порта:

```
interface ethernet 1/0
ip multicast ttl-threshold 200
```

### 25.4.2.5 Настройка быстрой многоадресной передачи

Запустите команду **ip multicast mroute-cache**, чтобы включить функцию быстрой многоадресной рассылки на порту. Для отмены функции выполните форму **no** этой команды.

| Команда                          | Описание   |
|----------------------------------|--|
| <b>ip multicast mroute-cache</b> | Включает функцию быстрой многоадресной передачи на порту |



➤ Пример

В следующем примере показано, как выключить функцию быстрой многоадресной передачи на порту:

```
interface ethernet 1/0  
no ip mroute-cache
```

### 25.4.2.6 Настройка статического многоадресного маршрута

Статическая многоадресная маршрутизация позволяет устанавливать маршруты для многоадресной передачи, которые могут отличаться от маршрутов для одноадресной передачи. При передаче многоадресных сообщений выполняется проверка обратного пути (RPF). Это означает, что маршрутизатор проверяет, пришло ли сообщение от ожидаемого порта, который является следующим узлом перехода для одноадресного маршрута, ведущего к отправителю сообщения. Если оно пришло по правильному пути, маршрутизатор продолжает его пересылать. Когда пути одноадресной и многоадресной передачи совпадают, проверка RPF имеет смысл. В некоторых случаях одноадресный путь должен отличаться от многоадресного.

Возьмем в качестве примера технологию туннелирования. Когда маршрутизатор на пути не поддерживает протокол многоадресной передачи, решением является настройка туннеля GRE между двумя маршрутизаторами. На следующем рисунке каждый маршрутизатор одноадресной рассылки поддерживает только одноадресные сообщения; каждый маршрутизатор многоадресной рассылки поддерживает только многоадресные сообщения. Исходный узел отправляет многоадресное сообщение на целевой узел через MR1 и MR2. MR2 пересылает многоадресное сообщение только тогда, когда оно получено через туннель. Когда целевой узел отправляет одноадресное сообщение на исходный узел, также используется туннель. При использовании технологии туннелирования скорость доставки сообщений ниже, чем при прямой передаче.

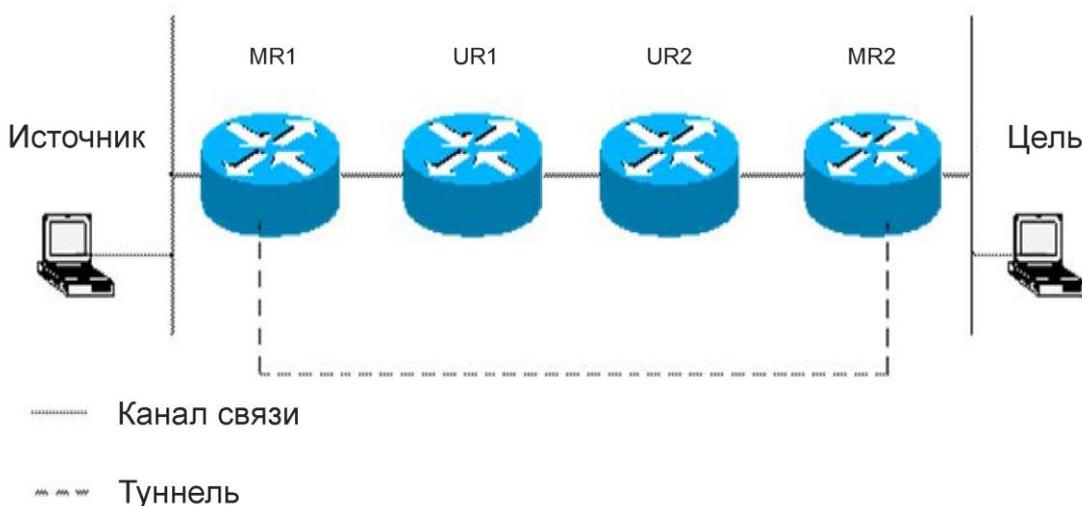


Рисунок 35 – GRE-туннель



После настройки статической многоадресной маршрутизации маршрутизатор может выполнить проверку RPF в соответствии с информацией о конфигурации. Проверка RPF больше не основана на таблице маршрутизации одноадресной рассылки. Поэтому многоадресное сообщение проходит через туннель, в то время как одноадресное передается обычным образом. Статический многоадресный маршрут существует только в локализованной области. Он не будет ни объявлен, ни перенаправлен.

Выполните следующую команду в режиме глобальной конфигурации, чтобы настроить статический многоадресный маршрут:

| Команда  | Описание                                      |
|--|---|
| <b>ip mroute</b> <i>source-address mask rpf-address type number [distance]</i> | Настраивает статический многоадресный маршрут |

### 25.4.3 Настройка границы многоадресной IP-передачи

Запустите команду **ip multicast boundary**, чтобы настроить границу многоадресной рассылки для порта. Запустите команду **no ip multicast boundary**, чтобы отменить настроенную границу. Повторное использование команды заменяет настройки, сделанные ранее.

| Команда   | Описание   |
|---|--|
| <b>ip multicast boundary</b> <i>access-list</i> | Настраивает границу многоадресной рассылки для порта |

#### ➤ Пример

В следующем примере показано, как настроить диапазон адресов, в котором порт может управлять многоадресной рассылкой:

```
interface ethernet 0/0
ip multicast boundary acl
ip access-list standard acl
permit 192.168.20.97 255.255.255.0
```

### 25.4.4 Настройка управления скоростью многоадресной IP-передачи

Чтобы ограничить скорость приема и отправки многоадресных сообщений в диапазоне источника/группы используется команда **ip multicast rate-limit**. Форма **no** этой команды отменяет ограничение скорости.

Выполните следующую команду, чтобы ограничить скорость входящего многоадресного потока до n кбит/с.



| Команда  | Описание   |
|--|--|
| <b>ip multicast rate-limit in group-list</b><br><i>access-list1 source-list access-list2</i><br><i>nkbps</i> | Настраивает ограничение максимальной скорости ввода многоадресного потока в определенном диапазоне |

Выполните следующую команду, чтобы ограничить скорость исходящего многоадресного потока до n кбит/с.

| Команда  | Описание  |
|--|---|
| <b>ip multicast rate-limit in group-list</b><br><i>access-list1 source-list access-list2</i><br><i>nkbps</i> | Настраивает ограничение максимальной скорости вывода многоадресного потока в определенном диапазоне |

## 25.4.5 Настройка помощника многоадресной передачи

Запустите команду **ip multicast helper-map**, чтобы использовать маршрут многоадресной рассылки для соединения двух ширококвещательных сетей в многоадресной сети. Запустите команду **no ip multicast helper-map**, чтобы отменить команду.

На первом переходе маршрутизатор подключен к исходной ширококвещательной сети:

| Команда   | Описание   |
|---|--|
| <b>interface</b> <i>type number</i>                                       | Вход в режим настройки интерфейса  |
| <b>ip multicast helper-map broadcast</b> <i>group-address access-list</i> | Настраивает помощник многоадресной рассылки для преобразования ширококвещательного сообщения в многоадресное |
| <b>ip directed-broadcast</b>  | Позволяет направленную трансляцию  |
| <b>ip forward-protocol</b> [ <i>port</i> ]                                | Настраивает номер порта, позволяющего пересылать сообщение   |

На маршрутизаторе последнего перехода, подключающемся к ширококвещательной сети назначения, выполните следующие операции:

| Команда                             | Описание                          |
|-------------------------------------|-----------------------------------|
| <b>interface</b> <i>type number</i> | Вход в режим настройки интерфейса |



|   |  |
|---|--|
| <b>ip directed-broadcast</b>  | Позволяет направленную трансляцию  |
| <b>ip multicast helper-map</b> <i>group-address broadcast-address access-list</i> | Настраивает помощник многоадресной рассылки для преобразования многоадресного сообщения в ширококвещательное сообщение |
| <b>ip forward-protocol</b> [port]   | Настраивает номер порта, позволяющего пересылать сообщение   |

## ➤ Пример

В следующем примере показано, как настроить помощник многоадресной рассылки.

