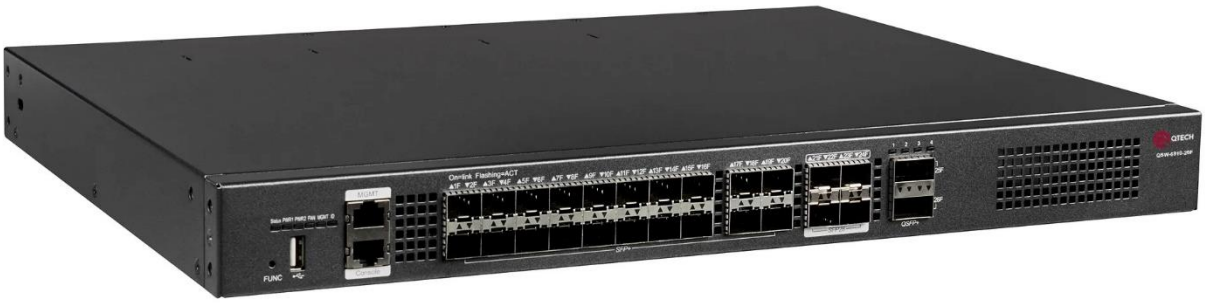

Руководство по настройке
Конфигурация Multicast
Ethernet-коммутаторы агрегации
серия QSW-6910

Оглавление

1. НАСТРОЙКА IP MULTICAST-МАРШРУТИЗАЦИИ 25
1.1. Обзор 25
1.2. Приложения 25
1.2.1. Приложения PIM-DM 25
1.2.1.1. Сценарий 25
1.2.1.2. Развертывание 26
1.2.2. Приложения PIM-SM 26
1.2.2.1. Сценарий 26
1.2.2.2. Развертывание 26
1.3. Функции 26
1.3.1. Базовые определения 26
1.3.2. Обзор 28
1.3.3. Настройка основных функций IP multicast-маршрутизации 29
1.3.3.1. Принцип работы 29
1.3.3.2. Сопутствующая конфигурация 29
1.3.4. Настройка порога TTL 29
1.3.4.1. Принцип работы 29
1.3.4.2. Сопутствующая конфигурация 29
1.3.5. Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации 30
1.3.5.1. Принцип работы 30
1.3.5.2. Сопутствующая конфигурация 30
1.3.6. Настройка границы IP multicast-маршрутизации 30
1.3.6.1. Принцип работы 30
1.3.6.2. Сопутствующая конфигурация 30
1.3.7. Настройка статического маршрута IP multicast-маршрутизации 30
1.3.7.1. Принцип работы 31
1.3.7.2. Сопутствующая конфигурация 31
1.3.8. Настройка управления направлением уровня 2 для multicast-потоков 31
1.3.8.1. Принцип работы 31
1.3.8.2. Сопутствующая конфигурация 31
1.3.9. Настройка выбора маршрута RPF на основе правила самого длинного совпадения 31
1.3.9.1. Принцип работы 31
1.3.9.2. Сопутствующая конфигурация 32
1.3.10. Настройка параметров непрерывной multicast-пересылки 32
1.3.10.1. Принцип работы 32

1.3.10.2. Сопутствующая конфигурация 32
1.3.11. Настройка механизма перезаписи при переполнении записей аппаратной multicast-пересылки 33
1.3.11.1. Принцип работы 33
1.3.11.2. Сопутствующая конфигурация 33
1.4. Конфигурация 33
1.4.1. Настройка основных функций IP multicast-маршрутизации 34
1.4.1.1. Эффект конфигурации 34
1.4.1.2. Примечания 34
1.4.1.3. Шаги настройки 34
1.4.1.4. Проверка 35
1.4.1.5. Связанные команды 35
1.4.1.6. Пример конфигурации 36
1.4.1.7. Распространенные ошибки 37
1.4.2. Настройка порога TTL 38
1.4.2.1. Эффект конфигурации 38
1.4.2.2. Примечания 38
1.4.2.3. Шаги настройки 38
1.4.2.4. Проверка 38
1.4.2.5. Связанные команды 38
1.4.2.6. Пример конфигурации 39
1.4.3. Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации 40
1.4.3.1. Эффект конфигурации 40
1.4.3.2. Примечания 40
1.4.3.3. Шаги настройки 40
1.4.3.4. Проверка 40
1.4.3.5. Связанные команды 41
1.4.3.6. Пример конфигурации 41
1.4.3.7. Распространенные ошибки 43
1.4.4. Настройка границы IP multicast-маршрутизации 43
1.4.4.1. Эффект конфигурации 43
1.4.4.2. Примечания 43
1.4.4.3. Шаги настройки 43
1.4.4.4. Проверка 43
1.4.4.5. Связанные команды 44
1.4.4.6. Пример конфигурации 44
1.4.4.7. Распространенные ошибки 45

1.4.5. Настройка статического маршрут IP multicast-маршрутизации 45
1.4.5.1. Эффект конфигурации 45
1.4.5.2. Примечания 45
1.4.5.3. Шаги настройки 45
1.4.5.4. Проверка 45
1.4.5.5. Связанные команды 46
1.4.5.6. Пример конфигурации 47
1.4.5.7. Распространенные ошибки 48
1.4.6. Настройка управления направлением уровня 2 для multicast-потоков 48
1.4.6.1. Эффект конфигурации 48
1.4.6.2. Примечания 48
1.4.6.3. Шаги настройки 48
1.4.6.4. Проверка 48
1.4.6.5. Связанные команды 48
1.4.6.6. Пример конфигурации 49
1.4.6.7. Распространенные ошибки 49
1.4.7. Настройка выбора маршрута RPF на основе правила самого длинного совпадения 49
1.4.7.1. Эффект конфигурации 49
1.4.7.2. Примечания 50
1.4.7.3. Шаги настройки 50
1.4.7.4. Проверка 50
1.4.7.5. Связанные команды 50
1.4.7.6. Пример конфигурации 51
1.4.7.7. Распространенные ошибки 52
1.4.8. Настройка параметров непрерывной multicast-пересылки 52
1.4.8.1. Эффект конфигурации 52
1.4.8.2. Примечания 52
1.4.8.3. Шаги настройки 52
1.4.8.4. Проверка 52
1.4.8.5. Связанные команды 52
1.4.8.6. Пример конфигурации 53
1.4.9. Настройка механизма перезаписи при переполнении записей аппаратной multicast-пересылки 54
1.4.9.1. Эффект конфигурации 54
1.4.9.2. Примечания 54
1.4.9.3. Шаги настройки 54
1.4.9.4. Проверка 54

1.4.9.5. Связанные команды 54
1.4.9.6. Пример конфигурации 54
1.5. Мониторинг 55
1.5.1. Очистка 55
1.5.2. Отображение 55
1.5.2.1. Отладка 56
2. НАСТРОЙКА MULTICAST IPV6 58
2.1. Обзор 58
2.1.1. Протоколы и стандарты 58
2.2. Приложения 58
2.2.1. Типичное применение PIM-SMv6 58
2.2.1.1. Сценарий 58
2.2.2. Развертывание 59
2.3. Функции 59
2.3.1. Базовые определения 59
2.3.2. Обзор 60
2.3.3. Настройка основных функций multicast IPv6 61
2.3.3.1. Принцип работы 61
2.3.3.2. Сопутствующая конфигурация 61
2.3.4. Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации IPv6 61
2.3.4.1. Принцип работы 62
2.3.4.2. Сопутствующая конфигурация 62
2.3.5. Настройка границы multicast IPv6 62
2.3.5.1. Принцип работы 62
2.3.5.2. Сопутствующая конфигурация 62
2.3.6. Настройка статической multicast-маршрутизации IPv6 62
2.3.6.1. Принцип работы 62
2.3.6.2. Сопутствующая конфигурация 62
2.3.7. Настройка управления направлением потока уровня 2 для multicast-потоков 63
2.3.7.1. Принцип работы 63
2.3.7.2. Сопутствующая конфигурация 63
2.3.8. Настройка выбора маршрута RPF по принципу самого длинного соответствия 63
2.3.8.1. Принцип работы 63
2.3.8.2. Сопутствующая конфигурация 64
2.4. Конфигурация 64

2.4.1. Настройка основных функций multicast IPv6 65
2.4.1.1. Эффект конфигурации 65
2.4.1.2. Примечания 65
2.4.1.3. Шаги настройки 65
2.4.1.4. Проверка 65
2.4.1.5. Сопутствующие команды 65
2.4.1.6. Пример конфигурации 66
2.4.1.7. Распространенные ошибки 68
2.4.2. Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации IPv6 68
2.4.2.1. Эффект конфигурации 68
2.4.2.2. Примечания 68
2.4.2.3. Шаги настройки 68
2.4.2.4. Проверка 68
2.4.2.5. Связанные команды 69
2.4.2.6. Пример конфигурации 69
2.4.2.7. Распространенные ошибки 71
2.4.3. Настройка границы multicast IPv6 71
2.4.3.1. Эффект конфигурации 71
2.4.3.2. Примечания 71
2.4.3.3. Шаги настройки 72
2.4.3.4. Проверка 72
2.4.3.5. Связанные команды 72
2.4.3.6. Пример конфигурации 72
2.4.3.7. Распространенные ошибки 73
2.4.4. Настройка статической multicast-маршрутизации IPv6 73
2.4.4.1. Эффект конфигурации 73
2.4.4.2. Примечания 73
2.4.4.3. Шаги настройки 73
2.4.4.4. Проверка 73
2.4.4.5. Связанные команды 74
2.4.4.6. Пример конфигурации 74
2.4.4.7. Распространенные ошибки 75
2.4.5. Настройка управления направлением потока уровня 2 для multicast-потоков 76
2.4.5.1. Эффект конфигурации 76
2.4.5.2. Примечания 76
2.4.5.3. Шаги настройки 76

2.4.5.4. Проверка 76
2.4.5.5. Связанные команды 76
2.4.5.6. Пример конфигурации 77
2.4.5.7. Распространенные ошибки 77
2.4.6. Настройка выбора маршрута RPF по принципу самого длинного соответствия 77
2.4.6.1. Эффект конфигурации 77
2.4.6.2. Примечания 77
2.4.6.3. Шаги настройки 78
2.4.6.4. Проверка 78
2.4.6.5. Связанные команды 78
2.4.6.6. Пример конфигурации 79
2.4.6.7. Распространенные ошибки 80
2.5. Мониторинг 80
2.5.1. Очистка 80
2.5.2. Отображение 80
2.5.3. Отладка 81
3. НАСТРОЙКА IGMP 83
3.1. Обзор 83
3.1.1. Протоколы и стандарты 83
3.2. Приложения 83
3.2.1. Локальный сервис IGMP 83
3.2.1.1. Сценарий 83
3.2.1.2. Развертывание 84
3.2.2. Прокси-сервис IGMP 84
3.2.2.1. Сценарий 84
3.2.2.2. Развертывание 84
3.3. Функции 85
3.3.1. Базовые определения 85
3.3.1.1. Обзор 85
3.3.2. IGMP-маршрутизатор 86
3.3.2.1. Принцип работы 86
3.3.2.2. Сопутствующая конфигурация 86
3.3.3. IGMP Querier 87
3.3.3.1. Принцип работы 87
3.3.3.2. Сопутствующая конфигурация 87
3.3.4. Групповая фильтрация IGMP 88
3.3.4.1. Принцип работы 88

3.3.4.2. Сопутствующая конфигурация 88
3.3.5. Статическая группа IGMP 88
3.3.5.1. Принцип работы 88
3.3.5.2. Сопутствующая конфигурация 88
3.3.6. Имитация хостов для присоединения к группам IGMP 88
3.3.6.1. Сопутствующая конфигурация 89
3.3.7. IGMP-прокси 89
3.3.7.1. Принцип работы 89
3.3.7.2. Сопутствующая конфигурация 89
3.3.8. Сопоставление IGMP SSM 89
3.3.8.1. Принцип работы 89
3.3.8.2. Сопутствующая конфигурация 90
3.3.9. Опция Router Alert (оповещения маршрутизатора) 90
3.3.9.1. Принцип работы 90
3.3.9.2. Сопутствующая конфигурация 90
3.4. Конфигурация 90
3.4.1. Настройка основных функций IGMP 92
3.4.1.1. Эффект конфигурации 92
3.4.1.2. Примечания 92
3.4.1.3. Шаги настройки 92
3.4.1.4. Проверка 92
3.4.1.5. Связанные команды 92
3.4.1.6. Пример конфигурации 93
3.4.1.7. Распространенные ошибки 93
3.4.2. Настройка маршрутизаторов IGMP 94
3.4.2.1. Эффект конфигурации 94
3.4.2.2. Примечания 94
3.4.2.3. Шаги настройки 94
3.4.2.4. Проверка 94
3.4.2.5. Связанные команды 94
3.4.2.6. Пример конфигурации 96
3.4.2.7. Распространенные ошибки 97
3.4.3. Настройка IGMP Querier 97
3.4.3.1. Эффект конфигурации 97
3.4.3.2. Примечания 97
3.4.3.3. Шаги настройки 97
3.4.3.4. Проверка 97
3.4.3.5. Связанные команды 98

3.4.3.6. Пример конфигурации 98
3.4.3.7. Распространенные ошибки 99
3.4.4. Настройка фильтрации группы IGMP 99
3.4.4.1. Эффект конфигурации 99
3.4.4.2. Примечания 99
3.4.4.3. Шаги настройки 99
3.4.4.4. Проверка 99
3.4.4.5. Связанные команды 99
3.4.4.6. Пример конфигурации 101
3.4.4.7. Распространенные ошибки 102
3.4.5. Настройка IGMP-прокси 102
3.4.5.1. Эффект конфигурации 102
3.4.5.2. Примечания 102
3.4.5.3. Шаги настройки 102
3.4.5.4. Проверка 102
3.4.5.5. Связанные команды 103
3.4.5.6. Пример конфигурации 103
3.4.5.7. Распространенные ошибки 104
3.4.6. Настройка сопоставления IGMP SSM 104
3.4.6.1. Эффект конфигурации 104
3.4.6.2. Примечания 104
3.4.6.3. Шаги настройки 104
3.4.6.4. Проверка 105
3.4.6.5. Связанные команды 105
3.4.6.6. Пример конфигурации 106
3.4.6.7. Распространенные ошибки 106
3.4.7. Настройка опции оповещения 106
3.4.7.1. Эффект конфигурации 106
3.4.7.2. Примечания 106
3.4.7.3. Шаги настройки 106
3.4.7.4. Проверка 106
3.4.7.5. Связанные команды 107
3.4.7.6. Пример конфигурации 107
3.4.7.7. Распространенные ошибки 108
3.5. Мониторинг 108
3.5.1. Очистка 108
3.5.2. Отображение 108
3.5.3. Отладка 109

4. НАСТРОЙКА MLD 110
4.1. Обзор 110
4.1.1. Протоколы и стандарты 110
4.2. Приложения 110
4.2.1. Настройка сервиса MLD в локальной сети 110
4.2.1.1. Сценарий 110
4.2.1.2. Развертывание 111
4.2.2. Настройка прокси-сервиса MLD 111
4.2.2.1. Сценарий 111
4.2.2.2. Развертывание 111
4.3. Функции 112
4.3.1. Базовые определения 112
4.3.1.1. Обзор 112
4.3.2. Настройка параметров маршрутизатора MLD 113
4.3.2.1. Принцип работы 113
4.3.2.2. Сопутствующая конфигурация 113
4.3.3. Процесс выбора Querier или механизм тайм-аута 114
4.3.3.1. Принцип работы 114
4.3.3.2. Сопутствующая конфигурация 114
4.3.4. Фильтрация групп MLD 114
4.3.4.1. Принцип работы 114
4.3.4.2. Сопутствующая конфигурация 115
4.3.5. Поддержка статических групп MLD 115
4.3.5.1. Принцип работы 115
4.3.5.2. Сопутствующая конфигурация 115
4.3.6. Настройка информации об имитируемой группе хостов 115
4.3.6.1. Сопутствующая конфигурация 115
4.3.7. Поддержка MLD-прокси 115
4.3.7.2. Сопутствующая конфигурация 116
4.3.8. Поддержка SSM-MAP 116
4.3.8.1. Принцип работы 116
4.3.8.2. Сопутствующая конфигурация 116
4.4. Конфигурация 117
4.4.1. Настройка основных функций MLD 118
4.4.1.1. Эффект конфигурации 118
4.4.1.2. Примечания 118
4.4.1.3. Шаги настройки 118
4.4.1.4. Проверка 118

4.4.1.5. Связанные команды 118
4.4.1.6. Пример конфигурации 119
4.4.1.7. Распространенные ошибки 119
4.4.2. Настройка параметров маршрутизатора MLD 120
4.4.2.1. Эффект конфигурации 120
4.4.2.2. Примечания 120
4.4.2.3. Шаги настройки 120
4.4.2.4. Проверка 120
4.4.2.5. Связанные команды 120
4.4.2.6. Пример конфигурации 122
4.4.2.7. Распространенные ошибки 123
4.4.3. Процесс выбора Querier или механизм тайм-аута 123
4.4.3.1. Эффект конфигурации 123
4.4.3.2. Примечания 123
4.4.3.3. Шаги настройки 123
4.4.3.4. Проверка 123
4.4.3.5. Связанные команды 124
4.4.3.6. Пример конфигурации 124
4.4.3.7. Распространенные ошибки 125
4.4.4. Фильтрация групп MLD 125
4.4.4.1. Эффект конфигурации 125
4.4.4.2. Примечания 125
4.4.4.3. Шаги настройки 125
4.4.4.4. Проверка 125
4.4.4.5. Связанные команды 125
4.4.4.6. Пример конфигурации 127
4.4.4.7. Распространенные ошибки 128
4.4.5. MLD-прокси 128
4.4.5.1. Эффект конфигурации 128
4.4.5.2. Примечания 128
4.4.5.3. Шаги настройки 128
4.4.5.4. Проверка 128
4.4.5.5. Связанные команды 129
4.4.5.6. Пример конфигурации 130
4.4.5.7. Распространенные ошибки 130
4.4.6. Поддержка SSM-MAP 130
4.4.6.1. Эффект конфигурации 130
4.4.6.2. Примечания 130

4.4.6.3. Шаги настройки 131
4.4.6.4. Проверка 131
4.4.6.5. Связанные команды 131
4.4.6.6. Пример конфигурации 132
4.4.6.7. Распространенные ошибки 132
4.5. Мониторинг 132
4.5.1. Очистка 132
4.5.2. Отображение 132
4.5.2.1. Отладка 133
5. НАСТРОЙКА PIM-DM 134
5.1. Обзор 134
5.1.1. Протоколы и стандарты 134
5.2. Приложения 134
5.2.1. Предоставление услуги multicast в одной сети 134
5.2.1.1. Сценарий 134
5.2.1.2. Развертывание 135
5.2.2. Применение PIM-DM в среде горячего резервирования 135
5.2.2.1. Сценарий 135
5.2.2.2. Развертывание 136
5.3. Функции 136
5.3.1. Базовые определения 136
5.3.1.1. Обзор 137
5.3.2. Сосед PIM-DM 137
5.3.2.1. Принцип работы 137
5.3.2.2. Сопутствующая конфигурация 138
5.3.3. PIM-DM MDT 138
5.3.3.1. Принцип работы 138
5.3.3.2. Сопутствующая конфигурация 139
5.3.4. PIM-DM SRM 139
5.3.4.1. Принцип работы 139
5.3.4.2. Сопутствующая конфигурация 139
5.3.5. MIB 140
5.3.5.1. Принцип работы 140
5.3.5.2. Сопутствующая конфигурация 140
5.4. Конфигурация 140
5.4.1. Настройка основных функций PIM-DM 141
5.4.1.1. Эффект конфигурации 141

5.4.1.2. Примечания 141
5.4.1.3. Шаги настройки 141
5.4.1.4. Проверка 141
5.4.1.5. Связанные команды 141
5.4.1.6. Пример конфигурации 142
5.4.1.7. Распространенные ошибки 144
5.4.2. Настройка соседей PIM-DM 144
5.4.2.1. Эффект конфигурации 144
5.4.2.2. Примечания 144
5.4.2.3. Шаги настройки 144
5.4.2.4. Проверка 144
5.4.2.5. Связанные команды 145
5.4.2.6. Пример конфигурации 146
5.4.2.7. Распространенные ошибки 148
5.4.3. Настройка SRM PIM-DM 148
5.4.3.1. Эффект конфигурации 148
5.4.3.2. Примечания 148
5.4.3.3. Шаги настройки 148
5.4.3.4. Проверка 149
5.4.3.5. Связанные команды 149
5.4.3.6. Пример конфигурации 149
5.4.3.7. Распространенные ошибки 151
5.4.4. Настройка MIB PIM-DM 152
5.4.4.1. Эффект конфигурации 152
5.4.4.2. Проверка 152
5.4.4.3. Связанные команды 152
5.5. Мониторинг 152
5.5.1. Очистка 152
5.5.2. Отображение 152
6. НАСТРОЙКА PIM-SM 154
6.1. Обзор 154
6.1.1. Протоколы и стандарты 154
6.2. Приложения 154
6.2.1. Включение ASM для PIM-SM 154
6.2.1.1. Сценарий 154
6.2.1.2. Развертывание 155
6.2.2. Включение SSM для PIM-SM 155

6.2.2.1. Сценарий 155
6.2.2.2. Развертывание 156
6.2.3. Применение PIM-SM в среде горячего резервного копирования 156
6.2.3.1. Сценарий 156
6.2.3.2. Развертывание 156
6.3. Функции 157
6.3.1. Базовые определения 157
6.3.2. Обзор 158
6.3.3. Сосед PIM-SM 159
6.3.3.1. Принцип работы 159
6.3.3.2. Сопутствующая конфигурация 160
6.3.4. Выбор DR 160
6.3.4.1. Принцип работы 160
6.3.4.2. Сопутствующая конфигурация 161
6.3.5. Механизм BSR 161
6.3.5.1. Принцип работы 161
6.3.5.2. Сопутствующая конфигурация 161
6.3.6. Механизм RP 162
6.3.6.1. Принцип работы 162
6.3.6.2. Сопутствующая конфигурация 162
6.3.7. Регистрация информации об источнике multicast 163
6.3.7.1. Принцип работы 163
6.3.7.2. Сопутствующая конфигурация 163
6.3.8. Создание RPT 165
6.3.8.1. Принцип работы 165
6.3.8.2. Сопутствующая конфигурация 166
6.3.9. Создание SPT 166
6.3.9.1. Принцип работы 166
6.3.9.2. Сопутствующая конфигурация 166
6.3.10. ASM и SSM 166
6.3.10.1. Принцип работы 167
6.3.10.2. Сопутствующая конфигурация 168
6.4. Конфигурация 168
6.4.1. Настройка основных функций PIM-SM 170
6.4.1.1. Эффект конфигурации 170
6.4.1.2. Примечания 170
6.4.1.3. Шаги настройки 171
6.4.1.4. Проверка 171

6.4.1.5. Связанные команды 171
6.4.1.6. Пример конфигурации 174
6.4.1.7. Распространенные ошибки 182
6.4.2. Настройка соседей PIM-SM 182
6.4.2.1. Эффект конфигурации 182
6.4.2.2. Примечания 183
6.4.2.3. Шаги настройки 183
6.4.2.4. Проверка 183
6.4.2.5. Связанные команды 183
6.4.2.6. Пример конфигурации 186
6.4.2.7. Распространенные ошибки 187
6.4.3. Настройка параметров BSR 187
6.4.3.1. Эффект конфигурации 187
6.4.3.2. Примечания 187
6.4.3.3. Шаги настройки 187
6.4.3.4. Проверка 188
6.4.3.5. Связанные команды 188
6.4.3.6. Пример конфигурации 189
6.4.3.7. Распространенные ошибки 192
6.4.4. Настройка параметров RP и DR 192
6.4.4.1. Эффект конфигурации 192
6.4.4.2. Примечания 193
6.4.4.3. Шаги настройки 193
6.4.4.4. Проверка 194
6.4.4.5. Связанные команды 195
6.4.4.6. Пример конфигурации 199
6.4.4.7. Распространенные ошибки 210
6.4.5. Настройка интервала отправки пакета Join/Prune 210
6.4.5.1. Эффект конфигурации 210
6.4.5.2. Примечания 211
6.4.5.3. Шаги настройки 211
6.4.5.4. Проверка 211
6.4.5.5. Связанные команды 211
6.4.5.6. Пример конфигурации 211
6.4.5.7. Распространенные ошибки 213
6.4.6. Настройка маршрутизатора последнего hop-а для переключения с RPT на SPT 213
6.4.6.1. Эффект конфигурации 213

6.4.6.2. Примечания 213
6.4.6.3. Шаги настройки 213
6.4.6.4. Проверка 213
6.4.6.5. Связанные команды 214
6.4.6.6. Пример конфигурации 214
6.5. Мониторинг 215
6.5.1. Очистка 215
6.5.2. Отображение 215
7. НАСТРОЙКА PIM-SMV6 217
7.1. Обзор 217
7.1.1. Протоколы и стандарты 217
7.2. Приложения 217
7.2.1. Реализация ASM с использованием PIM-SMv6 217
7.2.1.1. Сценарий 217
7.2.1.2. Развертывание 218
7.2.2. Реализация SSM с использованием PIM-SMv6 218
7.2.2.1. Сценарий 218
7.2.2.2. Развертывание 219
7.2.3. Пример применения встроенного RP 219
7.2.3.1. Сценарий 219
7.2.3.2. Развертывание 219
7.2.4. Приложение PIM-SMv6 в среде горячего резервного копирования 220
7.2.4.1. Сценарий 220
7.2.4.2. Развертывание 220
7.3. Функции 221
7.3.1. Базовые определения 221
7.3.2. Обзор 222
7.3.3. Установление соседских отношений PIM 223
7.3.3.1. Принцип работы 223
7.3.3.2. Сопутствующая конфигурация 224
7.3.4. Выбор DR 224
7.3.4.1. Принцип работы 225
7.3.4.2. Сопутствующая конфигурация 225
7.3.5. Механизм BSR 225
7.3.5.1. Принцип работы 225
7.3.5.2. Сопутствующая конфигурация 226
7.3.6. Механизм RP 226

7.3.6.1. Принцип работы 227
7.3.6.2. Сопутствующая конфигурация 227
7.3.7. Регистрационная информация об источнике multicast 228
7.3.7.1. Принцип работы 228
7.3.7.2. Сопутствующая конфигурация 228
7.3.8. Создание RPT 230
7.3.8.1. Принцип работы 230
7.3.8.2. Сопутствующая конфигурация 231
7.3.9. Создание SPT 231
7.3.9.1. Принцип работы 231
7.3.9.2. Сопутствующая конфигурация 231
7.3.10. Модели ASM и SSM 231
7.4. Конфигурация 233
7.4.1. Настройка основных функций PIM-SMv6 233
7.4.1.1. Эффект конфигурации 233
7.4.1.2. Примечания 233
7.4.1.3. Шаги настройки 233
7.4.1.4. Проверка 234
7.4.1.5. Связанные команды 234
7.4.1.6. Пример конфигурации 238
7.4.1.7. Распространенные ошибки 243
7.4.2. Настройка параметров соседа PIM 243
7.4.2.1. Эффект конфигурации 243
7.4.2.2. Примечания 243
7.4.2.3. Шаги настройки 243
7.4.2.4. Проверка 243
7.4.2.5. Связанные команды 244
7.4.2.6. Пример конфигурации 246
7.4.2.7. Распространенные ошибки 248
7.4.3. Настройка параметров BSR 248
7.4.3.1. Эффект конфигурации 248
7.4.3.2. Примечания 248
7.4.3.3. Шаги настройки 248
7.4.3.4. Проверка 248
7.4.3.5. Связанные команды 249
7.4.3.6. Пример конфигурации 250
7.4.3.7. Распространенные ошибки 254
7.4.4. Настройка параметров RP и DR 254

7.4.4.1. Эффект конфигурации 254
7.4.4.2. Примечания 254
7.4.4.3. Шаги настройки 254
7.4.4.4. Проверка 255
7.4.4.5. Связанные команды 256
7.4.4.6. Пример конфигурации 260
7.4.4.7. Распространенные ошибки 269
7.4.5. Настройка интервала передачи пакетов Join/Prune 270
7.4.5.1. Эффект конфигурации 270
7.4.5.2. Примечания 270
7.4.5.3. Шаги настройки 270
7.4.5.4. Проверка 270
7.4.5.5. Связанные команды 270
7.4.5.6. Пример конфигурации 270
7.4.5.7. Распространенные ошибки 272
7.4.6. Настройка устройства Last-Hop для переключения с RPT на SPT 272
7.4.6.1. Эффект конфигурации 272
7.4.6.2. Примечания 272
7.4.6.3. Шаги настройки 272
7.4.6.4. Проверка 272
7.4.6.5. Связанные команды 272
7.4.6.6. Пример конфигурации 273
7.5. Мониторинг 273
7.5.1. Очистка 273
7.5.2. Отображение 274
8. НАСТРОЙКА MSDP 275
8.1. Обзор 275
8.1.1. Протоколы и стандарты 275
8.2. Приложения 275
8.2.1. Междоменный multicast 275
8.2.1.1. Сценарий 275
8.2.1.2. Развертывание 276
8.2.2. Anycast-RP 276
8.2.2.1. Сценарий 276
8.2.2.2. Развертывание 277
8.3. Функции 277
8.3.1. Установление peer-отношений MSDP 277

8.3.1.1. Принцип работы 277
8.3.2. Получение и пересылка сообщений SA 278
8.3.2.1. Принцип работы 278
8.4. Конфигурация 280
8.4.1. Настройка междоменного multicast 282
8.4.1.1. Эффект конфигурации 282
8.4.1.2. Примечания 282
8.4.1.3. Шаги настройки 282
8.4.1.4. Проверка 283
8.4.1.5. Пример конфигурации 285
8.4.1.6. Распространенные ошибки 289
8.4.2. Настройка Anycast-RP 289
8.4.2.1. Эффект конфигурации 289
8.4.2.2. Примечания 289
8.4.2.3. Шаги настройки 289
8.4.2.4. Проверка 290
8.4.2.5. Пример конфигурации 291
8.4.2.6. Распространенные ошибки 295
8.4.3. Настройка Green Channel проверки Peer-RPF 295
8.4.3.1. Эффект конфигурации 295
8.4.3.2. Примечания 295
8.4.3.3. Шаги настройки 295
8.4.3.4. Проверка 296
8.4.3.5. Пример конфигурации 297
8.4.4. Включение мер безопасности 299
8.4.4.1. Эффект конфигурации 299
8.4.4.2. Примечания 299
8.4.4.3. Шаги настройки 299
8.4.4.4. Проверка 300
8.4.4.5. Пример конфигурации 301
8.4.5. Ограничение broadcast-а сообщений SA 302
8.4.5.1. Эффект конфигурации 302
8.4.5.2. Примечания 302
8.4.5.3. Шаги настройки 302
8.4.5.4. Проверка 305
8.4.5.5. Пример конфигурации 306
8.4.6. Управление peer-ами MSDP 308
8.4.6.1. Эффект конфигурации 308

8.4.6.2. Примечания 308
8.4.6.3. Шаги настройки 308
8.4.6.4. Проверка 309
8.4.6.5. Пример конфигурации 310
8.4.7. Изменение параметров протокола 311
8.4.7.1. Эффект конфигурации 311
8.4.7.2. Примечания 311
8.4.7.3. Шаги настройки 311
8.4.7.4. Проверка 313
8.4.7.5. Пример конфигурации 314
8.5. Мониторинг 314
8.5.1. Очистка 314
8.5.2. Отображение 315
8.5.2.1. Отладка 315
9. НАСТРОЙКА IGMP SNOOPING 316
9.1. Обзор 316
9.1.1. Протоколы и стандарты 316
9.2. Приложения 316
9.2.1. Управление multicast-ом уровня 2 317
9.2.1.1. Сценарий 317
9.2.1.2. Развертывание 317
9.2.2. Общие сервисы multicast (multicast-VLAN) 318
9.2.2.1. Сценарий 318
9.2.2.2. Развертывание 318
9.2.3. Премиум-каналы и предварительный просмотр 318
9.2.3.1. Сценарий 318
9.2.3.2. Развертывание 318
9.3. Функции 319
9.3.1. Базовые определения 319
9.3.2. Обзор 320
9.3.3. Прослушивание пакетов IGMP 320
9.3.3.1. Принцип работы 320
9.3.3.2. Сопутствующая конфигурация 322
9.3.4. Режимы работы IGMP Snooping 323
9.3.4.1. Принцип работы 323
9.3.4.2. Сопутствующая конфигурация 324
9.3.5. Управление безопасностью IGMP 324

9.3.5.1. Принцип работы 324
9.3.5.2. Сопутствующая конфигурация 326
9.3.6. IGMP-профиль 327
9.3.6.1. Принцип работы 327
9.3.6.2. Сопутствующая конфигурация 327
9.3.7. IGMP QinQ 327
9.3.7.1. Принцип работы 327
9.3.7.2. Сопутствующая конфигурация 328
9.3.8. IGMP Querier 328
9.3.8.1. Принцип работы 328
9.3.8.2. Сопутствующая конфигурация 329
9.4. Конфигурация 330
9.4.1. Настройка основных функций IGMP snooping (режим IVGL) 335
9.4.1.1. Эффект конфигурации 335
9.4.1.2. Примечания 335
9.4.1.3. Шаги настройки 335
9.4.1.4. Проверка 335
9.4.1.5. Связанные команды 336
9.4.1.6. Пример конфигурации 337
9.4.1.7. Распространенные ошибки 339
9.4.2. Настройка основных функций IGMP snooping (режим SVGL) 339
9.4.2.1. Эффект конфигурации 339
9.4.2.2. Шаги настройки 339
9.4.2.3. Проверка 339
9.4.2.4. Связанные команды 339
9.4.2.5. Пример конфигурации 341
9.4.2.6. Распространенные ошибки 343
9.4.3. Настройка основных функций IGMP snooping (режим IVGL-SVGL) 343
9.4.3.1. Эффект конфигурации 343
9.4.3.2. Шаги настройки 343
9.4.3.3. Проверка 344
9.4.3.4. Связанные команды 344
9.4.3.5. Пример конфигурации 346
9.4.3.6. Распространенные ошибки 348
9.4.4. Настройка обработки пакетов 348
9.4.4.1. Эффект конфигурации 348
9.4.4.2. Примечания 348
9.4.4.3. Шаги настройки 349

9.4.4.4. Проверка 349
9.4.4.5. Связанные команды 350
9.4.4.6. Пример конфигурации 355
9.4.4.7. Распространенные ошибки 358
9.4.5. Настройка управления безопасностью IGMP 358
9.4.5.1. Эффект конфигурации 358
9.4.5.2. Примечания 358
9.4.5.3. Шаги настройки 358
9.4.5.4. Проверка 359
9.4.5.5. Связанные команды 359
9.4.5.6. Пример конфигурации 364
9.4.5.7. Распространенные ошибки 370
9.4.6. Настройка профиля IGMP 370
9.4.6.1. Эффект конфигурации 370
9.4.6.2. Шаги настройки 370
9.4.6.3. Проверка 370
9.4.6.4. Связанные команды 371
9.4.6.5. Пример конфигурации 372
9.4.6.6. Распространенные ошибки 372
9.4.7. Настройка IGMP QinQ 372
9.4.7.1. Эффект конфигурации 372
9.4.7.2. Примечания 372
9.4.7.3. Шаги настройки 372
9.4.7.4. Проверка 372
9.4.7.5. Связанные команды 373
9.4.7.6. Пример конфигурации 373
9.4.7.7. Распространенные ошибки 373
9.4.8. Настройка IGMP Querier 373
9.4.8.1. Эффект конфигурации 373
9.4.8.2. Примечания 374
9.4.8.3. Шаги настройки 374
9.4.8.4. Проверка 374
9.4.8.5. Связанные команды 374
9.4.8.6. Пример конфигурации 377
9.4.8.7. Распространенные ошибки 378
9.5. Мониторинг 379
9.5.1. Очистка 379
9.5.2. Отображение 379

9.5.3. Отладка 379
10. НАСТРОЙКА MLD SNOOPING 381
10.1. Обзор 381
10.1.1. Протоколы и стандарты 381
10.1.2. Два типа портов MLD Snooping 381
10.1.3. Режим работы MLD Snooping 381
10.1.4. Принцип работы MLD Snooping 382
10.1.5. Проверка порта источника 383
10.2. Приложения 384
10.2.1. MLD Snooping SVGL Trans-VLAN Multicast по требованию 384
10.2.1.1. Сценарий 384
10.2.1.2. Развертывание 384
10.2.2. Фильтрация порта источника 384
10.2.2.1. Сценарий 384
10.2.2.2. Развертывание 385
10.3. Функции 385
10.3.1. Базовые определения 385
10.3.2. Обзор 386
10.3.3. Глобальное включение MLD Snooping 387
10.3.3.1. Принцип работы 387
10.3.3.2. Сопутствующая конфигурация 387
10.3.4. MLD Snooping на основе VLAN 387
10.3.4.1. Сопутствующая конфигурация 387
10.3.5. Время устаревания портов multicast-маршрутизатора 387
10.3.5.1. Сопутствующая конфигурация 387
10.3.6. Изучение динамического порта multicast-маршрутизатора 387
10.3.6.1. Принцип работы 387
10.3.6.2. Сопутствующая конфигурация 387
10.3.7. Время устаревания динамических портов-участников 388
10.3.8. Fast Leave портов-участников группы multicast 388
10.3.9. Подавление пакетов Report MLD 388
10.3.10. Проверка порта источника 388
10.3.10.1. Принцип работы 388
10.3.10.2. Сопутствующая конфигурация 388
10.3.11. Фильтрация групп multicast на основе портов 388
10.3.12. Максимальное количество групп multicast, поддерживаемых портом 388
10.4. Конфигурация 388

10.4.1. Настройка основных функций MLD Snooping 389
10.4.1.1. Эффект конфигурации 389
10.4.1.2. Примечания 389
10.4.1.3. Шаги настройки 389
10.4.1.4. Проверка 389
10.4.1.5. Связанные команды 390
10.5. Мониторинг 396
10.5.1. Очистка 396
10.5.2. Отображение 396
11. ОБЩАЯ ИНФОРМАЦИЯ 397
11.1. Гарантия и сервис 397
11.2. Техническая поддержка 397
11.3. Электронная версия документа 397

1. НАСТРОЙКА IP MULTICAST-МАРШРУТИЗАЦИИ

1.1. Обзор

IP multicast-маршрутизация — это абстрактный аппаратный multicast и расширенный протокол multicast-маршрутизации на стандартном уровне IP-сети.

При традиционной IP-передаче только один хост может отправлять пакеты одному хосту (unicast) или всем хостам (broadcast). Однако технология multicast предоставляет третий вариант: хост может отправлять пакеты определенным указанным хостам.

IP multicast-маршрутизация применима к мультимедийным приложениям one-to-many (один ко многим).

1.2. Приложения

Приложение	Описание
Приложения PIM-DM	Сервис multicast PIM-DM предоставляется в той же сети
Приложения PIM-SM	Сервис multicast PIM-SM предоставляется в той же сети

1.2.1. Приложения PIM-DM

1.2.1.1. Сценарий

Multicast-сервис PIM-DM предоставляется в той же сети.

Как показано на Рисунке 1-1:

- Источник multicast отправляет multicast-пакет, а приемник A и приемник B в одной сети получают multicast-пакет.

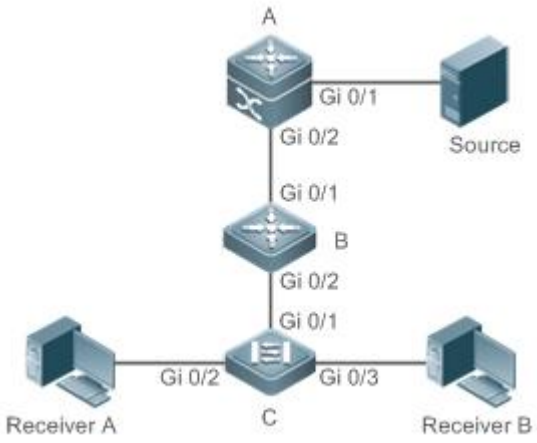

Рисунок 1-1.

A и B — устройства уровня 3, а C — устройство доступа уровня 2.

Источник подключен к интерфейсу Gi 0/1 устройства A, а приемник A и приемник B подключены к интерфейсам Gi 0/2 и Gi 0/3 устройства C.

1.2.1.2. Развертывание

- Запустите протокол Open Shortest Path First (OSPF) в той же сети, чтобы реализовать unicast-маршрутизацию.
- Запустите PIM-DM в той же сети, чтобы реализовать multicast-маршрутизацию.
- Запустите Internet Group Membership Protocol (IGMP) в сегменте сети хоста пользователя, чтобы реализовать управление участниками группы.

1.2.2. Приложения PIM-SM

1.2.2.1. Сценарий

Сервис multicast PIM-SM предоставляется в той же сети.

Как показано на Рисунке 1-2:

- Источник multicast отправляет multicast-пакет, а приемник A и приемник B в одной сети получают multicast-пакет.

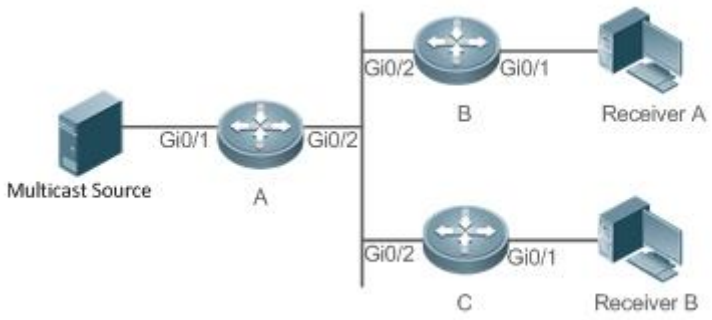

Рисунок 1-2.

A, B и C — маршрутизаторы уровня 3.

Источник multicast подключен к интерфейсу Gi 0/1 устройства A, приемник B подключен к интерфейсу Gi 0/1 устройства B, а приемник B подключен к интерфейсу Gi 0/1 устройства C.

1.2.2.2. Развертывание

- Запустите OSPF в той же сети, чтобы реализовать unicast-маршрутизацию.
- Запустите PIM-SM в той же сети, чтобы реализовать multicast-маршрутизацию.
- Запустите IGMP в сегменте сети хоста пользователя, чтобы реализовать управление участниками группы.

1.3. Функции

1.3.1. Базовые определения

PIM-маршрутизаторы и PIM-интерфейсы

Маршрутизаторы с поддержкой PIM называются PIM-маршрутизаторами. Интерфейсы, поддерживающие протокол PIM, называются PIM-интерфейсами.

Multicast-пакеты пересылаются на PIM-маршрутизаторы. PIM-интерфейсы для приема multicast-пакетов называются upstream-интерфейсами, а PIM-интерфейсы для отправки multicast-пакетов называются downstream-интерфейсами.

Сегменты сети, в которых расположены upstream-интерфейсы, называются upstream сетевыми сегментами. Сегменты сети, в которых расположены downstream-интерфейсы, называются downstream сетевыми сегментами.

Сеть PIM и домен PIM

PIM-маршрутизаторы подключаются через PIM-интерфейсы и образуют сеть PIM.

На некоторых интерфейсах PIM границы настроены таким образом, чтобы разделить большую сеть PIM на несколько доменов PIM. Границы могут отклонять определенные multicast-пакеты или ограничивать передачу сообщений PIM.