Выполните команду **ip directed-broadcast** на порту e0 маршрутизатора первого перехода для обработки направленного сообщения. Настройка **ip multicast helper-map broadcast 230.0.0.1 testacl1** позволяет преобразовать ширококвещательное сообщение UDP с номером порта 4000, отправленное с исходного адреса 192.168.20.97/24, в многоадресное сообщение с адресом назначения 230.0.0.1.

Выполните команду **ip directed-broadcast** на порту e1 маршрутизатора последнего перехода для обработки направленного сообщения. Настройка **ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2**, позволяет преобразовать многоадресное сообщение с номером порта 4000 и адресом назначения 230.0.0.1, отправленное с исходного адреса 192.168.20.97/24, в ширококвещательное сообщение с адресом назначения 172.10.255.255.

В маршрутизаторе первого перехода, подключающемся к исходной ширококвещательной сети, выполните следующие операции:

```
interface ethernet 0
ip directed-broadcast
ip multicast helper-map broadcast 230.0.0.1 testacl
ip pim-dm
!
ip access-list extended testacl permit udp 192.168.20.97 255.255.255.0 any
ip forward-protocol udp 4000
```

В маршрутизаторе последнего перехода, подключающемся к ширококвещательной сети назначения, выполните следующие операции:

```
interface ethernet 1
ip directed-broadcast
ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2
ip pim-dm
```



!

```
ip access-list extended testacl2 permit udp 192.168.20.97 255.255.255.0 any
ip forward-protocol udp 4000
```

## 25.4.6 Настройка тупикового многоадресного маршрута

Запустите команды **ip igmp helper-address** и **ip pim-dm neighbor-filter**, чтобы настроить многоадресный маршрут типа Stub.

На порту, к которому подключены stub-маршрутизатор и хост, выполните следующие операции:

| Команда  | Описание  |
|--|---|
| <b>interface</b> <i>type number</i>                      | Вход в режим настройки интерфейса   |
| <b>ip igmp helper-address</b> <i>destination-address</i> | Настраивает команду <b>ip igmp helper-address</b> для пересылки многоадресного сообщения на центральный маршрутизатор |

На порту, к которому подключены центральный маршрутизатор и stub-маршрутизатор, выполните следующие операции:

| Команда   | Описание   |
|---|--|
| <b>interface</b> <i>type number</i>                 | Вход в режим настройки интерфейса                  |
| <b>ip pim-dm neighbor-filter</b> <i>access-list</i> | Фильтрует все сообщения PIM на stub-маршрутизаторе |

### ➤ Пример

В следующем примере показана конфигурация маршрутизаторов А и В:

#### Настройка stub-маршрутизатора А

```
ip multicast-routing
ip pim-dm
ip igmp helper-address 10.0.0.2
```

#### Настройка центрального маршрутизатора В

```
ip multicast-routing
ip pim-dm
ip pim-dm neighbor-filter stubfilter
```



```
ip access-list stubfilter
deny 10.0.0.1
```

## 25.4.7 Мониторинг и поддержка многоадресного маршрута

### 1. Очистка многоадресного кэша и таблицы маршрутизации

Если специальные кэши или таблица маршрутизации недействительны, необходимо очистить их содержимое. Выполните следующие команды в режиме управления:

| Команда   | Описание   |
|---|--|
| <b>clear ip igmp group</b> [ <i>type number</i> ]<br>[ <i>group-address</i>   <cr>] | Очищает элементы кэша IGMP                             |
| <b>clear ip mroute</b> [*   <i>group-address</i>  <br><i>source-address</i> ]       | Очищает элементы в таблице многоадресной маршрутизации |

### 2. Отображение таблицы многоадресной маршрутизации и статистической информации системы.

Подробная информация о таблице многоадресной IP-маршрутизации, кэше или базе данных помогает оценить, как используются ресурсы и решить сетевые проблемы.

Выполните следующие команды в режиме управления, чтобы отобразить статистическую информацию о многоадресном маршруте:

| Команда   | Описание  |
|---|---|
| <b>show ip igmp groups</b> [ <i>type number</i>  <br><i>group-address</i> ] [ <b>detail</b> ] | Отображает информацию о группе многоадресной рассылки в кэше IGMP |
| <b>show ip igmp interface</b> [ <i>type number</i> ]  | Отображает информацию о конфигурации IGMP на интерфейсе           |
| <b>show ip mroute mfc</b>   | Отображает кэш многоадресной рассылки                             |
| <b>show ip rpf</b> [ <b>pim-dm</b>   <b>pim-sm</b> ]<br><i>source-address</i>                 | Отображает информацию RPF   |



## 25.5 IGMP

### 25.5.1 Введение

#### 1. IGMP

IGMP (Internet Group Management Protocol) – протокол, используемый для управления членами групп многоадресной рассылки. Это асимметричный протокол, включающий сторону хоста и сторону коммутатора. На стороне хоста протокол IGMP регулирует, как хост, будучи участником группы многоадресной рассылки, сообщает, к какой группе он принадлежит, и как отвечает на запросы от коммутатора. На стороне маршрутизатора протокол IGMP регулирует, как коммутатор узнает идентификатор члена группы многоадресной рассылки в локальной сети и как изменяет сохраненную информацию о членах группы в соответствии с отчетными сообщениями хоста.

Поскольку данные коммутаторы поддерживают протокол IGMP-Router, протоколу многоадресной маршрутизации может быть предоставлена информация о членах группы многоадресной рассылки в текущей сети, и коммутатор решает, пересылать ли многоадресное сообщение. Чтобы коммутатор поддерживал процесс многоадресной рассылки IP-сообщений, необходимо настроить протокол многоадресной маршрутизации и протокол IGMP-Router. В настоящее время коммутаторы поддерживают IGMP версии 3.

Для IGMP не существует независимых команд запуска. Функция протокола IGMP-Router запускается через протокол многоадресной маршрутизации.

#### 2. OLNK

Строго говоря, протокол IGMP only-link (OLNK) не является протоколом многоадресной маршрутизации, поскольку в нем нет процесса взаимодействия, как в других протоколах. Однако в некоторых особых случаях запуск OLNK в простой топологии дает хорошие результаты. Подобно протоколу PIM-DM, в котором также нет процесса согласования, OLNK может обрабатывать смену членов группы IGMP и оперативно настраивать интерфейс RPF в соответствии с изменением топологии. Таким образом, OLNK обеспечивает многоадресную пересылку без необходимости загрузки полосы пропускания управляющими сообщениями протокола многоадресной маршрутизации.

### 25.5.2 Изменение текущей версии IGMP

На данный момент протокол IGMP имеет три формальные версии. Соответствующие RFC следующие: RFC1112, RFC2236 и RFC3376. IGMP V1 поддерживает только функцию записи участников группы многоадресной рассылки. IGMP V2 может запрашивать назначенного участника группы многоадресной рассылки, генерирует сообщение о выходе, когда хост IGMP покидает группу, и сокращает задержку при изменении статуса участника группы. IGMP V3 имеет дополнительные функции для обновления и поддержания идентификаторов членов группы многоадресной рассылки, которые соответствуют адресам исходных хостов. Протокол IGMP-Router V3 полностью совместим с хост-стороной IGMP V1 и IGMP V2. Наше программное обеспечение поддерживает протоколы IGMP трех версий.



Вы можете настроить функцию IGMP-Router на разных интерфейсах (протокол многоадресной маршрутизации, настроенный на разных интерфейсах, может запускать функцию IGMP-Router), и на разных интерфейсах можно запускать разные версии IGMP.

Обратите внимание, что коммутатор многоадресной рассылки может запустить функцию IGMP-Router только на одном из портов, подключенных к одной сети.

Запустите следующую команду в режиме настройки интерфейса, чтобы изменить версию протокола IGMP на порту:

| Команда                                      | Описание  |
|--|---|
| <b>ip igmp version</b> <i>version_number</i> | Изменяет версию IGMP, работающую на текущем порту |

### 25.5.3 Настройка интервала запросов IGMP

Независимо от номера версии текущего протокола IGMP-Router, многоадресный коммутатор может отправлять сообщение общего запроса IGMP каждый определенный раз на порт, на котором запущена функция IGMP. Адрес передачи – 224.0.0.1. Целью многоадресного коммутатора является получение отчетного сообщения от хоста IGMP и, следовательно, знание того, к какой группе многоадресной рассылки принадлежит каждый хост IGMP в сети. Интервал отправки сообщения общего запроса называется интервалом запроса IGMP. Если для параметра «IGMP Query Interval» установлено большое значение, коммутатор не сможет сразу получить информацию о том, к какой группе многоадресной рассылки принадлежит определенный хост. Если для параметра «IGMP Query Interval» установлено небольшое значение, поток сообщений IGMP в текущей сети будет увеличиваться.

Запустите следующую команду в режиме настройки интерфейса, чтобы изменить интервал запросов IGMP на порту:

| Команда                                   | Описание  |
|---|---|
| <b>ip igmp query-interval</b> <i>time</i> | Изменяет интервал запросов IGMP на текущем интерфейсе (единица измерения – секунда) |

### 25.5.4 Настройка интервала проверки запросчика IGMP

Что касается версии 2 и версии 3 протокола IGMP-Router, то если в той же сети существует другой коммутатор, поддерживающий протокол IGMP-Router, вам необходимо выбрать запросчик. Запросчик (*querier*) означает коммутатор, который может отправлять сообщение запроса. Фактически это порт коммутатора, на котором включен протокол IGMP-Router. Обычно в одной сети есть только один запросчик, то есть только один коммутатор отправляет IGMP-запросы. В IGMP версии 1 нет процедуры выбора запросчика, и то, какой коммутатор будет отправлять сообщения запроса, определяет протокол многоадресной маршрутизации.



IGMP-Router V2 и IGMP-Router V3 имеют одинаковый механизм выбора запрашивающего, то есть коммутатор с минимальным IP-адресом является запросчиком в сети. Коммутатору, который не является запрашивающим, необходимо сохранять счетчик времени для отслеживания наличия запрашивающего. Если время истекает, то устройство, которое не является текущим запросчиком, становится им вместо предыдущего запросчика. Однако оно продолжит выполнять эту функцию только до тех пор, пока не получит запрос IGMP от другого устройства с IP-адресом, меньшим, чем у него. Для IGMP-Router V2 вы можете настроить интервалы проверки запросчика с помощью следующей команды:

| Команда                             | Описание   |
|-------------------------------------|--|
| <b>ip igmp querier-timeout time</b> | Настраивает интервал проверки запросчика (единица измерения – секунда) |

Для IGMP-Router V1 интервал проверки запросчика бесполезен. Для IGMP-Router V3 интервал настроить невозможно, поскольку он определяется самим протоколом. Таким образом, приведенные выше команды настройки действительны только для IGMP-Router V2.

## 25.5.5 Настройка максимального времени ответа IGMP

Для IGMP-Router V2 и IGMP-Router V3 специальное поле данных в передаваемом сообщении IGMP General Query регулирует максимальное время ответа хоста IGMP. То есть хост IGMP должен отправить ответное сообщение до истечения регламентированного максимального времени ответа, указывая на то, что сообщение общего запроса получено. Если максимальное время ответа установлено на большое значение, смена членов многоадресной группы задерживается. Если максимальное время ответа установлено на небольшое значение, поток сообщений IGMP будет увеличен в текущей сети.



Максимальное время ответа IGMP должно быть короче интервала запроса IGMP. Если значение максимального времени ответа больше интервала запроса, система автоматически установит максимальное время ответа равным интервалу запроса – 1.

Для IGMP-Router V2 и IGMP-Router V3 выполните следующую команду в режиме настройки интерфейса, чтобы установить максимальное время ответа IGMP:

| Команда                                     | Описание   |
|---|--|
| <b>ip igmp query-max-response-time time</b> | Настраивает максимальное время ответа IGMP (единица измерения – секунда) |



## 25.5.6 Настройка интервала запросов IGMP для последнего члена группы

Когда в IGMP-Router V2 и V3 отправляется запрос для конкретной многоадресной группы, интервал запроса, установленный для последнего участника этой группы, используется как максимальное время ожидания ответа от устройств.

Это означает, что устройство, участвующее в группе (IGMP-хост), должно отправить свой ответ до истечения максимального времени ожидания, установленного для последнего участника группы. Это позволяет указать, что запрос для конкретной группы был получен. Если хост определяет, что ему не нужно отвечать на запрос, он может не отправлять ответ после установленного интервала. В таком случае коммутатор, управляющий многоадресной группой, должен обновить информацию о членах группы.

Если интервал запроса, установленный для последнего участника группы, большой, это может привести к задержкам при изменении состава группы. Если интервал маленький, это может увеличить трафик обмена сообщениями IGMP в текущей сети.

Для IGMP-Router V2 и V3 выполните следующую команду в режиме конфигурации интерфейса, чтобы настроить интервал запросов IGMP для последнего участника группы:

| Команда  | Описание   |
|--|--|
| <b>ip igmp last-member-query-interval time</b> | Настраивает интервал запроса IGMP последнего члена группы (единица измерения – мс) |

Данная команда недействительна для IGMP-Router V1.

## 25.5.7 Статическая конфигурация IGMP

Помимо функций, регулируемых протоколом IGMP-Router, коммутаторы данной серии поддерживают настройку статической группы многоадресной рассылки на порту. Для хоста IGMP отношения с членами группы многоадресной рассылки могут различаться. Предположим, что хост IGMP принадлежит только группе многоадресной рассылки group1, он получает от нее многоадресные сообщения и отправляет свои в нее же. По истечении определенного периода времени он может принадлежать к группе group2, принимать от нее и отправлять в нее многоадресные сообщения. Позднее этот хост может не принадлежать ни к одной группе многоадресной рассылки. Поэтому информация о группах постоянно меняется.

В отличие от вышеупомянутой динамической группы многоадресной рассылки, в случае, если порт настроен как принадлежащий к статической группе, протокол многоадресной маршрутизации рассматривает его в качестве порта, который всегда получает и отправляет многоадресные сообщения этой группы. Для лучшей совместимости с IGMP-Router V3 статическую группу многоадресной рассылки можно настроить на получение многоадресных сообщений с назначенного адреса источника, то есть при получении сообщения добавляется функция фильтра источника.



Запустите следующую команду в режиме конфигурации интерфейса, чтобы настроить статическую многоадресную группу для порта:

| Команда  | Описание  |
|--|---|
| <b>ip igmp static-group</b> <i>{*   group-address}</i><br><b>{include source-address   &lt;cr&gt;}</b> | Настраивает атрибут статической группы многоадресной рассылки для порта |

## 25.5.8 Настройка списка немедленного выхода из группы IGMP

Если на порту коммутатора работает IGMP версии 2 и в сети, к которой подключен этот порт, имеется только один хост, использующий IGMP, вы можете реализовать функцию немедленного выхода для этого хоста, настроив соответствующий список доступа с перечислением групп, из которых возможен немедленный выход. По правилам IGMP версии 2, когда хост покидает мультикастовую группу, он отправляет сообщение Leave на ближайший маршрутизатор или коммутатор. После получения этого сообщения коммутатор отправляет IGMP-запрос, для подтверждения выхода. Если настроена функция «Немедленный выход», коммутатор сразу прекращает передачу многоадресного трафика хосту, что позволяет избежать задержек при изменении идентификаторов членов группы.