Multicast Distribution Tree, DR и RP

Multicast-пакеты передаются из одной точки в несколько точек. Путь пересылки имеет древовидную структуру. Этот путь пересылки называется Multicast Distribution Tree (MDT) и имеет следующие типы:

- Rendezvous Point Tree (RPT): RP рассматривается как «корень» (root), а назначенный маршрутизатор (DR), который объединяет участников группы, рассматривается как «лист».
- Shortest Path Tree (SPT). DR, соединяющий источники multicast, рассматривается как «корень» (root), а RP или DR, которые объединяют участников группы, рассматриваются как «листы».

DR и RP являются функциональными ролями для маршрутизатора PIM.

- RP собирает источники multicast и информацию об участниках группы в сети.
- DR, который соединяет источники multicast, сообщает информацию об источнике multicast RP. DR, который соединяет участников группы, передает информацию об участниках группы на RP.

(*,G) и (S,G)

- (*,G): пакеты, отправленные из любого источника в группу G, записи маршрутизации, соответствующие пакетам, и путь пересылки (RPT), соответствующий пакетам.
- (S,G): пакеты, отправленные из источника S в группу G, записи маршрутизации, соответствующие пакетам, и путь пересылки (SPT), соответствующий пакетам.

ASM и SSM

PIM-SM поддерживает следующие модели multicast, применимые к различным сегментам адресов multicast:

- Any-Source Multicast (ASM). В модели ASM пользовательские хосты не могут выбирать источники multicast. Хосты пользователей присоединяются к группе и получают пакеты, отправленные из всех источников в группу.
- Source-Specific Multicast (SSM). В модели SSM хосты пользователей могут выбирать источники multicast. Хосты пользователей указывают адреса источников при присоединении к группе и получают только пакеты, отправленные в группу из указанных источников.

ПРИМЕЧАНИЕ: требования к модели SSM: хосты пользователей должны заранее знать адрес источника multicast, используя другие сетевые сервисы, чтобы хосты могли выбирать источники multicast.

1.3.2. Обзор

Особенность	Описание
Настройка основных функций IP multicast-маршрутизации	Создает сеть PIM и обеспечивает источники данных и пользовательские терминалы в сети сервисом multicast IPv4
Настройка порога TTL	Настраивает порог TTL для интерфейса, то есть минимальное значение TTL для multicast-пакетов, разрешенных для интерфейса
Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации	Ограничивает количество записей, которые можно добавить в таблицу multicast-маршрутизации
Настройка границы IP multicast-маршрутизации	Настраивает интерфейс как границу multicast для указанной группы
Настройка статического маршрута IP multicast-маршрутизации	Позволяет пути multicast-пересылки отличаться от пути unicast-пересылки
Настройка управления направлением уровня 2 для multicast-потоков	Позволяет настроить указанный multicast-поток с помощью нескольких команд, то есть настроить несколько портов, которые могут пересылать поток. После настройки управления направлением для multicast-потока поток можно будет пересылать только через эти настроенные интерфейсы. Другим интерфейсам не разрешено пересылать поток
Настройка выбора маршрута RPF на основе правила самого длинного совпадения	Выбирает оптимальный маршрут соответственно из таблицы статической multicast-маршрутизации, таблицы маршрутизации MBGP и таблицы unicast-маршрутизации в соответствии с правилами RPF. Среди этих трех маршрутов в качестве маршрута RPF выбирается маршрут с самой длинной маской соответствия
Настройка параметров непрерывной multicast-пересылки	Во время обычной работы SSP синхронизирует аппаратную таблицу multicast-пересылки с платой управления в реальном времени. После включения платы управления, загружается команда для настройки multicast control plane на slave management board, и протокол multicast (например, PIM-SM или IGMP Snooping) повторно сходится (повторная конвергенция). Функция непрерывной multicast-пересылки обеспечивает непрерывную пересылку потоков multicast-данных во время повторной конвергенции протокола multicast

Особенность	Описание
Настройка механизма перезаписи при переполнении записей аппаратной multicast-пересылки	Удаляет самые ранние аппаратные записи и добавляет новые записи, если аппаратная таблица пересылки переполняется при создании записи multicast-пересылки

1.3.3. Настройка основных функций IP multicast-маршрутизации

Создайте сеть PIM и обеспечьте источники данных и пользовательские терминалы в сети сервисом multicast IPv4.

1.3.3.1. Принцип работы

Устройство поддерживает таблицу маршрутизации для пересылки multicast-пакетов через протоколы multicast-маршрутизации (такие как PIM-DM или PIM-SM) и изучает состояния участников группы в напрямую подключенном сегменте сети через IGMP. Хост отправляет сообщения Report IGMP для присоединения к указанной группе IGMP.

1.3.3.2. Сопутствующая конфигурация

Включение multicast-маршрутизации IPv4

По умолчанию multicast-маршрутизация IPv4 отключена.

Запустите **ip multicast-routing**, чтобы включить multicast-маршрутизацию IPv4.

Настройка IP multicast-маршрутизации на интерфейсе

По умолчанию IP multicast-маршрутизация на интерфейсе отключена.

Запустите **ip pim spase-mode** или **ip pim dense-mode**, чтобы включить IP multicast-маршрутизацию на интерфейсе.

1.3.4. Настройка порога TTL

Настройте порог TTL для интерфейса, то есть минимальное значение TTL для multicast-пакетов, разрешенное на интерфейсе.

1.3.4.1. Принцип работы

Настройте порог TTL для интерфейса и проверьте значения TTL multicast-пакетов. Multicast-пакеты, значения TTL которых превышают порог TTL интерфейса, пересылаются, а пакеты, значения TTL которых меньше, отбрасываются.

1.3.4.2. Сопутствующая конфигурация

Настройка порога TTL

По умолчанию порог TTL интерфейса равен 0.

Запустите **ip multicast ttl-threshold** *ttl-value*, чтобы изменить порог TTL интерфейса. Значение варьируется от 0 до 255.

Большее значение *ttl-value* означает большее значение TTL пересылаемых multicast-пакетов.

1.3.5. Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации

Каждый пакет данных multicast, полученный на устройстве, сохраняет соответствующую запись пересылки маршрута IP multicast. Однако избыточные записи multicast-маршрутизации могут исчерпать память устройства и ухудшить производительность устройства. Вы можете ограничить количество записей в таблице IP multicast-маршрутизации в зависимости от фактических требований к сети и производительности сервиса.

1.3.5.1. Принцип работы

Количество записей в таблице IP multicast-маршрутизации ограничено в зависимости от фактических требований к производительности сети и сервисов для обеспечения производительности устройства.

1.3.5.2. Сопутствующая конфигурация

Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации

По умолчанию в таблицу IP multicast-маршрутизации можно добавить максимум 1024 записи.

Запустите **ip multicast route-limit** *limit* [*threshold*], чтобы изменить количество записей, которые можно добавить в таблицу IP multicast-маршрутизации. Значение варьируется от 1 до 65 536.

Большее значение *limit* означает большее количество записей, которые можно добавить в таблицу IP multicast-маршрутизации.

1.3.6. Настройка границы IP multicast-маршрутизации

Настройте границу IP multicast-маршрутизации, чтобы указать диапазон передачи multicast-пакетов.

1.3.6.1. Принцип работы

Граница IP multicast-маршрутизации настраивается для указания диапазона передачи multicast-пакетов. Когда на интерфейсе настроена граница IP multicast-маршрутизации, этот интерфейс не может пересылать или принимать multicast-пакеты, в том числе отправленные с локального хоста.

1.3.6.2. Сопутствующая конфигурация

Настройка границы IP multicast-маршрутизации

По умолчанию граница IP multicast-маршрутизации не настроена.

Запустите **ip multicast boundary** *access-list* [**in** | **out**] для настройки границы IP multicast-маршрутизации.

1.3.7. Настройка статического маршрута IP multicast-маршрутизации

Настройте статический маршрут IP multicast-маршрутизации, чтобы указать интерфейс RPF или соседа RPF для пакетов multicast из указанных источников multicast.

1.3.7.1. Принцип работы

Проверка RPF выполняется после пересылки multicast-пакетов. Статический маршрут IP multicast-маршрутизации можно настроить для указания интерфейса RPF или соседа RPF для пакетов multicast из указанных источников multicast.

1.3.7.2. Сопутствующая конфигурация

Настройка статического маршрута IP multicast-маршрутизации

По умолчанию статический маршрут IP multicast-маршрутизации не настроен.

Запустите **ip mroute** *source-address mask* { [**bgp** | **isis** | **ospf** | **rip** | **static**] { *v4rpf-addrress* | *interface-type interface-number* } } [*distance*] для настройки статического маршрута IP multicast-маршрутизации.

1.3.8. Настройка управления направлением уровня 2 для multicast-потоков

Настройте управление направлением уровня 2 для multicast-потоков, чтобы управлять пересылкой multicast-потоков на интерфейсе.

1.3.8.1. Принцип работы

Настройте управление направлением уровня 2 для multicast-потоков и интерфейс пересылки, чтобы multicast-потоки можно было пересылать только через настроенные интерфейсы. В этом случае можно управлять пересылкой multicast-потоков уровня 2.

1.3.8.2. Сопутствующая конфигурация

Настройка управления направлением уровня 2 для multicast-потоков

По умолчанию управление направлением уровня 2 для multicast-потоков отключено.

Запустите **ip multicast static** *source-address group-address interface-type interface-number* для настройки управления направлением уровня 2 для multicast-потоков.

1.3.9. Настройка выбора маршрута RPF на основе правила самого длинного совпадения

Выберите оптимальный маршрут соответственно из таблицы статической multicast-маршрутизации, таблицы маршрутизации MBGP и таблицы unicast-маршрутизации и выберите маршрут с самой длинной маской соответствия в качестве маршрута RPF из трех оптимальных маршрутов.

1.3.9.1. Принцип работы

Статический маршрут multicast, маршрут MBGP и маршрут unicast-рассылки, которые можно использовать для проверки RPF, выбираются соответственно из таблицы статической multicast-маршрутизации, таблицы маршрутизации MBGP и таблицы unicast-маршрутизации в соответствии с правилами RPF.

- Если используется правило самого длинного соответствия, в качестве маршрута RPF выбирается маршрут с самой длинной маской соответствия. Если три маршрута имеют одинаковую маску, в качестве маршрута RPF выбирается маршрут с наивысшим приоритетом. Если они имеют одинаковый приоритет, маршруты RPF выбираются в последовательности статического multicast-маршрута, маршрута MBGP и unicast-маршрута.
- В противном случае в качестве маршрута RPF выбирается маршрут с наивысшим приоритетом. Если они имеют одинаковый приоритет, маршруты RPF выбираются

в последовательности статического multicast-маршрута, маршрута MBGP и unicast-маршрута.

1.3.9.2. Сопутствующая конфигурация

Настройка выбора маршрута RPF на основе правила самого длинного соответствия

По умолчанию в качестве маршрута RPF выбирается маршрут с наивысшим приоритетом. Если они имеют одинаковый приоритет, маршруты RPF выбираются в последовательности статического multicast-маршрута, маршрута MBGP и unicast-маршрута.

Запустите **ip multicast rpf longest-match**, чтобы настроить выбор маршрута RPF на основе правила самого длинного соответствия.

1.3.10. Настройка параметров непрерывной multicast-пересылки

Функция непрерывной пересылки обеспечивает непрерывную пересылку потоков multicast-данных во время повторной конвергенции протоколов multicast.

1.3.10.1. Принцип работы

Во время нормальной работы SSP синхронизирует аппаратную таблицу multicast-пересылки с платой управления в режиме реального времени. После включения платы управления загружается команда настройки control plane multicast исходной slave платы управления, и протокол multicast (например, PIM-SM или IGMP Snooping) повторно сходится (повторная конвергенция). Функция непрерывной multicast-пересылки обеспечивает непрерывную пересылку потоков multicast-данных во время повторной конвергенции multicast-протоколов.

По истечении заданного периода конвергенции протоколов все записи таблицы multicast-пересылки, которые не обновляются в течение периода конвергенции, удаляются.

1.3.10.2. Сопутствующая конфигурация

Настройка максимального периода для конвергенции протоколов multicast

По умолчанию максимальный период конвергенции multicast-протокола составляет 20 секунд.

Запустите команду **msf nsf convergence-time** *time*, чтобы настроить максимальный период конвергенции multicast-протокола. Значение варьируется от 0 до 3600 с.

Большее значение *time* означает более длительный максимальный период конвергенции multicast-протокола.

Настройка Leakage Period multicast-пакетов

По умолчанию Leakage Period multicast-пакетов составляет 30 с.

Запустите **msf nsf leak** *interval*, чтобы настроить Leakage Period multicast-пакетов. Значение варьируется от 0 до 3600 с.

Большее значение *interval* означает более длительный Leakage Period.

1.3.11. Настройка механизма перезаписи при переполнении записей аппаратной multicast-пересылки

Удаляются самые ранние аппаратные записи и добавляются новые записи, если таблица аппаратной пересылки переполняется при создании записей multicast-пересылки.

1.3.11.1. Принцип работы

Удаляются самые ранние аппаратные записи и добавляются новые записи, если таблица аппаратной пересылки переполняется при создании записей multicast-пересылки.

1.3.11.2. Сопутствующая конфигурация

Настройка механизма перезаписи при переполнении записей аппаратной multicast-пересылки

По умолчанию механизм перезаписи при переполнении записей аппаратной multicast-пересылки отключен.

Запустите **msf ipmc-overflow override** для настройки механизма перезаписи при переполнении записей аппаратной multicast-пересылки.

1.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций IP multicast-маршрутизации	(Обязательный) Он используется для настройки сервиса multicast	
	ip multicast-routing	Включает функцию multicast-маршрутизации IPv4
Настройка порога TTL	Опционально	
	ip multicast ttl-threshold *ttl-value*	Настраивает порог TTL для интерфейса
Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации	**ip multicast route-limit** *limit* [*threshold*]	Ограничивает количество записей, которые можно добавить в таблицу multicast-маршрутизации
Настройка границы IP multicast-маршрутизации	**ip multicast boundary** *access-list* [**in** | **out**]	Настраивает интерфейс как границу multicast для указанной группы
Настройка статического маршрут IP multicast-маршрутизации	**ip mroute** *source-address mask* { [**bgp** | **isis** | **ospf** | **rip** | **static**] { *v4rpf-addrress* | *interface-type interface-number* } } [*distance*]	Настраивает статический маршрут IP multicast-маршрутизации

Конфигурация	Описание и команда	
Настройка управления направлением уровня 2 для multicast-потоков	**ip multicast static** *source-address group-address interface-type interface-number*	Управляет направлением потоков данных на интерфейсах уровня 2
Настройка выбора маршрута RPF на основе правила самого длинного совпадения	**ip multicast rpf longest-match**	Настраивает выбор маршрута RPF на основе правила самого длинного соответствия
Настройка параметров непрерывной multicast-пересылки	**msf nsf convergence-time** *time*	Настраивает максимальный период конвергенции multicast-протокола
	msf nsf leak *time*	Настраивает Leakage Period multicast-пакетов
Настройка механизма перезаписи при переполнении записей аппаратной multicast-пересылки	**msf ipmc-overflow override**	Настраивает механизм перезаписи при переполнении записей аппаратной multicast-пересылки

1.4.1. Настройка основных функций IP multicast-маршрутизации

1.4.1.1. Эффект конфигурации

Создайте сеть PIM и обеспечьте источники данных и пользовательские терминалы в сети сервисом multicast IPv4.

1.4.1.2. Примечания

Сеть PIM должна использовать существующие unicast-маршруты в сети. Поэтому в сети необходимо настроить маршруты IPv4.

1.4.1.3. Шаги настройки

Включение multicast-маршрутизации IPv4

- Обязательный.
- Multicast-маршрутизация IPv4 должна быть включена на каждом маршрутизаторе, если не указано иное.

Включение IP multicast-маршрутизации для интерфейса

- Обязательный.
- Протокол IP multicast-маршрутизации должен быть включен на интерфейсах, если не указано иное.

1.4.1.4. Проверка

Включите источники multicast для отправки multicast-пакетов и хосты пользователей для присоединения к группам.

Проверьте, могут ли пользовательские хосты успешно получать пакеты из каждой группы.

1.4.1.5. Связанные команды

Включение multicast-маршрутизации IPv4

Команда	**ip multicast-routing**
Командный режим	Режим глобальной конфигурации

Настройка IP multicast-маршрутизации

ПРИМЕЧАНИЕ: для настройки IGMP см. раздел Настройка IGMP.

ПРИМЕЧАНИЕ: для настройки PIM-DM см. раздел Настройка PIM-DM.

ПРИМЕЧАНИЕ: для настройки PIM-SM см. раздел Настройка PIM-SM.

После включения multicast уровня 3 в private VLAN и super VLAN и наличии источника multicast в sub-VLAN, необходимо скопировать дополнительную запись, входом которой является sub-VLAN, в которую поступает multicast-поток, из-за проверки достоверности во время multicast-пересылки. Это приводит к занятию одной дополнительной аппаратной записи multicast и уменьшению на одну в емкости multicast.

Отображение информации о таблице multicast-пересылки

Команда	**show ip mroute** [*group-or-source-address* [*group-or-source-address*]] [**dense** | **sparse**] [**summary** | **count**]
Описание параметра	*group-or-source-address*: указывает адрес группы или адрес источника. *group-or-source-address*: указывает адрес группы или адрес источника. **dense**: отображает основную (core) запись multicast PIM-DM. **sparse**: отображает основную (core) запись multicast PIM-SM. **summary**: отображает сводную информацию о записях multicast-маршрутизации. **count**: отображает информацию о подсчете о записях multicast-маршрутизации
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	Эти три параметра являются необязательными, а адрес источника и адрес группы должны быть указаны одновременно. Если не указан адрес источника или адрес группы, отображаются все записи MFC. Если указаны только адрес источника и адрес группы, отображаются записи MFC об адресе источника и адресе группы

1.4.1.6. Пример конфигурации

Создание сервиса IP Multicast в сети IPv4 и поддержка PIM-DM

Сценарий:

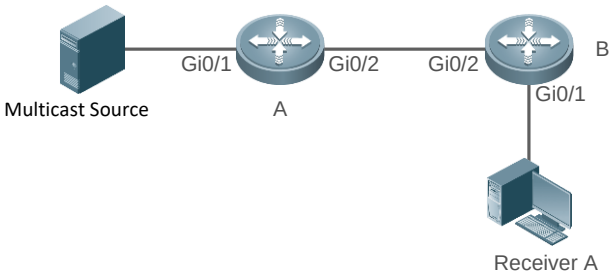

Рисунок 1-3.

Шаги настройки	• Настройте протокол unicast-маршрутизации IPv4 (например, OSPF) на маршрутизаторе. • Включите multicast-маршрутизацию IPv4 на всех маршрутизаторах. • Включите PIM-DM на интерфейсах взаимодействия (interconnection) устройств и интерфейсах для подключения пользовательских хостов и источников multicast
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if)# ip pim dense-mode A(config-if)# exit A(config)# interface GigabitEthernet 0/2 A(config-if)# ip pim dense-mode A(config-if)# exit
B	B# configure terminal B(config)# ip multicast-routing B(config)# interface GigabitEthernet 0/1 B(config-if)# ip pim dense-mode B(config-if)# exit B(config)# interface GigabitEthernet 0/2 B(config-if)# ip pim dense-mode B(config-if)# exit

Проверка	• Включите источник multicast (192.168.1.100) для отправки пакетов в G (233.3.3.3). Разрешите приемнику A присоединиться к G. • Проверьте multicast-пакеты, полученные приемником A. Приемник A должен иметь возможность получать multicast-пакеты от G. • Проверьте таблицы multicast-пересылки на A и B
A	A# show ip mroute IP Multicast Routing Table Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed, R - RPT, S - SPT, s - SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL) (192.168.1.100, 233.3.3.3), uptime 00:01:55, stat expires 00:02:19 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (1)
B	B# show ip mroute IP Multicast Routing Table Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed, R - RPT, S - SPT, s - SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL) (192.168.1.100, 233.3.3.3), uptime 00:00:35, stat expires 00:02:55 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1 (1)

1.4.1.7. Распространенные ошибки

- Unicast-маршрут IPv4 настроен неправильно.
- На маршрутизаторе не включена multicast-маршрутизация IPv4.
- IP multicast-маршрутизация не включена на интерфейсе.

1.4.2. Настройка порога TTL

1.4.2.1. Эффект конфигурации

Настройте порог TTL для интерфейса и проверьте значения TTL multicast-пакетов. Multicast-пакеты, значения TTL которых превышают порог TTL интерфейса, пересылаются, а пакеты, значения TTL которых меньше, отбрасываются.

1.4.2.2. Примечания

Необходимо настроить основные (basic) функции IP multicast-маршрутизации.

1.4.2.3. Шаги настройки

Установите порог TTL на интерфейсах маршрутизатора PIM, если не указано иное.

1.4.2.4. Проверка

- Включите источники multicast для отправки multicast-пакетов и хосты пользователей для присоединения к группам.
- Установите порог TTL на значение, превышающее значение TTL multicast-пакета на интерфейсе маршрутизатора PIM, напрямую подключенном к пользовательскому хосту, и проверьте, может ли пользователь получить multicast-пакет.

1.4.2.5. Связанные команды

Настройка порога TTL

Команда	**ip multicast ttl-threshold** *ttl-value*
Описание параметра	*ttl-value*: указывает порог TTL для интерфейса. Значение находится в диапазоне от 0 до 255. Значение по умолчанию — 0
Командный режим	Режим настройки интерфейса
Руководство по использованию	Устройство с поддержкой multicast может сохранять пороговое значение TTL для каждого интерфейса. Multicast-пакеты, значения TTL которых превышают порог TTL интерфейса, пересылаются, а пакеты, значения TTL которых меньше, отбрасываются. Порог TTL действует только для кадров multicast и должен быть настроен на интерфейсах уровня 3

1.4.2.6. Пример конфигурации

Создание сервиса IP Multicast в сети IPv4 и настройка порогового значения TTL

Сценарий:

Рисунок 1-4.

Шаги настройки	• Настройте основные функции IP multicast-маршрутизации. (пропущено) • Настройте порог TTL равным 100 на интерфейсе Gi 0/2 устройства A
A	A# configure terminal A(config)#int gigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#ip multicast ttl-threshold 100 A(config-if-GigabitEthernet 0/2)# exit
Проверка	Включите источник multicast (192.168.1.100) для отправки пакетов в G (233.3.3.3). Разрешите приемнику A присоединиться к G. • Настройте порог TTL равным 100 на интерфейсе Gi 0/2 устройства A, что превышает значение TTL multicast-пакета. • Проверьте разницу между записями пересылки маршрута до и после настройки порога TTL
Перед настройкой порога TTL	A# show ip mroute IP Multicast Routing Table Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed, R - RPT, S - SPT, s - SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL) (192.168.1.100, 233.3.3.3), uptime 00:00:08, stat expires 00:03:29

	Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (1)
После настройки порога TTL	A# show ip mroute IP Multicast Routing Table Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed, R - RPT, S - SPT, s - SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL) (192.168.1.100, 233.3.3.3), uptime 00:00:01, stat expires 00:03:29 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (100)

1.4.3. Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации

1.4.3.1. Эффект конфигурации

Каждый пакет данных multicast, полученный на устройстве, сохраняет соответствующую запись пересылки маршрута IP multicast. Однако избыточные записи multicast-маршрутизации могут исчерпать память устройства и ухудшить производительность устройства. Вы можете ограничить количество записей в таблице IP multicast-маршрутизации в зависимости от фактических требований к производительности сети и сервиса.

1.4.3.2. Примечания

Необходимо настроить основные функции IP multicast-маршрутизации.

1.4.3.3. Шаги настройки

Ограничьте количество записей в таблице IP multicast-маршрутизации в зависимости от фактических требований к производительности сети и сервиса.

1.4.3.4. Проверка

Отправьте N групп multicast-пакетов из источника multicast в сети, настройте хосты пользователей для присоединения к группам, настройте количество записей, которые можно добавить в таблицу IP multicast-маршрутизации, как N-1, и проверьте, что multicast-пакет, полученный пользовательским хостом, принадлежит группе N-1.

1.4.3.5. Связанные команды

Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации

Команда	**ip multicast route-limit** *limit* [*threshold*]
Описание параметра	*limit*: указывает количество записей в таблице multicast-маршрутизации. Значение находится в диапазоне от 1 до 65 536. Значение по умолчанию — 1024. *threshold*: указывает количество записей в таблице multicast-маршрутизации, при которых отображается предупреждающее сообщение. Значение по умолчанию — 65 536
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Из-за ограничений аппаратных ресурсов записи маршрутизации, выходящие за пределы диапазона, разрешенного оборудованием, могут быть перенаправлены только программным обеспечением, что ухудшает производительность

1.4.3.6. Пример конфигурации

Создание сервиса IP Multicast в сети IPv4 и настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации

Сценарий:

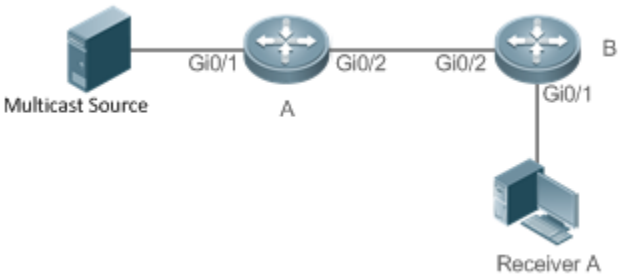

Рисунок 1-5.

Шаги настройки	• Настройте основные функции IP multicast-маршрутизации. (пропущено) • Настройте количество записей, которые можно добавить в таблицу multicast-маршрутизации на устройстве B, как 2
B	B# configure terminal B(config)# ip multicast route-limit 2

Проверка	Включите источник multicast (192.168.1.100) для отправки пакетов G1 (233.3.3.1), G2 (233.3.3.2) и G3 (233.3.3.3). Разрешите приемнику A присоединиться к G1, G2 и G3. • Проверьте multicast-пакеты, полученные приемником A. Приемник A должен иметь возможность получать multicast-пакеты из двух групп из G1, G2 и G3. • Проверьте записи multicast-маршрутизации на A и B. • Когда количество записей в таблице IP multicast-маршрутизации достигает верхнего порога, отображается сообщение с подсказкой
A	A# show ip mroute IP Multicast Routing Table Flags: I – Immediate Stat, T – Timed Stat, F – Forwarder installed, R – RPT, S – SPT, s – SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL) (192.168.1.100, 233.3.3.1), uptime 00:00:06, stat expires 00:03:24 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (1) (192.168.1.100, 233.3.3.2), uptime 00:00:05, stat expires 00:03:25 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (1) (192.168.1.100, 233.3.3.3), uptime 00:00:00, stat expires 00:03:30 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (1)
B	B# show ip mroute IP Multicast Routing Table

	Flags: I – Immediate Stat, T – Timed Stat, F – Forwarder installed, R – RPT, S – SPT, s – SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL) (192.168.1.100, 233.3.3.1), uptime 00:01:13, stat expires 00:03:23 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1 (1) (192.168.1.100, 233.3.3.3), uptime 00:06:08, stat expires 00:03:23 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1 (1)
	Когда количество записей в таблице IP multicast-маршрутизации достигает верхнего порога, отображается сообщение с подсказкой. B#*Dec 26 10:43:07: %MROUTE-4-ROUTELIMIT: IPv4 Multicast route limit 2 exceeded - VRF default

1.4.3.7. Распространенные ошибки

Unicast-маршрут IPv4 настроен неправильно.

1.4.4. Настройка границы IP multicast-маршрутизации

1.4.4.1. Эффект конфигурации

Настройте границу IP multicast-маршрутизации, чтобы указать диапазон передачи multicast-пакетов.

1.4.4.2. Примечания

Необходимо настроить основные функции IP multicast-маршрутизации.

1.4.4.3. Шаги настройки

Настройте границу IP multicast-маршрутизации на интерфейсах маршрутизатора PIM, если не указано иное.

1.4.4.4. Проверка

Включите источники multicast для отправки multicast-пакетов и хосты пользователей для присоединения к группам. Настройте границу IP multicast-маршрутизации на интерфейсе

маршрутизатора PIM, подключенном к хосту пользователя, и проверьте, может ли пользователь получать multicast-пакет.

1.4.4.5. Связанные команды

Включение multicast-маршрутизации IPv4

Команда	**ip multicast boundary** *access-list* [**in** | **out**]
Описание параметра	*access-list*: указывает диапазон адресов группы, определенный ACL. **in**: указывает на то, что граница IP multicast-маршрутизации вступает в силу во входящем направлении потока-multicast. **out**: указывает на то, что граница IP multicast-маршрутизации вступает в силу в исходящем направленим потока-multicast
Командный режим	Режим настройки интерфейса
Руководство по использованию	После выполнения этой команды пакеты IGMP и PIM-SM в диапазоне групп фильтруются на этом интерфейсе, и потоки multicast-данных не поступают и не выходят через этот интерфейс. ACL, связанный с этой командой, может быть стандартным или расширенным ACL. Для расширенных списков ACL сопоставляется только адрес назначения и адрес источника

1.4.4.6. Пример конфигурации

Создание службы IP Multicast в сети IPv4 и настройка границы IP multicast-маршрутизации

Сценарий:

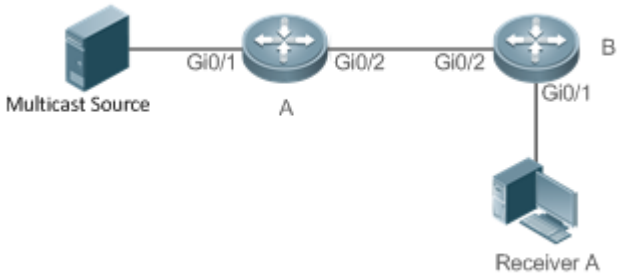

Рисунок 1-6.

Шаги настройки	• Настройте основные функции IP multicast-маршрутизации. (пропущено) • Настройте ACL на устройстве A. • Настройте границу IP multicast-маршрутизации на интерфейсе Gi 0/1 устройства A

A	A# configure terminal A(config)#ip access-list standard ip_multicast A(config-std-nacl)#deny any A(config-std-nacl)#exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ip multicast boundary ip_multicast A A(config-if-GigabitEthernet 0/1)# exit
Проверка	Включите источник multicast (192.168.1.100) для отправки пакетов в G (233.3.3.3). Разрешите приемнику A присоединиться к G. Запустите отладку **ip pim sparse-mode events**
A	A# debug ip pim sparse-mode events Jan 1 20:58:34: %7: VRF(0): No cache message: src 192.168.1.100 for 233.3.3.3 vif 2 *Jan 1 20:58:34: %7: VRF(0): Ignore No cache message: src 192.168.1.100 for 233.3.3.3 vif 2 in PIM_BOUNDARY_FLT_BOTH rang

1.4.4.7. Распространенные ошибки

Unicast-маршрут IPv4 настроен неправильно.

1.4.5. Настройка статического маршрут IP multicast-маршрутизации

1.4.5.1. Эффект конфигурации

Настройте статический маршрут IP multicast-маршрутизации, чтобы указать интерфейс RPF или соседа RPF для пакетов multicast из указанных источников multicast.

1.4.5.2. Примечания

Необходимо настроить основные функции IP multicast-маршрутизации.

1.4.5.3. Шаги настройки

Статический маршрут IP multicast-маршрутизации можно настроить на каждом устройстве, если не указано иное.

1.4.5.4. Проверка

Запустите **show ip rpf** *source-address*, чтобы проверить информацию RPF указанного источника.

1.4.5.5. Связанные команды

Настройка основных функций IP multicast-маршрутизации

Команда	**ip mroute** *source-address mask* { [**bgp** | **isis** | **ospf** | **rip** | **static**] { *v4rpf-addrress* | *interface-type interface-number* } } [*distance*]
Описание параметра	*source-address*: указывает адрес источника multicast. *mask*: указывает маску адреса источника multicast. *protocol*: указывает протокол unicast-маршрутизации, используемый в данный момент. *rpf-addrress*: указывает адрес соседа RPF (next hop источника multicast). *interface-type interface-number*: указывает интерфейс RPF (исходящий интерфейс источника multicast). *distance*: указывает расстояние управления маршрутом. Значение находится в диапазоне от 0 до 255. Значение по умолчанию — 0
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Статические маршруты multicast применимы только для проверки RPF. Если необходимо указать IP-адрес исходящего интерфейса, но не next hop статического multicast-маршрута, исходящий интерфейс должен быть типа «точка-точка» (point-to-point)

Отображение информации RFP для указанного адреса источника

Команда	**show ip rpf** *source-address*
Описание параметра	*source-address*: указывает IP-адрес источника
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	Эти три параметра являются необязательными, а адрес источника и адрес группы должны быть указаны одновременно. Если не указан адрес источника или адрес группы, отображаются все записи MFC. Если указаны только адрес источника и адрес группы, отображаются записи MFC адреса источника и адреса группы

1.4.5.6. Пример конфигурации

Создание сервиса IP Multicast в сети IPv4 и поддержка PIM-DM

Сценарий:

Рисунок 1-7.

Шаги настройки	• Настройте основные функции IP multicast-маршрутизации. (пропущено) • Настройте статический маршрут к приемнику на устройстве B
A	B# configure terminal B(config)# ip mroute 10.10.10.10 255.255.255.255 ospf 192.168.1.1 1
Проверка	Запустите **show ip rpf**, чтобы просмотреть информацию RPF на приемнике до и после настройки
Перед настройкой	B# show ip rpf 10.10.10.10 RPF information for 10.10.10.10 RPF interface: GigabitEthernet 0/2 RPF neighbor: 192.168.2.1 RPF route: 10.10.10.10/32 RPF type: unicast (ospf) RPF recursion count: 0 Doing distance-preferred lookups across tables Distance: 110 Metric: 1
После настройки	B# show ip rpf 10.10.10.10 RPF information for 10.10.10.10 RPF interface: GigabitEthernet 0/0 RPF neighbor: 192.168.1.1 RPF route: 10.10.10.10/32 RPF type: static RPF recursion count: 0 Doing distance-preferred lookups across tables Distance: 1

	Metric: 0

1.4.5.7. Распространенные ошибки

- Unicast-маршрут IPv4 настроен неправильно.
- На маршрутизаторе не включена multicast-маршрутизация IPv4.

1.4.6. Настройка управления направлением уровня 2 для multicast-потоков

1.4.6.1. Эффект конфигурации

Настройте управление направлением уровня 2 для multicast-потоков, чтобы управлять пересылкой multicast-потоков на интерфейсе.

1.4.6.2. Примечания

Необходимо настроить основные функции IP multicast-маршрутизации.

1.4.6.3. Шаги настройки

Управление направлением уровня 2 для multicast-потоков можно настроить на устройствах уровня 2, если не указано иное.

1.4.6.4. Проверка

Отправляйте multicast-пакеты в сеть, содержащую устройство A уровня 2, подключайте несколько пользовательских хостов к VLAN 1 устройства A уровня 2 для получения группы, настройте управление направлением уровня 2 для потоков multicast на устройстве A и проверьте, передаются ли multicast-пакеты на настроенный интерфейс уровня 2.

1.4.6.5. Связанные команды

Настройка управления направлением уровня 2 для multicast-потоков

Команда	**ip multicast static** *source-address group-address interface-type interface-number*
Описание параметра	*source-address*: определяет адрес источника multicast. *group-address*: определяет адрес группы multicast. *interface-type interface-number*: определяет интерфейс уровня 2, которому разрешено пересылать multicast-поток
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Разрешить настройку указанного multicast-потока с помощью нескольких команд, то есть настройку с использованием нескольких интерфейсов. После настройки управления направлением для multicast-потока поток можно будет пересылать только через эти настроенные интерфейсы. Другим интерфейсам не разрешено пересылать поток.

	Эта команда управляет только пересылкой multicast-потоков на интерфейсе, но не влияет напрямую на обработку multicast-протоколов в пакетах протоколов. Однако, поскольку некоторые функции multicast-протокола управляются потоками данных multicast, это также может повлиять на поведение протоколов multicast-маршрутизации

1.4.6.6. Пример конфигурации

Создание сервиса IP Multicast в сети IPv4 и настройка управления направлением уровня 2 для multicast-потоков

Сценарий:

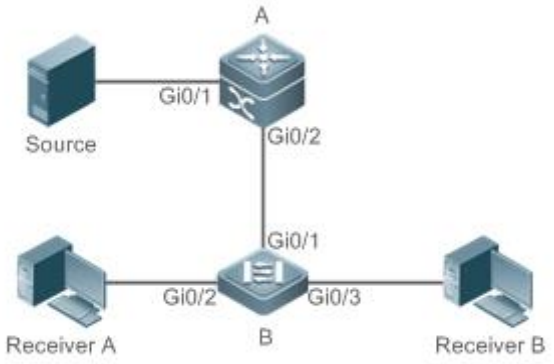

Рисунок 1-8.

Шаги настройки	• Настройте основные функции IP multicast-маршрутизации. (пропущено) • Настройте управление направлением уровня 2 для multicast-потоков на устройстве B, чтобы потоки отправлялись только на интерфейс Gi 0/2
B	A# configure terminal A(config)# ip multicast static 192.168.1.100 233.3.3.3 gigabitEthernet0/2
Проверка	Включите источник multicast (192.168.1.100) для отправки пакетов в G (233.3.3.1). Разрешите получателям A и B присоединиться к G. Проверьте multicast-пакеты, полученные приемником A. Приемник B не должен иметь возможности получать multicast-пакеты от G

1.4.6.7. Распространенные ошибки

Unicast-маршрут IPv4 настроен неправильно.

1.4.7. Настройка выбора маршрута RPF на основе правила самого длинного совпадения

1.4.7.1. Эффект конфигурации

Выберите оптимальный маршрут соответственно из таблицы статической multicast-маршрутизации, таблицы маршрутизации MBGP и таблицы

unicast-маршрутизации и выберите маршрут с самой длинной маской соответствия в качестве маршрута RPF из трех оптимальных маршрутов.

1.4.7.2. Примечания

Необходимо настроить основные функции IP multicast-маршрутизации.

1.4.7.3. Шаги настройки

Настройте выбор маршрута RPF на основе правила самого длинного соответствия на каждом устройстве, если не указано иное.

1.4.7.4. Проверка

Настройте статический маршрут multicast и статический маршрут unicast, чтобы они имели одинаковый приоритет, и настройте статический маршрут unicast, чтобы он имел большую длину маски.

Запустите **show ip rpf** *source-address*, чтобы проверить информацию RPF указанного источника.

1.4.7.5. Связанные команды

Настройка выбора маршрута RPF на основе правила самого длинного соответствия

Команда	**ip multicast rpf longest-match**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Шаги для выбора маршрутов RFP следующие: Выберите оптимальный маршрут соответственно из таблицы статической multicast-маршрутизации, таблицы маршрутизации MBGP и таблицы unicast-маршрутизации для проверки RPF. Выберите один из трех маршрутов в качестве маршрута RPF. Если используется правило самого длинного соответствия, выбирается маршрут с самой длинной маской соответствия. Если три маршрута имеют одинаковую маску, выбирается маршрут с наивысшим приоритетом. Если они имеют одинаковый приоритет, маршруты RPF выбираются в последовательности статического multicast-маршрута, маршрута MBGP и unicast-маршрута. Если правило самого длинного совпадения не используется, выбирается маршрут с высшим приоритетом. Если они имеют одинаковый приоритет, маршруты RPF выбираются в последовательности статического multicast-маршрута, маршрута MBGP и unicast-маршрута

1.4.7.6. Пример конфигурации

Создание сервиса IP Multicast в сети IPv4 и настройка выбора маршрута RPF на основе правила самого длинного соответствия

Сценарий:

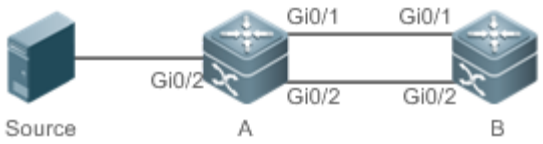

Рисунок 1-9.

Шаги настройки	• Настройте основные функции IP multicast-маршрутизации. (пропущено) • На устройстве B настройте статический IP multicast-маршрут, длина маски которого меньше длины маски статического unicast-маршрута. • Настройте выбор маршрута RPF на основе правила самого длинного соответствия на устройстве B
B	B# configure terminal B(config)# ip multicast-routing B(config)# ip mroute 10.10.10.10 255.255.0.0 ospf 192.168.1.1 B(config)# ip multicast rpf longest-match
Проверка	Запустите команду **show ip rpf**, чтобы проверить информацию RFP источника multicast до и после настройки выбора маршрута RPF на основе правила самого длинного соответствия
Перед настройкой	B#show ip rpf 10.10.10.10 RPF information for 10.10.10.10 RPF interface: GigabitEthernet 0/0 RPF neighbor: 192.168.1.1 RPF route: 10.10.0.0/16 RPF type: static RPF recursion count: 0 Doing distance-preferred lookups across tables Distance: 0 Metric: 0
После настройки	B# show ip rpf 10.10.10.10 RPF information for 10.10.10.10

	RPF interface: GigabitEthernet 0/2 RPF neighbor: 192.168.2.1 RPF route: 10.10.10.10/32 RPF type: unicast (ospf) RPF recursion count: 0 Doing prefix-length-preferred lookups across tables Distance: 110 Metric: 1

1.4.7.7. Распространенные ошибки

- Unicast-маршрут IPv4 настроен неправильно.
- На маршрутизаторе не включена multicast-маршрутизация IPv4.

1.4.8. Настройка параметров непрерывной multicast-пересылки

1.4.8.1. Эффект конфигурации

Функция непрерывной пересылки обеспечивает непрерывную пересылку потоков multicast-данных во время повторной конвергенции протоколов multicast.

1.4.8.2. Примечания

Необходимо настроить основные функции IP multicast-маршрутизации.

1.4.8.3. Шаги настройки

Настройка максимального периода для конвергенции протоколов multicast

Максимальный период конвергенции multicast-протокола можно указать на каждом устройстве, если не указано иное.

Настройка Leakage Period multicast-пакетов

Leakage Period multicast можно настроить на каждом устройстве, если не указано иное.

1.4.8.4. Проверка

Запустите команду **show msf nsf**, чтобы проверить настроенные параметры непрерывной multicast-пересылки.

1.4.8.5. Связанные команды

Настройка максимального периода для конвергенции протоколов multicast

Команда	**msf nsf convergence-time** *time*
Описание параметра	**convergence-time** *time*: определяет максимальный период конвергенции multicast-протокола. Значение варьируется от 0 до 3600 с. Значение по умолчанию — 20 с

Командный режим	Режим глобальной конфигурации

Настройка Leakage Period multicast-пакетов

Команда	**msf nsf leak** *interval*
Описание параметра	**leak** *interval*: определяет Leakage Period multicast-пакетов. Значение варьируется от 0 до 3600 с. Значение по умолчанию — 30.с
Командный режим	Режим глобальной конфигурации

Отображение конфигураций непрерывной multicast-пересылки

Команда	**show msf nsf**
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации

1.4.8.6. Пример конфигурации

Создание сервиса IP Multicast в сети IPv4 и поддержка PIM-DM

Сценарий	Базовая среда сервиса IP multicast-маршрутизации (пропущено)
Шаги настройки	• Настройте основные функции IP multicast-маршрутизации. (пропущено) • Настройте максимальный период конвергенции протоколов multicast. • Настройте Leakage Period multicast-пакетов
A	A# configure terminal A(config)# msf nsf convergence-time 200 A(config)# msf nsf leak 300
Проверка	Запустите команду **show msf nsf**, чтобы отобразить конфигурации непрерывной multicast-пересылки
A	A# show msf nsf Multicast HA Parameters ----------+------+ protocol convergence timeout 200 secs

1.4.9. Настройка механизма перезаписи при переполнении записей аппаратной multicast-пересылки

1.4.9.1. Эффект конфигурации

Удаляет самые ранние записи об оборудовании и добавляет новые записи, если таблица пересылки оборудования переполняется при создании записей multicast-пересылки.