Команда может быть выполнена как в режиме глобальной конфигурации, так и в режиме настройки интерфейса. Приоритет команды в глобальном режиме, выше, чем у команды в режиме интерфейса. Если команда уже была настроена в глобальном режиме, команда в режиме интерфейса, будет проигнорирована. Если команда выполнялась в режиме настройки интерфейса, ее глобальное выполнение удалит предыдущие настройки, выполненной на интерфейсе.

Для IGMP-Router V2 выполните следующую команду в режиме конфигурации интерфейса, чтобы настроить список немедленного выхода из группы IGMP:

| Команда  | Описание   |
|--|--|
| <b>ip igmp immediate-leave group-list</b> <i>list-name</i> | Настраивает список доступа, реализующий функцию немедленного выхода из группы многоадресной рассылки |
| <b>ip access-list standard</b> <i>list-name</i>            | Создает стандартный список IP-доступа с именем <i>list-name</i>                                      |
| <b>permit</b> <i>source-address</i>                        | Указывает IP-адрес хоста IGMP, который будет реализовывать функцию немедленного выхода               |

Данная команда недействительна для IGMP-Router V1 и V3.



## 25.5.9 Примеры настройки функций IGMP

### 1. Пример изменения версии IGMP

Протокол IGMP-Router последней версии совместим с хостом IGMP младшей версии, но не может быть совместим с протоколом IGMP-Router более ранней версии. Поэтому, если в текущей сети есть коммутаторы, использующие IGMP-Router более ранней версии, вам необходимо изменить версию протокола до самой ранней, работающий в том же сегменте сети.

Предположим, администратор знает, что в сети, к которой подключается локальный коммутатор, существуют коммутаторы, работающие под управлением IGMP-Router V1 и IGMP-Router V2. В таком случае ему необходимо изменить версию протокола IGMP-Router с версии 2 на версию 1 на соответствующем порту.

```
interface ethernet 1/0  
ip igmp version 1
```

### 2. Пример настройки интервала запроса IGMP

В следующем примере показано, как изменить интервал запроса IGMP до 50 секунд на интерфейсе ethernet 1/0:

```
interface ethernet 1/0  
ip igmp query-interval 50
```

### 3. Пример настройки интервала проверки запросчика IGMP

В следующем примере показано, как изменить интервал проверки запросчика на 100 секунд для интерфейса ethernet 1/0:

```
interface ethernet 1/0  
ip igmp querier-timeout 100
```

### 4. Пример настройки максимального времени ответа IGMP

В следующем примере показано, как изменить максимальное время ответа IGMP до 15 секунд на интерфейсе ethernet 1/0:

```
interface ethernet 1/0  
ip igmp query-max-response-time 15
```

### 5. Пример настройки интервала запроса IGMP для последнего члена группы

В следующем примере показано, как изменить интервал IGMP-запроса последнего члена группы на 2000 мс на интерфейсе ethernet 1/0:

```
interface ethernet 1/0
```



```
ip igmp last-member-query-interval 2000
```

## 6. Пример статической конфигурации IGMP

Команда настройки статической группы многоадресной рассылки может определять различные классы статических групп, принимая разные параметры. В следующих примерах показаны результаты выполнения различных параметров команды.

```
interface ethernet 1/0
```

```
ip igmp static-group *
```

Предыдущая команда настраивает все статические группы многоадресной рассылки на интерфейсе ethernet 1/0. Протокол многоадресной маршрутизации будет транслировать все многоадресные IP-сообщения на интерфейс ethernet 1/0.

```
interface ethernet 1/0
```

```
ip igmp static-group 224.1.1.7
```

Предыдущая команда настраивает статическую многоадресную группу 224.1.1.7 на интерфейсе ethernet 1/0, то есть интерфейс принадлежит группе многоадресной рассылки 224.1.1.7. Протокол многоадресной маршрутизации будет отправлять все многоадресные IP-сообщения, целью назначения которых является группа многоадресной рассылки 224.1.1.7, на интерфейс ethernet 1/0.

```
interface ethernet 1/0
```

```
ip igmp static-group 224.1.1.7 include 192.168.20.168
```

Предыдущая команда настраивает статическую группу многоадресной рассылки 224.1.1.7 на интерфейсе ethernet 1/0 и определяет фильтр источника для этой группы как 192.168.20.168. То есть интерфейс принадлежит к группе многоадресной рассылки 224.1.1.7, но он получает многоадресные IP-сообщения только с адреса 192.168.20.168. Протокол многоадресной маршрутизации будет отправлять все многоадресные IP-сообщения, полученные от 192.168.20.168 и целью назначения которых является группа 224.1.1.7, на интерфейс ethernet 1/0.

Выполните следующую команду в режиме настройки интерфейса, чтобы получить многоадресное IP-сообщение с адреса 192.168.20.169 и отправить его в группу многоадресной рассылки 224.1.1.7:

```
ip igmp static-group 224.1.1.7 include 192.168.20.169
```

Эту команду можно выполнять много раз, чтобы определить разные адреса источника.



В группе многоадресной рассылки нельзя одновременно настроить информацию о группе как для конкретного источника данных, так и для всех источников данных.



Если выполнить команду для настройки информации о группе с указанием всех источников, то команда с указанием конкретного источника, выполненная позже, будет проигнорирована. Например, если выполнить команду **ip igmp static-group 224.1.1.7 include 192.168.20.168** после выполнения команды **ip igmp static-group 224.1.1.7**, то команда **ip igmp static-group 224.1.1.7 include 192.168.20.168** будет проигнорирована.

#### 7. Пример настройки списка участников IGMP с немедленным выходом

В следующем примере показано, как настроить список доступа для реализации функции немедленного выхода на интерфейсе ethernet 1/0 и добавить IP-адрес 192.168.20.168 хоста IGMP в список доступа. Конфигурация гарантирует, что хост IGMP с IP-адресом 192.168.20.168 реализует функцию немедленного выхода.

```
interface ethernet 1/0
ip igmp immediate-leave imme-leave
!
ip access-list standard imme-leave
permit 192.168.20.168
```

## 25.6 PIM-DM

### 25.6.1 Введение

PIM-DM (Protocol Independent Multicast Dense Mode) – это протокол многоадресной маршрутизации в плотном режиме. По умолчанию, когда источник многоадресной рассылки начинает отправлять мультикастовые данные, их получают все сетевые узлы в домене, так как PIM-DM пересылает многоадресные пакеты в режиме ограниченной широковещательной рассылки. Когда источник многоадресной рассылки начинает отправлять данные, коммутаторы рядом с ним пересылают пакеты на все активированные интерфейсы PIM, кроме интерфейса RPF (Reverse Path Forwarding). Таким образом, все сетевые узлы в домене PIM-DM могут получать эти многоадресные пакеты. Чтобы завершить многоадресную пересылку, коммутаторам вместе необходимо создать соответствующий элемент многоадресной маршрутизации (S, G) для группы G и ее источника S. Элемент маршрутизации (S, G) включает в себя адрес источника многоадресной рассылки, адрес группы многоадресной рассылки, входной интерфейс, список выходных интерфейсов, таймер и метку.

Если в определенном сегменте сети нет члена группы многоадресной рассылки, PIM-DM отправит сообщение Prune о сокращении, «обрезке» широковещательного дерева, отключит интерфейс пересылки, соединяющий сегмент сети, а затем установит состояние сокращения. Оно длится соответственно таймеру тайм-аута. По истечении времени таймера система возвращается в состояние пересылки, и многоадресные данные могут пересылаться по ранее пресеченным ветвям. Кроме того, состояние сокращения содержит



информацию об источнике и группе многоадресной рассылки. Когда член группы появляется в отсеченной области, PIM-DM активно отправляет сообщение о присоединении на верхний уровень, не дожидаясь истечения таймера и перевода состояния в режим пересылки.

Пока источник S все еще транслирует данные в группу G, коммутатор первого перехода будет периодически отправлять обновляющую информацию элемента маршрутизации (S, G) в нижнее исходное ширококвещательное дерево для завершения обновления. Механизм обновления PIM-DM может обновлять состояние нисходящего канала, гарантируя, что сокращение ширококвещательного дерева не истечет по тайм-ауту.

В сети с множественным доступом, помимо выбора DR, PIM-DM также вводит следующие механизмы:

- механизм подтверждения для выбора уникального отправителя, чтобы предотвратить повторную пересылку многоадресного пакета;
- механизм ограничения добавления/сокращения для уменьшения избыточной информации join/prune;
- механизм запрета сокращения для предотвращения неправильных действий по сокращению.

В домене PIM-DM маршрутизаторы, на которых работает PIM-DM, периодически отправляют информацию Hello для достижения следующих целей:

- обнаружение соседних маршрутизаторов PIM;
- оценка конечных сетей и конечных маршрутизаторов;
- выбор назначенного маршрутизатора (DR) в сети с множественным доступом.

Чтобы быть совместимым с IGMP v1, PIM-DM отвечает за выбор DR. Когда все соседние маршрутизаторы PIM поддерживают настройку приоритета на интерфейсе, в качестве DR выбирается маршрутизатор с более высоким приоритетом. Если приоритет одинаковый, в качестве DR выбирается маршрутизатор с максимальным значением IP интерфейса. Если приоритет не отображается в сообщении Hello нескольких маршрутизаторов, в качестве DR выбирается маршрутизатор, интерфейс которого имеет наибольшее значение IP.

PIM-DM v2 коммутаторов данной серии поддерживает список фильтрации соседей, CIDR, VLSM и IGMP v1-v3.

## 25.6.2 Настройка таймера

Протокол маршрутизации использует несколько таймеров для определения частоты передачи сообщения Hello и управляющего сообщения обновления состояния. Интервал передачи сообщения Hello влияет на возможность корректного создания отношений соседства.

Выполните следующие команды в режиме глобальной конфигурации, чтобы установить таймер:



| Команда   | Описание  |
|---|---|
| <b>ip pim-dm hello-interval</b> <i>time</i>                     | Устанавливает интервал (единица измерения – секунда) для отправки сообщения Hello от интерфейса и соседа  |
| <b>ip pim-dm state-refresh origination-interval</b> <i>time</i> | Для коммутатора первого перехода, напрямую подключенного к источнику, интервал отправки сообщения обновления состояния действителен только для конфигураций восходящих портов. Для следующих коммутаторов интервал – это период получения и обработки сообщения об обновлении состояния |

### 25.6.3 Настройка обновления состояния

Управляющая информация о состоянии PIM-DM по умолчанию пересылается в режиме управления. Команды в режиме настройки интерфейса эффективны только для восходящих портов, когда коммутатор первого перехода, напрямую подключенный к источнику, периодически отправляет обновленное сообщение о текущем состоянии. Для следующих коммутаторов интервал – это период получения и обработки сообщения о состоянии.

| Команда   | Описание  |
|---|---|
| <b>no ip pim-dm state-refresh disable</b>                       | Позволяет отправлять и получать на порту сообщения обновления состояния               |
| <b>ip pim-dm state-refresh origination-interval</b> <i>time</i> | Настраивает интервал для отправки и получения на порту сообщения обновления состояния |

### 25.6.4 Настройка списка фильтрации

PIM-DM не устанавливает список фильтрации по умолчанию. Указанный список фильтрации включает в себя список фильтрации соседей и список граничной фильтрации многоадресной рассылки. Список фильтрации необходимо настроить в режиме настройки интерфейса.

Чтобы запретить коммутатору или коммутаторам в сегменте сети участвовать в согласовании PIM-DM, необходимо настроить список фильтрации соседей. Чтобы запретить или разрешить некоторым группам проходить через локальный регион, необходимо настроить список граничной фильтрации многоадресной рассылки.



| Команда                          | Описание   |
|----------------------------------|--|
| <b>ip pim-dm neighbor-filter</b> | Настраивает список фильтрации соседей                          |
| <b>ip multicast boundary</b>     | Настраивает список граничной фильтрации многоадресной рассылки |

## 25.6.5 Установка приоритета DR

Для совместимости с IGMP v1 требуется выбор DR. По умолчанию приоритет DR установлен на 1. Когда все соседние маршрутизаторы PIM на интерфейсе поддерживают приоритет DR, маршрутизатор с более высоким приоритетом выбирается в качестве DR. Если приоритет одинаковый, в качестве DR выбирается соседний маршрутизатор с максимальным значением IP интерфейса. Если приоритет не отображается в сообщении Hello нескольких маршрутизаторов, в качестве DR выбирается маршрутизатор, интерфейс которого имеет наибольшее значение IP.

Запустите следующую команду в режиме настройки интерфейса:

| Команда                      | Описание   |
|------------------------------|--|
| <b>ip pim-dm dr-priority</b> | Настраивает приоритет локального DR на назначенном порту |

## 25.6.6 Очистка элемента (S, G)

Периодически элемент (S, G) в локальной MRT или статистическое значение числа мультикаст-сообщений, пересылаемых через элемент (S, G) необходимо очищать. Для этого выполните следующие команды в режиме управления:

| Команда   | Описание   |
|---|--|
| <b>clear ip mroute pim-dm</b> <i>{*   group [source]}</i> | Очищает элемент (S, G) в локальной MRT. Операция заключается в удалении всех или части элементов локальной таблицы многоадресной маршрутизации. Это может повлиять на пересылку многоадресных сообщений. Команда используется для удаления только элементов (S, G), созданных протоколом многоадресной маршрутизации PIM-DM на восходящих портах |
| <b>clear ip pim-dm interface</b>                          | Сбрасывает значение статистики многоадресного сообщения, пересылаемого   |



|  |  |
|--|--|
|  | (S, G) на порт PIM-DM. Команда используется для сброса только элементов (S, G), созданных протоколом многоадресной маршрутизации PIM-DM на восходящих портах |
|--|--|

## 25.7 PIM-SM

### 25.7.1 Введение

PIM-SM (Protocol Independent Multicast Sparse Mode) – это протокол многоадресной маршрутизации в разреженном режиме. В домене PIM-SM коммутаторы, на которых запущен PIM-SM, периодически отправляют информацию Hello для достижения следующих целей:

обнаружение соседних коммутаторы PIM-SM;

выбор назначенного маршрутизатора (DR) в сети множественного доступа.

Как показано на следующем рисунке, DR отправляет сообщение join/prune напрямую подключенным членам группы в направлении дерева многоадресной рассылки или отправляет данные непосредственно подключенного источника в дерево многоадресной рассылки.