1.4.9.2. Примечания

Необходимо настроить основные функции IP multicast-маршрутизации.

1.4.9.3. Шаги настройки

Механизм перезаписи при переполнении записей аппаратной пересылки multicast можно настроить на каждом устройстве, если не указано иное.

1.4.9.4. Проверка

Запустите команду **show running-config**, чтобы проверить, настроен ли механизм перезаписи при переполнении записей аппаратной пересылки multicast.

1.4.9.5. Связанные команды

Настройка механизма перезаписи при переполнении записей аппаратной пересылки multicast

Команда	**msf ipmc-overflow override**
Командный режим	Режим глобальной конфигурации

1.4.9.6. Пример конфигурации

Создание сервиса IP Multicast в сети IPv4 и настройка механизма перезаписи при переполнении записей аппаратной пересылки multicast

Сценарий	Базовая среда сервиса IP multicast-маршрутизации (пропущено)
Шаги настройки	• Настройте основные функции IP multicast-маршрутизации. (пропущено) • Настройте механизм перезаписи при переполнении записей аппаратной пересылки multicast
A	A# configure terminal A(config)#msf ipmc-overflow override
Проверка	Запустите команду **show running-config**, чтобы проверить, настроен ли механизм перезаписи при переполнении записей аппаратной пересылки multicast

A	A# show running-config … msf ipmc-overflow override …

1.5. Мониторинг

1.5.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере важной информации и прерыванию работы служб.

Описание	Команда
Очищает таблицу multicast-пересылки IPv4	**clear ip mroute** { * | *v4group-address* [*v4source-address*] }
Сбрасывает статистику в таблице multicast-пересылки IPv4	**clear ip mroute statistics** { * | *v4group-address* [*v4source-address*] }

1.5.2. Отображение

Описание	Команда
Отображает справочную информацию для каждого модуля multicast	**multicast help**
Отображает состояние модулей multicast IPv4	**view multicast**
Отображает таблицу multicast-пересылки IPv4	**show ip mroute** [*group-or-source-address* [*group-or-source-address*]] [**dense** | **sparse**] [**summary** | **count**]
Отображает информацию о статическом multicast-маршруте IPv4	**show ip mroute static**
Отображает информацию RFP для указанного адреса источника IPv4	**show ip rpf** { *source-address* [*group-address*] [**rd** *route-distinguisher*] } [**metric**]
Отображает информацию о multicast-интерфейсах IPv4	**show ip mvif** [*interface-type interface-number*]

Описание	Команда
Отображает таблицу multicast-пересылки IPv4 уровня 3	**show ip mrf mfc**
Отображает таблицу многоуровневой multicast-пересылки IPv4	**show msf msc**
Отображает конфигурации непрерывной multicast-пересылки IPv4	**show msf nsf**

1.5.2.1. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Поэтому отключайте отладку сразу после использования.

Описание	Команда
Отладка работы ядра multicast	**debug nsm mcast all**
Отладка связи между ядром multicast IPv4 и модулем протокола	**debug nsm mcast fib-msg**
Отладка работы интерфейса ядра multicast IPv4	**debug nsm mcast vif**
Отладка интерфейса и обработки статистики входа ядра multicast IPv4	**debug nsm mcast stats**
Отладка процесса пересылки multicast-пакетов IPv4 уровня 3	**debug ip mrf forwarding**
Отладка операции с записями multicast-пересылки уровня 3 в сети IPv4	**debug ip mrf mfc**
Отладка обработки событий multicast-пересылки уровня 3 в сети IPv4	**debug ip mrf event**
Отладка обработки многоуровневой multicast-пересылки пакетов IPv4	**debug msf forwarding**

Описание	Команда
Отладка работы с записями многоуровневой multicast-пересылки в сети IPv4	**debug msf mfc**
Отладка аппаратной обработки нижнего уровня многоуровневой multicast-пересылки пакетов IPv4	**debug msf ssp**
Отлада вызова интерфейсов API, предоставляемых многоуровневой multicast-пересылкой IPv4	**debug msf api**
Отладка обработки событий многоуровневой multicast-пересылки в сети IPv4	**debug msf events**

2. НАСТРОЙКА MULTICAST IPV6

2.1. Обзор

Multicast IPv6 — это расширение и усовершенствование multicast IPv4. По сравнению с multicast IPv4 механизм multicast IPv6 значительно расширен.

При традиционной IP-передаче хосту разрешено отправлять пакеты только одному хосту (unicast) или всем хостам (broadcast). Технология multicast предоставляет третий вариант: хосту разрешено отправлять пакеты определенным хостам.

Технология IP multicast-маршрутизации применима к мультимедийным приложениям типа «один ко многим» (one-to-many).

2.1.1. Протоколы и стандарты

Multicast IPv6 охватывает следующие протоколы:

- Multicast Listener Discovery (MLD): выполняется между устройством multicast и хостом, а также отслеживает и изучает взаимоотношения между участниками группы.
- Protocol Independent Multicast — резервный режим для IPv6 (PIM-SMv6): работает между устройствами и реализует пересылку multicast-пакетов путем создания таблицы multicast-маршрутизации.

2.2. Приложения

Приложение	Описание
Типичное применение PIM-SMv6	Сервис multicast PIM-SMv6 предоставляется в той же сети

2.2.1. Типичное применение PIM-SMv6

2.2.1.1. Сценарий

Сервис multicast PIM-SMv6 предоставляется в той же сети.

Как показано на следующем Рисунке:

- R1 и источник multicast находятся в одной сети, R2 настроен как rendezvous point (RP), R3 находится в той же сети, что и приемник A, а R4 находится в той же сети, что и приемник B. Предположим, что устройства и хосты правильно подключены, IPv6 включен на каждом интерфейсе, а unicast IPv6 включена на каждом устройстве.

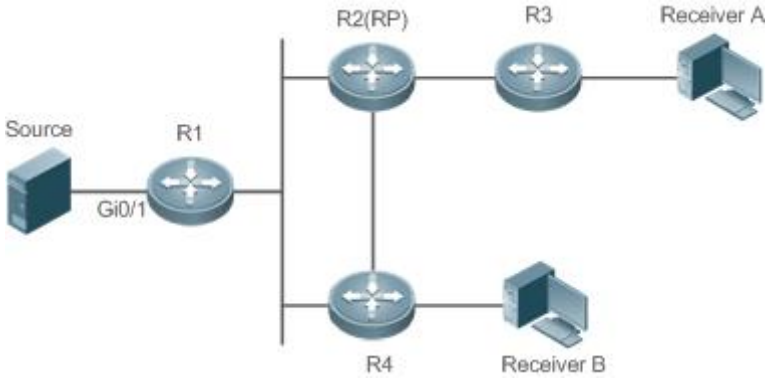

Рисунок 2-1.

R1, R2, R3 и R4 являются устройствами уровня 3, а R2 функционирует как RP.

Источник multicast напрямую подключен к R1, приемник A напрямую подключен к R3, а приемник B напрямую подключен к R4.

2.2.2. Развертывание

- Запустите протокол Open Shortest Path First для IPv6 (OSPFv6) в той же сети, чтобы реализовать unicast-маршрутизацию.
- Запустите протокол PIM-SMv6 в той же сети, чтобы реализовать multicast-маршрутизацию.

2.3. Функции

2.3.1. Базовые определения

PIM-маршрутизатор и PIM-интерфейс

Маршрутизаторы, на которых включен протокол PIM, называются маршрутизаторами PIM. Интерфейсы, в которых включен протокол PIM, называются интерфейсами PIM.

Multicast-пакеты пересылаются маршрутизаторами PIM. PIM-интерфейсы для приема multicast-пакетов называются upstream-интерфейсами, а PIM-интерфейсы для передачи multicast-пакетов называются downstream-интерфейсами.

Сегменты сети, в которых расположены upstream-интерфейсы, называются upstream сетевыми сегментами. Сегменты сети, в которых расположены downstream-интерфейсы, называются downstream сегментами сети.

Сеть PIM и домен PIM

PIM-маршрутизаторы подключаются через PIM-интерфейсы и образуют сеть PIM.

На некоторых интерфейсах PIM установлены границы, разделяющие большую сеть PIM на несколько доменов PIM. Границы могут отклонять определенные multicast-пакеты или ограничивать передачу сообщений PIM.

Multicast Distribution Tree, DR и RP

Multicast-пакеты передаются из одной точки в несколько точек. Путь пересылки представляет собой древовидную структуру. Этот путь пересылки называется multicast distribution tree (MDT). MDT подразделяются на два типа:

- Rendezvous point tree (RPT): rendezvous point (RP) используется в качестве «корня» (root), а назначенные маршрутизаторы (DR), подключенные к членам группы, в качестве «листьев».

- Shortest path tree (SPT): используйте DR, подключенный к источнику multicast, в качестве root, а RP или DR, подключенные к членам группы, в качестве «листьев».
- DR и RP — это функциональные роли маршрутизаторов PIM.
- RP собирает информацию об источниках multicast и членах групп в сети.
- DR, подключенный к источнику multicast, передает информацию об источнике multicast на RP, а DR, подключенные к членам группы, передают информацию об участниках группы на RP.

(*,G), (S,G)

- (*,G): указывает пакеты, переданные из любого источника в группу G, записи маршрутизации, соответствующие пакетам, и путь пересылки (RPT), соответствующий пакетам.
- (S,G): указывает пакеты, переданные из источника S в группу G, записи маршрутизации, соответствующие пакетам, и путь пересылки (SPT), соответствующий пакетам.

ASM, SSM

PIM-SM поддерживает две сервисные модели multicast: multicast-рассылку с любым источником (ASM) и multicast-рассылку с указанием источника (SSM), которые применимы к различным сегментам адреса multicast.

- ASM: в модели ASM пользовательский хост не может выбрать источник multicast. Хост пользователя присоединяется к группе multicast и получает все пакеты, отправленные из всех источников в группу multicast.
- SSM: в модели SSM пользовательский хост может выбрать источник multicast. Хост пользователя указывает адрес источника при присоединении к группе multicast, а затем получает пакеты только от указанного источника в группу multicast.

ПРИМЕЧАНИЕ: требование модели SSM: необходимо использовать другие сетевые сервисы, чтобы позволить хосту пользователя заранее знать положение источника multicast, чтобы хост пользователя мог выбрать источник multicast.

2.3.2. Обзор

Особенность	Описание
Настройка основных функций multicast IPv6	Создает сеть PIM для предоставления сервиса multicast IPv6 для источников данных и пользовательских терминалов в сети
Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации IPv6	Ограничивает количество записей, которые можно добавить в таблицу multicast-маршрутизации
Настройка границы multicast IPv6	Устанавливает интерфейс в качестве границы multicast определенного диапазона группы

Особенность	Описание
Настройка статической multicast-маршрутизации IPv6	Настраивает статическую маршрутизацию multicast для использования путей multicast-пересылки, отличных от путей unicast-пересылки
Настройка управления направлением потока уровня 2 для multicast-потоков	Для multicast-потока можно настроить несколько команд, то есть нескольким портам можно разрешить пересылку multicast-потока. Если управление направлением потока настроено для multicast-потока, multicast-поток может пересылаться только через настроенные порты. Другим портам не разрешено пересылать multicast-поток
Настройка выбора маршрута RPF по принципу самого длинного соответствия	В соответствии с правилами RPF из каждой таблицы статической маршрутизации multicast, таблицы маршрутизации MBGP и таблицы unicast-маршрутизации выбирается один оптимальный маршрут. Среди трех оптимальных маршрутов в качестве маршрута RPF выбирается маршрут с самым длинным совпадением маски подсети

2.3.3. Настройка основных функций multicast IPv6

Создайте сеть PIM для предоставления сервиса multicast IPv6 для источников данных и пользовательских терминалов в сети.

2.3.3.1. Принцип работы

Устройство поддерживает таблицу маршрутизации, используемую для пересылки multicast-пакетов по протоколу multicast-маршрутизации IPv6 (например, PIM-SMv6), и получает информацию о статусе участников группы в сегментах сети с прямым подключением по протоколу MLDv1/v2. Хост присоединяется к определенной группе multicast IPv6, передавая сообщение MLD REPORT.

2.3.3.2. Сопутствующая конфигурация

Включение функции multicast-маршрутизации IPv6

Функция multicast-маршрутизации IPv6 по умолчанию отключена.

Запустите команду **ipv6 multicast-routing**, чтобы включить функцию multicast-маршрутизации IPv6.

Настройка протокола IP Multicast на интерфейсе

Протокол multicast IPv6 отключен на интерфейсе по умолчанию.

Запустите команду **ipv6 pim dense-mode**, чтобы включить протокол multicast IPv6 на интерфейсе.

2.3.4. Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации IPv6

Каждый пакет данных multicast, полученный устройством, используется для поддержания соответствующих записей маршрутизации multicast IPv6. Однако чрезмерное количество записей multicast-маршрутизации может привести к исчерпанию памяти устройства и снижению производительности устройства. Пользователи могут ограничить количество

записей в таблице multicast-маршрутизации IPv6 в зависимости от реальных условий сети и требований к производительности сервиса.

2.3.4.1. Принцип работы

Ограничьте количество записей в таблице multicast-маршрутизации IPv6 в зависимости от реальных условий сети и требований к производительности сервиса, чтобы поддерживать производительность устройства.

2.3.4.2. Сопутствующая конфигурация

Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации IPv6

По умолчанию в таблицу IP multicast-маршрутизации можно добавить 1024 записи.

Запустите команду **ipv6 multicast route-limit** *limit* [*threshold*], чтобы настроить количество записей, которые можно добавить в таблицу multicast-маршрутизации IPv6. Значение варьируется от 1 до 65 536.

Большее значение *limit* означает, что в таблицу multicast-маршрутизации IPv6 можно добавить больше записей, а меньшее значение *limit* означает, что в таблицу multicast-маршрутизации IPv6 можно добавить меньше записей.

2.3.5. Настройка границы multicast IPv6

Настройте границу multicast-маршрутизации IPv6, чтобы ограничить область передачи multicast-пакетов.

2.3.5.1. Принцип работы

Настройте границу multicast, чтобы указать область передачи multicast-пакетов. Если на интерфейсе настроена граница multicast-пересылки, multicast-пакеты, включая multicast-пакеты, отправленные локальным устройством, не могут быть перенаправлены или получены этим интерфейсом.

2.3.5.2. Сопутствующая конфигурация

Настройка границы multicast IPv6

По умолчанию граница multicast не настроена.

Запустите **ipv6 multicast boundary** *access-list-name* [**in** | **out**] для настройки границы multicast.

2.3.6. Настройка статической multicast-маршрутизации IPv6

Настройте статическую маршрутизацию multicast IPv6, чтобы указать интерфейс пересылки обратного пути (reverse path forwarding) (RPF) или соседа RPF для multicast-пакетов из определенного источника multicast.

2.3.6.1. Принцип работы

Проверка RPF проводится во время пересылки multicast-пакетов. Статическую multicast-маршрутизацию IPv6 можно настроить для указания интерфейса RPF или соседа RPF для multicast-пакетов из определенного источника multicast.

2.3.6.2. Сопутствующая конфигурация

Настройка статической multicast-маршрутизации IPv6

По умолчанию статическая маршрутизация multicast не настроена.

Запустите команду **ipv6 mroute** *ipv6-prefix/prefix-length* [**bgp** | **isis** | **ospfv3** | **ripng** | **static**] { *ipv6-prefix* | *interface-type interface-number* } [*distance*] для настройки статической multicast-маршрутизации IPv6.

2.3.7. Настройка управления направлением потока уровня 2 для multicast-потоков

Настройте управление направлением потока уровня 2 для multicast-потоков, чтобы контролировать поведение пересылки multicast-потоков на портах.

2.3.7.1. Принцип работы

Настройте управление направлением потока уровня 2 для потоков multicast, чтобы настроить порты, которым разрешено пересылать потоки multicast. Затем multicast-потоки пересылаются только через настроенные порты, тем самым управляя пересылкой multicast-потоков уровня 2.

2.3.7.2. Сопутствующая конфигурация

Настройка управления направлением потока уровня 2 для multicast-потоков

По умолчанию управление направлением потока уровня 2 отключено для multicast-потоков.

Запустите команду **ipv6 multicast static** *source-address group-address interface-type interface-number*, чтобы настроить управление направлением потока уровня 2 для потоков multicast.

2.3.8. Настройка выбора маршрута RPF по принципу самого длинного соответствия

Среди трех оптимальных маршрутов, выбранных из таблицы статической multicast-маршрутизации, таблицы маршрутизации протокола многопротокольного пограничного шлюза (MBGP) и таблицы unicast-маршрутизации, выберите оптимальный маршрут с самой длинной маской подсети как маршрут RPF.

2.3.8.1. Принцип работы

В соответствии с правилами RPF выберите статический маршрут multicast, маршрут MBGP и unicast-маршрут, используемые для проверки RPF, соответственно из таблицы статической multicast-маршрутизации, таблицы маршрутизации MBGP и таблицы unicast-маршрутизации.

- Если настроен выбор маршрута по принципу самого длинного соответствия, то в качестве маршрута RPF из трех маршрутов выбирается маршрут по соответствию самой длинной маски подсети. Если три маршрута имеют одну и ту же маску подсети, выбирается маршрут с наивысшим приоритетом. Если три маршрута имеют одинаковый приоритет, маршрут RPF выбирается в соответствии с последовательностью статического multicast-маршрута, маршрута MBGP и unicast-маршрута.
- Если не настроен выбор маршрута по принципу самого длинного соответствия, выбирается маршрут с наивысшим приоритетом. Если три маршрута имеют одинаковый приоритет, маршрут RPF выбирается в соответствии с последовательностью статического multicast-маршрута, маршрута MBGP и unicast-маршрута.

2.3.8.2. Сопутствующая конфигурация

Настройка выбора маршрута RPF по принципу самого длинного соответствия

По умолчанию в качестве маршрута RPF выбирается маршрут с наивысшим приоритетом. Если маршруты имеют одинаковый приоритет, маршрут RPF выбирается в соответствии с последовательностью статического multicast-маршрута, маршрута MBGP и unicast-маршрута.

Запустите команду **ipv6 multicast rpf longest-match**, чтобы настроить выбор маршрута RPF в соответствии с принципом самого длинного соответствия.

2.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций multicast IPv6	(Обязательно) Используется для создания сервиса multicast	
	ipv6 multicast-routing	Включает функцию multicast-маршрутизации IPv6
Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации IPv6	Опционально	
	ipv6 multicast route-limit *limit* [*threshold*]	Ограничивает количество записей, которые можно добавить в таблицу multicast-маршрутизации
Настройка границы multicast IPv66	**ipv6 multicast boundary** *access-list-name* [**in** | **out**]	Устанавливает интерфейс в качестве границы multicast определенного диапазона группы
Настройка статической multicast-маршрутизации IPv6	**ipv6 mroute** *ipv6-prefix/prefix-length* [*protocol*] { *v6rpf-addrress* | *interface-type interface-number* } [*distance*]	Настраивает статическую multicast-маршрутизацию IPv6
Настройка управления направлением потока уровня 2 для multicast-потоков	**ipv6 multicast static** *source-address group-address interface-type interface-number*	Управляет направлением потоков данных на портах уровня 2
Настройка выбора маршрута RPF по принципу самого длинного соответствия	**ipv6 multicast rpf longest-match**	Настраивает выбор маршрута RPF по принципу самого длинного соответствия

2.4.1. Настройка основных функций multicast IPv6

2.4.1.1. Эффект конфигурации

Создайте сеть PIM для предоставления сервиса multicast IPv6 для источников данных и пользовательских терминалов в сети.

2.4.1.2. Примечания

Сеть PIM должна использовать существующую unicast-маршрутизацию в сети. Поэтому в сети необходимо настроить unicast-маршрутизацию IPv6.

2.4.1.3. Шаги настройки

Включение функции multicast-маршрутизации IPv6

- Обязательный.
- Включите функцию multicast-маршрутизации IPv6 на каждом маршрутизаторе, если не указано иное.

Включение протокола IP Multicast на интерфейсах

- Обязательный.
- Включите функцию multicast-протокола IPv6 на интерфейсах, если не указано иное.

2.4.1.4. Проверка

Сделайте, чтобы источники multicast в сети отправляли multicast-пакеты, и хост пользователя присоединился к группам.

- Проверьте, может ли хост пользователя успешно получать пакеты из каждой группы.

2.4.1.5. Сопутствующие команды

Включение функции multicast-маршрутизации IPv6

Команда	**ipv6 multicast-routing**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Функция multicast-маршрутизации IPv6 должна быть включена до включения различных протоколов multicast IPv6. Функция multicast-маршрутизации IPv6 и функция MLD snooping являются взаимоисключающими

Настройка протоколов multicast IPv6

ПРИМЕЧАНИЕ: подробную информацию о методе настройки MLD см. в разделе Настройка MLD.

ПРИМЕЧАНИЕ: подробные сведения о методе настройки PIM-SMv6 см. в разделе Настройка PIM-SMv6.

ПРИМЕЧАНИЕ: после включения функции multicast уровня 3 в private VLAN и Super VLAN, если в sub-VLAN есть источник multicast, необходимо дополнительно скопировать запись с входом sub-VLAN, куда поступают multicast-потоки, потому что проверка достоверности

должна проводиться на входе во время пересылки multicast-пакета. В результате занята еще одна аппаратная запись multicast, и емкость multicast необходимо уменьшить на единицу.

Отображение информации таблицы multicast-пересылки

Команда	**show ipv6 mroute** [*group-or-source-address* [*group-or-source-address*]] [**sparse**] [**summary** | **count**]
Описание параметра	*group-or-source-address*: указывает адрес группы или адрес источника. *group-or-source-address*: указывает адрес группы или адрес источника. **sparse**: отображает запись ядра таблицы multicast-маршрутизации PIM-SMv6. **summary**: отображает сводку записей multicast-маршрутизации IPv6. **count**: отображает информацию о количестве записей multicast-маршрутизации IPv6
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации и режим конфигурации интерфейса

2.4.1.6. Пример конфигурации

Создание сервиса multicast IPv6 в сети IPv6 для поддержки PIMv6-SM

Сценарий:

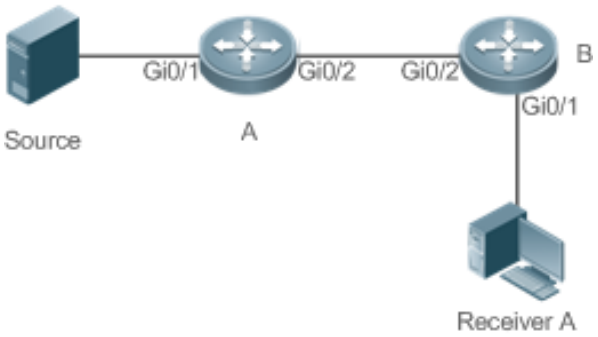

Рисунок 2-2.

Шаги настройки	• Настройте протокол unicast-маршрутизации IPv6 (например, OSPFv3) на маршрутизаторах. • Включите функцию multicast-маршрутизации IPv6 на всех маршрутизаторах. • Включите функцию PIMv6-SM на интерфейсах соединения устройств (device interconnection), интерфейсе подключения к пользовательскому хосту и интерфейсе подключения к источнику multicast
A	A# configure terminal A(config)# ipv6 multicast-routing

	A(config)# interface gigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ipv6 pim sparse-mode A(config-if)# exit A(config)# interface gigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#ipv6 pim sparse-mode A(config-if)# exit
B	B# configure terminal B(config)# ipv6 multicast-routing B(config)# interface gigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ipv6 pim sparse-mode B(config-if)# exit B(config)# interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)#ipv6 pim sparse-mode B(config-if)# exit
Проверка	Сделайте, чтобы источник multicast (2001::1) отправлял пакеты в G(ff16::16), и приемник A присоединился к G. • Проверьте multicast-пакеты, полученные приемником A. Приемник A должен иметь возможность получать multicast-пакеты от G. • Проверьте таблицу multicast-пересылки на приемнике A и устройстве B
A	A# show ipv6 mroute IPv6 Multicast Routing Table Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed, R - RPT, S - SPT, s - SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (2001::1, ff16::16), uptime 00:03:12, stat expires 00:02:03 Owner PIMSMV6, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2
B	B# show ipv6 mroute

	IPv6 Multicast Routing Table Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed, R - RPT, S - SPT, s - SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (2001::1, ff16::16), uptime 00:00:23, stat expires 00:03:07 Owner PIMSMV6, Flags: TFR Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1

2.4.1.7. Распространенные ошибки

- Unicast-маршрутизация IPv6 настроена неправильно.
- На маршрутизаторе не включена multicast-маршрутизация IPv6.
- На интерфейсе не включен протокол multicast IPv6.

2.4.2. Настройка количества записей, которые можно добавить в таблицу multicast-маршрутизации IPv6

2.4.2.1. Эффект конфигурации

Каждый пакет данных multicast, полученный устройством, используется для поддержания соответствующих записей маршрутизации multicast IPv6. Однако чрезмерное количество записей multicast-маршрутизации может привести к исчерпанию памяти устройства и снижению производительности устройства. Пользователи могут ограничить количество записей в таблице multicast-маршрутизации IPv6 в зависимости от реальных условий сети и требований к производительности сервиса.

2.4.2.2. Примечания

Необходимо настроить основные функции multicast IPv6.

2.4.2.3. Шаги настройки

Ограничьте количество записей в таблице multicast-маршрутизации IPv6 в зависимости от реальных условий сети и требований к производительности сервиса.

2.4.2.4. Проверка

Сделайте, чтобы источники multicast в сети отправляли multicast-пакеты в N различные группы multicast, и хост пользователя присоединился к этим группам. Установите количество записей, которые можно добавить в таблицу multicast-маршрутизации IPv6, равным N-1 на устройстве, и убедитесь, что multicast-пакеты, полученные хостом пользователя, принадлежат к группам N-1.

2.4.2.5. Связанные команды

Настройка количества записей, которые можно добавить в таблицу IP multicast-маршрутизации

Команда	**ipv6 multicast route-limit** *limit* [*threshold*]
Описание параметра	*limit*: указывает количество записей multicast-маршрутизации. Значение варьируется от 1 до 65 536, значение по умолчанию — 1 024. *threshold*: указывает количество записей multicast-маршрутизации для срабатывания сигнала предупреждения. Значение по умолчанию — 65 536
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Записи маршрутизации, выходящие за пределы допустимого аппаратного диапазона, могут пересылаться только программным обеспечением из-за ограничений аппаратных ресурсов, что приводит к ухудшению производительности

2.4.2.6. Пример конфигурации

Создание сервиса multicast IPv6 в сети IPv6 и настройка количества записей, которые можно добавить в таблицу маршрутизации multicast IPv6.

Сценарий:

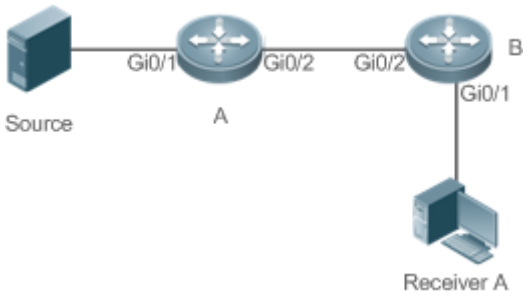

Рисунок 2-3.

Шаги настройки	• Настройте базовые функции IP multicast-маршрутизации (пропущено). • Установите количество записей, которые можно добавить в таблицу IP multicast-маршрутизации, равным 2 на устройстве B
B	B# configure terminal B(config)# ipv6 multicast route-limit 2

Проверка	Сделайте, чтобы источник multicast (2001: : 1) отправлял пакеты на G1(ff16::16), G2(ff16::17) и G3(ff16::18), и приемник A присоединился к G1, G2 и G3. • Проверьте multicast-пакеты, полученные приемником A. Приемник A должен иметь возможность получать multicast-пакеты из двух групп: G1, G2 и G3. • Проверьте записи multicast-маршрутизации на приемнике A и устройстве B. • Подсказка отображается, когда количество записей в таблице multicast-маршрутизации достигает верхнего предела
A	A# show ipv6 mroute IPv6 Multicast Routing Table Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed, R - RPT, S - SPT, s - SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (2001::1, ff16::16), uptime 00:01:01, stat expires 00:02:29 Owner PIMSMV6, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (2001::1, ff16::17), uptime 00:01:01, stat expires 00:02:29 Owner PIMSMV6, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (2001::1, ff16::18), uptime 00:00:57, stat expires 00:02:33 Owner PIMSMV6, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2

B	B# show ipv6 mroute IPv6 Multicast Routing Table Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed, R - RPT, S - SPT, s - SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (2001::1, ff16::16), uptime 00:00:29, stat expires 00:03:01 Owner PIMSMV6, Flags: TFR Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1 (2001::1, ff16::17), uptime 00:00:29, stat expires 00:03:01 Owner PIMSMV6, Flags: TFR Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1
Подсказка отображается, когда количество записей в таблице multicast-маршрутизации достигает верхнего предела	B#* Jan 3 21:40:07: %MROUTE-4-ROUTELIMIT: IPv6 Multicast route limit 2 exceeded

2.4.2.7. Распространенные ошибки

Unicast-маршрутизация IPv6 настроена неправильно.

2.4.3. Настройка границы multicast IPv6

2.4.3.1. Эффект конфигурации

Настройте границу IPv6 multicast-маршрутизации, чтобы ограничить область передачи multicast-пакетов.

2.4.3.2. Примечания

Необходимо настроить основные функции multicast IPv6.

2.4.3.3. Шаги настройки

Настройте границу IPv6 multicast-маршрутизации на каждом интерфейсе маршрутизатора PIM, если не указано иное.

2.4.3.4. Проверка

Сделайте, чтобы источники multicast отправляли multicast-пакеты в группы multicast, и хост пользователя присоединился к этим группам multicast. Настройте границу IPv6 multicast-маршрутизации на интерфейсе маршрутизатора PIM, подключенном к хосту пользователя, и проверьте, может ли хост пользователя получать multicast-пакеты.

2.4.3.5. Связанные команды

Включение функции multicast-маршрутизации IPv6

Команда	**ipv6 multicast boundary** *access-list-name* [**in** | **out**]
Описание параметра	*access-list-name*: использует диапазон адресов группы, определенный списком управления доступом (ACL). **in**: указывает, что граница multicast действует во входящем направлении multicast-потоков. **out**: указывает, что граница multicast действует в исходящем направлении multicast-потоков
Командный режим	Режим настройки интерфейса
Руководство по использованию	ACL, на который ссылается эта команда, может быть стандартным ACL или расширенным ACL. Если используется расширенный список ACL, необходимо сопоставить только адреса назначения. Эту команду можно использовать для фильтрации пакетов протоколов MLD и PIM-SMv6, относящихся к диапазону групп multicast IPv6. Потоки multicast-данных не передаются и не принимаются пограничными интерфейсами multicast

2.4.3.6. Пример конфигурации

Создание сервиса multicast IPv6 в сети IPv6 и настройка границы multicast IPv6

Сценарий:

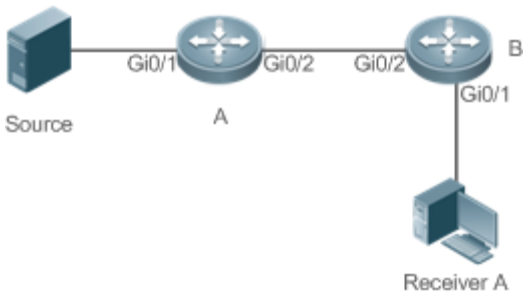

Рисунок 2-4.

Шаги настройки	• Настройте базовые функции IP multicast-маршрутизации (пропущено). • Настройте ACL на устройстве A. • Настройте границу IP multicast-маршрутизации на интерфейсе Gi0/1 устройства A
A	A# configure terminal A(config)# ipv6 access-list ip_multicast A(config-ipv6-acl)#deny udp any any A(config-ipv6-acl)#exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ip multicast boundary ip_multicast A A(config-if-GigabitEthernet 0/1)# exit
Проверка	Сделайте, чтобы источник multicast (192.168.1.100) отправлял пакеты в G (233.3.3.3), и приемник A присоединил к G. Запустите команду **debug ipv6 pim sparse-mode events**, чтобы отладить события multicast в режиме SM
A	A# debug ipv6 pim sparse-mode events Dec 28 11:54:07: %7: No cache message: src 2001::1 for ff16::16 vif 1 *Dec 28 11:54:07: %7: Ignore No cache message: src 2001::1 for ff16::16 vif 1 in PIM6_BOUNDARY_FLT_BOTH range

2.4.3.7. Распространенные ошибки

Unicast-маршрутизация IPv6 настроена неправильно.

2.4.4. Настройка статической multicast-маршрутизации IPv6

2.4.4.1. Эффект конфигурации

Настройте статическую маршрутизацию multicast IPv6, чтобы указать интерфейс RPF или соседа RPF для multicast-пакетов из определенного источника multicast.

2.4.4.2. Примечания

Необходимо настроить основные функции multicast IPv6.

2.4.4.3. Шаги настройки

Настройте статическую multicast-маршрутизацию IPv6 на каждом устройстве, если не указано иное.

2.4.4.4. Проверка

Настройте статическую маршрутизацию multicast IPv6, а затем запустите команду **show ipv6 rpf** *v6source-address*, чтобы проверить информацию RPF о конкретном источнике multicast.

2.4.4.5. Связанные команды

Настройка статической multicast-маршрутизации IPv6

Команда	**ipv6 mroute** *ipv6-prefix/prefix-length* [*protocol*] { *v6rpf-addrress* | *interface-type interface-number* } [*distance*]
Описание параметра	*ipv6-prefix*: указывает IPv6-адрес источника multicast. *prefix-length*: указывает маску подсети IPv6-адреса источника multicast. *protocol*: указывает протокол unicast-маршрутизации, который используется в данный момент. *v6rpf-addrress*: указывает адрес IPv6 соседа RPF (next hop к источнику multicast). *interface-type interface-number*: указывает интерфейс RPF (исходящий интерфейс к источнику multicast). *distance*: указывает расстояние управления маршрутом. Значение варьируется от 0 до 255, значение по умолчанию — 0
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Статическая multicast-маршрутизация IPv6 используется только для проверки RPF. Чтобы указать исходящий интерфейс, а не IP-адрес next-hop-а статической multicast-маршрутизации IPv6, исходящий интерфейс должен иметь тип «точка-точка» (point-to-point)

Отображение информации RPF об определенном адресе источника

Команда	**show ipv6 rpf** *v6source-address*
Описание параметра	*v6source-address*: указывает адрес источника IPv6
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации и режим конфигурации интерфейса

2.4.4.6. Пример конфигурации

Создание сервиса multicast IPv6 в сети IPv6 и настройка статической маршрутизации multicast IPv6

Сценарий:

Рисунок 2-5.

Шаги настройки	• Настройте основные функции multicast IPv6 (пропущено). • Настройте статический маршрут к приемнику на устройстве B
A	B# configure terminal B(config)# ipv6 mroute 2005::/64 ospfv3 2002::2
Проверка	Запустите команду **show ipv6 rpf**, чтобы отобразить информацию RPF, полученную приемником до и после настройки
Перед настройкой	B# show ipv6 rpf 2005::1 RPF information for 2005::1 RPF interface: GigabitEthernet 0/1 RPF neighbor: fe80::2d0:f8ff:fe22:341b RPF route: 2005::1/128 RPF type: unicast (ospf) RPF recursion count: 0 Doing distance-preferred lookups across tables Distance: 110 Metric: 1
После настройки	B# show ipv6 rpf 2005::1 RPF information for 2005::1 RPF interface: GigabitEthernet 0/2 RPF neighbor: 2002::2 RPF route: 2005::/64 RPF type: unicast (ospf) RPF recursion count: 0 Doing distance-preferred lookups across tables Distance: 110 Metric: 1

2.4.4.7. Распространенные ошибки

- Unicast-маршрутизация IPv6 настроена неправильно.
- На маршрутизаторе не включена multicast-маршрутизация IPv6.

2.4.5. Настройка управления направлением потока уровня 2 для multicast-потоков

2.4.5.1. Эффект конфигурации

Настройте управление направлением потока уровня 2 для multicast-потоков, чтобы контролировать поведение пересылки multicast-потоков на портах.

2.4.5.2. Примечания

Необходимо настроить основные функции multicast IPv6.

2.4.5.3. Шаги настройки

Настройте управление направлением потока уровня 2 для multicast-потоков на устройствах, если не указано иное.

2.4.5.4. Проверка

Сделайте, чтобы устройство A отправляло multicast-пакеты группам multicast в сети. Несколько пользовательских хостов, подключенных к VLAN 1 устройства A, получают multicast-пакеты от этих групп multicast. Настройте управление направлением потока уровня 2 для потоков multicast на устройстве A, чтобы multicast-пакеты отправлялись на настроенные порты.

2.4.5.5. Связанные команды

Настройка управления направлением потока уровня 2 для multicast-потоков

Команда	**ipv6 multicast static** *source-address group-address interface-type interface-number*
Описание параметра	*source-address*: указывает адрес источника multicast. *group-address*: указывает адрес группы multicast. *interface-type interface-number*: указывает порт уровня 2, которому разрешено пересылать multicast-потоки
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Для multicast-потока можно настроить несколько команд, то есть нескольким портам можно разрешить пересылку multicast-потока. Если управление направлением потока настроено для multicast-потока, multicast-поток может пересылаться только через настроенные порты. Другим портам не разрешено пересылать multicast-поток. Эта команда контролирует только поведение пересылки multicast-потоков на портах. Это не влияет напрямую на обработку пакетов протоколов multicast-протоколами. Некоторые функции протоколов multicast (например, PIM-SMv6) управляются потоками multicast-данных, поэтому на поведение протоколов multicast-маршрутизации все равно может влиять

2.4.5.6. Пример конфигурации

Создание сервиса multicast IPv6 в сети IPv6 и настройка управления направлением потока уровня 2 для потоков multicast

Сценарий:

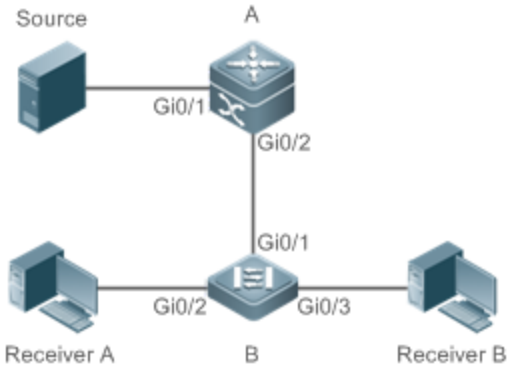

Рисунок 2-6.

Шаги настройки	• Настройте базовые функции IP multicast-маршрутизации (пропущено). • Настройте управление направлением потока уровня 2 для multicast-потоков на устройстве B так, чтобы multicast-потоки передавались только на интерфейс Gi0/2
B	A# configure terminal A(config)# ipv6 multicast static 2001::1 ff16::16 gigabitEthernet 0/2
Проверка	Сделайте, чтобы источник multicast (2001: : 1) отправлял пакеты в G (ff16::16), и приемник A, и приемник B присоединились к G. Приемник A должен иметь возможность получать multicast-пакеты от G, но приемник B не может получать multicast-пакеты от G

2.4.5.7. Распространенные ошибки

Unicast-маршрутизация IPv6 настроена неправильно.

2.4.6. Настройка выбора маршрута RPF по принципу самого длинного соответствия

2.4.6.1. Эффект конфигурации

Среди трех оптимальных маршрутов, выбранных из таблицы статической multicast-маршрутизации, таблицы маршрутизации MBGP и таблицы unicast-маршрутизации, выберите оптимальный маршрут с самой длинной маской подсети, совпадающей с маршрутом RPF.

2.4.6.2. Примечания

Необходимо настроить основные функции IP multicast-маршрутизации.

2.4.6.3. Шаги настройки

Настройте выбор маршрута RPF по принципу самого длинного соответствия на каждом устройстве, если не указано иное.

2.4.6.4. Проверка

Настройте статический маршрут multicast и статический маршрут unicast-рассылки с одинаковым приоритетом, а также настройте статический маршрут unicast-рассылки так, чтобы он имел самое длинное соответствие маски подсети.

- Запустите команду **show ipv6 rpf v6source-address**, чтобы проверить информацию RPF о конкретном источнике.

2.4.6.5. Связанные команды

Настройка выбора маршрута RPF по принципу наибольшего соответствия

Команда	**ipv6 multicast rpf longest-match**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Шаги выбора маршрута RPF следующие: Выберите один оптимальный маршрут, используемый для проверки RPF, из каждой таблицы статической маршрутизации multicast IPv6, таблицы маршрутизации IPv6 MBGP и таблицы unicast-маршрутизации IPv6. Выберите один маршрут из трех оптимальных в качестве маршрута RPF. Если настроена команда выбора маршрута RPF по принципу самого длинного соответствия, то из трех оптимальных маршрутов в качестве маршрута RPF выбирается маршрут с самым длинным совпадением маски подсети. Если три маршрута имеют одну и ту же маску подсети, выбирается маршрут с наивысшим приоритетом. Если маршруты имеют одинаковый приоритет, маршрут RPF выбирается в соответствии с последовательностью статического маршрута multicast IPv6, маршрута MBGP IPv6 и unicast-маршрута IPv6. Если не настроена команда выбора маршрута RPF по принципу наибольшего соответствия, то из трех оптимальных маршрутов в качестве маршрута RPF выбирается маршрут с наивысшим приоритетом. Если маршруты имеют одинаковый приоритет, маршрут RPF выбирается в соответствии с последовательностью статического маршрута multicast IPv6, маршрута MBGP IPv6 и unicast-маршрута IPv6

2.4.6.6. Пример конфигурации

Создание сервиса multicast IPv6 в сети IPv6 и настройка выбора маршрута RPF по принципу самого длинного соответствия

Сценарий:

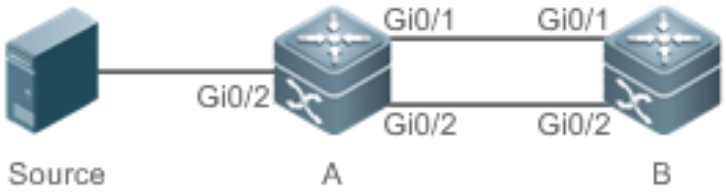

Рисунок 2-7.

Шаги настройки	• Настройте базовые функции IP multicast-маршрутизации (пропущено). • Настройте статический multicast-маршрут IPv6 с длиной маски подсети меньшей, чем соответствующая длина маски у unicast-маршрута на устройстве B. • Настройте выбор маршрута RPF по принципу самого длинного соответствия на Устройстве B
B	B# configure terminal B(config)# ipv6 multicast-routing B(config)# ipv6 mroute 2005::/64 ospfv3 2002::2 B(config)# ipv6 multicast rpf longest-match
Проверка	Запустите команду **show ipv6 rpf**, чтобы отобразить информацию RPF об источнике multicast до и после настройки выбора маршрута RPF по принципу самого длинного соответствия
Перед настройкой	B# show ipv6 rpf 2005::1 RPF information for 2005::1 RPF interface: GigabitEthernet 0/2 RPF neighbor: 2002::2 RPF route: 2005::/64 RPF type: unicast (ospf) RPF recursion count: 0 Doing distance-preferred lookups across tables Distance: 110 Metric: 1
После настройки	B# show ipv6 rpf 2005::1

	RPF information for 2005::1 RPF interface: GigabitEthernet 0/1 RPF neighbor: fe80::2d0:f8ff:fe22:341b RPF route: 2005::1/128 RPF type: unicast (ospf) RPF recursion count: 0 Doing distance-preferred lookups across tables Distance: 110 Metric: 1

2.4.6.7. Распространенные ошибки

- Unicast-маршрутизация IPv6 настроена неправильно.
- На маршрутизаторе не включена multicast-маршрутизация IPv6.