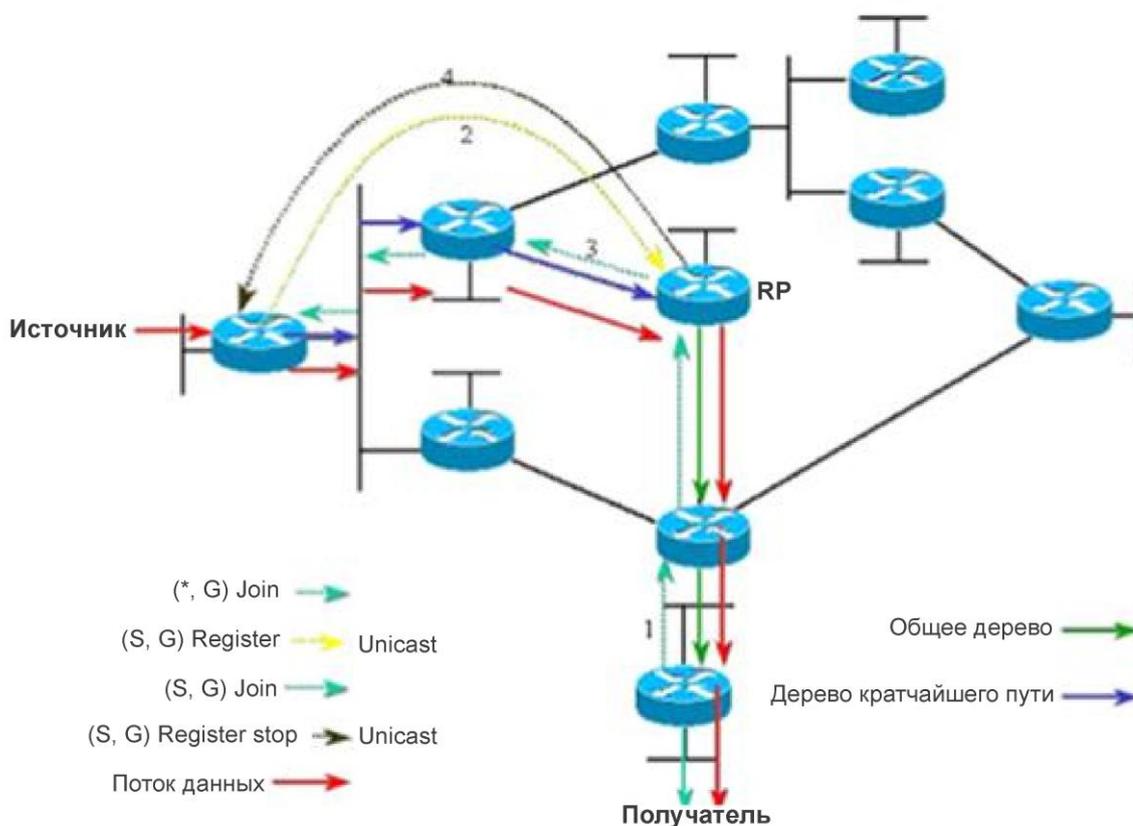


Рисунок 36 – Механизм присоединения PIM-SM



PIM-SM пересылает пакет многоадресной рассылки, создавая дерево многоадресной рассылки. Дерево можно разделить на две группы: общее дерево и дерево кратчайшего пути. Общее дерево использует RP группы G в качестве корня, в то время как дерево кратчайшего пути использует в качестве корня источник многоадресной рассылки. PIM-SM создает и поддерживает дерево многоадресной рассылки с помощью режима Join/Prune. Как показано на рисунке 36, когда DR получает сообщение Join от принимающей стороны, он будет передавать сообщение (\*, G)-Join на каждом переходе к RP группы G для присоединения к общему дереву. Когда исходный хост отправляет многоадресное сообщение группе, пакет исходного хоста упаковывается в регистрационное сообщение (Register) и передается в одноадресном режиме от DR к RP. Затем RP рассылает распакованный пакет исходного хоста каждому члену группы по общему дереву; RP отправляет сообщение (S,G)-Join первому коммутатору на пути к источнику для присоединения к дереву кратчайшего пути. Таким образом, пакет источника будет отправлен на RP по дереву кратчайшего пути без упаковки. Когда поступают первые многоадресные данные, RP отправляет сообщение о прекращении регистрации (Register-Stop) на DR источника, и DR останавливает процесс упаковки регистрационных сообщений. После этого многоадресные данные источника больше не упаковываются, а передаются к RP по дереву кратчайшего пути и затем RP рассылает их каждому члену группы через общее дерево. Когда многоадресные данные больше не нужны, DR выполняет многоадресную рассылку сообщения Prune по каждому переходу к RP группы G для обрезки общего дерева.

PIM-SM также управляет механизмом выбора RP. Один или несколько кандидатов BSR настраиваются в домене PIM-SM. Вы можете выбрать BSR среди кандидатов BSR в соответствии с определенными правилами. Кандидаты RP также настраиваются в домене PIM-SM. Они одноадресно рассылают пакеты, содержащие адрес RP и многоадресные группы, в BSR. BSR регулярно генерирует сообщение Bootstrap, содержащее ряд кандидатов RP и соответствующих групповых адресов. Сообщение Bootstrap отправляется пошагово во всем домене. Коммутатор получает и сохраняет сообщение Bootstrap. После того, как DR получает отчет об отношениях члена группы от напрямую подключенного хоста, если у DR нет элемента маршрутизации группы, он сопоставляет адрес группы с кандидатом RP через алгоритм хеширования. Затем DR рассылает многоадресное сообщение Join/Prune пошагово в направлении RP. После этого он упаковывает многоадресные данные в регистрационное сообщение и передает их в одноадресном режиме RP.

## 25.7.2 Запуск PIM-SM

Выполните на интерфейсе следующую команду для активации функции многоадресной рассылки в разреженном режиме:

| Команда          | Описание  |
|------------------|---|
| <b>ip pim-sm</b> | В режиме настройки интерфейса активирует процесс многоадресной маршрутизации PIM-SM |



### 25.7.3 Настройка статического RP

Если масштаб сети небольшой, для PIM-SM можно настроить статический RP. Конфигурация RP всех маршрутизаторов в домене PIM-SM должна быть одинаковой, что гарантирует правильность маршрута многоадресной рассылки.

Если какой-либо маршрутизатор в домене PIM-SM выполняет функции BootStrap Router (BSR), порядок проверки RP будет следующим: предпочтение отдается статическому RP с настроенной опцией **override**. Если данный параметр для статического RP не настроен, предпочтение будет отдано устройству из списка сопоставления RP, распределяемого BSR.

Выполните следующую команду в режиме глобальной конфигурации.

| Команда  | Описание  |
|--|---|
| <b>ip pim-sm rp-address</b> <i>rp-add</i><br>[ <b>override</b>   <i>acl-name</i> ]<br><b>no ip pim-sm rp-address</b> <i>rp-add</i> | Настраивает статический RP для локального коммутатора |

### 25.7.4 Настройка кандидата на роль BSR

Данная настройка позволяет генерировать уникальный глобальный BSR в домене PIM-SM. Глобальный BSR собирает и распределяет RP в домене, обеспечивая уникальность сопоставления RP.