2.5. Мониторинг

2.5.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере важной информации и, таким образом, к прерыванию работы сервисов.

Описание	Команда
Очищает таблицу multicast-пересылки IPv6	**clear ipv6 mroute** { ***** | *v6group-address* [*v6source –address*] }
Очищает статистику в таблице multicast-пересылки IPv6	**clear ipv6 mroute statistics** { ***** | *v6group-address* [*v6source-address*] }

2.5.2. Отображение

Описание	Команда
Отображает информацию таблицы multicast-пересылки IPv6	**show ipv6 mroute** [*group-or-source-address* [*group-or-source-address*]] [**sparse**] [**summary** | **count**]
Отображает информацию RPF об определенном адресе IPv6 источника	**show ipv6 rpf** *v6source-address*
Отображает информацию о статическом multicast-маршруте IPv6	**show ipv6 mroute static**

Описание	Команда
Отображает информацию о настроенном multicast-интерфейсе IPv6, который вступает в силу	**show ipv6 mvif** [*interface-type interface-number*]
Отображает таблицу multicast-пересылки IPv6 уровня 3	**show ipv6 mrf mfc**
Отображает таблицу многоуровневой multicast-пересылки IPv6	**show msf6 msc**

2.5.3. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Поэтому отключайте отладку сразу после использования.

Описание	Команда
Отладка всех запущенных процессов multicast IPv6	**debug nsm mcast6 all**
Отладка связи между multicast-рассылкой IPv6 и модулем протокола	**debug nsm mcast6 fib-msg**
Отладка интерфейса multicast IPv6	**debug nsm mcast6 mif**
Отладка обработки интерфейсов и статистики поведения multicast IPv6	**debug nsm mcast6 stats**
Отладка multicast-пересылки уровня 3 IPv6	**debug ipv6 mrf forwarding**
Отладка процесса работы записей multicast-пересылки IPv6 уровня 3	**debug ipv6 mrf mfc**
Отладка обработки событий multicast-пересылки IPv6 уровня 3	**debug ipv6 mrf event**
Отладка пересылки многоуровневых multicast-пакетов IPv6	**debug msf6 forwarding**
Отладка процесса работы записей многоуровневой multicast-пересылки IPv6	**debug msf6 mfc**

Описание	Команда
Отладка базового оборудования для многоуровневой multicast-пересылки IPv6	**debug msf6 ssp**
Отладка API для многоуровневой multicast-пересылки IPv6	**debug msf6 api**
Отладка обработки событий многоуровневой multicast-пересылки IPv6	**debug msf6 event**

3. НАСТРОЙКА IGMP

3.1. Обзор

Internet Group Management Protocol (IGMP) является членом семейства протоколов TCP/IP. Он управляет участниками multicast IP и используется для установления и поддержания членства в группах multicast между хостами и непосредственно соседними маршрутизаторами multicast. Поведение IGMP подразделяется на поведение хоста и поведение устройства.

- В настоящее время доступны три версии IGMP: IGMPv1, IGMPv2 и IGMPv3.
- Все версии IGMP поддерживают модель Any-Source Multicast (ASM).
- IGMPv3 можно напрямую использовать для модели Source-Specific Multicast (SSM).
- IGMPv1 и IGMPv2 можно использовать для модели SSM только в том случае, если поддерживается технология сопоставления IGMP SSM.

3.1.1. Протоколы и стандарты

- RFC 1112: расширения хоста для IP multicast-маршрутизации.
- RFC 2236: протокол управления интернет-группами, версия 2.
- RFC 3376: протокол управления интернет-группами, версия 3.
- RFC 4605: протокол управления группами Интернета (IGMP)/Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying").

3.2. Приложения

Приложение	Описание
Локальный сервис IGMP	Реализует сервис IGMP в локальной сети
Прокси-сервис IGMP	В простой древовидной топологии сети используйте прокси-сервис IGMP вместо сервиса PIM

3.2.1. Локальный сервис IGMP

3.2.1.1. Сценарий

Как показано на Рисунке 3-1, приемники 1 и 2 и маршрутизаторы A и B образуют локальную сеть.

Пакеты запросов, отправленные маршрутизатором A или B, действительны в локальной сети, тогда как пакеты Report, отправленные получателями 1 и 2, также действительны локально.

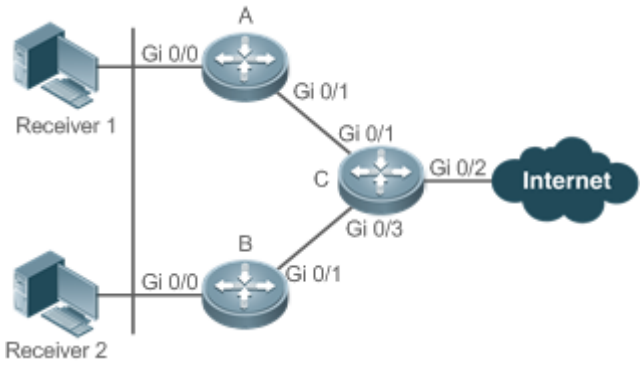

Рисунок 3-1.

C — устройство выходного шлюза (EG).

A и B — основные маршрутизаторы.

3.2.1.2. Развертывание

- Маршрутизаторы A, B и C используют OSPF.
- Интерфейсы A, B и C используют протоколы multicast (PIM-SM или PIM-DM).

3.2.2. Прокси-сервис IGMP

3.2.2.1. Сценарий

Как показано на Рисунке 3-2 Маршрутизатор A реализует функцию прокси, работая в качестве хоста, и образует локальную сетевую группу с маршрутизатором B. Маршрутизатор A пересылает пакеты Report, отправленные приемниками 1 и 2.

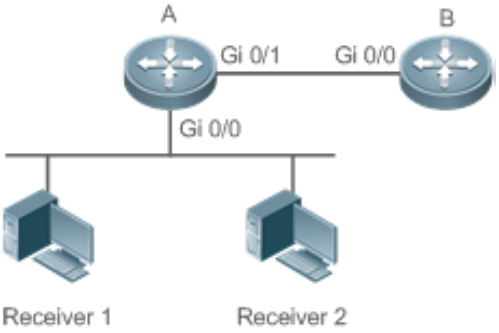

Рисунок 3-2.

Маршрутизатор A реализует функцию прокси.

Маршрутизатор B предоставляет службу PIM.

3.2.2.2. Развертывание

- Маршрутизаторы A и B используют OSPF.
- Интерфейсы A и B используют протоколы multicast (PIM-SM или PIM-DM).
- Функция multicast-прокси реализована на интерфейсах Gi0/0 и Gi0/1 маршрутизатора A.

3.3. Функции

3.3.1. Базовые определения

Поведение хоста и поведение устройства

- Устройства multicast уровня 3, на которых используются протоколы управления multicast-рассылкой, называются устройствами, а их поведение — поведением устройства.
- ПК или смоделированные ПК, на которых используются протоколы управления multicast-рассылкой, называются хостами, а их поведение — поведением хоста.

Querier

Устройства конкурируют друг с другом, сравнивая IP-адреса. Устройства с более низкими IP-адресами становятся Querier и регулярно отправляют пакеты Query.

Интерфейс прокси-сервиса IGMP

Этот интерфейс выполняет действия хоста, получает пакеты Query, отправленные upstream-устройствами (поэтому также называется uplink-интерфейсом), и отправляет Report с информацией, собранной прокси-сервером маршрутизатора.

Интерфейс IGMP Mroute–Proxy

Этот интерфейс реализует функции маршрутизатора, отправляет пакеты, полученные интерфейсом IGMP PROXY-SERVICE (поэтому также называется downlink-интерфейсом), собирает информацию о хосте и отправляет информацию о хосте на интерфейс IGMP PROXY-SERVICE.

Сопоставление IGMP SSM

Сопоставление модели SSM. IGMPv1 и IGMPv2 не поддерживают модель SSM, но могут включить функцию SSM-MAP для поддержки модели SSM.

3.3.1.1. Обзор

Особенность	Описание
IGMP-маршрутизатор	Отправляет пакеты Query и получает информацию о локальных участниках
IGMP Querier	Выбирает уникальный Querier из сегмента сети
Групповая фильтрация IGMP	Фильтрует участников группы и ограничивает количество участников группы
Статическая группа IGMP	Статическая информация о группе доступна на маршрутизаторе; поэтому хосту нет необходимости отправлять пакет Report для получения информации о статической группе
Имитация хостов для присоединения к группам IGMP	Имитируйте поведение хоста для прямого присоединения к группе multicast на интерфейсе

Особенность	Описание
IGMP-прокси	Используйте эту функцию в простой древовидной топологии сети, где не требуется выполнять сложные протоколы multicast-маршрутизации (например, PIM)
Сопоставление IGMP SSM	Обеспечьте поддержку модели SSM для IGMPv1 и IGMPv2. Когда хост присоединяется к группе, вы можете указать источник, чтобы сэкономить полосу пропускания и предотвратить занятие пропускной способности сети нежелательными и недействительными потоками multicast-данных, особенно в сетевой среде, где несколько источников multicast используют один адрес multicast

3.3.2. IGMP-маршрутизатор

Эта функция используется для отправки пакетов Query и получения информации о локальных участниках.

3.3.2.1. Принцип работы

- В multicast-сети, использующей IGMP, multicast-устройство периодически отправляет пакеты IGMP Query и подтверждает информацию о локальных участниках на основе ответов.
- Только одно multicast-устройство отправляет пакеты IGMP Query в одном сегменте сети, и это устройство называется Querier. Querier определяется путем выбора. Изначально все устройства multicast находятся в состоянии Querier. Когда устройство получает Query на участие от устройства с меньшим IP-адресом, устройство переходит из состояния «Querier» в состояние «Non-querier». Таким образом, только одно устройство окончательно находится в состоянии Quierer. Это устройство имеет самый низкий IP-адрес среди всех multicast-устройств в сети.
- Querier отправляет пакеты IGMP разных версий в зависимости от настроек версии IGMP. Кроме того, можно изменить следующие параметры Querier: частота отправки Querier-ом пакетов IGMP Query, время Query и интервал Query для последнего участника, максимальное время ответа пакетов IGMP Query и время keepalive текущего Querier.

3.3.2.2. Сопутствующая конфигурация

Включение IGMP

IGMP отключен на интерфейсе по умолчанию.

Вы можете запустить команду **ip pim** { **sparse-mode**| **dense-mode** } для включения или отключения IGMP для интерфейса.

IGMP можно включить только в том случае, если на интерфейсе настроен режим Sparse (SM) или режим Dense (DM).

Указание версии IGMP

IGMPv2 включен по умолчанию.

Вы можете запустить команду **ip igmp version** { **1** | **2** | **3** } для установки или сброса версии IGMP.

Настройка интервала Query последнего участника

Интервал отправки пакетов Query последнего участнкиа по умолчанию составляет 1 секунду.

Вы можете запустить команду **ip igmp last-member-query-interval** *interval*, чтобы установить или сбросить интервал для интерфейса для отправки пакетов Query.

Большее значение означает больший интервал; меньшее значение означает меньший интервал.

Настройка количества Query последнего участника

По умолчанию количество Query последнего участника равно 2.

Вы можете запустить команду **ip igmp last-member-query-count** *count*, чтобы установить или сбросить количество Query последнего участника.

Большее значение означает большее количество Query последнего элемента; меньшее значение означает меньшее количества Query последнего участика.

Настройка интервала Query общего участника

По умолчанию интервал Query общего участника составляет 125 секунд.

Вы можете запустить команду **ip igmp query-interval** *seconds*, чтобы установить или сбросить интервал Query общего участника.

Большее значение означает больший общий интервал Query; меньшее значение означает меньший общий интервал Query.

Настройка максимального времени ответа

По умолчанию максимальное время ответа составляет 10 секунд.

Вы можете запустить команду **ip igmp query-max-response-time** *seconds*, чтобы установить или сбросить максимальное время ответа.

Большее значение означает более длительное время ответа; меньшее значение означает более короткое время отклика.

3.3.3. IGMP Querier

Выберите уникальный Querier из сегмента сети. Querier отправляет пакеты Query для получения групповой информации локальной сети.

3.3.3.1. Принцип работы

В multicast-сети, использующей протокол IGMP, для отправки пакетов запросов IGMP указывается устройство multicast. Это устройство определяется путем выбора. Вначале все устройства находятся в состоянии Quierer. Когда устройства получают Query на участие от устройства с меньшим IP-адресом, устройства переходят из состояния «Querier» в состояние «Non-querier». Таким образом, только одно устройство окончательно находится в состоянии Quierer. Это устройство имеет самый низкий IP-адрес среди всех multicast-устройств в сети. Если выбранный Querier терпит неудачу, IGMPv2 также работает. Устройства Non-querier, поддерживают интервальный таймер для выживания Querier. Этот таймер сбрасывается каждый раз, когда устройство получает пакет Query на участие. Если время таймера истекает, начинается новый раунд выбора Querier.

3.3.3.2. Сопутствующая конфигурация

Настройка тайм-аута Querier

По умолчанию тайм-аут Querier составляет 255 секунд.

Вы можете запустить команду **ip igmp query-timeout** *seconds*, чтобы установить тайм-аут Querier.

Большее значение означает более длительное время выживания; меньшее значение означает более короткое время выживания.

3.3.4. Групповая фильтрация IGMP

Фильтруйте участников группы и ограничивайте количество участников группы.

3.3.4.1. Принцип работы

Чтобы запретить хостам в сегменте сети, где находится интерфейс, присоединяться к группе multicast, вы можете настроить ACL на этом интерфейсе в качестве фильтра. Интерфейс будет фильтровать полученные пакеты Report IGMP об участие на основе этого ACL, поддерживать участие в группе только для групп multicast, разрешенных этим ACL, и устанавливать максимальное количество участников маршрутизатора.

3.3.4.2. Сопутствующая конфигурация

Настройка ACL группы IGMP

По умолчанию ACL не используется, и любая группа может присоединиться.

Вы можете запустить команду **ip igmp access-group** *access-list-name*, чтобы установить или сбросить ACL группы multicast.

После настройки ACL маршрутизатор получает только пакеты, указанные в ACL.

Настройка максимального количества участников группы IGMP

По умолчанию максимальное количество участников группы IGMP составляет 1024.

Вы можете запустить команду **ip igmp limit** *number*, чтобы установить или сбросить максимальное количество участников группы multicast.

Большее значение означает больше участников; меньшее значение означает меньшее количество участников.

3.3.5. Статическая группа IGMP

Если на маршрутизаторе доступны статические группы IGMP, хосту нет необходимости отправлять пакет Report для получения информации о статической группе. Маршрутизатор может напрямую обмениваться информацией о группе с маршрутизатором PIM.

3.3.5.1. Принцип работы

Вам необходимо установить информацию о статической группе вручную.

3.3.5.2. Сопутствующая конфигурация

Настройка статической группы

По умолчанию статическая группа не настроена.

Вы можете запустить команду **ip igmp static-group** *group-address*, чтобы настроить статическую группу.

3.3.6. Имитация хостов для присоединения к группам IGMP

Имитируйте поведение хоста для прямого присоединения к группе multicast на интерфейсе.

3.3.6.1. Сопутствующая конфигурация

Настройка функции присоединения к группе

По умолчанию информация о присоединеним к группе не установлена.

Вы можете запустить команду **ip igmp join-group** *group-address*, чтобы настроить адрес группы multicast, к которой должен присоединиться имитируемый хост.

3.3.7. IGMP-прокси

Используйте эту функцию в простой древовидной топологии сети, где не требуется выполнять сложные протоколы multicast-маршрутизации (например, PIM). Таким образом, downstream прокси-хост может отправлять пакеты IGMP и поддерживать участие.

3.3.7.1. Принцип работы

Когда upstream-маршрутизатор настроен как интерфейс прокси-сервиса IGMP, он равен хосту, который может получать пакеты Query, отправленные upstream-маршрутизаторами, или пересылать групповую информацию, отправленную downstream-хостами. Когда downstream-маршрутизатор настроен как прокси-интерфейс multicast IGMP, он приравнивается к маршрутизатору, который может пересылать пакеты Query, отправленные upstream-маршрутизаторами, или получать пакеты Report, отправленные downstream-маршрутизаторами.

3.3.7.2. Сопутствующая конфигурация

Настройка прокси-сервиса IGMP

Функция прокси-сервиса IGMP по умолчанию отключена.

Вы можете запустить команду **ip igmp proxy-service**, чтобы включить прокси-сервис IGMP.

Эта функция является обязательной при использовании прокси.

Настройка IGMP Mroute Proxy

Функция IGMP Mroute Proxy отключена по умолчанию.

Вы можете запустить команду **ip igmp mroute-proxy** *interfacename*, чтобы включить IGMP Mroute Proxy.

Эта функция является обязательной при использовании прокси.

3.3.8. Сопоставление IGMP SSM

Обеспечьте поддержку модели SSM для IGMPv1 и IGMPv2. Когда хост присоединяется к группе, вы можете указать источник, чтобы сэкономить полосу пропускания и предотвратить занятие пропускной способности сети нежелательными и недействительными потоками multicast-данных, особенно в сетевой среде, где несколько источников multicast используют один адрес multicast.

3.3.8.1. Принцип работы

Основанный на IGMP v1/v2, IGMPv3 предоставляет дополнительную функцию, а именно функцию фильтра источника multicast. В IGMPv1/v2 хост решает присоединиться к группе только на основе адреса группы, а затем получает потоки multicast, отправленные на этот групповой адрес из любого источника. Хост, использующий IGMPv3, объявляет группу multicast, к которой хочет присоединиться хост, и адреса источников multicast, от которых этот хост хочет получать пакеты. IGMPv1 и IGMPv2 также в некотором смысле реализуют «фильтрацию исходных адресов»; однако они реализуют эту функцию на приемниках

multicast, включив функцию сопоставления SSM и настроив статическую группу сопоставления SSM.

3.3.8.2. Сопутствующая конфигурация

Включение сопоставления IGMP SSM

Функция сопоставления SSM отключена по умолчанию.

Вы можете запустить команду **ip igmp ssm-map enable**, чтобы включить эту функцию.

Обязательный.

Настройка статического сопоставления IGMP SSM

По умолчанию статическое сопоставление SSM не установлено.

Вы можете запустить команду **ip igmp ssm-map static** *access-list-num A.B.C.D*, чтобы настроить статическое сопоставление SSM.

3.3.9. Опция Router Alert (оповещения маршрутизатора)

Проверьте, содержат ли пакеты IGMP опцию Router Alert (оповещения маршрутизатора), и отбросьте пакеты без опции Router Alert.

Поддерживает отправку пакетов IGMP, содержащих опцию Router Alert.

3.3.9.1. Принцип работы

Если пакет содержит опцию Router Alert, устройству необходимо тщательно проверить пакет и соответствующим образом обновить управляющие данные. Если пакет не содержит опции, устройство не проверяет пакет.

После включения проверки опции Router Alert пакеты IGMP, не содержащие опцию Router Alert, отбрасываются.

После включения функции отправки пакетов с опцией Router Alert устройство отправляет пакеты IGMP с инкапсулированной опцией Router Alert.

3.3.9.2. Сопутствующая конфигурация

Проверка опции Router Alert

Проверка опции Router Alert отключена по умолчанию.

Вы можете запустить команду **ip igmp enforce-router-alert**, чтобы включить эту функцию.

Отправка пакетов IGMP с инкапсулированной опцией Router Alert

По умолчанию пакеты отправляются без опции Router Alert.

Вы можете запустить команду **ip igmp send-router-alert**, чтобы включить эту функцию.

3.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций IGMP	(Обязательно) Используется для настройки услуги multicast	
	ip multicast-routing	Включает функцию multicast-маршрутизации IPv4

Конфигурация	Описание и команда	
Настройка основных функций IGMP	**ip pim** { **sparse-mode**| **dense-mode** }	Включает функцию PIM-SM или PIM-DM
Настройка маршрутизаторов IGMP	**ip igmp version** { **1** | **2** | **3** }	Указывает версию IGMP
	ip igmp last-member-query-interval *interval*	Настраивает интервал Query последнего участника
	ip igmp last-member-query-count *count*	Настраивает время Query последнего участника
	ip igmp query-interval *seconds*	Настраивает интервал Query участия
	ip igmp query-max-response-time *seconds*	Настраивает максимальное время ответа
Настройка IGMP Querier	**ip igmp query-timeout** *seconds*	Настраивает тайм-аут Querier
Настройка фильтрации группы IGMP	**ip igmp access-group** *access-list*	Настраивает ACL группы IGMP
	ip igmp limit *number* [**except** *access-list*]	Настраивает максимальное количество участников группы IGMP
Настройка IGMP-прокси	**ip igmp proxy-service**	Настраивает прокси-сервис IGMP
	ip igmp mroute-proxy *interface-type interface-number*	Настраивает прокси-сервер IGMP mroute
Настройка сопоставления IGMP SSM	**ip igmp ssm-map enable**	Включает сопоставление IGMP SSM
	ip igmp ssm-map static *access-list source-address*	Настраивает статическое сопоставление IGMP SSM
Настройка опции оповещения	**ip igmp enforce-router-alert**	Проверяет параметр Router Alert
	ip igmp send-router-alert	Отправляет пакеты IGMP, содержащие опцию Router Alert

3.4.1. Настройка основных функций IGMP

3.4.1.1. Эффект конфигурации

Включите функцию multicast-маршрутизации локальной сети и соберите информацию о группах локальной сети.

3.4.1.2. Примечания

Интерфейс должен быть активирован с функцией PIM-SM или PIM-DM.

3.4.1.3. Шаги настройки

Включение функции multicast-маршрутизации IPv4

- Обязательный.
- Если нет особых требований, функция multicast-маршрутизации IPv4 должна быть включена на каждом маршрутизаторе в локальной сети.

Включение функции PIM-SM или PIM-DM

- Обязательный.
- Если нет особых требований, функцию PIM-SM или PIM-DM следует включить непосредственно на интерфейсе локальной сети.

3.4.1.4. Проверка

Запустите команду **show ip igmp interface** *interface-type interface-number*, чтобы проверить, включен ли IGMP на интерфейсе.

3.4.1.5. Связанные команды

Включение функции multicast-маршрутизации IPv4

Команда	**ip multicast-routing**
Командный режим	Режим глобальной конфигурации

Включение функции PIM-SM или PIM-DM

Команда	**ip pim** { **sparse-mode**| **dense-mode** }
Командный режим	Режим настройки интерфейса
Руководство по использованию	PIM-интерфейсы должны быть интерфейсами уровня 3, включая интерфейсы маршрутизации, L3AP, SVI и loopback-интерфейсы. Все PIM-интерфейсы должны быть доступны для unicast-маршрутов IPv4

3.4.1.6. Пример конфигурации

Включение IGMP для локальной сети

Сценарий	• Настройте протокол unicast-маршрутизации IPv4 (например, OSPF) на маршрутизаторе и убедитесь, что loopback-интерфейс доступен для unicast-маршрута. • Включите функцию multicast-маршрута IPv4 на всех маршрутизаторах. • Включите функцию PIM-SM или PIM-DM на интерфейсах, соединяющих устройства, и интерфейсах, соединяющих пользовательские хосты и источники multicast
	QTECH(config)#ip multicast-routing QTECH(config)#int gi 0/5 QTECH(config-if-GigabitEthernet 0/5)#ip add 192.168.1.90 255.255.255.0 QTECH(config-if-GigabitEthernet 0/5)#ip pim sparse-mode
Проверка	Запустите команду **show ip igmp interface** *interface-type interface-number*, чтобы проверить, включен ли IGMP на интерфейсе
	QTECH#show ip igmp interface gigabitEthernet 0/5 Interface GigabitEthernet 0/5 (Index 5) IGMP Active, Querier, Version 2 (default) Internet address is 192.168.1.90 IGMP interface limit is 1024 IGMP interface has 1 group-record states IGMP interface has 0 static-group records IGMP activity: 3 joins, 0 leaves IGMP query interval is 125 seconds IGMP querier timeout is 255 seconds IGMP max query response time is 10 seconds Last member query response interval is 10 Last member query count is 2 Group Membership interval is 260 seconds Robustness Variable is 2

3.4.1.7. Распространенные ошибки

- Маршрутизаторы в сети не поддерживают функцию multicast-маршрутизации.
- В сети нет интерфейса multicast.

3.4.2. Настройка маршрутизаторов IGMP

3.4.2.1. Эффект конфигурации

Изменение параметров маршрутизатора IGMP повлияет на тип отправляемых пакетов, метод отправки и интервал keealive.

3.4.2.2. Примечания

Необходимо настроить основные функции IGMP.

3.4.2.3. Шаги настройки

Указание версии IGMP

Необязательный.

Если нет особых требований, вы можете выполнить эту настройку на всех интерфейсах маршрутизатора, напрямую подключенных к локальной сети.

Настройка интервала Query последнего участника

Необязательный.

Если нет особых требований, вы можете выполнить эту настройку на всех интерфейсах маршрутизатора, напрямую подключенных к локальной сети.

Настройка количества Query последнего участника

Необязательный.

Если нет особых требований, вы можете выполнить эту настройку на всех интерфейсах маршрутизатора, напрямую подключенных к локальной сети.

Настройка интервала Query общего участника

Необязательный.

Если нет особых требований, вы можете выполнить эту настройку на всех интерфейсах маршрутизатора, напрямую подключенных к локальной сети.

Настройка максимального времени ответа

Необязательный.

Если нет особых требований, вы можете выполнить эту настройку на всех интерфейсах маршрутизатора, напрямую подключенных к локальной сети.

3.4.2.4. Проверка

Запустите команду **show ip igmp interface** *interface-type interface-number*, чтобы отобразить конфигурации интерфейса.

3.4.2.5. Связанные команды

Указание версии IGMP

Команда	**ip igmp version** { **1** | **2** | **3** }
Описание параметра	**1**: указывает IGMPv 1. **2**: указывает IGMPv 2. **3**: указывает IGMPv 3

Командный режим	Режим настройки интерфейса
Руководство по использованию	После настройки этой команды IGMP автоматически перезапустится

Настройка интервала Query последнего участника

Команда	**ip igmp last-member-query-interval** *interval*
Описание параметра	*interval*: указывает интервал для отправки пакетов Query определенной группы. Диапазон значений от 1 до 255 с шагом 0,1 секунды, а значение по умолчанию — 10 (а именно 1 секунда)
Командный режим	Режим настройки интерфейса
Руководство по использованию	Эта команда применима только к IGMPv2 или IGMPv3. Когда интерфейс получает пакет Leave, интерфейс отправляет пакеты Query группы постоянно и ждет ответа от хоста. После истечения тайм-аута маршрутизатор IGMP предполагает, что участник группы не существует в сегменте напрямую подключенной сети, и удаляет интерфейс из группы IGMP. Продолжительность тайм-аута равна значению **last-member-query-interval**, умноженное на **last-member-query-count** плюс 1/2 от **query-max-response-time**

Настройка количества Query последнего участника

Команда	**ip igmp last-member-query-count** *count*
Описание параметра	*count*: указывает количества раз отправки пакетов Query определенной группы в диапазоне от 2 до 7. Значение по умолчанию — 2
Командный режим	Режим настройки интерфейса
Руководство по использованию	Эта команда применима только к IGMPv2 или IGMPv3. Когда интерфейс получает пакет Leave, интерфейс отправляет пакеты Query группы постоянно и ждет ответа от хоста. После истечения тайм-аута маршрутизатор IGMP предполагает, что участник группы не существует в сегменте напрямую подключенной сети, и удаляет интерфейс из группы IGMP. Продолжительность тайм-аута равна значению **last-member-query-interval**, умноженное на **last-member-query-count** плюс 1/2 от **query-max-response-time**

Настройка интервала Query общего участника

Команда	**ip igmp query-interval** *seconds*
Описание параметра	*seconds*: указывает интервал Query общего участника в диапазоне от 1 до 18 000 с. Значение по умолчанию — 125
Командный режим	Режим настройки интерфейса

Настройка максимального времени ответа

Команда	**ip igmp query-max-response-time** *seconds*
Описание параметра	*seconds*: указывает максимальное время отклика в диапазоне от 1 до 25 с. Значение по умолчанию — 10
Командный режим	Режим настройки интерфейса
Руководство по использованию	После отправки пакетов Query интерфейс ожидает ответа. Если происходит тайм-аут, маршрутизатор IGMP предполагает, что участник группы не существует в напрямую подключенном сегменте сети, и удаляет информацию о группе

3.4.2.6. Пример конфигурации

Настройка основных параметров маршрутизатора

Сценарий	• Настройте основные функции IGMP. • Укажите IGMPv3. • Настройте интервал Query последнего участника на 15 (1,5 с). • Настройте количество Query последнего участника на 3. • Настройте интервал Query общего участника на 130 с. • Настройте максимальное время ответа на 15 с
	QTECH(config-if-GigabitEthernet 0/5)#ip igmp version 3 QTECH(config-if-GigabitEthernet 0/5)#ip igmp last-member-query-count 3 QTECH(config-if-GigabitEthernet 0/5)#ip igmp last-member-query-interval 15 QTECH(config-if-GigabitEthernet 0/5)#ip igmp query-interval 130 QTECH(config-if-GigabitEthernet 0/5)#ip igmp query-max-response-time 15
Проверка	Запустите команду **show ip igmp interface** *interface-type interface-number*, чтобы проверить функции IGMP интерфейса
	QTECH#show ip igmp interface gigabitEthernet 0/5

	Interface GigabitEthernet 0/5 (Index 5) IGMP Enabled, Active, Querier, Version 3 Internet address is 192.168.1.90 IGMP interface limit is 1024 IGMP interface has 1 group-record states IGMP interface has 0 static-group records IGMP activity: 3 joins, 0 leaves IGMP query interval is 130 seconds IGMP querier timeout is 267 seconds IGMP max query response time is 15 seconds Last member query response interval is 15 Last member query count is 3 Group Membership interval is 275 seconds Robustness Variable is 2 QTECH#

3.4.2.7. Распространенные ошибки

Основные функции IGMP не включены.

3.4.3. Настройка IGMP Querier

3.4.3.1. Эффект конфигурации

Выберите уникальный Query в локальной сети.

3.4.3.2. Примечания

Необходимо настроить основные функции IGMP.

3.4.3.3. Шаги настройки

- При необходимости тайм-аут Querier можно настроить.
- Если нет особых требований, вы можете выполнить настройку на всех интерфейсах с поддержкой IGMP в локальной сети.

3.4.3.4. Проверка

Запустите команду **show ip igmp interface** *interface-type interface-number*, чтобы отобразить конфигурации интерфейса.

3.4.3.5. Связанные команды

Настройка тайм-аута Querier

Команда	**ip igmp query-timeout** *seconds*
Описание параметра	*seconds*: указывает время keepalive Querier-а в диапазоне от 60 до 300 с. Значение по умолчанию — 255 с
Командный режим	Режим настройки интерфейса
Руководство по использованию	После отправки пакетов Query интерфейс ожидает пакетов Query, отправленных другими устройствами. Если происходит тайм-аут, Маршрутизатор IGMP предполагает, что Querier уникален в напрямую подключенном сегменте сети

3.4.3.6. Пример конфигурации

Настройка тайм-аута Querier

Сценарий	• Настройте основные функции IGMP. • Установите тайм-аут запроса на 280 с
	QTECH(config-if-GigabitEthernet 0/5)#ip igmp query-timeout 280
Проверка	Запустите команду **show ip igmp interface** in*terface-type interface-number,* чтобы проверить функции IGMP интерфейса
	QTECH#show ip igmp interface gigabitEthernet 0/5 Interface GigabitEthernet 0/5 (Index 5) IGMP Enabled, Active, Querier, Version 3 Internet address is 192.168.1.90 IGMP interface limit is 1024 IGMP interface has 1 group-record states IGMP interface has 0 static-group records IGMP activity: 11 joins, 0 leaves IGMP query interval is 130 seconds IGMP querier timeout is 280 seconds IGMP max query response time is 15 seconds Last member query response interval is 15 Last member query count is 3 Group Membership interval is 275 seconds Robustness Variable is 2

	QTECH#

3.4.3.7. Распространенные ошибки

Основные функции IGMP не включены.

3.4.4. Настройка фильтрации группы IGMP

3.4.4.1. Эффект конфигурации

Маршрутизатор фильтрует участников группы IGMP.

3.4.4.2. Примечания

Необходимо настроить основные функции IGMP.

3.4.4.3. Шаги настройки

Настройка ACL группы IGMP

- Опционально.
- Если нет особых требований, вы можете выполнить эту настройку на всех интерфейсах маршрутизатора, напрямую подключенных к локальной сети.

Настройка максимального количества участников группы IGMP

- Опционально.
- Если нет особых требований, вы можете выполнить эту настройку на всех интерфейсах маршрутизатора, напрямую подключенных к локальной сети.

3.4.4.4. Проверка

ACL группы IGMP

- Настройте интерфейс, чтобы разрешить присоединяться только группам из ACL 1. Адреса доступа ACL 1: 225.0.0.1~225.0.0.255.
- Настройте интерфейс для присоединения к группе с адресом 225.0.0.5.
- Настройте интерфейс для присоединения к группе с адресом 236.0.0.5.
- Просмотр информации о группе текущего интерфейса.

Максимальное количество участников группы IGMP

- Установите максимальное количество участников на интерфейсе равным 5.
- Настройте интерфейс для присоединения к группе с адресами от 225.0.0.5 до 225.0.0.10.
- Просмотрите информацию о группе интерфейса.

3.4.4.5. Связанные команды

Настройка ACL группы IGMP

Команда	**ip igmp access-group** *access-list*
Описание параметра	*access-list*: определяет диапазон адресов группы с использованием стандартного IP ACL или расширенного ACL. Значение варьируется от 1 до 199, от 1300 до 2699 символов

Командный режим	Режим настройки интерфейса
Руководство по использованию	Настройте эту команду на интерфейсе для управления группами, к которым могут присоединяться хосты в напрямую подключенном сегменте сети. Используйте ACL, чтобы ограничить диапазон адресов группы. Если получены пакеты Report, отклоненные ACL, они будут отброшены. Когда IGMPv3 включен, эта команда поддерживает расширенный список ACL. Если полученная информация Report IGMP равна (S1,S2,S3…Sn,G), эта команда применит соответствующий ACL к информации (0,G) для сопоставления. Поэтому необходимо настроить запись (0,G) явным образом для расширенного ACL, чтобы нормально фильтровать (S1,S2,S3…Sn,G)

Настройка максимального количества участников группы IGMP

Команда	**ip igmp limit** *number* [**except** *access-list*]
Описание параметра	*number*: указывает максимальное количество участников группы IGMP, диапазон значений которого зависит от устройства. Значение по умолчанию — 1024 для интерфейса и 65 536 глобально. **except** *access-list*: указывает, что группы в списке ACL не учитываются. **access-list** указывает стандартный IP ACL. Значение варьируется от 1 до 99, от 1300 до 1999 и названия
Командный режим	Режим настройки интерфейса
Руководство по использованию	Режим глобальной конфигурации: ограничивает максимальное количество участников группы IGMP в системе. Режим конфигурации интерфейса: ограничивает максимальное количество участников группы IGMP на интерфейсе. Если количество участников группы превышает интерфейсный или глобальный лимит, полученные впоследствии пакеты Report будут игнорироваться. Если настроен список исключений ACL, пакеты Report в пределах указанного диапазона могут обрабатываться нормально; поэтому сгенерированные участники группы не учитываются. Интерфейс и глобальные настройки могут выполняться независимо. Если глобальный предел количества меньше, чем для интерфейса, должна использоваться глобальная конфигурация

3.4.4.6. Пример конфигурации

Настройка фильтрации группы IGMP

Сценарий	• Настройте основные функции IGMP. • Настройте диапазон адресов доступа ACL 1 от 225.0.0.1 до 225.0.0.255. • Установите адрес группы, к которой нужно присоединиться, 225.0.0.5. • Установите адрес группы, к которой нужно присоединиться, 236.0.0.5
	QTECH(config)#access-list 1 permit 225.0.0.1 225.0.0.255 QTECH(config-if-GigabitEthernet 0/5)#ip igmp access-group 1 QTECH(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.5 QTECH(config-if-GigabitEthernet 0/5)#ip igmp join-group 236.0.0.5
Проверка	Запустите **show ip igmp groups** [*interface-type interface-number*] [*group-address*] [**detail**], чтобы отобразить информацию о группе интерфейса
	QTECH(config-if-GigabitEthernet 0/5)#show ip igmp groups IGMP Connected Group Membership Group Address Interface Uptime Expires Last Reporter 225.0.0.5 GigabitEthernet 0/5 00:14:00 00:02:45 192.168.1.90

Настройка максимального количества участников группы IGMP

Сценарий	• Настройте основные функции IGMP. • Настройте максимальное количество участников группы IGMP для интерфейса до 5. • Добавьте информацию о группе (225.0.0.5~225.0.0.12). • Просмотр информации о группе
	QTECH(config-if-GigabitEthernet 0/5)#ip igmp limit 5 QTECH(config-if-GigabitEthernet 0/5)# QTECH(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.5 QTECH(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.6 QTECH(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.7 QTECH(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.8 QTECH(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.9 QTECH(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.10 QTECH(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.11 QTECH(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.12

Проверка	Запустите **show ip igmp groups** [*interface-type interface-number*] [*group-address*] [**detail**], чтобы отобразить информацию о группе интерфейса

```
QTECH(config-if-GigabitEthernet 0/5)#show ip igmp groups
IGMP Connected Group Membership
Group Address  Interface            Uptime    Expires   Last Reporter
225.0.0.5      GigabitEthernet 0/5  00:20:15  00:03:09  192.168.1.90
225.0.0.6      GigabitEthernet 0/5  00:20:24  00:02:58  192.168.1.90
225.0.0.7      GigabitEthernet 0/5  00:00:15  00:04:29  192.168.1.90
225.0.0.8      GigabitEthernet 0/5  00:00:13  00:04:34  192.168.1.90
225.0.0.9      GigabitEthernet 0/5  00:00:11  00:04:33  192.168.1.90
```

3.4.4.7. Распространенные ошибки

Основные функции IGMP не включены.

3.4.5. Настройка IGMP-прокси

3.4.5.1. Эффект конфигурации

Настройте функцию прокси-сервера маршрутизатора и соберите информацию о локальных участниках.

3.4.5.2. Примечания

Необходимо настроить основные функции IGMP.

3.4.5.3. Шаги настройки

Настройка прокси-сервиса IGMP

- Опционально.
- Если нет особых требований, вы можете выполнить эту настройку на напрямую подключенных интерфейсах upstream-маршрутизатора.

Настройка прокси-сервера IGMP Mroute

- Опционально.
- Если нет особых требований, вы можете выполнить эту настройку на напрямую подключенных интерфейсах downstream-хостов.

3.4.5.4. Проверка

- Установите интерфейс 7 для прямого подключения к upstream-маршрутизатору в качестве прокси-сервера multicast.
- Установите интерфейс 1 для прямого подключения к downstream-хосту в качестве прокси-сервера multicast.
- Настройте интерфейс 1 для присоединения групп с адресами 225.0.0.6 и 225.5.5.5.
- Просмотр текущей информации о группе.

3.4.5.5. Связанные команды

Настройка прокси-сервиса IGMP

Команда	**ip igmp proxy-service**
Командный режим	Режим настройки интерфейса
Руководство по использованию	Запустите команду **ip igmp proxy-service**, чтобы настроить uplink-интерфейс как интерфейс Proxy-Service. Запустите команду **ip igmp mroute-proxy**, чтобы установить downlink-интерфейс в качестве интерфейса Mroute-Proxy. Пересылайте пакеты Query IGMP из интерфейса Proxy-Service в интерфейс Mroute-Proxy. Пересылайте пакеты Report IGMP из интерфейса Mroute-Proxy в интерфейс Proxy-Service. Устройство поддерживает максимум 32 интерфейса Proxy-Service. После того как интерфейс Proxy-Service получает пакет Query IGMP, интерфейс отправляет ответ на основе записей участников группы IGMP. Если команда **switchport** выполняется на интерфейсе Proxy-Service, команда **ip igmp mroute-proxy**, настроенная на интерфейсе Mroute-Proxy, будет удалена автоматически

Настройка IGMP Mroute

Команда	**ip igmp mroute-proxy** *interface-type interface-number*
Командный режим	Режим настройки интерфейса
Руководство по использованию	Запустите команду **ip igmp proxy-service**, чтобы настроить uplink-интерфейс как интерфейс Proxy-Service. Запустите команду **ip igmp mroute-proxy**, чтобы установить downlink-интерфейс в качестве интерфейса Mroute-Proxy. Пересылайте пакеты Query IGMP из интерфейса Proxy-Service в интерфейс Mroute-Proxy. Пересылайте пакеты Report IGMP из интерфейса Mroute-Proxy в интерфейс Proxy-Service

3.4.5.6. Пример конфигурации

Сценарий	• Настройте основные функции IGMP. • Настройте интерфейс 7 в качестве прокси-сервера. • Настройте интерфейс 1 как прокси-сервер multicast. • Настройте интерфейс 1 для присоединения групп с адресами 225.0.0.6 и 225.5.5.5

	QTECH(config-if-GigabitEthernet 0/7)#ip igmp proxy-service QTECH(config-if-GigabitEthernet 0/7)#exit QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)#ip igmp mroute-proxy gigabitEthernet 0/7 QTECH(config-if-GigabitEthernet 0/1)#ip igmp join-group 225.0.0.6 QTECH(config-if-GigabitEthernet 0/1)#ip igmp join-group 225.5.5.5
Проверка	Запустите команду **show ip igmp groups** [*interface-type interface-number*] [*group-address*] [**detail**], чтобы отобразить информацию о группе интерфейса
	QTECH(config-if-GigabitEthernet 0/1)#show ip igmp groups IGMP Connected Group Membership Group Address Interface Uptime Expires Last Reporter 225.0.0.6 GigabitEthernet 0/1 00:23:05 00:02:40 192.168.36.90 225.5.5.5 GigabitEthernet 0/1 00:22:06 00:02:41 192.168.36.90 IGMP Proxy-server Connected Group Membership Group Address Interface Uptime 225.0.0.6 GigabitEthernet 0/7 00:23:05 225.5.5.5 GigabitEthernet 0/7 00:22:06 QTECH(config-if-GigabitEthernet 0/1)#

3.4.5.7. Распространенные ошибки

Основные функции IGMP не включены.

3.4.6. Настройка сопоставления IGMP SSM

3.4.6.1. Эффект конфигурации

IGMPv3 поддерживает фильтрацию источников; однако IGMPv1 и IGMPv2 не поддерживают фильтрацию источников, но предоставляют функцию сопоставления SSM для фильтрации источников.

3.4.6.2. Примечания

Необходимо настроить основные функции IGMP.

3.4.6.3. Шаги настройки

Включение сопоставления SSM

(Обязательно) Включите функцию сопоставления SSM.