Выполните следующую команду в режиме глобальной конфигурации.

| Команда   | Описание  |
|---|---|
| <b>ip pim-sm bsr-candidate</b> <i>type-number</i><br>[ <i>hash-mask-length</i> ]<br>[ <i>priority</i> ]<br><b>no ip pim-sm bsr-candidate</b> <i>type-number</i> | Настраивает локальный маршрутизатор в качестве кандидата на роль BSR и позволяет ему участвовать в конкуренции с глобальным BSR. При этом локальный маршрутизатор изучает сообщения BSM (Bootstrap Messages), которые отправляются глобальным BSR |

### 25.7.5 Настройка кандидата на роль RP

Настройте кандидата на роль RP, чтобы он периодически отправлял информацию в BSR, который затем распространяет эту информацию на все маршрутизаторы PIM-SM в домене, обеспечивая уникальность сопоставления RP. Для этого выполните следующую команду в режиме глобальной конфигурации:

| Команда | Описание |
|---------|----------|
|         |          |



|  |  |
|--|--|
| <pre>ip pim-sm rp-candidate [type-number] [interval   group-list acl-name] no ip pim-sm rp-candidate [type-number]</pre> | <p>Настраивает локальный маршрутизатор в качестве кандидата на роль RP</p> |
|--|--|

## 25.7.6 Отображение маршрута многоадресной рассылки PIM-SM

Выполните следующую команду, чтобы проверить информацию о маршрутах многоадресной рассылки PIM-SM:

| Команда   | Описание  |
|---|---|
| <pre>show ip mroute pim-sm [group-address] [source-address] [type-number] [summary] [count] [active kbps]</pre> | <p>Отображает соответствующую информацию о маршрутах PIM-SM</p> |

## 25.7.7 Удаление маршрутов многоадресной рассылки PIM-SM

Выполните следующую команду, чтобы очистить маршруты многоадресной рассылки, изученные PIM-SM:

| Команда  | Описание   |
|--|--|
| <pre>clear ip mroute pim-sm [ *   group-address ] [source-address]</pre> | <p>При возникновении ошибок очищает информацию многоадресной маршрутизации, сохраненную в маршрутизаторе.</p> <p>* – удаляет все многоадресные маршруты, созданные PIM-SM;</p> <p><i>group-address</i> – удаляет многоадресную маршрутизацию связанной группы;</p> <p><i>source-address</i> – удаляет многоадресный маршрут соответствующего источника</p> |

## 25.7.8 Примеры настройки PIM-SM

### 25.7.8.1 Настройка маршрутизации

В следующем примере показано, как два коммутатора изучают и пересылают маршруты многоадресной рассылки PIM-SM.

**Устройство А:**



```
!  
ip multicast-routing  
!  
interface Loopback0  
ip address 192.166.100.142 255.255.255.0  
ip pim-sm  
!  
interface Ethernet1/1  
ip address 192.166.1.142 255.255.255.0  
ip pim-sm  
ip pim-sm dr-priority 100  
!  
interface Serial2/0  
ip address 192.168.21.142 255.255.255.0  
physical-layer speed 128000  
ip pim-sm  
!  
router rip  
network 192.168.21.0  
network 192.166.1.0  
network 192.166.100.0  
version 2  
!  
ip pim-sm bsr-candidate Loopback0 30 201  
ip pim-sm rp-candidate Loopback0  
!  
Устройство В:  
!  
ip multicast-routing  
!  
interface Ethernet0/1  
ip address 192.168.200.144 255.255.255.0  
ip pim-sm
```



```
ip pim-sm dr-priority 200
!  
interface Serial0/0  
ip address 192.168.21.144 255.255.255.0  
ip pim-sm  
!
```

### 25.7.8.2 Настройка BSR

В следующем примере показана конфигурация BSR двух коммутаторов.

#### Устройство А:

```
!  
ip multicast-routing  
!  
interface Loopback0  
ip address 192.166.100.142 255.255.255.0  
ip pim-sm  
!  
interface Ethernet1/1  
ip address 192.166.1.142 255.255.255.0  
ip pim-sm  
!  
interface Serial2/0  
ip address 192.168.21.142 255.255.255.0  
physical-layer speed 128000  
ip pim-sm  
!  
router rip  
network 192.168.21.0  
network 192.166.100.0  
!  
ip pim-sm bsr-candidate Loopback0 30 201  
!
```

#### Устройство В:



```
!  
ip multicast-routing  
!  
interface Loopback0  
ip address 192.168.100.144 255.255.255.0  
ip pim-sm  
!  
interface Ethernet0/1  
ip address 192.168.200.144 255.255.255.0  
ip pim-sm  
!  
interface Serial0/0  
ip address 192.168.21.144 255.255.255.0  
ip pim-sm  
!  
ip pim-sm bsr-candidate Loopback0 30  
!
```



## Расшифровка аббревиатур

|       |   |  |
|-------|---|--|
| AAA   | Authentication Authorization and Accounting | Система аутентификации авторизации и учета событий   |
| ABR   | Area Border Router                          | Граничный маршрутизатор  |
| ACL   | Access Control List                         | Список управления доступом   |
| AS    | Autonomous System                           | Автономная система   |
| ASBR  | Autonomous System Boundary Router           | Граничный маршрутизатор автономной системы в OSPF  |
| ARP   | Address Resolution Protocol                 | Протокол определения MAC-адреса другого узла по известному IP-адресу   |
| BPDU  | Bridge Protocol Data Unit                   | Блок данных протокола управления сетевыми мостами  |
| BSR   | BootStrap Router                            | Элемент в протоколе PIM, который служит в качестве централизованного узла, помогая автоматически обнаруживать и регистрировать многоадресные группы, а также управлять распределением многоадресных данных |
| CHAP  | Challenge Handshake Authentication Protocol | Протокол аутентификации с косвенным согласованием. Является алгоритмом проверки подлинности и предусматривает передачу не самого пароля пользователя, а косвенных сведений о нём                           |
| CIDR  | Classless Inter-Domain Routing              | Бесклассовая междоменная маршрутизация   |
| CIST  | Common and Internal Spanning Tree           | Общее и внутреннее связующее дерево  |
| CLI   | Command Line Interface                      | Интерфейс командной строки   |
| CoS   | Class of Service                            | Класс сервиса  |
| CRC   | Cyclic Redundancy Check                     | Циклический избыточный код. Алгоритм нахождения контрольной суммы, предназначенный для проверки целостности данных   |
| CST   | Common Spanning Tree                        | Общее связующее дерево   |
| CVLAN | Customer VLAN                               | Клиентская VLAN  |
| DAI   | Dynamic ARP Inspection                      | Функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP   |
| DHCP  | Dynamic Host Configuration Protocol         | Протокол динамической настройки узла   |
| DLF   | Destination Lookup Failure                  | Сбой поиска адреса назначения  |
| DNS   | Domain Name System                          | Система доменных имен  |
| DoS   | Denial of Service                           | Отказ в обслуживании (тип сетевой атаки)   |
| DR    | Designated Router                           | Назначенный маршрутизатор  |



|               |  |   |
|---------------|--|---|
| DSCP          | Differentiated Services Code Point           | Точка кода дифференцированных услуг. Использует 6-битное поле 8-битного IP-заголовка DS   |
| EAP           | Protected Extensible Authentication Protocol | Расширяемый протокол аутентификации   |
| EAPS          | Ethernet Automatic Protection Switching      | Протокол канального уровня для построения и защиты кольцевой топологии Ethernet   |
| ERPS          | Ethernet Ring Protection Switching           | Кольцевой протокол, использующийся для исключения образования петель в топологии  |
| FCS           | Frame Check Sequence                         | Часть кадра, содержащая контрольную сумму (CRC), используемую для проверки целостности данных внутри кадра  |
| FDB           | Forwarding Data Base                         | Таблица коммутации  |
| FTP           | File Transfer Protocol                       | Протокол передачи файлов  |
| GARP          | Generic Attribute Registration Protocol      | Протокол регистрации основных атрибутов   |
| GRE           | Generic Routing Encapsulation                | Протокол инкапсуляции сетевых пакетов, разработанный компанией Cisco Systems. Он позволяет инкапсулировать пакеты одного протокола сетевого уровня в пакеты другого протокола             |
| GVRP          | GARP (Generic) VLAN Registration Protocol    | Протокол GARP для регистрации VLAN  |
| HTTP          | Hyper Text Transfer Protocol                 | Протокол передачи гипертекста   |
| HTTPS         | Hypertext Transfer Protocol Secure           | Безопасный протокол передачи гипертекста  |
| ICMP          | Internet Control Message Protocol            | Протокол межсетевых управляющих сообщений   |
| IGMP          | Internet Group Management Protocol           | Протокол управления многоадресной передачей данных в сетях, основанных на протоколе IP. Используется только в сетях IPv4. Аналогичную роль в стеке протоколов IPv6 выполняет протокол MLD |
| IGMP Snooping | Internet Group Management Protocol Snooping  | Протокол отслеживания сетевого трафика IGMP   |
| IP            | Internet Protocol                            | Интернет-протокол   |
| IST           | Internal Spanning Tree                       | Внутреннее связующее дерево   |
| LACP          | Link Aggregation Control Protocol            | Протокол агрегирования каналов  |
| LAN           | Local Area Network                           | Локальная сеть  |
| LLDP          | Link Layer Discovery Protocol                | Протокол обнаружения канального уровня  |
| LLDPDU        | Link Layer Discovery Protocol Data Unit      | Блок данных протокола обнаружения канального уровня   |