Включите функцию сопоставления SSM на маршрутизаторе.

Настройка статического сопоставления SSM

Опционально.

Настройте эту функцию на маршрутизаторах с поддержкой сопоставления SSM.

3.4.6.4. Проверка

Запустите команду **show ip igmp ssm-mapping** [*group-address*], чтобы отобразить информацию сопоставления SSM.

3.4.6.5. Связанные команды

Включение сопоставления SSM

Команда	**ip igmp ssm-map enable**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите команду **ip igmp ssm-map enable**, чтобы включить функцию сопоставления SSM. Запустите команду **ip igmp ssm-map static**, чтобы установить записи статического сопоставления. Запустите IGMPv3 на интерфейсе. При получении пакетов Report IGMPv1 или IGMPv2 можно добавить адреса источника статических сопоставлений

Настройка статического сопоставления SSM

Команда	**ip igmp ssm-map static** *access-list source-address*
Описание параметра	*access-list*: указывает диапазон адресов группы, установленный стандартным IP ACL. Значение варьируется от 1 до 99, от 1300 до 1999 и названия. *source-address*: указывает адрес источника
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите команду **ip igmp ssm-map enable**, чтобы включить функцию сопоставления SSM. Запустите команду **ip igmp ssm-map static**, чтобы установить записи статического сопоставления. Запустите IGMPv3 на интерфейсе. При получении пакетов Report IGMPv1 или IGMPv2 можно добавить адреса источника статических сопоставлений

3.4.6.6. Пример конфигурации

Сценарий	• Настройте основные функции IGMP. • Включите сопоставление SSM. • Настройте статическое сопоставление ACL SSM 1
	QTECH(config)#ip igmp ssm-map enable QTECH(config)#ip igmp ssm-map static 1 192.168.5.9
Проверка	Запустите команду **show ip igmp ssm-mapping** [**group-address**], чтобы отобразить информацию о сопоставлении SSM
	QTECH#show ip igmp ssm-mapping SSM Mapping : Enabled Database : Static mappings configured

3.4.6.7. Распространенные ошибки

Основные функции IGMP не включены.

3.4.7. Настройка опции оповещения

3.4.7.1. Эффект конфигурации

- Проверьте, содержат ли пакеты IGMP опцию Router Alert, и отклоните пакеты без опции Router Alert.
- Поддержка отправки пакетов IGMP с помощью опции Router Alert.

3.4.7.2. Примечания

Необходимо настроить основные функции IGMP.

3.4.7.3. Шаги настройки

Проверка опции Router Alert

Опционально.

Отправка пакетов IGMP с инкапсулированной опцией Router Alert

Опционально.

3.4.7.4. Проверка

Проверка опции Router Alert

Проверьте, отбрасывает ли интерфейс с поддержкой IGMP пакеты IGMP без опции Router Alert.

Отправка пакетов IGMP с инкапсулированной опцией Router Alert

Проверьте, отправляет ли интерфейс с поддержкой IGMP пакеты IGMP, содержащие опцию Router Alert.

3.4.7.5. Связанные команды

Проверка опции Router Alert

Команда	**ip igmp enforce-router-alert**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите **ip igmp enforce-router-alert** для включения проверки опции Router Alert. Запустите **no ip igmp enforce-router-alert** для отключения проверки опции Router Alert

Отправка пакетов IGMP с инкапсулированной опцией Router Alert

Команда	**ip igmp send-router-alert**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите команду **ip igmp send-router-alert** для включения функции отправки пакетов IGMP, содержащих опцию Router Alert. Запустите **no ip igmp send-router-alert** для отключения этой функции

3.4.7.6. Пример конфигурации

Проверка опции оповещения маршрутизатора

Сценарий	• Настройте основные функции IGMP. • Настройте проверку опции Router Alert
	`QTECH(config)#ip igmp enforce-router-alert`
Проверка	Пакеты IGMP, содержащие опцию Router Alert 225.1.1.1 отправляются на интерфейс с поддержкой IGMP, и эти пакеты обрабатываются. Запустите команду **show ip igmp groups**, и вы увидите 225.1.1.1. Пакеты IGMP, не содержащие опцию Router Alert 225.1.1.2 отправляются на интерфейс с поддержкой IGMP, и эти пакеты отбрасываются. Запустите команду **show ip igmp groups**, и вы не увидите 225.1.1.2

Отправка пакетов IGMP с инкапсулированной опцией Router Alert

Сценарий	• Настройте основные функции IGMP. • Настройте функцию отправки пакетов IGMP, содержащую опцию Router Alert
	`QTECH(config)#ip igmp send-router-alert`

Проверка	Проверьте, отправляет ли интерфейс с поддержкой IGMP пакеты IGMP, содержащие опцию Router Alert

3.4.7.7. Распространенные ошибки

Основные функции IGMP не включены.

3.5. Мониторинг

3.5.1. Очистка

Описание	Команда
Удаляет участие в динамической группе из буфера IGMP	**clear ip igmp group**
Очищает информацию об интерфейсе из буфера IGMP	**clear ip igmp interface** *interface-type interface-number*

3.5.2. Отображение

Описание	Команда
Отображает все группы в подсети с прямым подключением	**show ip igmp groups**
Отображает подробные сведения обо всех группах в подсети с прямым подключением	**show ip igmp groups detail**
Отображает указанные группы в подсети с прямым подключением	**show ip igmp groups** *A.B.C.D*
Отображает подробные сведения об указанных группах в подсети с прямым подключением	**show ip igmp groups** *A.B.C.D* **detail**
Отображает конфигурации IGMP указанного интерфейса в подсети с прямым подключением	**show ip igmp interface** *interface-type interface-number*
Отображает подробные сведения обо всех группах указанного интерфейса в подсети с прямым подключением	**show ip igmp groups** *interface-type interface-number* **detail**

Описание	Команда
Отображает информацию об указанной группе указанного интерфейса в подсети с прямым подключением	**show ip igmp groups** *interface-type interface-number A.B.C.D*
Отображает подробные сведения об указанной группе указанного интерфейса в подсети с прямым подключением	**show ip igmp groups** *interface-type interface-number A.B.C.D* **detail**
Отображает конфигурации интерфейса IGMP	**show ip igmp interface** [*interface-type interface-number*]
Отображает конфигурации всех интерфейсов IGMP	**show ip igmp interface**
Отображает конфигурации сопоставления IGMP SSM	**show ip igmp ssm-mapping**
Отображает информацию о сопоставлении IGMP SSM с *A.B.C.D*	**show ip igmp ssm-mapping** *A.B.C.D*

3.5.3. Отладка

Описание	Команда
Показывает, включена ли отладка IGMP	**show debugging**
Отладка всей информации IGMP	**debug ip igmp all**
Отладка декодирования пакетов IGMP	**debug ip igmp decode**
Отладка кодирования пакетов IGMP	**debug ip igmp encode**
Отладка событий IGMP	**debug ip igmp events**
Отладка IGMP FSM	**debug ip igmp fsm**
Отладка state machine IGMP	**debug ip igmp tib**
Отладка предупреждений IGMP	**debug ip igmp warning**

4. НАСТРОЙКА MLD

4.1. Обзор

Multicast Listener Discovery (MLD) — это протокол, используемый в технологии multicast.

Этот протокол получает отношения участников multicast между хостами и маршрутизаторами для определения пересылки потока multicast. Используя информацию, полученную от MLD, устройство поддерживает таблицу состояний Multicast Listener на основе интерфейса. Таблица состояний Multicast Listener активируется только в том случае, если хотя бы один хост в канале интерфейса является участником группы.

В настоящее время MLD имеет две версии: MLDv1 и MLDv2.

- MLD обеих версий поддерживает модель Any-Source Multicast (ASM).
- MLDv2 можно напрямую применить к модели Source-Specific Multicast (SSM).
- MLDv1 можно применить к модели SSM только в том случае, если настроено сопоставление MLD SSM.

4.1.1. Протоколы и стандарты

- RFC2710: обнаружение Multicast Listener (MLDv1) для IPv6.
- RFC3810: обнаружение Multicast Listener версии 2 (MLDv2) для IPv6.

4.2. Приложения

Приложение	Описание
Настройка сервиса MLD в локальной сети	Реализует сервис MLD в локальной сети
Настройка прокси-сервиса MLD	В простой древовидной топологии вместо сервиса PIM используется прокси-служба MLD

4.2.1. Настройка сервиса MLD в локальной сети

4.2.1.1. Сценарий

Как показано на Рисунке 4-1, локальная сеть состоит из приемника 1, приемника 2, маршрутизатора A и маршрутизатора B.

Сообщения Query, отправленные маршрутизатором A или маршрутизатором B, действительны в локальной сети, а сообщения Report, отправленные получателями A и получателями B, также действительны в локальной сети.

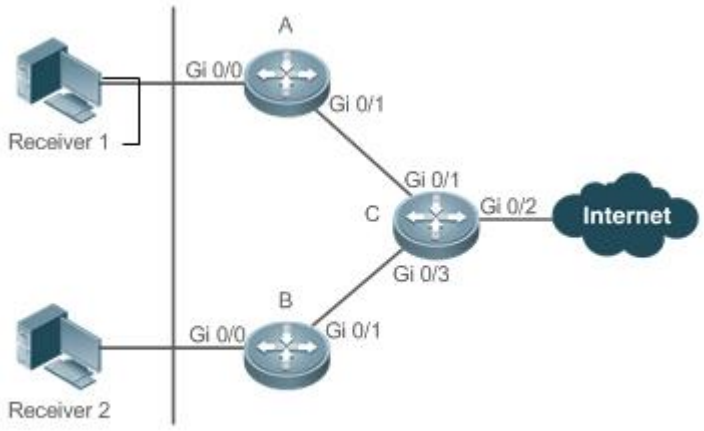

Рисунок 4-1.

Маршрутизатор C — это выходной шлюз.

Маршрутизаторы A и B являются локальными маршрутизаторами.

4.2.1.2. Развертывание

- Маршрутизаторы A, B и C используют протокол OSPFv6.
- Интерфейсы маршрутизаторов A, B и C используют протокол multicast (PIM SMv6).

4.2.2. Настройка прокси-сервиса MLD

4.2.2.1. Сценарий

Как показано на Рисунке 4-2, функция прокси включена на маршрутизаторе A. Маршрутизатор A действует как хост и образует локальную группу управления с маршрутизатором B. Маршрутизатор A пересылает сообщения Report от получателей 1 и 2.

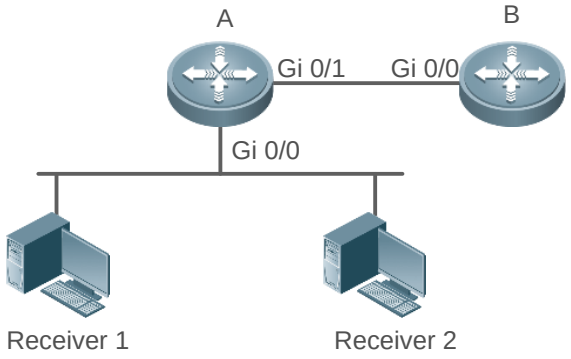

Рисунок 4-2.

Маршрутизатор A действует как прокси.

Маршрутизатор B предоставляет службу PIM.

4.2.2.2. Развертывание

- Маршрутизаторы A и B используют протокол OSPFv6.
- Интерфейсы на маршрутизаторах A и B используют протокол multicast (PIM SMv6).

- Сервис прокси-multicast включена на Gi 0/0 и Gi 0/1 маршрутизатора A.

4.3. Функции

4.3.1. Базовые определения

Поведение хоста и поведение устройства

Устройства multicast уровня 3, использующие протоколы управления multicast-рассылкой, называются устройствами, а их поведение — поведением устройства.

ПК или смоделированные ПК, на которых работают протоколы управления multicast-рассылкой, называются хостами, а их поведение — поведением хоста.

Querier

Устройства взаимодействуют и конкурируют друг с другом. После сравнения IP-адресов устройство с меньшим IP-адресом становится Querier и периодически отправляет сообщения Query.

Интерфейс MLD PROXY-SERVICE

Этот интерфейс, также называемый uplink-интерфейсом, реализует поведение хоста. Он получает сообщения Query, отправленные upstream-устройствами, и отправляет сообщения Report, собранные прокси-сервером маршрутизатора.

Интерфейс MLD MROUTE-PROXY

Этот интерфейс, также называемый downlink-интерфейсом, реализует функции маршрутизатора. Он отправляет сообщения, полученные интерфейсом прокси-сервиса, а также собирает и отправляет информацию о хосте в интерфейс прокси-сервиса.

MLD SSM-MAP

Сопоставление SSM относится к сопоставлению multicast, зависящей от источника. MLDv1 не поддерживает модель SSM, пока не будет включена функция SSM-MAP.

4.3.1.1. Обзор

Особенность	Описание
Настройка параметров маршрутизатора MLD	Отправляет сообщения Query для получения информации о локальных участниках
Процесс выбора Querier или механизм тайм-аута	Выбирает уникального Querier в текущем сегменте сети
Фильтрация групп MLD	Фильтрует участников группы и ограничивает количество участников группы
Поддержка статических групп MLD	Сохраняет статическую информацию о группе на локальном маршрутизаторе вместо получения информации о группе путем отправки сообщений Report

Особенность	Описание
Настройка информации об имитируемой группе хостов	Имитирует поведение хоста для прямой настройки информации о присоединении группы
Поддержка MLD-прокси	Использует эту функцию в простой древовидной топологии вместо сложных протоколов multicast-маршрутизации, таких как PIM
Поддержка SSM-MAP	Предоставляет модель SSM для MLDv1. Когда хост добавляется в группу, можно указать конкретный источник, чтобы избежать использования полосы пропускания сети ненужными и недействительными multicast-потоками данных. Эта функция особенно полезна в сети, где несколько источников multicast используют один и тот же адрес multicast

4.3.2. Настройка параметров маршрутизатора MLD

Отправляет сообщения Query для получения информации о локальных участниках.

4.3.2.1. Принцип работы

Устройство периодически отправляет сообщения Query, чтобы убедиться, что в группе есть хотя бы один хост. Если в группе нет доступного хоста, группа будет удалена.

4.3.2.2. Сопутствующая конфигурация

Включение MLD

По умолчанию MLD отключен на интерфейсе.

Запустите команду **ipv6 pim** { **sparse-mode** }, чтобы включить или отключить MLD на интерфейсе.

MLD можно включить только после включения PIM SM на интерфейсе.

Настройка версии MLD

По умолчанию версия MLD — 2.

Запустите команду **ipv6 mld version** { **1** | **2** } для настройки или восстановления версии MLD интерфейса.

Настройка интервала Query последнего участника

По умолчанию интервал отправки сообщений Query составляет 1 с.

Запустите команду **ipv6 mld last-member-query-interval** *interval*, чтобы настроить или восстановить интервал для отправки сообщений Query.

Большее значение означает более длительный интервал отправки сообщений Query.

Настройка количества Query к последнему участнику

По умолчанию количество Query к последнему участнику равно 2.

Запустите команду **ipv6 mld last-member-query-count** *count*, чтобы настроить или восстановить количество Query к последнему участнику.

Большее значение означает большее количество Query к последнему участнику.

Настройка интервала для Query общего участника

По умолчанию интервал Query общего участника составляет 125 секунд.

Запустите команду **ipv6 mld query-interval** *seconds*, чтобы настроить или восстановить интервал для Query общего участника.

Большее значение означает более длинный интервал для запроса общего участника.

Настройка максимального времени ответа

По умолчанию максимальное время ответа составляет 10 с.

Запустите команду **ipv6 mld query-max-response-time** *seconds*, чтобы настроить или восстановить максимальное время ответа.

Большее значение означает большее максимальное время отклика.

4.3.3. Процесс выбора Querier или механизм тайм-аута

Выбирает уникальный Querier в текущем сегменте сети. Querier отправляет сообщение Query для получения информации о группе в локальной сети.

4.3.3.1. Принцип работы

В multicast-сети, использующей MLD, устройство multicast, предназначенное для отправки Query, отправляет сообщения Query MLD. Устройство определяется выбор. Изначально все устройства находятся в состоянии Querier. При получении сообщений Query об отношениях участников от устройств с более низкими IP-адресами устройства переключаются из состояния получателя в состояние non-querier. Таким образом, в конечном итоге в состоянии Query находится только одно устройство. Это устройство имеет самый низкий IP-адрес среди всех multicast-устройств в сети. Когда устройство Querier не работает, MLD также работает. Устройства non-querier поддерживают таймер интервала keepalive для других устройств Querier. Таймер сбрасывается, как только устройство получает сообщение Query об отношениях участников. Если время таймера истекает, устройство начинает отправлять сообщения Query и начинается выбор нового Querier.

4.3.3.2. Сопутствующая конфигурация

Настройка интервала keepalive для Querier

По умолчанию интервал keepalive у Querier составляет 255 секунд.

Запустите команду **ipv6 mld querier-timeout** *seconds*, чтобы настроить или восстановить интервал keepalive для Querier.

Большее значение означает более длительный интервал keepalive для Querier.

4.3.4. Фильтрация групп MLD

Фильтрует участников группы и ограничивает количество участников группы.

4.3.4.1. Принцип работы

Если вы не хотите, чтобы хосты в сегменте сети, где находится интерфейс, добавлялись в определенные группы multicast, вы можете настроить правила ACL на интерфейсе в качестве фильтра. Интерфейс будет фильтровать полученные сообщения об отношениях участников MLD на основе правил ACL и поддерживать отношения участников только для групп multicast, разрешенных правилами. Также можно установить наибольшее количество участников маршрутизатора.

4.3.4.2. Сопутствующая конфигурация

Настройка контроля доступа для групп multicast

По умолчанию контроль доступа не настроен, и хосты можно добавлять в любые группы.

Запустите команду **ipv6 mld access-group** *access-list-name*, чтобы настроить или восстановить контроль доступа для групп multicast.

После настройки роутер может получать сообщения только от хостов в группах, указанных в списке доступа.

Настройка максимального количества участников группы MLD

По умолчанию группа MLD имеет максимум 1024 участника.

Запустите команду **ipv6 mld limt** *number*, чтобы настроить или восстановить максимальное количество участников группы MLD.

Большее значение означает большее количество участников группы.

4.3.5. Поддержка статических групп MLD

Сохраняет статическую информацию о группе на локальном маршрутизаторе вместо получения информации о группе путем отправки сообщений Report. Локальный маршрутизатор может напрямую обмениваться информацией о группе с маршрутизатором PIM.

4.3.5.1. Принцип работы

Настройте информацию о статической группе вручную.

4.3.5.2. Сопутствующая конфигурация

Настройка статической группы

По умолчанию информация о статических группах не настроена.

Запустите команду **ipv6 mld static-group** *group-address*, чтобы настроить или отменить информацию о статической группе.

4.3.6. Настройка информации об имитируемой группе хостов

Имитирует поведение хоста для прямой настройки информации о присоединении к группе.

4.3.6.1. Сопутствующая конфигурация

Настройка группы присоединения (Join-Group)

По умолчанию информация о группе присоединения не настроена.

Запустите команду **ipv6 mld join-group** *group-address*, чтобы настроить или отменить информацию о группе присоединения.

4.3.7. Поддержка MLD-прокси

В простой древовидной топологии нет необходимости запускать сложные протоколы multicast-маршрутизации (например, PIM). В этом случае прокси-сервер MLD можно использовать для отправки сообщений MLD downstream-хостам и поддержания отношений участников.

4.3.7.1.1. Принцип работы

Когда upstream-маршрутизатор настроен как интерфейс сервиса прокси-сервера MLD, он функционирует как хост и может получать сообщения Query от

upstream-маршрутизаторов, а также пересылать групповую информацию downstream-хостов. Когда downstream-маршрутизатор настроен как multicast прокси-интерфейс MLD, он функционирует как маршрутизатор и может пересылать сообщения Query upstream-маршрутизаторов, а также получать сообщения Report от downstream-маршрутизаторов.

4.3.7.2. Сопутствующая конфигурация

Настройка MLD PROXY-SERVICE

По умолчанию прокси-сервис MLD отключен на интерфейсе.

Запустите команду **ipv6 mld proxy-service**, чтобы настроить или отменить функцию прокси-сервера MLD на интерфейсе.

Эту функцию необходимо настроить при использовании прокси.

Настройка MLD MROUTE–PROXY

По умолчанию сервис multicast прокси отключена на интерфейсе.

Запустите команду **ipv6 mld mroute-proxy** *interface-name*, чтобы настроить или отменить функцию multicast прокси на интерфейсе.

Эту функцию необходимо настроить при использовании прокси.

4.3.8. Поддержка SSM-MAP

Эта функция предоставляет модель SSM для MLDv1. Когда хост добавляется в группу, можно указать конкретный источник, чтобы избежать использования пропускной способности сети ненужными и недействительными потоками multicast-данных. Эта функция особенно полезна в сети, где несколько источников multicast используют один и тот же адрес multicast.

4.3.8.1. Принцип работы

Основанный на MLDv1, MLDv2 предоставляет дополнительную функцию, а именно multicast-фильтрацию источника. В MLDv1 хост решает присоединиться к группе только на основе адреса группы и получает потоки multicast, отправленные на адрес группы из любого источника. Однако хост MLDv2 объявляет группу multicast, к которой хочет присоединиться хост, и адрес источника multicast, который он хочет получить. В MLDv1 фильтрация адресов источника может быть реализована в некоторой степени, но фильтрация реализуется путем включения SSM-MAP и настройки статических групп SSM-MAP на приемниках multicast-потока.

4.3.8.2. Сопутствующая конфигурация

Включение MLD SSM-MAP

По умолчанию SSM-MAP отключен.

Запустите команду **ipv6 mld ssm-map enable**, чтобы включить или отключить функцию SSM-MAP.

Эту функцию необходимо включить при использовании SSM-MAP.

Настройка MLD SSM-MAP STATIC

По умолчанию таблица статических каналов SSM-MAP не настроена.

Запустите команду **ipv6 mld ssm-map static** *access-list-num A.B.C.D*, чтобы включить или отключить таблицу статических каналов SSM-MAP.

4.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций MLD	(Обязательно) Используется для настройки услуги multicast	
	Ipv6 multicast-routing	Включает функцию multicast-маршрутизации IPv6
	Ipv6 pim sparse-mode	Включает функцию PIM-SM
Настройка параметров маршрутизатора MLD	**Ipv6 mld version** { **1** | **2** }	Настраивает версию MLD
	Ipv6 mld last-member-query-interval *interval*	Настраивает интервал Query последнего участника
	Ipv6 mld last-member-query-count *count*	Настраивает количество Query последнего участника
	Ipv6 mld query-interval *seconds*	Настраивает интервал Query общего участника
	Ipv6 mld query-max-response-time *seconds*	Настраивает максимальный интервал ответа
Процесс выбора Querier или механизм тайм-аута	**ipv6 mld querier-timeout** *seconds*	Настраивает интервал keepalive Querier
Фильтрация групп MLD	**Ipv6 mld access-group** *access-list*	Фильтрует участников групп MLD
MLD-прокси	**Ipv6 mld proxy-service**	Настраивает MLD PROXY-SERVICE
	ipv6 mld mroute-proxy *interface-type interface-number*	Настраивает MLD MROUTE-PROXY
Поддержка SSM-MAP	**Ipv6 mld ssm-map enable**	Включает функцию SSM-MAP
	Ipv6 mld ssm-map static *access-list source-address*	Настраивает таблицу статического канала SSM-MAP

4.4.1. Настройка основных функций MLD

4.4.1.1. Эффект конфигурации

Включите функцию multicast-маршрутизации и соберите информацию о группах в локальной сети.

4.4.1.2. Примечания

Функция PIM SM должна быть включена на интерфейсе.

4.4.1.3. Шаги настройки

Включение функции multicast-маршрутизации IPv6

- Обязательный.
- Функция multicast-маршрутизации IPv6 должна быть включена на всех маршрутизаторах локальной сети, если не указано иное.

Включение функции PIM SM

- Обязательный.
- Функция PIM SM должна быть включена непосредственно на интерфейсе локальной сети, если не указано иное.

4.4.1.4. Проверка

Запустите команду **show ipv6 mld interface** ***interface-type*** *interface-number*, чтобы проверить, включен ли MLD на интерфейсе.

4.4.1.5. Связанные команды

Включение функции multicast-маршрутизации IPv6

Команда	**ipv6 multicast-routing**
Командный режим	Режим глобальной конфигурации

Включение функции PIM SM

Команда	**ipv6 pim { sparse-mode }**
Командный режим	Режим настройки интерфейса
Руководство по использованию	PIM-интерфейсы должны быть интерфейсами уровня 3, включая интерфейсы маршрутизации, L3AP, SVI и loopback-интерфейсы. Unicast-маршруты IPv6 должны быть доступны для всех интерфейсов PIM

4.4.1.6. Пример конфигурации

Включение MLD в локальной сети

Шаги настройки	• Настройте протокол unicast-маршрутизации IPv6 (например, OSPF) на маршрутизаторе и убедитесь, что unicast-маршруты доступны для loopback-интерфейса. (пропущено) • Включите функцию multicast-маршрутизации IPv6 на всех маршрутизаторах. • Включите функцию PIM SM на интерфейсах соединения устройств и интерфейсах подключения пользовательских хостов и источников multicast
	QTECH(config)#ipv6 multicast-routing QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)# ipv6 address 2001::1/64 QTECH(config-if-GigabitEthernet 0/1)#ipv6 pim sparse-mode
Проверка	Запустите команду **show ipv6 mld interface** *interface-type interface-number*, чтобы проверить, включен ли MLD на интерфейсе
	QTECH#show ipv6 mld interface gigabitEthernet 0/1 Interface GigabitEthernet 0/1 (Index 1) MLD Active, Querier, Version 2 (default) Internet address is fe80::2d0:f8ff:fe22:33b1 MLD interface limit is 1024 MLD interface has 0 group-record states MLD interface has 0 join-group records MLD interface has 0 static-group records MLD activity: 0 joins, 0 leaves MLD query interval is 125 seconds MLD querier timeout is 255 seconds MLD max query response time is 10 seconds Last member query response interval is 10 (1/10s) Last member query count is 2 Group Membership interval is 260 Robustness Variable is 2

4.4.1.7. Распространенные ошибки

- Multicast-маршрутизация отключена на маршрутизаторах в сети.
- В сети нет интерфейса multicast.

4.4.2. Настройка параметров маршрутизатора MLD

4.4.2.1. Эффект конфигурации

Измените параметры маршрутизатора MLD, чтобы изменить тип сообщения или режим отправки.

4.4.2.2. Примечания

Необходимо настроить основные функции MLD.

4.4.2.3. Шаги настройки

Настройка версии MLD

Необязательный.

Этот параметр можно настроить на всех интерфейсах маршрутизатора, напрямую подключенных к локальной сети, если не указано иное.

Настройка интервала Query последнего участника

Необязательный.

Этот параметр можно настроить на всех интерфейсах маршрутизатора, напрямую подключенных к локальной сети, если не указано иное.

Настройка количества Query последнего участника

Необязательный.

Этот параметр можно настроить на всех интерфейсах маршрутизатора, напрямую подключенных к локальной сети, если не указано иное.

Настройка интервала Query общего участника

Необязательный.

Этот параметр можно настроить на всех интерфейсах маршрутизатора, напрямую подключенных к локальной сети, если не указано иное.

Настройка максимального интервала ответа

Необязательный.

Этот параметр можно настроить на всех интерфейсах маршрутизатора, напрямую подключенных к локальной сети, если не указано иное.

4.4.2.4. Проверка

Запустите команду **show ipv6 mld interface** *interface-type interface-number*, чтобы просмотреть информацию о конфигурации.

4.4.2.5. Связанные команды

Настройка версии MLD

Команда	**ipv6 mld version { 1 | 2 }**
Описание параметра	**1**: указывает на версию 1. **2**: указывает на версию 2

Командный режим	Режим настройки интерфейса
Руководство по использованию	После того, как эта команда выполнена, MLD автоматически перезапустится

Настройка интервала Query последнего участника

Команда	**ipv6 mld last-member-query-interval** *interval*
Описание параметра	*interval*: указывает интервал отправки сообщений Query указанной группы. Единица измерения — 0,1 с, значение находится в диапазоне от 1 до 255, значение по умолчанию — 10 (1 с)
Командный режим	Режим настройки интерфейса
Руководство по использованию	После получения сообщения Done интерфейс будет непрерывно отправлять сообщения Query указанной группы и ждать ответов от хоста. По истечении времени ожидания считается, что участник группы не существует в сегменте сети с прямым подключением, и интерфейс удаляется из записи участника группы MLD. Интервал тайм-аута рассчитывается следующим образом: Интервал тайм-аута = интервал Query последнего участника x количество Query последнего участника + максимальное время ответа Query/2

Настройка количества Query последнего участника

Команда	**ipv6 mld last-member-query-count** *count*
Описание параметра	*count*: указывает количество раз отправки сообщений Query указанной группы. Значение варьируется от 2 до 7. Значение по умолчанию — 2
Командный режим	Режим настройки интерфейса
Руководство по использованию	После получения сообщения Done интерфейс будет непрерывно отправлять сообщения Query указанной группы и ждать ответов от хоста. По истечении времени ожидания считается, что участник группы не существует в сегменте сети с прямым подключением, и интерфейс удаляется из записи участника группы MLD. Интервал тайм-аута рассчитывается следующим образом: Интервал тайм-аута = интервал Query последнего участника x количество Query последнего участника + максимальное время ответа Query/2

Настройка интервала Query общего участника

Команда	**ipv6 mld query-interval** *seconds*
Описание параметра	*seconds*: указывает интервал Query общего участника. Единица измерения — с, значение находится в диапазоне от 1 до 18 000, значение по умолчанию — 125
Командный режим	Режим настройки интерфейса

Настройка максимального интервала ответа

Команда	**ipv6 mld query-max-response-time** *seconds*
Описание параметра	*seconds*: указывает максимальное время ответа. Единица измерения — с, значение находится в диапазоне от 1 до 25, значение по умолчанию — 10
Командный режим	Режим настройки интерфейса
Руководство по использованию	После отправки сообщений Query интерфейс ожидает ответов. По истечении времени ожидания считается, что в сегменте сети с прямым подключением нет участников группы, и информация о группе удаляется

4.4.2.6. Пример конфигурации

Настройка основных параметров маршрутизатора

Шаги настройки	• Настройте основные функции MLD. (пропущено) • Настройте MLD версии 2. • Настройте интервал Query последнего участника как 15 (1,5 с). • Настройте количество Query последнего участника как 3. • Настройте интервал Query общего участника как 130 с. • Настройте максимальное время ответа как 15 секунд
	QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld version 2 QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld last-member-query-count 3 QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld last-member-query-interval 15 QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld query-interval 130 QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld query-max-response-time 15
Проверка	Запустите команду **show ipv6 mld interface** *interface-type interface-number*, чтобы проверить, включен ли MLD на интерфейсе

	QTECH(config-if-GigabitEthernet 0/1)# show ipv6 mld interface gi 0/1 Interface GigabitEthernet 0/1 (Index 1) MLD Enabled, Active, Querier, Version 2 (default) Internet address is fe80::2d0:f8ff:fe22:33b1 MLD interface limit is 1024 MLD interface has 0 group-record states MLD interface has 0 join-group records MLD interface has 0 static-group records MLD activity: 0 joins, 0 leaves MLD query interval is 130 seconds MLD querier timeout is 267 seconds MLD max query response time is 15 seconds Last member query response interval is 15 (1/10s) Last member query count is 3 Group Membership interval is 275 Robustness Variable is 2

4.4.2.7. Распространенные ошибки

Основные функции MLD не включены.

4.4.3. Процесс выбора Querier или механизм тайм-аута

4.4.3.1. Эффект конфигурации

Выберите уникальный Querier в локальной сети.

4.4.3.2. Примечания

Необходимо настроить основные функции MLD.

4.4.3.3. Шаги настройки

- Эту функцию необходимо настроить, если необходимо настроить интервал keepalive Querier.
- Эту функцию можно настроить на всех интерфейсах с поддержкой MLD в локальной сети.

4.4.3.4. Проверка

Запустите команду **show ipv6 mld interface** *interface-type interface-number*, чтобы просмотреть информацию о конфигурации интерфейса.

4.4.3.5. Связанные команды

Настройка интервала keepalive других Querier

Команда	**ipv6 mld querier-timeout** *seconds*
Описание параметра	*seconds*: определяет интервал keepalive для других Querier. Единица — с, значение находится в диапазоне от 60 до 300, а значение по умолчанию — 255
Командный режим	Режим настройки интерфейса
Руководство по использованию	После отправки сообщений Query интерфейс ожидает сообщений Query от других устройств. По истечении времени ожидания считается, что это единственный Querier в сегменте сети с прямым подключением

4.4.3.6. Пример конфигурации

Настройка интервала keepalive других Querier

Шаги настройки	• Настройте основные функции MLD. (пропущено) • Настройте интервал keepalive Querier как 280 с
	QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld querier-timeout 280
Проверка	Запустите команду **show ipv6 mld interface** *interface-type interface-number*, чтобы проверить, включен ли MLD на интерфейсе
	QTECH#show ipv6 mld interface gigabitEthernet 0/1 Interface GigabitEthernet 0/1 (Index 1) MLD Enabled, Active, Querier, Version 2 (default) Internet address is fe80::2d0:f8ff:fe22:33b1 MLD interface limit is 1024 MLD interface has 0 group-record states MLD interface has 0 join-group records MLD interface has 0 static-group records MLD activity: 0 joins, 0 leaves MLD query interval is 130 seconds MLD querier timeout is 280 seconds MLD max query response time is 15 seconds Last member query response interval is 15 (1/10s) Last member query count is 3 Group Membership interval is 275

	Robustness Variable is 2

4.4.3.7. Распространенные ошибки

Основные функции MLD не включены.

4.4.4. Фильтрация групп MLD

4.4.4.1. Эффект конфигурации

Маршрутизатор фильтрует информацию о группе MLD.

4.4.4.2. Примечания

Необходимо настроить основные функции MLD.

4.4.4.3. Шаги настройки

Настройка контроля доступа для групп multicast

Опционально.

Эту функцию можно настроить на всех интерфейсах маршрутизатора, напрямую подключенных к локальной сети, если не указано иное.

Настройка максимального количества участников группы MLD

Опционально.

Эту функцию можно настроить на всех интерфейсах маршрутизатора, напрямую подключенных к локальной сети, если не указано иное.

4.4.4.4. Проверка

Фильтрация групп MLD

Настройте интерфейс так, чтобы разрешить доступ только к группам из таблицы канала 1. Адрес доступа к таблице канала 1 — (FF66::100/64).

Настройте интерфейс для добавления группы FF66::05.

Настройте интерфейс для добавления группы FF65::05.

Проверьте информацию о группе на интерфейсе.

Настройка максимального количества участников группы MLD

Настройте количество участников группы на интерфейсе как 5.

Настройте интерфейс для добавления группы (FF66::05-FF65::0B).

Проверьте информацию о группе на интерфейсе.

4.4.4.5. Связанные команды

Настройка контроля доступа для групп multicast

Команда	**ipv6 mld access-group** *access-list*
Описание параметра	*access-list*: определяет диапазон адресов группы с помощью стандартных IP ACL или расширенных IP ACL. Значение находится в диапазоне от 1 до 199, от 1300 до 2699 и название

Командный режим	Режим настройки интерфейса
Руководство по использованию	После запуска этой команды на интерфейсе вы можете управлять группами, к которым могут присоединяться хосты в сегменте сети с прямым подключением. Используйте списки ACL для ограничения диапазона адресов группы. Сообщения Report, отклоненные списками ACL, будут отброшены. Когда MLDv2 включен, эта команда поддерживает расширенные списки ACL для точной фильтрации информации о записи источника в сообщениях MLDv2. Когда полученное сообщение Report MLD имеет вид (S1,S2,S3…Sn,G), эта команда будет соответствовать (0,G) с использованием соответствующих списков ACL. Следовательно, чтобы нормально использовать эту команду, необходимо явно настроить (0, G) в расширенных списках ACL для фильтрации (S1,S2,S3…Sn,G)

Настройка максимального количества участников группы MLD

Команда	**ipv6 mld limit** *number* [**except** *access-list*]
Описание параметра	*number*: указывает максимальное количество участников группы MLD. Диапазон значений зависит от конкретного устройства. Значение интерфейса по умолчанию — 1024, глобальное — 65 536. **except** *access-list*: группы в списке доступа не учитываются. Список доступа представляет собой стандартный IP ACL. Значение варьируется от 1 до 99, 1300 до 1999 и название
Командный режим	Режим настройки интерфейса
Руководство по использованию	Режим глобальной конфигурации: ограничивает количество участников группы MLD на всем устройстве. Режим конфигурации интерфейса: ограничивает количество участников группы MLD интерфейса. Если количество участников группы превышает предел интерфейса или глобальный предел, последующие сообщения Report будут игнорироваться. Если настроен список исключений, сообщения Report в указанном диапазоне могут обрабатываться нормально. Поэтому участники группы не учитываются. Интерфейс и глобальные ограничения можно настроить отдельно. Если глобальное ограничение меньше ограничения интерфейса, используйте глобальное ограничение

4.4.4.6. Пример конфигурации

Настройка групповой фильтрации

Шаги настройки	• Настройте основные функции MLD. (пропущено) • Настройте адрес доступа таблицы канала 1 как (FF66::100/64). • Настройте группу для присоединения как FF66::05. • Настройте группу для присоединения как FF65::05
	QTECH(config)#ipv6 access-list acl QTECH(config-ipv6-acl)#permit ipv6 ::/64 ff66::100/64 QTECH(config-ipv6-acl)#permit ipv6 2222::3333/64 ff66::100/64 QTECH(config-ipv6-acl)#exit QTECH(config)# QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld access-group acl QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld join-group ff66::5 QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld join-group ff65::5
Проверка	Запустите команду **show ipv6 mld groups** [*interface-type interface-number*] [*group-address*] [**detail**] для просмотра информации о группе на интерфейсе
	QTECH#show ipv6 mld groups MLD Connected Group Membership Group Address Interface Uptime Expires Last Reporter ff66::5 GigabitEthernet 0/1 00:05:07 00:03:46 fe80::2d0:f8ff:fe22:33b1

Настройка максимального количества участников группы MLD

Шаги настройки	• Настройте основные функции MLD. (пропущено) • Настройте максимальное количество участников группы на интерфейсе как 5. • Добавьте информацию о группе (FF66::5-FF66::0B). • Посмотреть информацию о группе
	QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld limit 5 QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld join-group ff66::5 QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld join-group ff66::6 QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld join-group ff66::7 QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld join-group ff66::8 QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld join-group ff66::9

	QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld join-group ff66::A QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld join-group ff66::B
Проверка	Запустите команду **show ipv6 mld groups** [*interface-type interface-number*] [*group-address*] [**detail**] для просмотра информации о группе на интерфейсе
	MLD Connected Group Membership Group Address Interface Uptime Expires Last Reporter ff66::5 GigabitEthernet 0/1 00:00:36 00:04:00 fe80::2d0:f8ff:fe22:33b1 ff66::6 GigabitEthernet 0/1 00:00:34 00:04:01 fe80::2d0:f8ff:fe22:33b1 ff66::7 GigabitEthernet 0/1 00:00:22 00:04:13 fe80::2d0:f8ff:fe22:33b1 ff66::8 GigabitEthernet 0/1 00:00:18 00:04:19 fe80::2d0:f8ff:fe22:33b1 ff66::9 GigabitEthernet 0/1 00:00:14 00:04:21 fe80::2d0:f8ff:fe22:33b1

4.4.4.7. Распространенные ошибки

Основные функции MLD не включены.

4.4.5. MLD-прокси

4.4.5.1. Эффект конфигурации

Настройте функцию прокси-сервера маршрутизатора и соберите информацию о локальных участниках.

4.4.5.2. Примечания

Необходимо настроить основные функции MLD.

4.4.5.3. Шаги настройки

Настройка MLD PROXY-SERVICE

Опционально.

Эту функцию можно настроить на интерфейсе маршрутизаторов, напрямую подключенных к upstream-устройствам, если не указано иное.

Настройка MLD MROUTE–PROXY

Опционально

Эту функцию можно настроить на интерфейсе хостов, напрямую подключенных к downstream-устройствам, если не указано иное.

4.4.5.4. Проверка

- Настройте интерфейс, который напрямую соединяет интерфейс 7 и upstream-маршрутизатор, в качестве прокси-сервиса multicast.

- Настройте интерфейс, который напрямую соединяет интерфейс 1 и downstream-хост, в качестве прокси-сервера multicast.
- Настройте группы FF66::05 и FF66::06 для добавления к интерфейсу 1.
- Проверьте информацию текущей группы.

4.4.5.5. Связанные команды

Настройка MLD PROXY-SERVICE

Команда	**ipv6 mld proxy-service**
Командный режим	Режим настройки интерфейса
Руководство по использованию	Запустите команду **ipv6 mld proxy-service**, чтобы настроить upstream-интерфейс как интерфейс прокси-сервиса. Запустите команду **ipv6 mld mroute-proxy**, чтобы настроить downstream-интерфейс как интерфейс mroute-proxy. Настройте интерфейс прокси-сервиса для пересылки сообщений Query MLD на интерфейс mroute-proxy. Настройте интерфейс mroute-proxy для пересылки сообщений Report MLD на интерфейс прокси-сервиса. На устройстве можно настроить максимум 32 интерфейса прокси-сервиса. После получения сообщений Query MLD интерфейс прокси-сервиса отправляет ответ на основе записей участников группы MLD. Если вы запустите команду **switchport** на интерфейсе прокси-сервиса, команда **ipv6 mld mroute-proxy**, настроенная на интерфейсе mroute-proxy, будет автоматически удалена

Настройка MLD MROUTE–PROXY

Команда	**ipv6 mld mroute-proxy** *interface-type interface-number*
Командный режим	Режим настройки интерфейса
Руководство по использованию	Запустите команду **ipv6 mld proxy-service**, чтобы настроить upstream-интерфейс как интерфейс прокси-сервиса. Запустите команду **ipv6 mld mroute-proxy**, чтобы настроить downstream-интерфейс как интерфейс mroute-proxy. Настройте интерфейс прокси-сервиса для пересылки сообщений Query MLD на интерфейс mroute-proxy. Настройте интерфейс mroute-proxy для пересылки сообщений Report MLD на интерфейс прокси-сервиса

4.4.5.6. Пример конфигурации

Шаги настройки	• Настройте базовые функции MLD. (пропущено) • Настройте интерфейс 7 в качестве прокси-сервера. • Настройте интерфейс 1 в качестве прокси-сервера multicast. • Настройте группы FF66::05 и FF66::06 для добавления к интерфейсу 1
	QTECH(config-if-GigabitEthernet 0/7)#ipv6 mld proxy-service QTECH(config-if-GigabitEthernet 0/7)#exit QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld mroute-proxy gigabitEthernet 0/7 QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld join-group ff66::05 QTECH(config-if-GigabitEthernet 0/1)#ipv6 mld join-group ff66::06
Проверка	Запустите команду **show ipv6 mld groups** [*interface-type interface-number*] [*group-address*] [**detail**] для просмотра информации о группе на интерфейсе
	QTECH(config-if-GigabitEthernet 0/1)#show ipv6 mld groups MLD Connected Group Membership Group Address Interface Uptime Expires Last Reporter ff66::5 GigabitEthernet 0/1 00:00:11 00:04:31 fe80::2d0:f8ff:fe22:33b1 ff66::6 GigabitEthernet 0/1 00:00:11 00:04:33 fe80::2d0:f8ff:fe22:33b1 MLD Proxy-server Connected Group Membership Group Address Interface Uptime ff66::5 GigabitEthernet 0/7 00:00:11 ff66::6 GigabitEthernet 0/7 00:00:11

4.4.5.7. Распространенные ошибки

Основные функции MLD не включены.

4.4.6. Поддержка SSM-MAP

4.4.6.1. Эффект конфигурации

MLDv2 поддерживает фильтрацию источников, а MLDv1 — нет. Однако MLDv1 предоставляет функцию SSM-MAP для реализации фильтрации источников.

4.4.6.2. Примечания

Необходимо настроить основные функции MLD.

4.4.6.3. Шаги настройки

Включение SSM-MAP

Эту функцию необходимо настроить, если SSM-MAP.

Эту функцию необходимо включить на маршрутизаторе, где включен SSM-MAP.

Настройка таблицы статических каналов SSM-MAP

Опционально.

Эту функцию необходимо включить на маршрутизаторе, где включен SSM-MAP.

4.4.6.4. Проверка

Запустите команду **show ipv6 mld ssm-mapping** [*group-address*], чтобы отобразить информацию SSM-MAP.

4.4.6.5. Связанные команды

Включение SSM-MAP

Команда	**ipv6 mld ssm-map enable**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите команду **ipv6 mld ssm-map enable**, чтобы включить функцию SSM-MAP. Запустите команду **ipv6 mld ssm-map static** для настройки элементов таблицы статического сопоставления. Интерфейс использует MLDv2. При получении сообщений Report от MLDv1 интерфейс добавляет адрес источника статического сопоставления

Настройка таблицы статических каналов SSM-MAP

Команда	**ipv6 mld ssm-map static access-list source-address**
Описание параметра	**access-list**: определяет диапазон адресов группы, настроенны с помощью ACL. **source-address**: адрес источника
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите команду **ipv6 mld ssm-map enable**, чтобы включить функцию SSM-MAP. Запустите команду **ipv6 mld ssm-map static** для настройки элементов таблицы статического сопоставления.

	Интерфейс использует MLDv2. При получении сообщений Report от MLDv1 интерфейс добавляет адрес источника статического сопоставления

4.4.6.6. Пример конфигурации

Шаги настройки	• Настройте основные функции MLD. (пропущено) • Включите SSM-MAP. • Настройте таблицу статических каналов 3 SSM-MAP
	QTECH(config)#ipv6 mld ssm-map enable QTECH(config)#ipv6 mld ssm-map static 3 1500::5
Проверка	Запустите команду **show ipv6 mld ssm-mapping** [*group-address*], чтобы посмотреть информацию о сопоставлении SSM
	QTECH(config)#show ipv6 mld ssm-mapping SSM Mapping : Enabled Database : Static mappings configured

4.4.6.7. Распространенные ошибки

Основные функции MLD не включены.

4.5. Мониторинг

4.5.1. Очистка

Описание	Команда
Очищает записи участников динамической группы в MLD-кеш	**clear ipv6 mld group** [*group-address*] [*interface-type interface-number*]
Очищает всю статистику MLD и записи участников группы в интерфейсе	**clear ipv6 mld interface** *interface-type interface-number*

4.5.2. Отображение

Описание	Команда
Отображает группы, напрямую подключенные к устройству, и информацию о группах, полученную от MLD	**show ipv6 mld groups** [*group-address* | *interface-type interface-number*] [**detail**]

Описание	Команда
Отображает настройки интерфейса	**show ipv6 mld interface** [*interface-type interface-number*]
Отображает информацию SSM-MAP	**show ipv6 mld ssm-mapping** [*group-address*]

4.5.2.1. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Поэтому отключайте отладку сразу после использования.

Описание	Команда
Отображает состояние переключателя отладки MLD	**show debugging**
Отладка всей информации MLD	**debug ipv6 mld all**
Отладка разрешения пакетов MLD	**debug ipv6 mld decode**
Отладка кодирования пакетов MLD	**debug ipv6 mld encode**
Отладка информации события MLD	**debug ipv6 mld events**
Отладка MLD Finite State Machine (FSM)	**debug ipv6 mld fsm**
Отладка информации state machine MLD	**debug ipv6 mld tib**
Отладка предупреждений MLD	**debug ipv6 mld warning**

5. НАСТРОЙКА PIM-DM

5.1. Обзор

Protocol Independent Multicast (PIM) — это протокол внутридоменной multicast-маршрутизации.

Источник multicast отправляет пакет на групповой адрес. Пакет пересылается сетевыми устройствами hop за hop-ом и, наконец, достигает участников группы. На сетевых устройствах уровня 3 PIM используется для создания и обслуживания записей multicast-маршрутизации для поддержки multicast-пересылки.

PIM работает в двух режимах: Protocol Independent Multicast - Sparse Mode (PIM-SM) и Protocol Independent Multicast - Dense Mode (PIM-DM).

- PIM-SM применим к крупномасштабным сетям, где участники группы редко распределены в широком диапазоне.
- PIM-DM применим к небольшим сетям, где члены группы густо распределены.

5.1.1. Протоколы и стандарты

- RFC3973: Protocol Independent Multicast - Dense Mode (PIM-DM).
- RFC2715: правила совместимости для протоколов multicast-маршрутизации.

5.2. Приложения

Приложение	Описание
Предоставление услуги multicast в одной сети	Услуга multicast предоставляется в той же сети
Применение PIM-DM в среде горячего резервирования	Запустите PIM-DM в среде горячего резервного копирования

5.2.1. Предоставление услуги multicast в одной сети

5.2.1.1. Сценарий

Сервис multicast предоставляется в той же сети.

В качестве примера взят следующий Рисунок:

- Источник multicast отправляет multicast-пакет, а приемник A и приемник B в одной сети получают multicast-пакет.

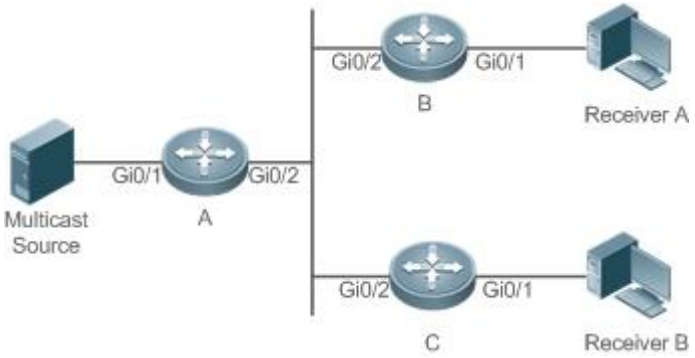

Рисунок 5-1.

A, B и C — маршрутизаторы уровня 3.

Источник multicast подключен к интерфейсу Gi0/1 устройства A, приемник A подключен к интерфейсу Gi0/1 устройства B, а приемник B подключен к интерфейсу Gi0/1 устройства C.

5.2.1.2. Развертывание

- Запустите протокол Open Shortest Path First (OSPF) в той же сети, чтобы реализовать unicast-маршрутизацию.
- Запустите протокол PIM-DM в той же сети, чтобы реализовать multicast-маршрутизацию.
- Запустите Internet Group Management Protocol (IGMP) в сегменте сети хоста пользователя, чтобы реализовать управление участниками группы.

5.2.2. Применение PIM-DM в среде горячего резервирования

5.2.2.1. Сценарий

В среде горячего резервного копирования запустите PIM-DM. Устройство выполняет горячее резервное переключение, чтобы гарантировать, что трафик не прерывается.

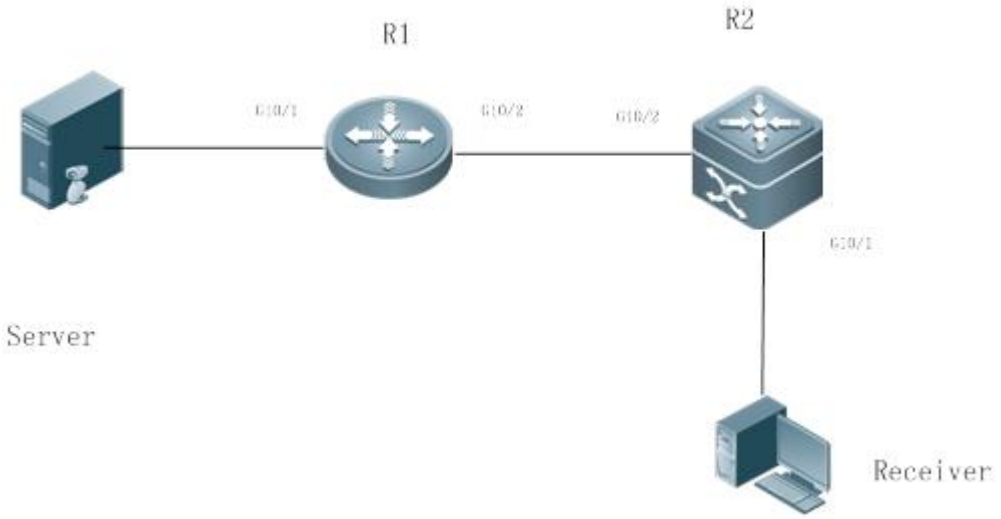

Рисунок 5-2.

R1 подключен к видеосерверу, R2 напрямую подключен к Приемнику, а R2 работает в режиме горячего резервирования.

Протокол multicast уровня 3 работает на маршрутизаторах R1 и R2.

5.2.2.2. Развертывание

- Запустите OSPF на маршрутизаторах R1 и R2, чтобы реализовать unicast-маршрутизацию.
- Запустите PIM-DM на маршрутизаторах R1 и R2, чтобы реализовать multicast-маршрутизацию.
- Заставьте R2 работать в среде горячего резервного копирования.

ПРИМЕЧАНИЯ: R2 может выполнять горячее резервное переключение в среде горячего резервного копирования. В этом случае интервал Query пакетов Hello PIM (значение по умолчанию — 30 секунд) необходимо настроить на маршрутизаторе R2, поскольку срок действия таймера keepalive соседа в пакетах Hello PIM маршрутизатора R1 мог истечь (значение по умолчанию в 3,5 раза превышает интервал Query, то есть 105 секунд). Функция multicast в настоящее время опирается на функцию unicast-рассылки, и функция multicast начинает конвергенцию после завершения конвергенции функции unicast-рассылки. Например, время конвергенции graceful restart (GR) (плавной перезагрузки) по умолчанию для функции unicast-рассылки составляет 120 секунд. Рекомендуется установить интервал Query пакетов Hello PIM равным 60 секундам. Время keepalive соседа в пакетах PIM Hello составляет 210 секунд. В этом сценарии интервал Query пакетов Hello PIM должен быть установлен со ссылкой на время сходимости GR функции unicast-рассылки, а значение, в 3,5 раза превышающее интервал Query пакетов Hello PIM, должно быть больше, чем время сходимости GR функции unicast-рассылки. В среде горячего резервного копирования рекомендуется, чтобы интервал Query пакетов Hello PIM был больше значения по умолчанию (30 секунд). В противном случае таймер keepalive соседа в пакетах Hello PIM на peer end истечет во время переключения горячего резервного копирования.

5.3. Функции

5.3.1. Базовые определения

PIM-маршрутизатор и PIM-интерфейс

Маршрутизаторы, на которых включен протокол PIM, называются маршрутизаторами PIM. Интерфейсы, на которых включен протокол PIM, называются интерфейсами PIM.

Multicast-пакеты пересылаются на PIM-маршрутизаторы. PIM-интерфейсы, на которых принимаются multicast-пакеты, называются upstream-интерфейсами, а PIM-интерфейсы, на которых отправляются multicast-пакеты, называются downstream-интерфейсами.

Сегменты сети, в которых расположены upstream-интерфейсы, называются upstream сетевыми сегментами. Сегменты сети, в которых расположены downstream-интерфейсы, называются downstream сетевыми сегментами.

Сеть PIM и домен PIM

PIM-маршрутизаторы подключаются через PIM-интерфейсы и образуют сеть PIM.

На некоторых интерфейсах PIM можно установить границы, чтобы разделить большую сеть PIM на несколько доменов PIM. Границы могут отклонять определенные multicast-пакеты или ограничивать передачу сообщений PIM.

Multicast Distribution Tree

Multicast-пакеты — это пакеты, передаваемые из одной точки в несколько точек. Путь пересылки имеет древовидную структуру. Этот путь пересылки называется Multicast Distribution Tree (MDT).

(*,G), (S,G)

- (*,G): пакеты, отправленные из любого источника в группу G, соответствующие записи маршрутизации и путь пересылки, называемый Rendezvous Point Tree (RPT).
- (S,G): пакеты, отправленные из источника S в группу G, соответствующие записи маршрутизации и путь пересылки, называемый Shortest Path Tree (SPT).

5.3.1.1. Обзор

Особенность	Описание
Сосед PIM-DM	Отношения соседства устанавливаются между маршрутизаторами PIM для формирования сети PIM
PIM-DM MDT	PIM-DM создает MDT, используя flooding, pruning и grafting
PIM-DM SRM	PIM-DM использует State Refresh Message (SRM) для обновления состояния сети
MIB	Диспетчер Simple Network Management Protocol (SNMP) использует информацию из Management Information Base (MIB) для непосредственного управления функцией PIM-DM

5.3.2. Сосед PIM-DM

Отношения соседства устанавливаются между маршрутизаторами PIM для формирования сети PIM. Отношения соседства должны быть установлены между маршрутизаторами PIM, прежде чем можно будет обмениваться управляющими сообщениями PIM или пересылать multicast-пакеты.

5.3.2.1. Принцип работы

Сообщение Hello отправляется из интерфейса PIM. Для multicast-пакета IPv4 с инкапсулированным сообщением Hello адресом назначения является 224.0.0.13 (с указанием всех маршрутизаторов PIM в одном сегменте сети), исходным адресом является IP-адрес интерфейса PIM и значение Time To Live (TTL) равно 1. Для multicast-пакета IPv6 с инкапсулированным сообщением Hello адрес назначения — ff02::d.

Функция сообщения Hello: оно используется для обнаружения соседей, координации параметров протокола и поддержания отношений соседства.

Обнаружение соседей

PIM-маршрутизаторы в том же сегменте сети получают multicast-пакеты с адреса назначения 224.0.0.13 или ff02::d. Таким образом, PIM-маршрутизаторы получают информацию о соседях и устанавливают отношения соседства.

Когда интерфейс PIM включен или обнаруживает нового соседа, сообщение Triggered-Hello-Delay используется для генерации случайного времени. Через некоторое время интерфейс отправляет пакеты Hello.

Координация параметров протокола

Сообщение Hello включает в себя несколько параметров протокола, которые описаны следующим образом:

– DR_Priority: интерфейсы маршрутизатора конкурируют за designated router (DR) на основе своих приоритетов DR. Более высокий приоритет означает более высокий шанс на победу.

– Holdtime: время, в течение которого сосед удерживается в достижимом состоянии.

– LAN_Delay: задержка LAN для передачи сообщения Prune в общем сегменте сети.

– Override-Interval: время Prune override, передаваемое в сообщении Hello.

Когда маршрутизатор PIM получает сообщение Prune от upstream-интерфейса, это указывает на наличие downstream-интерфейсов в общем сегменте сети. Если маршрутизатору PIM по-прежнему необходимо получать multicast-данные, маршрутизатор PIM должен отправить сообщение Prune Override upstream-интерфейсу в течение Override-Interval.

LAN_Delay + Override-Interval = PPT (Prune-Pending Timer). После того, как маршрутизатор PIM получает сообщение Prune от downstream-интерфейса, маршрутизатор PIM не будет немедленно выполнять pruning до тех пор, пока не истечет время PPT. Если во время PPT маршрутизатор PIM получает сообщение Prune rejection от downstream-интерфейса, маршрутизатор PIM отменяет pruning.

Поддержание отношений с соседями

Сообщение Hello периодически отправляется между маршрутизаторами PIM. Если пакет Hello не получен от соседа PIM в течение времени Holdtime, сосед считается недоступным и удаляется из списка соседей. Любое изменение соседей PIM приведет к изменению топологии multicast в сети. Если upstream- или downstream-сосед в MDT недоступен, multicast-маршруты снова сходятся, и MDT изменяется.

5.3.2.2. Сопутствующая конфигурация

Включение PIM-DM на интерфейсе

По умолчанию PIM-DM отключен на интерфейсе.

Используйте команду **ip pim dense-mode**, чтобы включить или отключить PIM-DM на интерфейсе.

PIM-DM должен быть включен на интерфейсе, чтобы включить интерфейс в протокол PIM.

Настройка интервала сообщений Hello на интерфейсе

По умолчанию сообщение Hello отправляется с интервалом в 30 секунд.

Команда **ip pim query-interval** *interval-seconds* используется для настройки интервала сообщений Hello. Значение интервала находится в диапазоне от 1 до 65 535.

Сообщение Hello передается реже, если значение интервала в секундах больше.

5.3.3. PIM-DM MDT

PIM-DM создает MDT, используя flooding, pruning и grafting.

5.3.3.1. Принцип работы

Когда источник multicast отправляет multicast-пакеты, система может пересылать их на исходящие интерфейсы соседей multicast и локальных участников в зависимости от результатов проверки Reverse Path Forwarding (RPF). Пакеты, не прошедшие проверку RPF, отбрасываются. Если исходящий интерфейс существует, для пересылки принимаются пакеты, прошедшие проверку RPF; если исходящий интерфейс отсутствует, пакет prune отправляется upstream-устройствам. После того как upstream-интерфейс получает пакет prune, upstream-интерфейс переводит исходный интерфейс пакета prune в

состояние Pruned и устанавливает таймер Prune Timer (PT). Таким образом создается MDT на основе источника multicast.

Когда система получает сообщение Join от локального участника, если downstream-устройство в состоянии Pruned отправляет сообщение Graft upstream-устройству, upstream-устройство возвращает сообщение Graft Ack и возобновляет multicast-пересылку на интерфейсы downstream-устройства после получения сообщения Graft.

ПРИМЕЧАНИЕ: при развертывании сети, когда несколько соседей PIM-DM создаются через несколько каналов между устройствами, и downstream-устройства не имеют или имеют меньшую потребность в приеме, загрузка ЦП может быть высокой. В этом сценарии рекомендуется развернуть среду PIM-SM.

5.3.3.2. Сопутствующая конфигурация

Настройка интервала Prune Override на интерфейсе

По умолчанию интервал Prune Override составляет 500 мс.

Команда **ip pim override-interval** *interval-milliseconds* используется для изменения интервала Prune Override.

5.3.4. PIM-DM SRM

PIM-DM использует SRM для обновления состояния сети.

5.3.4.1. Принцип работы

Устройства, подключенные к источнику multicast, периодически отправляют SRM downstream-устройствам, чтобы уведомить об изменениях топологии сети. После получения SRM соседние устройства, получающие SRM, добавляют к сообщениям информацию о состоянии локальной топологии, изменяя некоторые поля в SRM, и отправляют сообщения downstream-устройствам. Когда сообщения достигают конечных устройств, информация о состоянии всей сети обновляется.

5.3.4.2. Сопутствующая конфигурация

Отключение обработки и пересылки SRM

По умолчанию обработка и пересылка SRM включены.

Команда **ip pim state-refresh disable** используется для отключения обработки и пересылки SRM.

ПРИМЕЧАНИЕ: отключение функции SRM может привести к повторной конвергенции PIM-DM MDT, что приводит к ненужной потере полосы пропускания и flapping-у таблицы multicast-маршрутизации. Поэтому рекомендуется не отключать SRM в обычных условиях.

Установка интервала SRM

По умолчанию SRM отправляется с интервалом 60 секунд.

Команда **ip pim state-refresh origination-interval** *interval-seconds* используется для регулировки интервала SRM. Значение интервала находится в диапазоне от 1 до 100.

SRM передаются реже, если значение *interval-seconds* больше.

ПРИМЕЧАНИЕ: только устройства, которые напрямую подключены к источнику multicast, будут периодически отправлять PIM SRM на downstream-интерфейсы. Для устройства, не подключенного напрямую к источнику multicast, интервал SRM на его downstream-интерфейсах недействителен.

5.3.5. MIB

Подключенный к другим агентам диспетчер Simple Network Management Protocol (SNMP) использует информацию из Management Information Base (MIB) для непосредственного управления функцией PIM-DM.

5.3.5.1. Принцип работы

MIB определяет переменные (а именно информацию, которая может быть запрошена и установлена процессом управления), поддерживаемые сетевыми элементами, и напрямую управляет функцией PIM-DM.

5.3.5.2. Сопутствующая конфигурация

Включение MIB PIM-DM

По умолчанию функция PIM-DM MIB включена.

Команда **ip pim mib dense-mode** используется для включения функции PIM-DM MIB.

5.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций PIM-DM	(Обязательно) Используется для создания сервиса multicast	
	ip multicast-routing	Включает multicast-маршрутизацию IPv4
	ip pim dense-mode	Включает PIM-DM
Настройка соседей PIM-DM	(Опционально) Используется для ограничения пар (S,G) допустимых multicast-пакетов в модели Any Source Multicast (ASM)	
	ip pim query-interval *interval-seconds*	Устанавливает интервал сообщений Hello на интерфейсе
	ip pim propagation-delay *interval-milliseconds*	Устанавливает задержку prune propagation на интерфейсе
	ip pim override-interval *interval-milliseconds*	Устанавливает интервал prune override на интерфейсе
	ip pim neighbor-filter *access-list*	Настраивает фильтрацию соседей на интерфейсе
Настройка SRM PIM-DM	**ip pim state-refresh disable**	Отключает обработку и пересылку SRM

Конфигурация	Описание и команда	
Настройка SRM PIM-DM	**ip pim state-refresh origination-interval** *interval-seconds*	Устанавливает интервал SRM на интерфейсе
Настройка MIB PIM-DM	**ip pim mib dense-mode**	Включает MIB PIM-DM

5.4.1. Настройка основных функций PIM-DM

5.4.1.1. Эффект конфигурации

Создает сеть PIM-DM и обеспечивает источники данных и пользовательские терминалы в сети сервисом multicast IPv4.

5.4.1.2. Примечания

PIM-DM необходимо использовать unicast-маршруты, существующие в сети. Поэтому в сети необходимо настроить unicast-маршрутизацию IPv4.

5.4.1.3. Шаги настройки

Включение multicast-маршрутизации IPv4

- Обязательный
- Multicast-маршрутизация IPv4 должна быть включена на каждом маршрутизаторе, если не указано иное.

Включение PIM-DM

- Обязательный
- PIM-DM следует включить на следующих интерфейсах, если не указано иное: взаимосвязанных интерфейсах на маршрутизаторах и интерфейсах, соединяющих источники multicast и пользовательские хосты.

5.4.1.4. Проверка

Сделайте, чтобы источники multicast отправляли multicast-пакеты и хосты пользователей присоединялись к группам.

- Проверьте, могут ли пользовательские хосты успешно получать пакеты из каждой группы.
- Проверьте, созданы ли на маршрутизаторах правильные записи маршрутизации PIM-DM.

5.4.1.5. Связанные команды

Включение multicast-маршрутизации IPv4

Команда	**ip multicast-routing**
Командный режим	Режим глобальной конфигурации

Включение PIM-DM

Команда	**ip pim dense-mode**
Командный режим	Режим настройки интерфейса
Руководство по использованию	PIM-интерфейсы должны находиться на уровне 3, включая: интерфейсы маршрутизации, агрегируемые порты (AP), виртуальные интерфейсы коммутатора (SVI) и интерфейсы loopback. Для всех интерфейсов PIM должны быть доступны unicast-маршруты IPv4

Отображение таблицы маршрутизации PIM-DM

Команда	**show ip pim dense-mode mroute** [*group-or-source-address* [*group-or-source-address*]] [**summary**]
Описание параметра	*group-or-source-address*: указывает адрес группы или адрес источника. *group-or-source-address*: указывает групповой адрес или адрес источника (два адреса не могут быть групповыми адресами или адресами источника одновременно). **summary**: отображает сводку таблицы маршрутизации
Командный режим	Режим Privileged EXEC/Режим глобальной конфигурации/Режим конфигурации интерфейса
Руководство по использованию	Проверьте, предоставлено ли достаточно записей маршрутизации. Проверьте списки upstream- и downstream-интерфейсов и убедитесь, что создано правильное «дерево» SPT

5.4.1.6. Пример конфигурации

Включение multicast-маршрутизации IPv4 в сети IPv4

Сценарий:

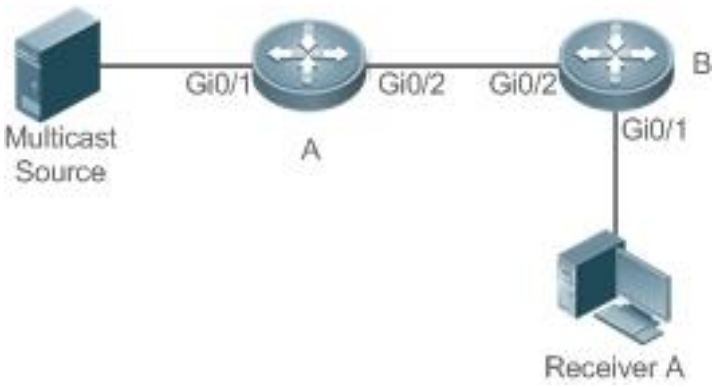

Рисунок 5-3.

Шаги настройки	• Настройте протоколы unicast-маршрутизации IPv4 (например, OSPF) на всех маршрутизаторах. • Включите функцию multicast-маршрутизации IPv4 на всех маршрутизаторах. • Включите функцию PIM-DM на всех взаимосвязанных интерфейсах маршрутизаторов, источника и приемника
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if)# ip pim dense-mode A(config-if)# exit A(config)# interface GigabitEthernet 0/2 A(config-if)# ip pim dense-mode A(config-if)# exit
B	B# configure terminal B(config)# ip multicast-routing B(config)# interface GigabitEthernet 0/1 B(config-if)# ip pim dense-mode B(config-if)# exit B(config)# interface GigabitEthernet 0/2 B(config-if)# ip pim dense-mode B(config-if)# exit
Проверка	Настройте источник multicast (192.168.1.10) для отправки пакетов в G (229.1.1.1). Сделайте, чтобы приемник A присоединился к G. • Проверьте, получены ли multicast-пакеты от источника G приемником A. • Проверьте таблицы маршрутизации PIM-DM на маршрутизаторах A и B
A	A# show ip pim dense-mode mroute PIM-DM Multicast Routing Table (192.168.1.10, 229.1.1.1) MRT lifetime expires in 182 seconds Source directly connected on GigabitEthernet 0/1 State-Refresh Originator State: Originator SRT:57, SAT:147 Upstream IF: GigabitEthernet 0/1

	Upstream State: Forwarding Assert State: NoInfo Downstream IF List: GigabitEthernet 0/2, in -olist-: Downstream State: NoInfo Assert State: NoInfo
B	B# show ip pim dense-mode mroute PIM-DM Multicast Routing Table (192.168.1.10, 229.1.1.1) MRT lifetime expires in 130 seconds RPF Neighbor: 192.168.2.1, Nexthop: 192.168.2.1, GigabitEthernet 0/2 Upstream IF: GigabitEthernet 0/2 Upstream State: Forwarding Assert State: Loser, AT:125 Downstream IF List: GigabitEthernet 0/1, in -olist-: Downstream State: NoInfo Assert State: NoInfo

5.4.1.7. Распространенные ошибки

- Unicast-маршрутизация IPv4 настроена неправильно.
- Multicast-маршрутизация IPv4 не включена на определенном маршрутизаторе.
- PIM-DM не включен на определенном интерфейсе.

5.4.2. Настройка соседей PIM-DM

5.4.2.1. Эффект конфигурации

- Согласуйте параметры протокола и настройте параметры в пакете Hello.
- Включите фильтрацию соседей, чтобы повысить безопасность сети.

5.4.2.2. Примечания

Необходимо настроить основные функции PIM-DM.

5.4.2.3. Шаги настройки

Установите параметры на интерфейсах маршрутизатора PIM, если не указано иное.

5.4.2.4. Проверка

- Задайте параметры в пакете Hello на интерфейсе и запустите команду **debug ip pim dense-mode encode**, чтобы проверить параметры.

- Включите фильтрацию соседей и запустите команду **show ip pim dense-mode decode**, чтобы отобразить информацию о фильтрации соседей.
- Запустите команду **show running-config interface** [*interface-type interface-number*], чтобы отобразить конфигурации интерфейса.

5.4.2.5. Связанные команды

Настройка интервала сообщений Hello

Команда	**ip pim query-interval** *interval-seconds*
Описание параметра	*interval-seconds*: значение варьируется от 1 до 65 535 в секундах
Командный режим	Режим настройки интерфейса
Руководство по использованию	Если установлен интервал Hello, значение holdtime будет обновлено в 3,5 раза
ПРИМЕЧАНИЕ: каждый раз, когда обновляется интервал сообщений Hello, значение holdtime автоматически обновляется как 3,5-кратное значение интервала. Если результат интервала сообщений Hello, умноженный на 3,5, превышает 65 535, значение holdtime обновляется как 65 535	

Настройка задержки Prune Propagation

Команда	**ip pim propagation-delay** *interval-milliseconds*
Описание параметра	*interval-milliseconds*: значение варьируется от 1 до 32 767 в миллисекундах
Командный режим	Режим настройки интерфейса
Руководство по использованию	Установите **propagation-delay** интерфейса, то есть настройте задержку prune propagation интерфейса

Установка интервала Prune Override

Команда	**ip pim override-interval** *interval-milliseconds*
Описание параметра	*interval-milliseconds*: значение варьируется от 1 до 32 767 в миллисекундах
Командный режим	Режим настройки интерфейса

Руководство по использованию	Установите **override-interval** интерфейса, то есть настройте время prune override интерфейса

Настройка фильтрации соседей PIM-DM

Команда	**ip pim neighbor-filter** *access-list*
Описание параметра	*access-list*: поддерживаемый список ACL находится в диапазоне от 1 до 99. Также поддерживается присвоение имени ACL
Командный режим	Режим настройки интерфейса
Руководство по использованию	Только адреса, соответствующие условиям фильтрации ACL, могут использоваться в качестве соседей PIM текущего интерфейса. В противном случае отфильтрованные адреса не могут быть соседями. Peering означает обмен пакетами протоколов между соседями PIM. Если Peering с устройством PIM приостановлен, отношения соседства с ним не могут быть сформированы, поэтому пакеты протокола PIM не будут получены от устройства

5.4.2.6. Пример конфигурации

Настройка соседей PIM-DM в сети IPv4

Сценарий:

Рисунок 5-4.

Шаги настройки	• Настройте базовые функции PIM-DM (пропущено). • Установите параметры протокола в пакете Hello на интерфейсе Gi0/1 устройства A
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if)# ip pim query-interval 60 A(config-if)# ip pim propagation-delay 800 A(config-if)# ip pim override-interval 1000 A(config-if)# exit

Проверка	• Запустите команду **show running-config interface** [*interface-type interface-number*], чтобы отобразить конфигурации интерфейса. • Запустите команду **debug ip pim dense-mode encode** для отладки параметров в пакете Hello
A	A# (config)#show running-config interface gigabitEthernet 0/1 Building configuration... Current configuration : 245 bytes ! interface GigabitEthernet 0/1 ip pim dense-mode ip pim query-interval 60 ip pim propagation-delay 800 ip pim override-interval 1000
	A# debug ip pim dense-mode encode *Dec 22 15:00:58: %7: [ENCODE] Enc Hello: Hello Hold-Time 210 *Dec 22 15:00:58: %7: [ENCODE] Enc Hello: Hello Gen-ID 1362200073 *Dec 22 15:00:58: %7: [ENCODE] Enc Hello: Hello PD=800 ms, OI=1000 ms *Dec 22 15:00:58: %7: [ENCODE] Enc Hello: Hello SR-Interval 60 *Dec 22 15:00:58: %7: [ENCODE] Enc Msg Hdr: Hello Checksum=65396, MsgLen=34 Assert State: Loser, AT:125

Настройка фильтрации соседей PIM-DM в сети IPv4

Сценарий:

Рисунок 5-5.

Шаги настройки	• Настройте базовые функции PIM-DM (пропущено). • Настройте ACL на устройстве A. • Настройте фильтрацию соседей PIM на интерфейсе Gi0/1 устройства A
A	A# configure terminal

	A(config)# interface GigabitEthernet 0/1 A(config-if)# ip pim query-interval 60 A(config-if)# ip pim propagation-delay 800 A(config-if)# ip pim override-interval 1000 A(config-if)# exit
Проверка	• Запустите команду **show running-config interface** [*interface-type interface-number*], чтобы отобразить конфигурации интерфейса. • Запустите команду **debug ip pim dense-mode decode** для отладки параметров в пакете Hello
A	A#show running-config interface gigabitEthernet 0/2 Building configuration... Current configuration : 187 bytes ! interface GigabitEthernet 0/1 ip pim dense-mode ip pim neighbor-filter pim-dm
	A# debug ip pim dense-mode decode Dec 22 15:15:47: %7: [DECODE] Dec Msg: PIM Hello message, version 2 Dec 22 15:09:47: %7: [DECODE] Dec Msg: Neighbor 192.168.2.2/32 on GigabitEthernet 0/1 denied by access-list pim-dm

5.4.2.7. Распространенные ошибки

- Unicast-маршрутизация IPv4 настроена неправильно.
- Multicast-маршрутизация IPv4 не включена на определенном маршрутизаторе.
- PIM-DM не включен на определенном интерфейсе.

5.4.3. Настройка SRM PIM-DM

5.4.3.1. Эффект конфигурации

- Включите или отключите функцию PIM-DM SRM.
- Отрегулируйте интервал SRM.

5.4.3.2. Примечания

Необходимо настроить основные функции PIM-DM.

5.4.3.3. Шаги настройки

Интервал SRM применим только к интерфейсам маршрутизатора PIM, которые напрямую подключены к источнику multicast.

5.4.3.4. Проверка

- Настройте SRM PIM-DM и запустите команду **show running-config**, чтобы отобразить состояние SRM.
- Запустите команду **show ip pim dense-mode track**, чтобы отобразить номер SRM.
- Запустите команду **show running-config interface** [*interface-type interface-number*], чтобы отобразить конфигурации интерфейса.

5.4.3.5. Связанные команды

Отключение обработки и пересылки SRM

Команда	**ip pim state-refresh disable**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если обработка и пересылка SRM отключены, опция State Refresh Capable не включается в пакет Hello и не обрабатывается при получении пакета Hello. Отключение функции SRM может привести к повторной конвергенции PIM-DM MDT, что приводит к ненужной потере полосы пропускания и flapping-у таблицы multicast-маршрутизации. Поэтому рекомендуется не отключать эту функцию в обычных условиях

Установка интервала SRM

Команда	**ip pim state-refresh origination-interval** *interval-seconds*
Описание параметра	*interval-seconds*: значение варьируется от 1 до 100 в секундах
Командный режим	Режим настройки интерфейса

5.4.3.6. Пример конфигурации

Отключение обработки и пересылки SRM на интерфейсе сети IPv4

Сценарий:

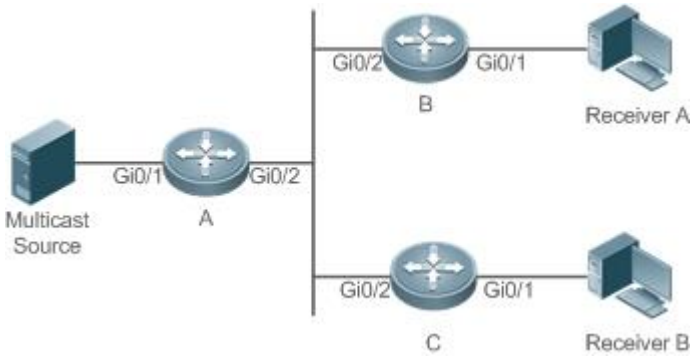

Рисунок 5-6.

Шаги настройки	• Настройте базовые функции PIM-DM (пропущено). • Отключите обработку и пересылку PIM-DM SRM на интерфейсе устройства A
A	A# configure terminal A(config)# ip pim state-refresh disable
Проверка	Запустите команду **show running-config**, чтобы проверить конфигурацию
A	A# (config)# show running-config … ! ip pim state-refresh disable ! …

Настройка интервала SRM в сети IPv4

Сценарий:

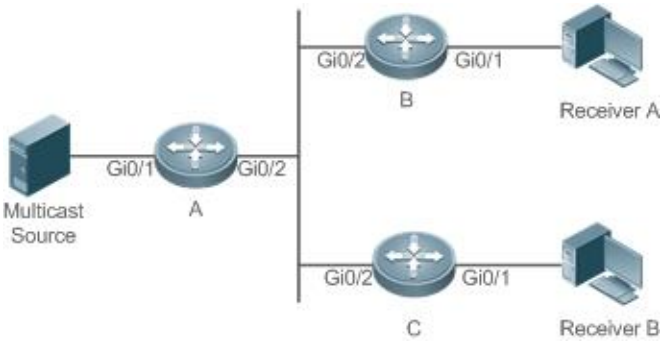

Рисунок 5-7.

Шаги настройки	• Настройте базовые функции PIM-DM (пропущено). • Установите интервал SRM PIM-DM на интерфейсе Gi0/1 устройства A
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if)# ip pim state-refresh origination-interval 5 A(config-if)# exit
Проверка	• Запустите команду **show running-config interface** [*interface-type interface-number*], чтобы отобразить конфигурации интерфейса. • Запустите команду **show ip pim dense-mode track**, чтобы отобразить номер SRM
A	A#show running-config interface gigabitEthernet 0/1

	Building configuration... Current configuration : 201 bytes ! interface GigabitEthernet 0/1 ip pim dense-mode ip pim state-refresh origination-interval 5
	A #show ip pim dense-mode track PIM packet counters Elapsed time since counters cleared: 00:18:54 Received sent Valid PIMDM packets: 38 102 Hello: 38 76 Join/Prune: 0 0 Graft: 0 0 Graft-Ack: 0 0 Assert: 0 0 State-Refresh: 0 26 PIM-SM-Register: 0 PIM-SM-Register-Stop: 0 PIM-SM-BSM: 0 PIM-SM-C-RP-ADV: 0 Unknown Type: 0 Errors: Malformed packets: 0 Bad checksums: 0 Unknown PIM version: 0 Send errors: 0

5.4.3.7. Распространенные ошибки

- Unicast-маршрутизация IPv4 настроена неправильно.
- Multicast-маршрутизация IPv4 не включена на определенном маршрутизаторе.
- PIM-DM не включен на определенном интерфейсе.

5.4.4. Настройка MIB PIM-DM

5.4.4.1. Эффект конфигурации

Включите функцию MIB для PIM-DM.

5.4.4.2. Проверка

Настройте функцию MIB PIM-SM и запустите команду **show running-config**, чтобы проверить, настроена ли эта функция.

5.4.4.3. Связанные команды

Включение MIB PIM-DM

Команда	**ip pim mib dense-mode**
Командный режим	Режим глобальной конфигурации

5.5. Мониторинг

5.5.1. Очистка

Описание	Команда
Сбрасывает время начала статистики и очищает счетчики пакетов PIM-DM	**clear ip pim dense-mode track**

5.5.2. Отображение

Описание	Команда
Отображает справочную информацию по командам с IP PIM в качестве ключевого слова	**ip pim help**
Отображает информацию PIM-DM интерфейса	**show ip pim dense-mode interface** [*interface-type interface-number*] [**detail**]
Отображает соседей PIM-DM	**show ip pim dense-mode neighbor** [*interface-type interface-number*]
Отображает информацию о next-hop PIM-DM	**show ip pim dense-mode nexthop**
Отображает таблицу маршрутизации PIM-DM	**show ip pim dense-mode mroute** [*group-or-source-address* [*group-or-source-address*]] [**summary**]

Описание	Команда
Отображает количество отправленных и полученных пакетов PIM-DM с момента начала статистики	**show ip pim dense-mode track**

6. НАСТРОЙКА PIM-SM

6.1. Обзор

Protocol Independent Multicast (PIM) — это протокол внутридоменной multicast-маршрутизации.

Источник multicast отправляет пакет на групповой адрес. Пакет пересылается сетевыми устройствами hop за hop-ом и, наконец, достигает участников группы. На сетевых устройствах уровня 3 PIM используется для создания и обслуживания записей multicast-маршрутизации для поддержки multicast-пересылки.

PIM работает в двух режимах: Protocol Independent Multicast - Sparse Mode (PIM-SM) и Protocol Independent Multicast - Dense Mode (PIM-DM).

- PIM-SM применим к крупномасштабным сетям, где участники группы распределены в широком пространстве редко.
- PIM-DM применим к небольшим сетям, где члены группы густо распределены.

6.1.1. Протоколы и стандарты

- RFC4601: Protocol Independent Multicast -Sparse Mode (PIM-SM).
- RFC5059: механизм Bootstrap Router (BSR) для Protocol Independent Multicast (PIM).
- RFC3962: Protocol Independent Multicast - Dense Mode protocol.
- RFC4607: Multicast-рассылка с учетом источника для IP.

6.2. Приложения

Приложение	Описание
Включение ASM для PIM-SM	Приемник принимает любой источник multicast
Включение SSM для PIM-SM	Приемник получает только конкретный источник multicast
Применение PIM-SM в среде горячего резервного копирования	Запустите PIM-SM в среде горячего резервного копирования

6.2.1. Включение ASM для PIM-SM

6.2.1.1. Сценарий

Предоставляет сервисы multicast только в пределах одного домена.

Например, на следующем рисунке приемник принимает любой источник multicast.

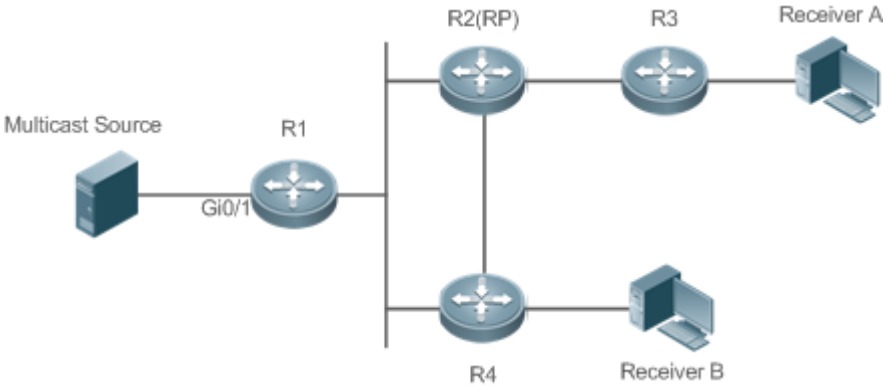

Рисунок 6-1.

R1 подключен непосредственно к источнику multicast.

R2 работает как rendezvous point (RP).

R3 подключен напрямую к приемнику A.

R4 подключен напрямую к приемнику B.

6.2.1.2. Развертывание

- Запустите протокол Open Shortest Path First (OSPF), чтобы реализовать unicast-маршрутизацию.
- Запустите PIM-SM, чтобы реализовать multicast-маршрутизацию.
- Запустите Internet Group Management Protocol (IGMP) в сегменте сети хоста пользователя для управления участниками группы.

6.2.2. Включение SSM для PIM-SM

6.2.2.1. Сценарий

Предоставляет услуги multicast только в пределах одного домена.

Например, на следующем рисунке приемник получает определенный источник multicast.