|           |                                   |   |
|-----------|-----------------------------------|---|
| LSA       | Link State Advertisement          | Сообщение с описанием локального состояния маршрутизатора или сети  |
| MED       | Multi-Exit Discriminator          | Метка, которая используется для указания предпочтений по входящему трафику для маршрутов, которые объявляются из одной и той же автономной системы. Более низкое значение MED указывает на более предпочтительный маршрут |
| MIB       | Management Information Base       | Виртуальная база данных, используемая для управления объектами в сети связи   |
| MLD       | Multicast Listener Discovery      | Протокол стека IPv6, встроенный в ICMPv6. Используется для определения получателей мультивещательных запросов. Аналогичную роль в стеке протоколов IPv4 выполняет протокол IGMP   |
| MST       | Multiple Spanning Tree            | Множественное связующее дерево  |
| MSTI      | Multiple Spanning Tree Instance   | Экземпляр множественного связующего дерева  |
| MSTP      | Multiple Spanning Tree Protocol   | Протокол множественного связующего дерева   |
| MTU       | Maximum Transmission Unit         | Максимальный размер передаваемого кадра   |
| NBMA      | Non-Broadcast Multi-Access        | Сеть множественного доступа без широковещательных доменов, в которой подключено несколько хостов, но данные передаются только напрямую от одного компьютера к другому по виртуальному каналу или через коммутаторы        |
| NetBIOS   | Network Basic Input/Output System | Базовая сетевая система ввода-вывода  |
| NMS       | Network Management System         | Система сетевого управления   |
| NNI       | Network-Network Interface         | Межсетевой интерфейс  |
| NTP       | Network Time Protocol             | Протокол синхронизации сетевого времени   |
| OID       | Object Identifier                 | Идентификатор объекта   |
| OLNK IGMP | Only Link IGMP                    | Упрощенный способ управления многоадресным трафиком, относится к протоколу IGMP, работающему без взаимодействия между маршрутизаторами  |
| OSPF      | Open Shortest Path First          | Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и передающий информацию по наилучшему пути  |
| PCP       | Priority Code Point               | Поле в теге VLAN, которое указывает приоритет кадра. Используется для   |



|          |  |   |
|----------|--|---|
|          |  | определения уровня приоритета трафика и может принимать значения от 0 (низкий) до 7 (высокий)   |
| PDP      | Protocol Discovery Protocol                | Протокол, позволяющий находить все соседние устройства, связанные с определенным устройством в сети   |
| PPP      | Point-to-Point Protocol                    | Протокол «точка-точка», который используется для установления прямого соединения между двумя узлами   |
| PPPoE    | Point-to-Point Protocol over Ethernet      | Протокол «точка-точка» на основе Ethernet-соединения  |
| PVID     | Port VLAN Identifier                       | Идентификатор VLAN по умолчанию для порта   |
| QinQ     | 802.1Q in 802.1Q                           | Технология, позволяющая добавлять в маркированные кадры Ethernet второй тег IEEE 802.1Q   |
| QoS      | Quality of Service                         | Качество обслуживания (технология предоставления различным классам трафика различных приоритетов в обслуживании)  |
| RADIUS   | Remote Authentication Dial-In User Service | Служба удаленной аутентификации пользователей по коммутируемым линиям   |
| RIP      | Routing Information Protocol               | Протокол дистанционно-векторной маршрутизации   |
| RMON     | Remote Network Monitoring                  | Дистанционный мониторинг сети (расширение SNMP, разработанное IETF)   |
| RPL Port | Ring Protection Link Port                  | Порт, служащий для обеспечения связности и защиты кольца в ERPS. Он не передает обычный трафик, а используется только для обмена управляющими сообщениями между узлами кольца. RPL-порт обеспечивает резервный путь в кольце и активируется только в случае сбоя на основном пути |
| RSA      | Rivest, Shamir, Adleman                    | Криптографический алгоритм с открытым ключом  |
| RSTP     | Rapid Spanning Tree Protocol               | Быстрый протокол связующего дерева (версия протокола STP с ускоренной реконфигурацией дерева)   |
| SFP      | Small Form-factor Pluggable                | Промышленный стандарт модульных компактных приемопередатчиков (трансиверов), используемых для передачи и приема данных в телекоммуникациях  |



|         |  |  |
|---------|--|--|
| SMTP    | Simple Mail Transfer Protocol                    | Протокол для передачи электронной почты через Интернет   |
| SNAP    | Subnetwork Access Protocol                       | Поле заголовка LLC, указывающее протокол сетевого уровня, которому должен быть передан кадр  |
| SNMP    | Simple Network Management Protocol               | Простой протокол сетевого управления (интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP)                               |
| SPVLAN  | Service Provider's VLAN                          | VLAN поставщика услуг  |
| SSH     | Secure Shell                                     | «Безопасная оболочка», сетевой протокол прикладного уровня   |
| SSTP    | Single Spanning Tree Protocol (802.1D STP)       | Протокол единого связующего дерева   |
| STP     | Spanning Tree Protocol                           | Протокол связующего дерева   |
| TACACS+ | Terminal Access Controller Access Control System | Сеансовый протокол аутентификации, авторизации и учета доступа   |
| TCP     | Transmission Control Protocol                    | Протокол управления передачей  |
| TFTP    | Trivial File Transfer Protocol                   | Простой протокол передачи файлов   |
| TLS     | Transport Layer Security                         | Криптографический протокол защиты транспортного уровня на базе SSL, обеспечивающий безопасную передачу данных между узлами в сети                          |
| TLV     | Type Length Value                                | Структура данных, используемая в протоколе LLDP для передачи информации о сетевых устройствах  |
| ToS     | Type of Service                                  | Однооктетное поле в структуре IP-пакета, характеризует то, как должна обрабатываться дейтограмма   |
| TPID    | Tag Protocol Identifier                          | Идентификатор протокола тега – поле в теге VLAN, которое указывает тип протокола тега. Стандарт IEEE 802.1Q требует, чтобы значение этого поля было 0x8100 |
| TTL     | Time to Live                                     | Предельный период времени или число итераций (переходов), которые пакет данных может осуществить (прожить) до своего исчезновения                          |
| UDP     | User Datagram Protocol                           | Протокол пользовательских дейтаграмм   |
| UNI     | User Network Interface                           | Интерфейс подключения конечного пользователя   |
| VLAN    | Virtual Local Area Network                       | Виртуальная локальная сеть   |
| VLSM    | Variable Length Subnet Mask                      | Маска подсети с переменной длиной  |
| VPN     | Virtual Private Network                          | Виртуальная частная сеть   |
| VSA     | Vendor-Specific Attributes                       | Атрибуты, специфичные для поставщика   |



|     |                      |   |
|-----|----------------------|---|
| VTY | VirtualTeletype      | Виртуальный интерфейс, который обеспечивает удаленный доступ к устройству |
| WRR | Weighted Round Robin | Взвешенная очередь  |