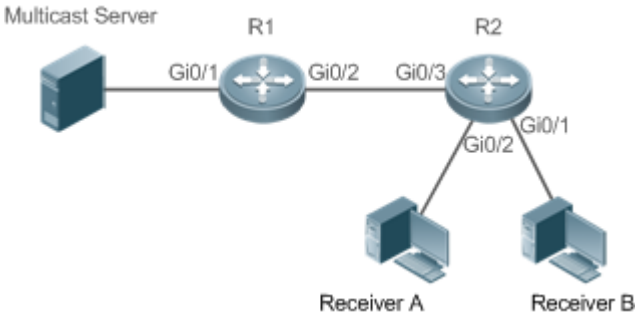

Рисунок 6-2.

R1 подключен непосредственно к источнику multicast.

R2 служит в качестве RP.

R2 подключен напрямую к приемнику A.

R2 подключен напрямую к приемнику B.

6.2.2.2. Развертывание

- Запустите протокол OSPF для реализации unicast-маршрутизации.
- Запустите PIM-SM, чтобы реализовать multicast-маршрутизацию.
- Запустите multicast-рассылку PIM-SM для конкретного источника (SSM) в домене.
- Запустите IGMPv3 в сегменте сети хоста пользователя для управления участниками группы.

6.2.3. Применение PIM-SM в среде горячего резервного копирования

6.2.3.1. Сценарий

В среде горячего резервного копирования запустите PIM-SM. Устройство выполняет горячее резервное переключение, чтобы гарантировать, что трафик не прерывается.

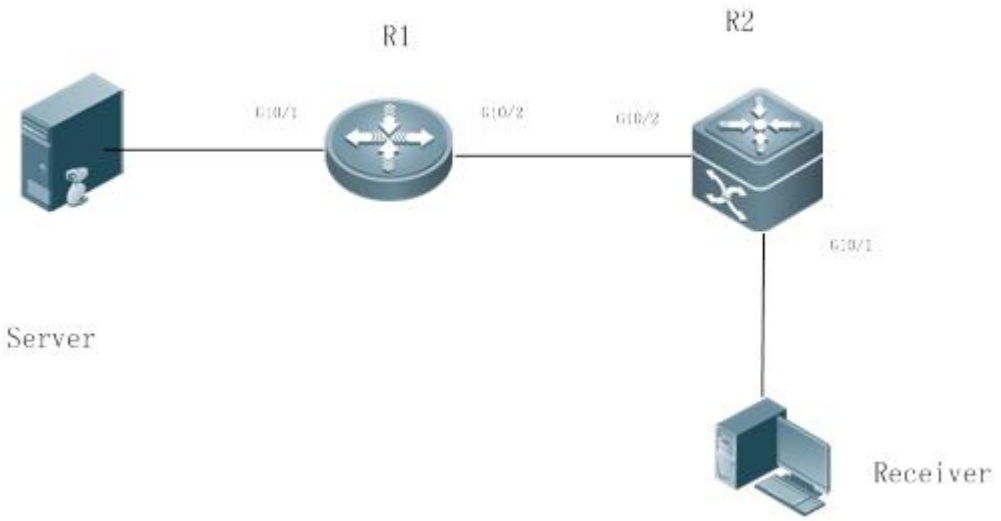

Рисунок 6-3.

R1 подключен к видеосерверу, R2 напрямую подключен к приемнику, а R2 работает в режиме горячего резервирования.

Протокол multicast уровня 3 работает на маршрутизаторах R1 и R2.

6.2.3.2. Развертывание

- Запустите OSPF на маршрутизаторах R1 и R2, чтобы реализовать unicast-маршрутизацию.
- Запустите PIM-SM на маршрутизаторах R1 и R2, чтобы реализовать multicast-маршрутизацию.
- Сделайте, чтобы R2 работал в среде горячего резервного копирования.

ПРИМЕЧАНИЯ: R2 может выполнять горячее резервное переключение в среде горячего резервного копирования. В этом случае интервал отправки сообщений Join/Prune PIM и интервал объявления кандидата RP необходимо скорректировать. Функция multicast в настоящее время опирается на функцию unicast-рассылки, и функция multicast начинает конвергенцию после завершения конвергенции функции unicast-рассылки. Например, время конвергенции graceful restart (GR) по умолчанию для функции unicast-рассылки составляет 120 секунд. Интервал отправки сообщений Join/Prune PIM по умолчанию составляет 60 секунд. Время keepalive сообщений Join/Prune PIM по умолчанию

составляет 210 секунд. Если R2 является динамическим IP-адресом, необходимо настроить интервал объявления кандидата RP. Время keepalive в 2,5 раза превышает интервал объявления кандидата RP. Если время конвергенции unicast-передачи превышает 150 с, интервал подключения кандидата RP необходимо соответствующим образом скорректировать.

Настройка интервала отправки сообщений Join/Prune PIM может привести к негативному эффекту, например, к потере пакетов Join/Prune PIM. R1 может не создать запись пересылки, и ему придется ждать, пока R2 снова отправит пакеты Join/Prune PIM. Время ожидания — это интервал отправки сообщений о Join/Prune PIM.

6.3. Функции

6.3.1. Базовые определения

PIM-маршрутизатор и PIM-интерфейс

Маршрутизатор, на котором работает PIM, называется маршрутизатором PIM. Интерфейсы, на которых работает PIM, называются интерфейсом PIM.

Multicast-пакеты пересылаются на PIM-маршрутизаторы. PIM-интерфейсы, на которых принимаются multicast-пакеты, называются upstream-интерфейсами, а PIM-интерфейсы, на которых отправляются multicast-пакеты, называются downstream-интерфейсами.

Сегменты сети, в которых расположены upstream-интерфейсы, называются upstream сетевыми сегментами, а сетевые сегменты, в которых расположены downstream-интерфейсы, называются downstream сетевыми сегментами.

Сеть PIM и домен PIM

PIM-маршрутизаторы подключаются через PIM-интерфейсы и образуют сеть PIM.

На некоторых интерфейсах PIM можно установить границы, чтобы разделить большую сеть PIM на несколько доменов PIM. Границы могут запрещать прохождение определенных multicast-пакетов или ограничивать передачу пакетов PIM.

Multicast Distribution Tree, DR и RP

Multicast-пакеты передаются из одной точки в несколько точек, образуя древовидный путь пересылки. Такой путь пересылки называется Multicast Distribution Tree (MDT), которое включает в себя следующие два типа:

- «Дерево» RP (RPT): оно основано на RP и использует назначенный маршрутизатор (DR) подключенных к нему групп участников в качестве своих «листьев».
- «Дерево» кратчайшего пути (SPT): оно основано на DR, подключенном к источнику multicast, и использует RP или DR подключенных к нему групп участников в качестве своих «листьев».

И DR, и RP являются функциями маршрутизатора PIM.

- RP собирает информацию об источнике multicast или участнике multicast в сети.
- DR, подключенный к источнику multicast, объявляет информацию об источнике multicast RP; DR, подключенный к участникам группы multicast, объявляет информацию об участниках группы multicast RP.

(*, G), (S, G)

- (*, G): указывает пакеты, отправленные из любого источника в группу (G), соответствующие записи маршрута и RPT.
- (S, G): указывает пакеты, отправленные из источника (S) в группу (G), соответствующие записи маршрутизации и SPT.

ASM, SSM

PIM-SM поддерживает как any-source multicast (ASM), так и SSM, и применим к различным сегментам адреса группы multicast.

- ASM: в этой модели пользователю не разрешено выбирать источник multicast. Пользовательский хост присоединяется к группе и получает пакеты, отправленные из всех источников.
- SSM: в этой модели пользователь может выбрать источник multicast. Пользовательский хост присоединяется к группе и указывает адрес источника. Тогда принимаются только пакеты, отправленные с этого адреса источника.

ПРИМЕЧАНИЕ: требования для использования модели SSM: Прежде чем выбирать источник multicast, вам необходимо узнать адрес источника multicast с помощью других сетевых служб.

6.3.2. Обзор

Особенность	Описание
Сосед PIM-SM	Установить соседские отношения между маршрутизаторами RIM для формирования сети PIM
Выбор DR	В сегменте сети, где расположены хосты-участники группы, соседи PIM конкурируют за DR, и тот, кто побеждает при выборе, становится DR для подключения к участникам группы. В сегменте сети, где расположен источник multicast, соседи PIM конкурируют за DR, и тот, кто побеждает при выборе, становится DR для подключения к источнику multicast
Механизм BSR	В сети PIM BSR периодически генерирует кандидатов RP и пакеты начальной загрузки соответствующих адресов группы
Механизм RP	В сети PIM посредством статической конфигурации RP или динамического выбора RP каждый маршрутизатор PIM может узнать местоположение RP
Регистрация информации об источнике multicast	Когда источник multicast обнаружен в сети, источник DR отправляет пакет Register на RP, который получает информацию об источнике и multicast-пакете
Создание RPT	Когда участник группы обнаружен в сети, DR, подключающийся к участникам группы, отправляет пакеты в сторону RP для формирования RPT. Если источник multicast уже существует в сети, пакеты, поступившие на RP, могут быть отправлены участникам группы по RPT

Особенность	Описание
Создание SPT	Когда пакеты данных достигают DR, подключающегося к участникам группы, DR отправляет эти пакеты к источнику multicast для формирования SPT, а multicast-пакеты отправляются участникам группы по SPT
ASM и SSM	Маршрутизатор PIM может одновременно предоставлять сервисы multicast как по модели ASM, так и по модели SSM. Модель SSM применяется к группам, адреса которых находятся в диапазоне адресов SSM. Для других групп используйте модель ASM

6.3.3. Сосед PIM-SM

Отношения соседства устанавливаются между маршрутизаторами PIM для формирования сети PIM. Отношения соседства должны быть установлены между маршрутизаторами PIM до того, как можно будет обмениваться управляющими пакетами PIM или пересылать multicast-пакеты.

6.3.3.1. Принцип работы

Интерфейс PIM отправляет пакет Hello. Для multicast-пакета IPv4, пакет Hello которого инкапсулирован, адрес назначения — 224.0.0.13 (с указанием всех маршрутизаторов PIM в одном сегменте сети), адрес источника — IP-адрес интерфейса PIM, а значение Time To Live (TTL) равно 1. Для multicast-пакета IPv6, пакет Hello которого инкапсулирован, адрес назначения — ff02::d.

Пакет Hello используется для обнаружения соседей, координации параметров протокола и поддержания отношений соседства.

Обнаружение соседей

PIM-маршрутизаторы в том же сегменте сети получают multicast-пакеты с адреса назначения 224.0.0.13. Таким образом, PIM-маршрутизаторы получают информацию о соседях и устанавливают отношения соседства.

Когда интерфейс PIM включен или обнаруживает нового соседа, пакет triggered-hello-delay используется для генерации случайного времени. Через некоторое время интерфейс отправляет пакеты Hello.

Координация параметров протокола

Пакет Hello включает в себя несколько параметров протокола, которые описаны следующим образом:

- DR_Priority: указывает приоритет интерфейса маршрутизатора для конкуренции за DR. Более высокий приоритет означает более высокий шанс на победу.
- Holdtime: указывает время, в течение которого сосед удерживается в состоянии доступности.
- LAN_Delay: указывает задержку LAN для передачи пакета Prune в общем сегменте сети.
- Override-Interval: указывает время prune override, передаваемое в пакете Hello.

Когда маршрутизатор PIM получает пакет Prune от upstream-интерфейса, это указывает на наличие downstream-интерфейсов в общем сегменте сети. Если маршрутизатору PIM

по-прежнему необходимо получать multicast-данные, маршрутизатор PIM должен отправить пакет Prune Override на upstream-интерфейс в течение интервала Override.

LAN_Delay + интервал Override = PPT (Prune-Pending Timer). После того, как маршрутизатор PIM получит пакет Prune от downstream-интерфейса, маршрутизатор PIM не будет немедленно выполнять pruning, пока не истечет время PPT. Если во время PPT маршрутизатор PIM получает пакет Prune rejection от downstream-интерфейса, маршрутизатор PIM отменяет pruning.

Поддержание отношений с соседями

Пакет Hello периодически отправляется между маршрутизаторами PIM. Если пакет Hello не получен от соседа PIM в течение времени Holdtime, сосед считается недоступным и удаляется из списка соседей. Любое изменение соседей PIM приведет к изменению топологии multicast в сети. Если upstream- или downstream-сосед в MDT недоступен, multicast-маршруты снова конвергируются, и MDT изменяется.

6.3.3.2. Сопутствующая конфигурация

Включение PIM-SM на интерфейсе

По умолчанию PIM-SM отключен на интерфейсе.

Запустите **ip pim sparse-mode**, чтобы включить или отключить PIM-SM на интерфейсе.

PIM-SM должен быть включен на интерфейсе, чтобы включить интерфейс в протокол PIM. Если PIM-SM не включен для интерфейса DR, статического RP, кандидата RP (C-RP) или кандидата BSR (C-BSR), соответствующие роли протокола PIM не могут быть запущены.

Установка интервала пакетов Hello на интерфейсе

По умолчанию пакет Hello отправляется каждые 30 секунд.

Запустите **ip pim query-interval** *interval-seconds*, чтобы настроить интервал пакетов Hello. Значение варьируется от 1 до 65 535.

Пакет Hello передается реже, если значение интервала в секундах больше.

6.3.4. Выбор DR

В сегменте сети, где расположены хосты-участники группы, соседи PIM конкурируют за DR, и тот, кто побеждает при выборе, становится DR для подключения к участникам группы.

В сегменте сети, где расположен источник multicast, соседи PIM конкурируют за DR, и тот, кто побеждает при выборе, становится DR для подключения к источнику multicast.

DR отправляет пакеты Join/Prune в сторону MDT или отправляет исходные данные multicast в MDT.

6.3.4.1. Принцип работы

При создании соседа PIM вы можете отправить пакет Hello, чтобы получить IP-адрес и приоритет DR соседа для выбора DR.

Два параметра играют ключевую роль в победе при выборе DR: приоритет DR интерфейса и IP-адрес интерфейса.

Приоритет DR интерфейса

Во время выбора DR маршрутизатор RIM с наивысшим приоритетом DR будет выбран в качестве DR.

IP-адрес интерфейса

Если во время выбора DR приоритет интерфейсов одинаковый, то IP-адреса интерфейсов будут сравниваться. Интерфейс с максимальным IP-адресом будет выбран в качестве DR.

6.3.4.2. Сопутствующая конфигурация

Включение PIM-SM на интерфейсе

По умолчанию PIM-SM отключен на интерфейсе.

Запустите **ip pim sparse-mode**, чтобы включить или отключить PIM-SM на интерфейсе.

PIM-SM должен быть включен на интерфейсе, чтобы включить интерфейс в протокол PIM. Если PIM-SM не включен для интерфейса DR, статического RP, C-RP или C-BSR, соответствующие протоколы не могут быть запущены.

Настройка приоритета DR интерфейса

По умолчанию приоритет DR равен 1.

Запустите **ip pim dr-priority** *priority-value*, чтобы настроить приоритет DR интерфейса. Значение находится в диапазоне от 0 до 4 294 967 294.

Приоритет DR используется при выборе DR в сегменте сети, напрямую подключенном к интерфейсу. Большее значение указывает на более высокий приоритет.

6.3.5. Механизм BSR

В сети PIM BSR периодически генерирует кандидаты RP и пакеты начальной загрузки соответствующих адресов группы. Эти пакеты начальной загрузки передаются hop за hop-ом в домене. Все маршрутизаторы во всей сети будут получать эти пакеты начальной загрузки, записывать этих кандидатов RP и соответствующие им групповые адреса.

6.3.5.1. Принцип работы

Один или несколько кандидатов BSR настраиваются в домене PIM-SM. Вам необходимо применить определенный алгоритм для выбора BSR из этих BSR-кандидатов.

6.3.5.2. Сопутствующая конфигурация

Настройка BSR-кандидатов

По умолчанию кандидаты BSR не настроены.

Запустите **ip pim bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority-value*]], чтобы настроить или отменить настройку BSR-кандидатов.

Посредством обучения пакета начальной загрузки (BSM) и конкуренции кандидатов BSR создается уникальный BSR для домена PIM-SM.

Настройка границ BSR

По умолчанию границы BSR не настроены.

Запустите **ip pim bsr-border**, чтобы настроить или отменить настройку границ BSR.

После настройки этой команды сообщения BSM, полученные интерфейсом, будут отброшены и не будут пересылаться этим интерфейсом, что предотвращает флуд BSM.

Фильтрация BSM

По умолчанию BSM из BSR не фильтруются.

Запустите **ip pim accept-bsr list** { <1-99> | <1300-1999> | *WORD* }, чтобы настроить фильтрацию BSM.

Если эта функция включена, интерфейс принимает только разборчивые BSM; если эта функция отключена, все внешние BSM будут приниматься устройством, на котором работает PIM-SM.

Настройка разборчивых адресов C-RP и групп multicast, которые обслуживают для BSR-кандидата

По умолчанию пакеты Candidate-RP-Advertisement (C-RP-Adv) не фильтруются BSR-кандидатом.

Запустите **ip pim accept-crp list** { *<100-199>* | *<2000-2699>* | *WORD* }, чтобы настроить, фильтровать ли пакеты C-RP-Adv.

Если эта функция включена, адреса C-RP и соответствующие группы multicast фильтруются кандидатом BSR. Если эта функция отключена, все внешние пакеты C-RP-Adv принимаются кандидатом BSR.

Разрешение C-BSR получать пакет C-RP-ADV, счетчик префикса (Prefix-Count) которого равен 0

По умолчанию кандидат BSR не может получить пакет C-RP-ADV, счетчик префикса (Prefix Count) которого равен 0.

Запустите **ip pim accept-crp-with-null-group**, чтобы настроить, следует ли получать пакет C-RP-ADV, счетчик префикса которого равен 0.

Если эта функция включена, пакет C-RP-ADV, счетчик префикса которого равен 0, может быть получен кандидатом BSR. Если эта функция отключена, пакет C-RP-ADV, счетчик префикса которого равен 0, не может быть получен кандидатом BSR.

6.3.6. Механизм RP

В сети PIM посредством статической конфигурации RP или динамического выбора RP каждый маршрутизатор PIM может узнать местоположение RP. RP как root RPT — это точка, в которой находится RPT и откуда пересылается трафик данных RPT.

6.3.6.1. Принцип работы

Все PIM-маршрутизаторы в одном домене PIM должны быть сопоставлены с тем же RP, что и конкретный адрес группы multicast. В сети PIM RP можно настроить как статический или динамический.

Статическая RP

В статической конфигурации RP адреса RP настраиваются непосредственно на маршрутизаторах PIM, и эти адреса изучаются всей сетью PIM.

Динамическая RP

В домене PIM-SM существуют RP-кандидаты, которые отправляют unicast-пакеты (включая адреса RP и группы multicast, которые они обслуживают) в BSR, который периодически генерирует RP-кандидатов и пакеты начальной загрузки соответствующих адресов группы. Эти пакеты начальной загрузки передаются hop за hop-ом в домене, а также принимаются и сохраняются маршрутизаторами PIM, которые применяют хэш-функцию для сопоставления адресов группы с кандидатом RP, который может предоставлять сервисы. Затем соответствие RP этим групповым адресам multicast может быть подтверждено.

6.3.6.2. Сопутствующая конфигурация

Настройка статических адресов RP

По умолчанию адрес RP не настроен.

Запустите **ip pim rp-address** *rp-address* [*access-list*], чтобы настроить статический RP-адрес для маршрутизатора PIM.

Чтобы использовать статические адреса RP, статические адреса RP всех маршрутизаторов в домене PIM-SM должны быть одинаковыми, чтобы multicast-маршрутизация PIM SM оставалась согласованной.

Настройка адресов кандидатов C-RP

По умолчанию адрес C-RP не настроен.

Запустите **ip pim rp-candidate** *interface-type interface-number* [priority *priority-value*] [**interval** *interval-seconds*] [**group-list** *access-list*] для настройки или отмены маршрутизатора PIM в качестве кандидата C-RP.

После того, как кандидат RP настроен, он может периодически отправлять пакеты C-RP-Adv в BSR, и информация, переносимая этими пакетами C-RP-Adv, будет объявлена всем PIM-SM в домене, обеспечивая уникальность сопоставления RP.

Игнорирование приоритета RP в RP-Set

По умолчанию настроен C-RP наивысшего приоритета.

Запустите **ip pim ignore-rp-set-priority**, чтобы выбрать или отменить выбор приоритета RP при выборе соответствующего RP в группе multicast.

Если вы хотите выбрать RP из нескольких RP, которые обслуживают один и тот же адрес группы multicast, вы можете запустить эту команду, чтобы игнорировать приоритет RP. Если эта команда не настроена, приоритет RP будет учитываться при сравнении двух RP.

6.3.7. Регистрация информации об источнике multicast

Когда источник multicast обнаружен в сети, DR источника отправляет пакет Register на RP, который получает информацию об источнике и multicast-пакет.

6.3.7.1. Принцип работы

Когда DR источника получает multicast-пакет от хоста, напрямую подключенного к нему, DR источника инкапсулирует multicast-пакет в пакет Register и отправляет unicast-пакет в RP для формирования записи (S, G).

Если у RP есть исходящий интерфейс для записи пересылки, он инкапсулирует пакет данных и пересылает его на исходящий интерфейс.

Если у RP нет записи пересылки текущей группы, она генерирует запись (S, G) и включает таймер. Если время таймера истекло, RP отправляет пакет Register-Stop на DR, чтобы удалить запись. DR источника отправляет пакет проверки до истечения времени после получения пакета Register-Stop.

Если DR не получил пакет Register-Stop, DR в источнике данных тайм-аута инкапсулирует данные multicast в пакет Register и отправит unicast-пакет на RP.

Если пакет Register-Stop получен DR, задержка будет выполнена еще раз, и пакет проверки будет отправлен до задержки.

6.3.7.2. Сопутствующая конфигурация

Обнаружение доступности пакета Register

По умолчанию доступность RP не определяется.

Запустите **ip pim register-rp-reachability**, чтобы настроить или отменить обнаружение доступности RP.

Вы можете включить эту функцию, если хотите определить, доступен ли RP для пакета Register, отправленного из DR. После включения этой функции DR определит доступность пакета Register перед его отправкой на RP, а именно, DR проверит, существует ли маршрут к RP в записи unicast-маршрутизации и записи статической multicast-маршрутизации. Если маршрут не существует, пакет Register не будет отправлен.

Настройка RP для фильтрации адресов пакетов Register

По умолчанию все пакеты Register получают RP.

Запустите **ip pim accept-register** { **list** *access-list* [**route-map** *map-name*] | **route-map** *map-name* [**list** *accesslist*] } для настройки RP для фильтрации или отмены фильтрации исходных адресов полученных пакетов Register.

Вы можете запустить эту команду, если хотите отфильтровать адреса источника полученных пакетов Register. Если эта функция не включена, все пакеты Register будут получены RP. Если эта функция отключена, обрабатываются только те пакеты Register, чьи адреса источника и адреса групп multicast включены в списки управления доступом (ACL); в противном случае пакеты будут фильтроваться.

Ограничение скорости отправки пакета Register

По умолчанию скорость отправки пакета Register не ограничена.

Запустите **ip pim register-rate-limit** *rate*, чтобы ограничить или отменить ограничение скорости отправки пакета Register.

Если настроена форма **no** этой команды, скорость не ограничивается. Эта команда действует только для пакета Register каждого (S, G) пакета, но не для всех пакетов Register во всей системе.

Вычисление контрольной суммы всей длины пакета Register

По умолчанию контрольная сумма пакета Register рассчитывается, как это предусмотрено протоколом.

Запустите **ip pim register-checksum-wholepkt [group-list *access-list*]**, чтобы настроить контрольную сумму длины пакета Register.

Вы можете включить эту функцию, если хотите включить длину инкапсулированных multicast-пакетов в контрольную сумму длины пакета Register. Если эта функция отключена, контрольная сумма пакета Register рассчитывается, как это предусмотрено протоколом.

Настройка RP для пересылки пакетов multicast-данных на downstream-интерфейсы после декапсуляции пакетов Register

По умолчанию пакеты Register не декапсулируются, а multicast-пакеты не пересылаются на интерфейсы.

Запустите **ip pim register-decapsulate-forward**, чтобы переслать или отменить пересылку пакетов данных на downstream-интерфейсы.

Вы можете запустить эту команду, если хотите декапсулировать пакет Register и переслать multicast-пакет. Если эта функция отключена, multicast-пакет не будет пересылаться.

Настройка IP-адреса источника пакета Register

По умолчанию IP-адрес источника пакета Register совпадает с адресом интерфейса DR, подключенного к источнику multicast.

Запустите **ip pim register-source** { *local_address* | *Interface-type interface-number* } для настройки IP-адреса источника.

Вы можете запустить эту команду, если хотите настроить IP-адрес источника пакета Register, отправленного DR. Если эта функция отключена или используется форма этой команды **no**, адрес источника пакета Register будет таким же, как адрес интерфейса DR, подключенного к источнику multicast. Если вы хотите настроить *local_address*, настроенный адрес должен быть доступен для unicast-маршрута. *Interface-type interface-number* может быть типичным loopback-интерфейсом или интерфейсом других типов. Адрес интерфейса должен быть объявлен unicast-маршрутом.

Настройка времени подавления (Suppression Time) пакета Register

По умолчанию время подавления пакета Register составляет 60 с.

Запустите **ip pim register-suppression** *seconds*, чтобы настроить время подавления.

Если вы запустите эту команду на DR, вы можете изменить время подавления пакетов Register, отправленных с DR. Если вы запустите эту команду, но не запустите **ip pim rp-register-kat** на RP, период keepalive RP будет изменен.

Настройка времени проверки пустого пакета (Null) Register

По умолчанию время проверки составляет 5 с.

Запустите **ip pim probe-interval** *interval-seconds*, чтобы настроить время проверки.

В интервале времени до истечения тайм-аута подавления пакетов Register DR источника может отправить пустой пакет Register на RP. Этот временной интервал называется временем проверки и по умолчанию составляет 5 с.

Настройка времени RP KAT

По умолчанию используется значение по умолчанию для таймера keepalive (KAT). Значение по умолчанию рассчитывается следующим образом: Время подавления пакета Register x 3 + Время проверки пустого пакета Register.

Запустите **ip pim rp-register-kat** *seconds*, чтобы настроить время KAT.

Вы можете запустить эту команду, если хотите настроить время keepalive (S, G) пакета Register, отправленного с RP.

6.3.8. Создание RPT

Когда участник группы обнаружен в сети, DR, подключающийся к участникам группы, отправляет пакеты в сторону RP для формирования RPT. Если источник multicast уже существует в сети, пакеты, поступившие на RP, могут быть отправлены участникам группы по RPT.

6.3.8.1. Принцип работы

Чтобы создать RPT, выполните следующие действия:

DR-приемник получает пакет Report о включении IGMP (*, G) от принимающей стороны.

Если DR не является RP этой группы (G), DR отправит пакет (*, G) Join в сторону RP. Маршрутизатор, получающий этот (*, G) пакет Join, будет отправлять пакет hop за hop-ом, пока он не будет получен RP, что означает, что RP присоединился к RPT.

Когда хост источника данных отправляет multicast-данные группе, исходные данные инкапсулируются в пакете Register и отправляются от DR источника к RP в unicast-режиме. Затем RP декапсулирует пакет Register, извлекает пакеты данных и пересылает эти пакеты каждому участнику группы по RPT.

RP отправляет пакеты (S, G) Join по источнику данных, чтобы присоединиться к SPT этого источника.

После создания SPT между RP и исходным DR пакеты данных из источника данных будут отправлены в декапсулированном виде на RP вдоль SPT.

Когда первый пакет multicast-данных поступает на RP по SPT, RP отправляет пакет Register-Stop исходному DR, чтобы прекратить отправку пакета Register. После того как DR источника получает пакет Register-Stop, он прекращает инкапсулировать пакет Register и отправляет пакет по SPT на RP, который пересылает пакет каждому участнику группы.

6.3.8.2. Сопутствующая конфигурация

Настройка интервала отправки пакета Join/Prune

По умолчанию интервал отправки пакета Join/Prune составляет 60 секунд.

Запустите **ip pim jp-timer** *seconds*, чтобы настроить интервал отправки пакета Join/Prune.

Вы можете запустить эту команду, чтобы настроить интервал отправки пакета Join/Prune. Если не настроено, значением по умолчанию будет 60 с.

6.3.9. Создание SPT

Когда пакеты данных достигают DR, подключающегося к участникам группы, DR отправляет эти пакеты к источнику multicast для формирования SPT, а multicast-пакеты отправляются участникам группы по SPT. Таким образом снижается нагрузка на RP в RPT, и DR источника будет приходить к приемнику DR с меньшим количеством hop-ов.

6.3.9.1. Принцип работы

Чтобы создать SPT, выполните следующие действия:

DR-приемник отправляет пакеты (*, G) Join к исходному DR по SPT, а пакеты (*, G) Join затем отправляются hop за hop-ом, пока они не будут получены исходным DR, образуя SPT.

6.3.9.2. Сопутствующая конфигурация

По умолчанию переключение SPT не включено.

Запустите **ip pim spt-threshold** [**group-list** *access-list*], чтобы настроить, следует ли переключаться на SPT.

Если эта функция включена, при приеме первого (S, G) пакета запускается пакет PIM Join и создается SPT. Если указан **group-list**, все указанные группы будут переключены на SPT. Если используется форма **no** этой команды и **group-list** не указан, RPT не будет переключен на SPT, а DR останется в RPT и отправит пакет Prune к исходному DR; если используется форма **no** этой команды и указан **group-list** и что списки ACL настроены, это означает, что связь между **group-list** и списками ACL отменяется, и всем группам разрешено переключаться с RPT в SPT.

6.3.10. ASM и SSM

Маршрутизатор PIM может одновременно предоставлять услуги multicast как по модели ASM, так и по модели SSM. Модель SSM применяется к группам, адреса которых находятся в диапазоне адресов SSM. Для других групп используйте модель ASM. В модели ASM для получателя multicast указывается только группа multicast (G), а источник multicast (S) не указывается. В модели SSM для получателя multicast могут быть указаны как источник multicast (S), так и группа multicast (G).

6.3.10.1. Принцип работы

ПРИМЕЧАНИЕ: чтобы реализовать SSM в маршрутизаторе IPv4, необходимо применить IGMPv3 для управления участием между хостом и устройствами, а PIM-SM необходимо применить для подключения к устройствам.

В модели SSM, поскольку приемник multicast узнал (S, G) источника multicast через определенный канал (например, посетив сервер или получив объявление), когда приемнику multicast необходимо запросить сервис multicast, приемник multicast может отправить пакет Join IGMP (S, G) маршрутизатору последнего hop-а. Например, как показано на Рисунке 6-4, приемник multicast 1 отправляет пакет Join IGMP (S, G) для запроса сервиса multicast (S, G). После того как маршрутизатор последнего hop-а получает пакет Join IGMP (S, G), он отправляет пакет Join PIM (S, G) источнику multicast hop за hop-ом. Как показано на Рисунке ниже, когда R1 получает пакет Join IGMP (S, G), отправленный от multicast-приемника 1, R1 отправляет пакет Join PIM (S, G) на R3, который затем отправляет пакет на R4, тем самым формируя соединение SPT приемника multicast и источника multicast.

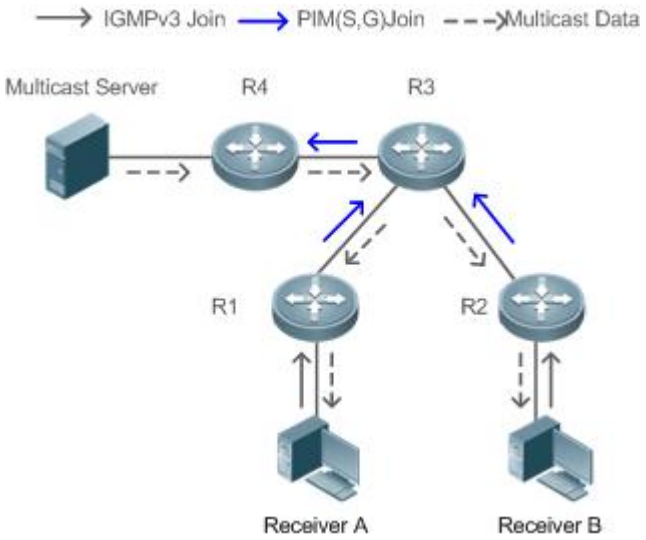

Рисунок 6-4. Модель SSM

Для создания модели SSM необходимо выполнить следующие требования:

- Приемнику multicast необходимо заранее узнать (S, G) источника multicast, и необходимо отправить пакет Join IGMP (S, G), если приемнику необходимо запросить сервис multicast.
- IGMPv3 должен быть запущен на интерфейсе маршрутизатора последнего hop-а, подключающегося к приемнику multicast. IGMPv1 и IGMPv2 не поддерживают SSM.
- PIM-SM и SSM должны быть запущены на устройствах, соединяющих приемник multicast и источник multicast.

ПРИМЕЧАНИЕ: диапазон групп SSM по умолчанию — 232/8. Вы можете запустить команду, чтобы изменить значение.

SSM имеет следующие особенности:

- Приемник multicast может заранее узнать информацию об источнике multicast по определенному каналу (например, посетив сервер или получив объявление).
- Модель SSM — это определенная подсеть PIM-SM. Он обрабатывает только пакеты PIM (S, G) Join и PIM (S, G) Prune и отбрасывает пакеты, связанные с RPT, например, пакеты PIM (*, G) Join/Prune, которые находятся в области действия

SSM. Если SSM обнаружит пакет Register в пределах области действия, он немедленно ответит пакетом Register-Stop.

- Если RP не требуется, выбор и распространение информации RP не выполняются. Все MDT в SSM являются SPT.

6.3.10.2. Сопутствующая конфигурация

ASM включен по умолчанию.

Запустите **ip pim ssm** { **default** | **range** *access-list* }, чтобы настроить, следует ли переключаться на SSM.

В SSM multicast-пакеты могут быть получены источником multicast напрямую, но не по «дереву» RP.

6.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций PIM-SM	(Обязательно) Используется для настройки услуги multicast	
	ip multicast-routing	Включает multicast-маршрутизацию IPv4
	ip pim sparse-mode	Включает PIM-SM
	ip pim rp-address	Настраивает статическую RP
	ip pim rp-candidate	Настраивает C-RP
	ip pim bsr-candidate	Настраивает C-BSR
	ip pim ssm	Включает SSM
Настройка соседей PIM-SM	(Опционально) Используется для настройки параметров отправки и получения пакетов Hello между соседями	
	ip pim query-interval *interval-seconds*	Настраивает интервал отправки пакетов Hello
	ip pim propagation-delay *milliseconds*	Настраивает задержку prune propagation
	ip pim override-interval *milliseconds*	Настраивает интервал prune override
	ip pim neighbor-tracking	Включает возможность подавления интерфейса для отправки пакетов Join

Конфигурация	Описание и команда	
Настройка соседей PIM-SM	**ip pim triggered-hello-delay** *interval-seconds*	Настраивает задержку отправки пакетов Hello
	ip pim dr-priority *priority-value*	Настраивает приоритет DR пакета Hello
	ip pim neighbor-filter *access_list*	Настраивает фильтрацию соседей
Настройка параметров BSR	(Опционально) Используется для настройки BSR	
	ip pim bsr-border	Настраивает границы BSR
	ip pim accept-bsr list { <1-99> | <1300-1999> | *WORD* }	Настраивает ограничение пакетов BSM на маршрутизаторе PIM
	ip pim accept-crp list *access-list*	Настраивает C-BSR для проверки диапазона адресов C-PR
Настройка параметров RP и DR	(Опционально) Используется для настройки параметров RP или DR	
	ip pim ignore-rp-set-priority	Игнорирует приоритет C-RP
	ip pim register-rp-reachability	Позволяет исходному DR обнаруживать доступность RP
	ip pim accept-register list *access-list*	Настраивает диапазон источника зарегистрированных (S, G) адресов
	ip pim register-rate-limit *rate*	Ограничивает скорость отправки пакетов Register
	ip pim register-checksum-wholepkt [**group-list** *access-list*]	Вычисляет контрольную сумму всего пакета Register

Конфигурация	Описание и команда	
Настройка параметров RP и DR	**ip pim register-decapsulate-forward**	Включает RP для декапсуляции пакета Register и пересылает multicast-пакет на интерфейсы
	ip pim register-source { *local_address* | *Interface-type interface-number* }	Настраивает IP-адрес источника пакета Register
	ip pim register-suppression *seconds*	Настраивает время подавления пакета Register
	ip pim probe-interval *seconds*	Настраивает время проверки пустого пакета Register
	ip pim rp-register-kat *seconds*	Настраивает интервал KAT на RP
Настройка интервала отправки пакета Join/Prune	(Опционально) Используется для указания интервала отправки пакета Join/Prune	
	ip pim jp-timer *seconds*	Настраивает интервал для отправки пакета Join/Prune
Настройка маршрутизатора последнего hop-а для переключения с RPT на SPT	(Дополнительно) Используется для переключения с SPT на RPT	
	ip pim spt-threshold [**group-list** *access-list*]	Включает переключение SPT

6.4.1. Настройка основных функций PIM-SM

6.4.1.1. Эффект конфигурации

- Создайте сеть PIM-SM и обеспечьте источники данных и пользовательские терминалы в сети сервисом multicast IPv4.
- Можно настроить любую модель ASM, SSM или обе.

6.4.1.2. Примечания

- PIM-SM необходимо использовать существующие unicast-маршруты в сети. Поэтому в сети необходимо настроить unicast-маршруты IPv4.
- Если сеть PIM должна поддерживать сервисы multicast SSM, необходимо настроить сопоставление IGMPv3 или SSM.

6.4.1.3. Шаги настройки

Включение multicast-маршрутизации IPv4

- Обязательный.
- Если не указано, multicast-маршрутизация IPv4 должна быть включена на каждом маршрутизаторе.

Включение PIM-SM

- Обязательный.
- Если не указано, PIM-SM должен быть включен на следующих интерфейсах: интерфейсах межсетевого маршрутизатора, интерфейсах статических RP, C-RP и C-BSR, а также интерфейсах, подключающихся к источнику multicast и пользовательским хостам.

Настройка RP

- RP должен быть настроен, если сервис multicast ASM должен быть предоставлен в сети PIM.
- RP можно настроить в трех моделях: настройка только статического RP, настройка только динамического RP и настройка как статического, так и динамического RP. Если настроены как статическая RP, так и динамическая RP, динамическая RP имеет приоритет над статической RP.
- Настройка статического RP: если не указано, статический RP должен быть настроен на каждом маршрутизаторе.
- Настройка динамического RP: если не указано, C-RP и C-BSR должны быть настроены на одном или нескольких маршрутизаторах.

Включение SSM

- SSM необходимо включить, если в сети PIM необходимо предоставлять сервис multicast SSM.
- Если не указано, SSM должен быть включен на каждом маршрутизаторе.

6.4.1.4. Проверка

Отправляйте multicast-пакеты из источника multicast группам в диапазоне адресов ASM и SSM и присоединяйте хосты пользователей к этим группам.

- Проверьте, могут ли пользовательские хосты успешно получать пакеты из каждой группы.
- Проверьте, правильно ли созданы записи маршрутизации PIM-SM на маршрутизаторах.

6.4.1.5. Связанные команды

Включение multicast-маршрутизации IPv4

Команда	**ip multicast-routing**
Командный режим	Режим глобальной конфигурации

Включение PIM-SM

Команда	**ip pim sparse-mode**
Командный режим	Режим настройки интерфейса
Руководство по использованию	PIM-интерфейсы должны находиться на уровне 3, включая: интерфейсы маршрутизации, порты агрегирования (AP), виртуальные интерфейсы коммутатора (SVI) и loopback-интерфейсы. Для всех интерфейсов PIM должны быть доступны unicast-маршруты IPv4

Настройка статического RP

Команда	**ip pim rp-address** *rp-address* [*access_list*]
Описание параметра	*rp-address*: указывает адрес RP. *access_list*: указывает диапазон адресов группы multicast, обслуживаемых статическим RP с использованием ACL. По умолчанию RP обслуживает все группы
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для размещения статического RP. Статический RP должен иметь хорошую производительность маршрутизации. Рекомендуется использовать адрес loopback-интерфейса в качестве статического адреса RP. Статический RP всех маршрутизаторов должен быть одинаковым (включая адрес RP и диапазон адресов группы multicast, которые он обслуживает). Рекомендуется использовать адрес loopback-интерфейса в качестве статического адреса RP. Нагрузку можно разделить, если вы настроите несколько статических RP для обслуживания разных адресов групп multicast. Рекомендуется использовать адрес loopback-интерфейса в качестве статического адреса RP

Настройка C-RP

Команда	**ip pim rp-candidate** *interface-type interface-number* [**priority** *priority-value*] [**interval** *seconds*] [**group-list** *access_list*]
Описание параметра	*interface-type interface-number*: использует адрес этого интерфейса в качестве адреса C-RP. **priority** *priority-value*: соревнуется за приоритет RP. Большее значение указывает на более высокий приоритет. Значение находится в диапазоне от 0 до 255 (по умолчанию 192).

	interval *seconds*: указывает интервал отправки пакета C-RP в BSR. Значение варьируется от 1 до 16 383 (по умолчанию 60). **group-list** *access_list*: указывает диапазон адресов группы multicast, обслуживаемых C-RP с использованием ACL. По умолчанию C-RP обслуживает все группы multicast
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для настройки маршрутизатора как C-RP. C-RP должен иметь хорошую производительность маршрутизации. C-RP и C-BSR могут находиться на одном и том же маршрутизаторе или на разных маршрутизаторах. Рекомендуется использовать адрес loopback-интерфейса в качестве адреса C-RP. Если одну и ту же группу обслуживают несколько C-RP, можно реализовать избыточность. Если несколько C-RP обслуживают разные группы, нагрузку можно разделить

Настройка C-BSR

Команда	**ip pim bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority-value*]]
Описание параметра	*interface-type interface-number*: использует адрес этого интерфейса в качестве адреса C-BSR. *hash-mask-length*: указывает длину хэш-маски, используемой для борьбы за RP. Значение находится в диапазоне от 0 до 32 (по умолчанию 10). *priority-value*: указывает приоритет борьбы за BSR. Большее значение указывает на более высокий приоритет. Значение варьируется от 0 до 255 (по умолчанию 64)
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для настройки маршрутизатора как C-BSR. C-BSR должен иметь хорошую производительность маршрутизации. C-RP и C-BSR могут находиться на одном и том же маршрутизаторе или на разных маршрутизаторах. Рекомендуется использовать адрес loopback-интерфейса в качестве адреса C-BSR. Настройка нескольких C-BSR может обеспечить избыточность

Включение SSM

Команда	**ip pim ssm** { **default** | **range** *access_list* }
Описание параметра	**default**: указывает диапазон адресов группы SSM по умолчанию: 232.0.0.0/8. **range** *access_list*: указывает диапазон адресов группы SSM с использованием ACL
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Групповые адреса SSM, настроенные на всех маршрутизаторах, должны быть одинаковыми

Отображение записи маршрутизации PIM-SM

Команда	**show ip pim sparse-mode mroute** [*group-or-source-address* [*group-or-source-address*]]
Описание параметра	*group-or-source-address*: указывает адрес группы multicast или адрес источника (два адреса не могут быть адресами группы multicast или адресами источника одновременно)
Командный режим	Режим Privileged EXEC/Режим глобальной конфигурации/Режим конфигурации интерфейса
Руководство по использованию	Проверьте, предоставлено ли достаточно записей маршрутизации. Проверьте списки upstream- и downstream-интерфейсов и убедитесь, что создано правильное «дерево» SPT

6.4.1.6. Пример конфигурации

Включение multicast-маршрутизации IPv4 для поддержки ASM и SSM

Сценарий:

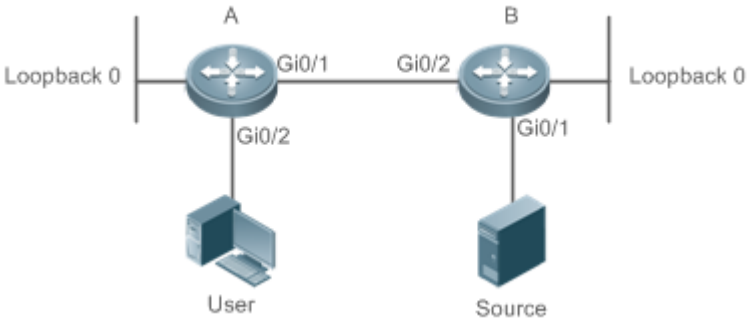

Рисунок 6-5.

Шаги настройки	• Настройте протокол unicast-маршрутизации IPv4 (например, OSPF) на маршрутизаторе, и маршрутизатор будет доступен для unicast-маршрута loopback-интерфейса. (пропущено) • Включите multicast-маршрутизацию IPv4 на всех маршрутизаторах. • Включите PIM-SM на всех взаимосвязанных интерфейсах маршрутизаторов, источника и приемника. • Настройте C-RP и C-BSR на loopback-интерфейсах маршрутизатора A и маршрутизатора B и включите PIM-SM на loopback-интерфейсах. • Включите SSM на всех маршрутизаторах. • Включите IGMPv3 на интерфейсах маршрутизатора, подключающихся к пользовательским терминалам. (пропущено)
A	A# configure terminal A(config)# ip multicast-routing A(config)# ip pim ssm default A(config)# interface GigabitEthernet 0/1 A(config-if)# ip pim sparse-mode A(config-if)# exit A(config)# interface GigabitEthernet 0/2 A(config-if)# ip pim sparse-mode A(config-if)# exit A(config)# interface loopback 0 A(config-if)# ip pim sparse-mode A(config-if)# exit A(config)# ip pim rp-candidate loopback 0
B	B# configure terminal B(config)# ip multicast-routing B(config)# ip pim ssm default B(config)# interface GigabitEthernet 0/1 B(config-if)# ip pim sparse-mode B(config-if)# exit B(config)# interface GigabitEthernet 0/2 B(config-if)# ip pim sparse-mode B(config-if)# exit B(config)# interface loopback 0 B(config-if)# ip pim sparse-mode B(config-if)# exit

	B(config)# ip pim bsr-candidate loopback 0
Проверка	Отправьте пакеты из S (192.168.1.10) в G1 (229.1.1.1) и G2 (232.1.1.1). Добавьте пользователя в G1 и G2 и укажите источник, когда пользователь присоединяется к G2. • Убедитесь, что multicast-пакеты от S (192.168.1.10) до G1 и G2 получены пользователем. • Проверьте записи маршрутизации PIM-SM на маршрутизаторах A и B. Должны отображаться записи (*, 229.1.1.1), (192.168.1.10, 229.1.1.1) и (192.168.1.10, 232.1.1.1)
A	switch#show ip pim sparse-mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 3 (S,G) Entries: 2 (S,G,rpt) Entries: 2 FCR Entries: 0 REG Entries: 0 (*, 229.1.1.1) RP: 192.168.10.10 RPF nbr: 0.0.0.0 RPF idx: None Upstream State: JOINED 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . . . i . . . . . . 1 . . . . . . Joined 0 . . . . . . 1 . . . . . . Asserted 0 . . . . . . 1 . . . . . . FCR:

```
(192.168.1.10, 229.1.1.1)
RPF nbr: 192.168.2.1
RPF idx: GigabitEthernet 0/2
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 8 seconds
kat expires in 207 seconds
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0 . . . . . .
1 . . . . . .
Joined
0 . . . . . .
1 . . . . . .
Asserted
0 . . . . . .
1 . . . . . .
Outgoing
0 . . . o . . . . . .
1 . . . . . .

(192.168.1.10, 229.1.1.1, rpt)
RP: 192.168.10.10
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: PRUNED
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0 . . . . . .
1 . . . . . .
Pruned
0 . . . . . .
1 . . . . . .
Outgoing
```

```
0 . . . o . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

(*, 232.1.1.1)
RP: 192.168.10.10
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0 . . . i . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Joined
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
FCR:
(192.168.1.10, 232.1.1.1)
RPF nbr: 192.168.2.1
RPF idx: GigabitEthernet 0/2
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 8 seconds
kat expires in 207 seconds
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Joined
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Asserted
```

0 . . . . . .

1 . . . . . .

Outgoing

0 . . . o . . . . . .

1 . . . . . .

(192.168.1.10, 232.1.1.1, rpt)

RP: 192.168.10.10

RPF nbr: 0.0.0.0

RPF idx: None

Upstream State: PRUNED

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Local

0 . . . . . .

1 . . . . . .

Pruned

0 . . . . . .

1 . . . . . .

Outgoing

0 . . . o . . . . . .

1 . . . . . .

(*, 239.255.255.250)

RP: 192.168.10.10

RPF nbr: 0.0.0.0

RPF idx: None

Upstream State: JOINED

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Local

0 . . . i . . . . . .

1 . . . . . .

Joined

0 . j . . . . . .

1 . . . . . .

Asserted

	0 . . . . . . 1 . . . . . . FCR: A#
B	B#show ip pim sparse-mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 1 (192.168.1.10, 229.1.1.1) RPF nbr: 0.0.0.0 RPF idx: None SPT bit: 1 Upstream State: JOINED kat expires in 38 seconds 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . . . . . . Joined 0 . . j . . . . . . Asserted 0 . . . . . . Outgoing 0 . . o . . . . . . (192.168.1.10, 229.1.1.1, rpt) RP: 192.168.10.10 RPF nbr: 192.168.2.2 RPF idx: GigabitEthernet 0/2

```
Upstream State: RPT NOT JOINED
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0 . . . . . .
Pruned
0 . . . . . .
Outgoing
0 . . . . . .

(192.168.1.10, 232.1.1.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
kat expires in 38 seconds
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0 . . . . . .
Joined
0 . . j . . . . . .
Asserted
0 . . . . . .
Outgoing
0 . . o . . . . . .

(192.168.1.10, 232.1.1.1, rpt)
RP: 192.168.10.10
RPF nbr: 192.168.2.2
RPF idx: GigabitEthernet 0/2
Upstream State: RPT NOT JOINED
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0 . . . . . .
```

	Pruned 0 . . . . . . Outgoing 0 . . . . . . (*, 239.255.255.250) RP: 192.168.10.10 RPF nbr: 192.168.2.2 RPF idx: GigabitEthernet 0/2 Upstream State: JOINED jt_timer expires in 15 seconds 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . i . . . . . . Joined 0 . . . . . . Asserted 0 . . . . . . FCR:

6.4.1.7. Распространенные ошибки

- Unicast-маршрутизация IPv4 настроена неправильно.
- Multicast-маршрутизация IPv4 не включена на определенном маршрутизаторе.
- SSM не включен на маршрутизаторе, или адрес группы SSM отличается от адресов других групп.
- PIM-SM не включен на интерфейсе (например, интерфейс настроен как интерфейс C-RP или C-BSR, используется для подключения к пользовательскому хосту или используется в качестве интерфейса источника multicast).
- IGMPv3 не включен на интерфейсе, подключающемся к используемому хосту.
- RP не настроен в сети.
- Статический RP не настроен на маршрутизаторе, или настроенный статический RP отличается от такового на других маршрутизаторах.
- C-RP настроены в сети, а C-BSR — нет.
- Статические RP, C-RP или C-BSR недоступны для unicast-маршрутов.

6.4.2. Настройка соседей PIM-SM

6.4.2.1. Эффект конфигурации

- Согласуйте параметры протокола и настройте параметры в пакете Hello.

- Маршрутизатор RIM используется для обнаружения соседей, координации параметров протокола и поддержания отношений между соседями.
- Поддерживайте отношения с соседями и фильтруйте соседей.

6.4.2.2. Примечания

Необходимо настроить основные функции PIM-SM.

6.4.2.3. Шаги настройки

Настройте параметры на интерфейсах маршрутизатора PIM, если они не указаны.

6.4.2.4. Проверка

Настройте параметры пакета Hello, отправленного с интерфейса, и запустите **debug ip pim sparse-mode packet**, чтобы отобразить параметры.

Включите фильтрацию соседей и запустите **show ip pim sparse-mode neighbor**, чтобы отобразить информацию о соседях.

6.4.2.5. Связанные команды

Настройка интервала отправки пакетов Hello

Команда	**ip pim query-interval** *interval-seconds*
Описание параметра	Указывает интервал отправки пакетов Hello. Указывает время подавления пакета Register в секундах. Значение варьируется от 1 до 65 535 (по умолчанию 30)
Командный режим	Режим настройки интерфейса
Руководство по использованию	Каждый раз, когда обновляется интервал отправки пакетов Hello, значение времени удержания (holdtime) автоматически обновляется как 3,5-кратное значение интервала. Если результат интервала отправки пакетов Hello, умноженный на 3,5, превышает 65 535, значение времени удержания принудительно обновляется до 18 725

Настройка задержки Prune Propagation

Команда	**ip pim propagation-delay** *milliseconds*
Описание параметра	*milliseconds*: единица измерения — мс. Значение варьируется от 1 до 32 767 (по умолчанию 500)
Командный режим	Режим настройки интерфейса
Руководство по использованию	После изменения задержки prune propagation или интервала prune override пакет Join/Prune будет изменен. Как указано в протоколе, интервал override пакета Join/Prune должен быть меньше времени holdtime пакета Join/Prune; в противном случае

	может произойти кратковременное прерывание трафика. Администратор должен поддерживать такую конфигурацию

Настройка интервала Prune Override

Команда	**ip pim override-interval** *milliseconds*
Описание параметра	*milliseconds*: единица измерения — мс. Значение варьируется от 1 до 65 535 (по умолчанию 2 500)
Командный режим	Режим настройки интерфейса
Руководство по использованию	После изменения задержки prune propagation или интервала prune override пакет Join/Prune будет изменен. Как указано в протоколе, интервал override пакета Join/Prune должен быть меньше времени holdtime пакета Join/Prune; в противном случае может произойти кратковременное прерывание трафика. Администратор должен поддерживать такую конфигурацию

Включение возможности подавления интерфейса для отправки пакетов Join

Команда	**ip pim neighbor-tracking**
Командный режим	Режим настройки интерфейса
Руководство по использованию	После включения подавления пакетов Join интерфейса, когда текущий маршрутизатор должен отправить пакет Join upstream-соседу, который отправил пакет Join своему upstream-соседу, текущий маршрутизатор не будет отправлять пакет Join; если подавление пакетов Join отключено, пакет Join будет отправлен. Когда подавление пакетов Join от downstream-получателей отключено, upstream-соседи узнают, сколько существует downstream-соседей, путем подсчета полученных пакетов Join, что называется отслеживанием соседей

Настройка задержки отправки пакетов Hello

Команда	**ip pim triggered-hello-delay** *interval-seconds*
Описание параметра	seconds: измеряется в секундах. Значение варьируется от 1 до 5 (по умолчанию 5)
Командный режим	Режим настройки интерфейса

Руководство по использованию	Когда интерфейс PIM включен или обнаруживает нового соседа, пакет triggered-hello-delay используется для генерации случайного времени. Через некоторое время интерфейс отправляет пакеты Hello

Настройка приоритета DR пакета Hello

Команда	**ip pim dr-priority** *priority-value*
Описание параметра	*priority-value*: указывает приоритет. Большее значение указывает на более высокий приоритет. Значение варьируется от 0 до 4 294 967 294 (по умолчанию 1)
Командный режим	Режим настройки интерфейса
Руководство по использованию	DR может быть выбран на основе следующих принципов: Если все пакеты Hello, отправленные маршрутизаторами в локальной сети (LAN), настроены с приоритетами, при выборе DR приоритеты будут сравниваться, и в качестве DR будет выбран маршрутизатор с наивысшим приоритетом. Если приоритет всех маршрутизаторов одинаковый, их IP-адреса будут сравниваться, и в качестве DR будет выбран маршрутизатор с максимальным IP-адресом. Если приоритет пакетов Hello, отправляемых с определенного маршрутизатора, не настроен, IP-адреса маршрутизаторов будут сравниваться, и в качестве DR будет выбран маршрутизатор с максимальным IP-адресом

Настройка фильтрации соседей

Команда	**ip pim neighbor-filter** *access_list*
Описание параметра	*access_list*: настраивает диапазон соседских адресов с использованием стандартного IP ACL. Значение может быть установлено от 1 до 99 или название
Командный режим	Режим настройки интерфейса
Руководство по использованию	Включение фильтрации соседей может повысить безопасность сети PIM и ограничить диапазон изучаемых адресов соседей. После того как сосед отфильтрован, PIM-SM не будет устанавливать с ним peering или прекращать peering

Отображение информации о соседях интерфейса

Команда	**show ip pim sparse-mode neighbor** [**detail**]
Описание параметра	**detail**: отображает подробную информацию
Командный режим	Режим Privileged EXEC/Режим глобальной конфигурации/Режим конфигурации интерфейса

6.4.2.6. Пример конфигурации

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • Настройте интервал отправки пакетов Hello как 50 секунд. • Настройте задержку prune propagation как 400 мс. • Настройте интервал prune override на 3000 мс. • Включите возможность подавления интерфейса для отправки пакетов соединения. • Настройте задержку отправки пакетов Hello как 3 секунды. • Настройте приоритет DR пакета приветствия как 5
	QTECH# configure terminal QTECH (config)#int gi 0/1 QTECH (config-if-GigabitEthernet 0/1)#ip pim query-interval 50 QTECH (config-if-GigabitEthernet 0/1)#ip pim propagation-delay 400 QTECH (config-if-GigabitEthernet 0/1)#ip pim override-interval 3000 QTECH (config-if-GigabitEthernet 0/1)#ip pim triggered-hello-delay 3 QTECH (config-if-GigabitEthernet 0/1)#ip pim neighbor-tracking
Проверка	Запустите **debug ip pim sparse-mode packet**, чтобы отобразить параметры пакета Hello
	QTECH# debug ip pim sparse-mode packet 00:01:49:43: %7: VRF(0): Hello send to GigabitEthernet 0/1 00:01:49:43: %7: Send Hello packet 00:01:49:43: %7: Holdtime: 175 00:01:49:43: %7: T-bit: on 00:01:49:43: %7: Propagation delay: 400 00:01:49:43: %7: Override interval: 3000 00:01:49:43: %7: DR priority: 5 00:01:49:43: %7: Gen ID: 355154648

	00:01:49:43: %7: RPF Vector capable
Шаги настройки	Настройте фильтрацию соседей и установите разрешенный диапазон адресов 192.168.1.0. к 192.168.1.255
	QTECH# configure terminal QTECH (config)#int gi 0/1 QTECH (config-if-GigabitEthernet 0/1)# ip pim neighbor-filter 1 % access-list 1 not exist QTECH(config)# access-list 1 permit 192.168.1.0 0.0.0.255 QTECH(config)#
Проверка	Отображать информацию о соседях до настройки фильтрации соседей
	QTECH# show ip pim sparse-mode neighbor Neighbor Interface Uptime/Expires Ver DR Address Priority/Mode 192.168.36.89 GigabitEthernet 0/1 01:12:13/00:01:32 v2 1 / P
	Отображать информацию о соседях после настройки фильтрации соседей
	QTECH# show ip pim sparse-mode neighbor

6.4.2.7. Распространенные ошибки

Основные функции PIM-SM не настроены или конфигурация не удалась.

6.4.3. Настройка параметров BSR

6.4.3.1. Эффект конфигурации

Настройте диапазон адресов пакетов BSM.

6.4.3.2. Примечания

- Необходимо настроить основные функции PIM-SM.
- Необходимо настроить C-RP и C-BSR.
- Границы должны быть настроены на интерфейсах между доменами.

6.4.3.3. Шаги настройки

Настройка границ

- Границы должны быть настроены, если имеется несколько доменов.
- Границы настраиваются на интерфейсах, разделяющих два домена.

Настройка ограничения пакетов BSM на маршрутизаторе PIM

- Опционально.

- Если не указано, ограничение пакетов BSM можно настроить на всех маршрутизаторах PIM.

Настройка C-BSR для проверки диапазона адресов C-PR

- Опционально.
- Если не указано иное, проверку диапазона C-PR можно настроить на всех C-BSR.

Разрешение C-BSR получать пакет C-RP-ADV, счетчик префикса (Prefix-Count) которого равен 0

- Опционально.
- Если не указано, эту функцию можно настроить на всех C-BSR.

6.4.3.4. Проверка

Проверка границ

Включите базовые функции PIM-SM. Настройте два маршрутизатора в разных доменах, настройте маршрутизатор B как C-BSR, а маршрутизатор A — для приема пакетов BSM.

Настройте соединение маршрутизатора A и маршрутизатора B в качестве границы, чтобы маршрутизатор A не получал пакеты BSM.

Настройка для проверки ограничения пакетов BSM на маршрутизаторе PIM

Когда основные функции PIM-SM включены и маршрутизатор B установлен как C-BSR, маршрутизатор A может принимать пакеты BSM. Если диапазон адресов C-BSR ограничен на маршрутизаторе A, пакеты BSM не будут приниматься маршрутизатором A.

Настройка C-BSR для проверки диапазона адресов C-PR

Когда базовые функции PIM-SM включены, маршрутизатор B устанавливается как C-BSR, а маршрутизатор A — как C-RP. Если диапазон адресов C-RP ограничен на C-BSR, маршрутизатор B не будет получать пакеты, отправленные из C-RP.

6.4.3.5. Связанные команды

Настройка границ BSR

Команда	**ip pim bsr-border**
Командный режим	Режим настройки интерфейса
Руководство по использованию	Чтобы предотвратить флудинг BSM, вы можете настроить границу BSR на интерфейсе, чтобы пакеты BSM, поступающие на этот интерфейс, отбрасывались, но не пересылались

Настройка ограничения пакетов BSM на маршрутизаторе PIM

Команда	**ip pim accept-bsr list { <1-99> | <1300-1999> | WORD }**
Описание параметра	**list** *access-list*: настраивает диапазон адресов BSR с использованием стандартного IP ACL. Значение может быть от 1 до 99, от 1300 до 1999 или название

Командный режим	Режим глобальной конфигурации
Руководство по использованию	После включения этой функции маршрутизаторы PIM-SM получают только пакеты BSM, отправленные с разборчивого BSR

Настройка C-BSR для проверки диапазона адресов C-PR

Команда	**ip pim accept-crp list** *access-list*
Описание параметра	**list** *access-list*: указывает диапазон адресов C-RP и адресов группы multicast, которые они обслуживают с использованием расширенного IP ACL. Значение может быть от 100 до 199, от 2000 до 2699, или название
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эту команду следует настроить на C-BSR. Когда C-BSR становится BSR, он может установить диапазон разборчивых адресов C-RP и диапазон адресов группы multicast, которые они обслуживают

Отображение информации о пакетах BSM

Команда	**show ip pim sparse-mode bsr-router**
Командный режим	Режим Privileged EXEC/Режим глобальной конфигурации/Режим конфигурации интерфейса

Отображение пакетов всех RP и адресов групп multicast, которые они обслуживают

Команда	**show ip pim sparse-mode rp mapping**
Командный режим	Режим Privileged EXEC/Режим глобальной конфигурации/Режим конфигурации интерфейса

6.4.3.6. Пример конфигурации

Настройка границ BSR

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • На маршрутизаторе A настройте адрес C-RP как 192.168.8.8. • На маршрутизаторе B настройте адрес C-RP как 192.168.5.5, а адрес C-BSR — как 192.168.6.6. • Настройте границу BSR на соединении маршрутизатора A и маршрутизатора B

	QTECH# configure terminal QTECH(config)# int GigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# ip pim bsr-border QTECH(config)# end
Проверка	Перед настройкой границы отобразите информацию BSM на маршрутизаторе A
	QTECH# show ip pim sparse-mode bsr-router PIMv2 Bootstrap information This system is the Bootstrap Router (BSR) BSR address: 192.168.6.6 Uptime: 01:14:25, BSR Priority: 64, Hash mask length: 10 Next bootstrap packet in 00:00:52 Role: Candidate BSR Priority: 64, Hash mask length: 10 State: Elected BSR Candidate RP: 192.168.8.8(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:06
	ПРИМЕЧАНИЕ: кандидат RP: указывает все C-RP, настроенные на существующем маршрутизаторе. Он не включает C-RP, настроенные на других маршрутизаторах
	После настройки границы отобразите информацию BSM на маршрутизаторе A
	QTECH# show ip pim sparse-mode bsr-router

Настройка ограничения пакетов BSM на маршрутизаторе PIM, фильтрация исходных адресов BSM и настройка диапазона исходных адресов BSM от 192.168.1.1 до 192.168.1.255

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • На маршрутизаторе A настройте адрес C-RP как 192.168.8.8. • На маршрутизаторе B настройте адрес C-RP как 192.168.5.5, а адрес C-BSR — как 192.168.6.6. • На маршрутизаторе A настройте диапазон разрешенных исходных адресов BSM от 192.168.1.1 до 192.168.1.255
	QTECH# configure terminal QTECH(config)# ip pim accept-bsr list 1

	% access-list 1 not exist QTECH(config)# access-list 1 permit 192.168.1.0 0.0.0.255 QTECH(config)#
Проверка	Прежде чем настраивать лимит пакетов BSM, отобразите информацию BSM на маршрутизаторе A
	QTECH#show ip pim sparse-mode bsr-router PIMv2 Bootstrap information BSR address: 192.168.6.6 Uptime: 00:00:11, BSR Priority: 64, Hash mask length: 10 Expires: 00:01:59 Role: Non-candidate BSR Priority: 0, Hash mask length: 10 State: Accept Preferred Candidate RP: 192.168.8.8(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:06
	После настройки лимита пакетов BSM отобразите информацию BSM на маршрутизаторе A
	QTECH# show ip pim sparse-mode bsr-router Candidate RP: 192.168.8.8(Loopback 0) Advertisement interval 60 seconds

Настройка C-BSR для проверки диапазона адресов C-PR, фильтрации адресов C-RP и настройки диапазона адресов C-RP от 192.168.1.1 до 192.168.1.255

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • На маршрутизаторе A настройте адрес C-RP как 192.168.8.8. • На маршрутизаторе B настройте адрес C-RP как 192.168.5.5, а адрес C-BSR — как 192.168.6.6. • На маршрутизаторе B настройте диапазон разрешенных исходных адресов C-RP от 192.168.1.1 до 192.168.1.255
	QTECH# configure terminal QTECH(config)# ip pim accept-crp list 100 % access-list 1 not exist QTECH(config)# access-list 1 permit 192.168.1.0 0.0.0.255 QTECH(config)#

Проверка	Прежде чем настраивать фильтрацию C-RP, отобразите информацию обо всех группах RP на маршрутизаторе B
	QTECH#show ip pim sparse-mode rp mapping PIM Group-to-RP Mappings This system is the Bootstrap Router (v2) Group(s): 224.0.0.0/4 RP: 192.168.8.8(Not self) Info source: 192.168.8.8, via bootstrap, priority 192 Uptime: 00:15:16, expires: 00:02:18 RP: 192.168.5.5(Self) Info source: 192.168.6.6, via bootstrap, priority 192 Uptime: 18:52:30, expires: 00:02:00
	После настройки фильтрации C-RP отобразите информацию обо всех группах RP на маршрутизаторе B
	QTECH#show ip pim sparse-mode rp mapping PIM Group-to-RP Mappings This system is the Bootstrap Router (v2) Group(s): 224.0.0.0/4 RP: 192.168.5.5(Self) Info source: 192.168.6.6, via bootstrap, priority 192 Uptime: 21:38:20, expires: 00:02:10
	ПРИМЕЧАНИЕ: после настройки фильтрации C-RP на маршрутизаторе фильтруются только пакеты C-RP, отправленные с других маршрутизаторов, а пакеты, отправленные с текущего маршрутизатора, не фильтруются

6.4.3.7. Распространенные ошибки

- Основные функции PIM-SM не настроены или конфигурация не удалась.
- C-BSR не настроены.
- Граница BSR не настроена на интерфейсах разных доменов.

6.4.4. Настройка параметров RP и DR

6.4.4.1. Эффект конфигурации

- Игнорируйте приоритет C-RP и повторно выберите RP.
- Определите доступность RP для DR источника.
- Настройте диапазон адресов (S, G) пакетов Register источника и разрешите ASM обслуживать только multicast-пакеты в этом диапазоне.

- Ограничьте скорость DR источника для отправки пакетов Register.
- Настройте контрольную сумму длины пакета Register.
- Настройте RP для декапсуляции пакетов Register и пересылки multicast-пакетов на downstream-интерфейсы.
- Настройте IP-адрес источника пакета Register.
- Настройте время подавления пакета Register.
- Настройте время проверки пустого пакета Register.
- Настройте время жизни (S, G) на основе пакета Register, полученного RP.

6.4.4.2. Примечания

Необходимо настроить основные функции PIM-SM.

6.4.4.3. Шаги настройки

Игнорирование приоритета C-RP и повторный выбор RP

- Опционально.
- Если не указано, приоритет C-RP можно отключить на каждом маршрутизаторе.

Обнаружение доступности RP для DR источника

- Опционально.
- Если не указано, эту функцию можно включить на DR, подключенном непосредственно к источнику данных.

Настройка диапазона адресов Register (S, G) источника

- Опционально.
- Если не указано, фильтрацию адреса исходного Register можно включить на всех C-RP или статических RP.

Ограничение скорости DR источника для отправки пакетов Register

- Опционально.
- Если не указано, эту функцию можно включить на DR источника.

Настройка контрольной суммы длины пакета Register

- Опционально.
- Если не указано, эту функцию можно включить на всех C-RP или статических RP.

Настройка пересылки multicast-пакета после декапсуляции пакета Register

- Опционально.
- Если не указано, эту функцию можно включить на всех C-RP или статических RP.

Настройка IP-адреса источника пакета Register

- Опционально.
- Если не указан, IP-адрес источника пакета Register можно настроить на DR, подключенном непосредственно к источнику данных.

Настройка времени подавления пакета Register

- Опционально.
- Если не указано, время подавления пакета Register можно настроить на DR, подключенном непосредственно к источнику данных.

Настройка времени проверки пустого пакета Register

- Опционально.
- Если не указано, время проверки пустого пакета Register можно настроить на DR, подключенном непосредственно к источнику данных.

Настройка время жизни (S, G) на основе пакета Register, полученного RP

- Опционально.
- Если не указано, время жизни (S, G) можно настроить на всех C-RP или статических RP.

6.4.4.4. Проверка

Игнорирование приоритета C-RP

На маршрутизаторе A настройте адрес C-RP как 192.168.8.8 и приоритет по умолчанию — 192. На маршрутизаторе B настройте адрес C-RP как 192.168.5.5, приоритет как 200 и адрес C-BSR как 192.168.6.6.

- Запустите **show ip pim sparse-mode rp 233.3.3.3**, чтобы отобразить RP текущей группы.

Включение DR источника для обнаружения доступности RP

На маршрутизаторе A настройте адрес C-RP как 192.168.8.8 и приоритет по умолчанию — 192. На маршрутизаторе B настройте адрес C-RP как 192.168.5.5, приоритет как 192 и адрес C-BSR как 192.168.6.6. Включите маршрутизатор B для обнаружения доступности RP.

- Запустите **show running-config**, чтобы проверить, вступили ли в силу предыдущие конфигурации.

Настройка диапазона адресов Register (S, G) источника

На маршрутизаторе A настройте адрес C-RP как 192.168.8.8 и приоритет по умолчанию — 192. На маршрутизаторе B настройте адрес C-BSR как 192.168.6.6. Настройте адрес источника 192.168.1.100 и адрес группы multicast 233.3.3.3. На маршрутизаторе A настройте диапазон разрешенных адресов источника группы multicast от 192.168.2.0 до 192.168.2.255.

- Запустите **show ip pim sparse-mode mroute**, чтобы отобразить запись (S, G).

Ограничение скорости DR источника для отправки пакетов Register

Настройте скорость маршрутизатора B для отправки пакетов Register и запустите **show ip pim sparse-mode track**, чтобы отобразить количество отправленных пакетов.

Настройка контрольной суммы длины пакета Register

На маршрутизаторе A настройте расчет контрольной суммы для всей длины пакета Register, а не только для заголовка пакета. Запустите **show running-config**, чтобы проверить конфигурацию.

Пересылка пакета Register RP после его декапсуляции

На маршрутизаторе A настройте пересылку пакета Register после его декапсуляции. Запустите **show running-config**, чтобы отобразить конфигурацию.

Настройка IP-адреса источника пакета Register

Настройте адрес источника пакета Register на маршрутизаторе B и запустите **show running-config**, чтобы отобразить конфигурацию.

Настройка времени подавления пакета Register и времени проверки пустого пакета Register

На маршрутизаторе B настройте время подавления и время проверки пакета Register и запустите **show ip pim sparse-mode track**, чтобы отобразить конфигурацию.

Настройка RP для получения пакетов Register и времени жизни (S, G)

На маршрутизаторе A настройте RP для получения пакетов Register и времени жизни (S, G) и запустите **show ip pim sparse-mode mroute**, чтобы отобразить максимальное время жизни (S, G).

6.4.4.5. Связанные команды

Игнорирование приоритета C-RP

Команда	**ip pim ignore-rp-set-priority**
Командный режим	Режим глобальной конфигурации

Отображение RP, соответствующего группе

Команда	**show ip pim sparse-mode rp-hash** *group-address*
Описание параметра	*group-address*: указывает проанализированный адрес группы multicast
Командный режим	Режим Privileged EXEC/Режим глобальной конфигурации/Режим конфигурации интерфейса

Включение DR источника для обнаружения доступности RP

Команда	**ip pim register-rp-reachability**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После включения этой функции DR источника определит доступность RP перед отправкой пакета Register. Если RP недоступен, пакет не будет отправлен

Настройка диапазона адресов Register (S, G) источника

Команда	**ip pim accept-register** { **list** *access-list* [**route-map** *map-name*] | **route-map** *map-name* [**list** *access-list*] }
Описание параметра	**list** *access-list*: настраивает диапазон адресов (S, G) с использованием расширенного IP ACL. Значение может быть от 100 до 199, от 2000 до 2699 или название. **route-map** *map-name*: настраивает диапазон адресов (S, G) с помощью карты маршрутов

Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда запускается на статическом RP или C-RP для указания адреса источника и адреса группы multicast пакета Register

Отображение записи multicast-маршрутизации

Команда	**show ip pim sparse-mode mroute** [*group-or-source-address* [*group-or-source-address*]]
Описание параметра	*group-or-source-address*: указывает адрес группы multicast или адрес источника (два адреса не могут быть адресами группы multicast или адресами источника одновременно)
Командный режим	Режим Privileged EXEC/Режим глобальной конфигурации/Режим конфигурации интерфейса
Руководство по использованию	Вы можете указать либо адрес группы multicast, либо адрес источника, либо адрес группы multicast и адрес источника; или вы не можете указать ни адрес группы multicast, ни адрес источника. Два адреса не могут одновременно быть адресами групп multicast или адресами источника

Ограничение скорости DR источника для отправки пакетов Register

Команда	**ip pim register-rate-limit** *rate*
Описание параметра	*rate*: указывает максимальное количество пакетов Register, которые можно отправлять каждую секунду. Значение варьируется от 1 до 65 535
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда действует только для пакета Register каждого (S, G) пакета, но не для всех пакетов Register во всей системе. Включение этой команды может снизить нагрузку на исходные DR и RP. Могут быть отправлены только пакеты в пределах ограничения скорости

Отображение счетчиков пакетов PIM-SM

Команда	**show ip pim sparse-mode track**
Командный режим	Режим Privileged EXEC/Режим глобальной конфигурации/Режим конфигурации интерфейса

Руководство по использованию	Время начала подсчета пакетов PIM-SM автоматически включается при запуске системы. Запустите команду **clear ip pim sparse-mode track**, чтобы сбросить время начала и очистить счетчики пакетов PIM-SM

Вычисление контрольной суммы всей длины пакета Register

Команда	**ip pim register-checksum-wholepkt** [**group-list** *access-list*]
Описание параметра	**group-list** *access-list*: настраивает адреса групп multicast, применимые к этой конфигурации, с помощью ACL. *access-list*: значение может быть установлено от 1 до 99 и от 1300 до 1999. Он также поддерживает наименование ACL
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Вы можете включить эту функцию, если хотите вычислить длину всего пакета PIM-SM, включая длину multicast-пакета, инкапсулированного в пакете Register, а не только длину заголовка пакета PIM-SM. Если указан **group-list** *access-list*, эта конфигурация вступает в силу для всех адресов группы multicast

Разрешение RP декапсулировать пакет Register и пересылать multicast-пакет на интерфейсы

Команда	**ip pim register-decapsulate-forward**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда настраивается на статическом RP или C-RP. Он используется для декапсуляции пакета Register с помощью multicast-пакета и пересылки multicast-пакета на интерфейсы. Если пакетов Register, подлежащих декапсуляции, слишком много, процессор будет сильно перегружен. В этом случае данную функцию рекомендуется отключить

Настройка IP-адреса источника пакета Register

Команда	**ip pim register-source** { *local_address* | *Interface-type interface-number* }
Описание параметра	*local_address*: указывает IP-адрес источника пакета Register. *Interface-type interface-number*: указывает IP-адрес этого интерфейса в качестве IP-адреса источника пакета Register

Командный режим	Режим глобальной конфигурации
Руководство по использованию	Указанный адрес должен быть доступен. Когда RP отправляет пакет Register-Stop, маршрутизатор PIM, соответствующий этому адресу, должен ответить. Поэтому рекомендуется использовать loopback-адрес (или другие физические адреса). Эта конфигурация не требует включения PIM

Настройка времени подавления пакета Register

Команда	**ip pim register-suppression** *seconds*
Описание параметра	*seconds*: указывает время подавления пакета Register в секундах. Значение варьируется от 1 до 65 535 (по умолчанию 60)
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если вы настроите этот параметр на DR, время подавления пакета Register, отправленного с DR, будет изменено. Если **ip pim rp-register-kat** не настроен, и, если вы настроите этот параметр на RP, keepalive RP будет изменена

Настройка времени проверки пустого пакета Register

Команда	**ip pim probe-interval** *seconds*
Описание параметра	*seconds*: указывает время проверки пустого пакета Register в секундах. Значение варьируется от 1 до 65 535 (по умолчанию 5)
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Время проверки пустого пакета Register указывает период времени для отправки пустого пакета Register на RP до истечения времени подавления. Время проверки не может превышать половины времени подавления; в противном случае конфигурация не вступит в силу, и будет отображено предупреждающее сообщение. При этом результат времени подавления, умноженный на 3 плюс время проверки, не может превышать 65 535, в противном случае будет отображено предупреждение

Настройка интервала KAT на RP

Команда	**ip pim rp-register-kat** *seconds*
Описание параметра	*seconds*: указывает интервал KAT. Измеряется в секундах. Значение варьируется от 1 до 65 535 (по умолчанию 210)
Командный режим	Режим глобальной конфигурации

6.4.4.6. Пример конфигурации

Настройка RP соответствующих адресов групп multicast, когда приоритет C-RP учитывается или не учитывается

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • На маршрутизаторе A настройте адрес C-RP как 192.168.8.8. • На маршрутизаторе B настройте адрес C-RP как 192.168.5.5, приоритет 200 и адрес C-BSR как 192.168.6.6. • Отобразите группу, соответствующую 233.3.3.3. • Настройте игнорирование приоритета C-RP на маршрутизаторе B
	QTECH# configure terminal QTECH(config)# ip pim ignore-rp-set-priority
Проверка	Отобразите информацию перед настройкой игнорирования приоритета C-RP
	QTECH# show ip pim sparse-mode rp-hash 233.3.3.3 RP: 192.168.8.8 Info source: 192.168.8.8, via bootstrap PIMv2 Hash Value 10(mask 255.192.0.0) RP 192.168.8.8, via bootstrap, priority 192, hash value 1084558102 RP 192.168.5.5, via bootstrap, priority 200, hash value 1094656709
	Отобразите информацию после настройки игнорирования приоритета C-RP
	QTECH# show ip pim sparse-mode rp-hash 233.3.3.3 RP: 192.168.5.5 Info source: 192.168.6.6, via bootstrap

	PIMv2 Hash Value 10(mask 255.192.0.0) RP 192.168.8.8, via bootstrap, priority 192, hash value 1084558102 RP 192.168.5.5, via bootstrap, priority 200, hash value 1094656709

Настройка для проверки доступности RP источника

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • Настройте проверку доступности RP источника
	QTECH(config)# ip pim register-rp-reachability
Проверка	Запустите **show running-config**, чтобы проверить, отображается ли следующая информация
	QTECH(config)#show running-config ip pim register-rp-reachability

Настройка диапазона адресов Register (S, G) источника

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • Настройте фильтрацию адресов источника на маршрутизаторе A. Разрешенный диапазон адресов — от 192.168.2.0 до 192.168.2.255
	QTECH#show ip pim sparse-mode mroute QTECH(config)#ip pim accept-register list 101 % access-list 101 not exist QTECH(config)#access-list 101 permit ip 192.168.2.0 0.0.0.255 any QTECH#show ip pim sparse-mode mroute
Проверка	Прежде чем включать фильтрацию адресов источника, запустите **show ip pim sparse-mode mroute**, чтобы отобразить запись multicast, и проверьте, существуют ли записи (S, G) и (S, G, RPT)
	QTECH#show ip pim sparse-mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 0

(192.168.1.100, 233.3.3.3)
RPF nbr: 192.168.36.90
RPF idx: VLAN 1
SPT bit: 0
Upstream State: NOT JOINED
kat expires in 187 seconds
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0 . . . . . .
Joined
0 . . . . . .
Asserted
0 . . . . . .
Outgoing
0 . . . . . .

(192.168.1.100, 233.3.3.3, rpt)
RP: 192.168.8.8
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: RPT NOT JOINED
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0 . . . . . .
Pruned
0 . . . . . .
Outgoing
0 . . . . . .

(*, 239.255.255.250)
RP: 192.168.8.8
RPF nbr: 0.0.0.0
RPF idx: None

	Upstream State: JOINED 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . . . . . . Joined 0 . j . . . . . . Asserted 0 . . . . . . FCR:
	После включения фильтрации адресов источника запустите **show ip pim sparse-mode mroute**, чтобы отобразить запись multicast, и проверьте, существуют ли записи (S, G) и (S, G, RPT)
	QTECH#show ip pim sparse-mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 0 (S,G,rpt) Entries: 0 FCR Entries: 0 REG Entries: 0 (*, 239.255.255.250) RP: 192.168.8.8 RPF nbr: 0.0.0.0 RPF idx: None Upstream State: JOINED 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . . . . . . Joined 0 . j . . . . . . Asserted

	0 . . . . . . FCR:

Ограничение скорости DR источника для отправки пакетов Register

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • Проверьте количество пакетов PIM-SM, отправленных маршрутизатором B. • Проверьте количество пакетов PIM-SM, отправленных маршрутизатором B за 1 с. • Настройте скорость маршрутизатора B для отправки пакетов Register. • Проверьте количество пакетов PIM-SM, отправленных маршрутизатором B за 1 с
	QTECH (config)#ip pim register-rate-limit 1
Проверка	Отобразите количество пакетов PIM-SM, отправленных маршрутизатором B, прежде чем настраивать скорость. Информация должна отображаться следующим образом:

```
QTECH#show ip pim sparse-mode track
PIM packet counters track
Elapsed time since counters cleared: 04d01h01m
                          Received        sent
Valid PIM packets:        18754           29771
Hello:                    11149           17842
Join-Prune:               0               3234
Register:                 0               3211
Register-Stop:            3192            0
Assert:                   0               0
BSM:                      0               5484
C-RP-ADV:                 4413            0
PIMDM-Graft:              0
PIMDM-Graft-Ack:          0
PIMDM-State-Refresh:      0
Unknown PIM Type:         0
Errors:
Malformed packets:                        0
Bad checksums:                            0
Send errors:                              0
```

	Packets received with unknown PIM version: 0 QTECH#
	Отображение количества пакетов PIM-SM, отправленных маршрутизатором B за 1 с до настройки скорости. Информация должна отображаться следующим образом:
	QTECH #show ip pim sparse-mode track PIM packet counters track Elapsed time since counters cleared: 04d01h04ms Received sent Valid PIM packets: 18765 29789 Hello: 11154 17852 Join-Prune: 0 3236 Register: 0 3214 Register-Stop: 3195 0 Assert: 0 0 BSM: 0 5487 C-RP-ADV: 4416 0 PIMDM-Graft: 0 PIMDM-Graft-Ack: 0 PIMDM-State-Refresh: 0 Unknown PIM Type: 0 Errors: Malformed packets: 0 Bad checksums: 0 Send errors: 0 Packets received with unknown PIM version: 0 QTECH#
	Отображение количества пакетов PIM-SM, отправленных маршрутизатором B после настройки скорости. Информация должна отображаться следующим образом:
	QTECH#show ip pim sparse-mode track PIM packet counters track Elapsed time since counters cleared: 04d01h06m received sent Valid PIM packets: 18777 29808

	Hello: 11159 17862 Join-Prune: 0 3239 Register: 0 3215 Register-Stop: 3196 0 Assert: 0 0 BSM: 0 5489 C-RP-ADV: 4419 0 PIMDM-Graft: 0 PIMDM-Graft-Ack: 0 PIMDM-State-Refresh: 0 Unknown PIM Type: 0 Errors: Malformed packets: 0 Bad checksums: 0 Send errors: 0 Packets received with unknown PIM version: 0 QTECH#

Настройка контрольной суммы длины пакета Register

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • Вычислите контрольную сумму всей длины пакета Register. • Запустите **show running-config**, чтобы проверить, вступили ли в силу предыдущие конфигурации
	QTECH(config)#ip pim register-checksum-wholepkt
Проверка	Отобразите конфигурации маршрутизатора A, которые должны быть следующими:
	QTECH#show running-config 。。。。。 ! ip pim register-checksum-wholepkt ip pim rp-candidate Loopback 0 ! 。。。。

Разрешение RP декапсулировать пакет Register и пересылать multicast-пакет на интерфейсы

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • Включите маршрутизатор A для пересылки пакета Register. • Запустите **show running-config**, чтобы проверить, вступили ли в силу предыдущие конфигурации
	QTECH(config)#ip pim register-decapsulate-forward
Проверка	Отобразите конфигурации маршрутизатора A, которые должны быть следующими:
	QTECH#show running-config 。。。。。。 !! ip pim register-decapsulate-forward ip pim register-checksum-wholepkt ip pim rp-candidate Loopback 0 ! !! 。。。。。。

Настройка IP-адреса источника пакета Register

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • Настройте адрес источника Loop 2 как 192.168.2.2. • Настройте интерфейс адреса источника для пакета Register маршрутизатора B как Loop 2. • Запустите **show running-config**, чтобы проверить, вступили ли в силу предыдущие конфигурации
Проверка	Отобразите конфигурации маршрутизатора B, которые должны быть следующими:
	QTECH#show running-config ! ! ! ip pim register-source Loopback 1 ip pim bsr-candidate Loopback 0 !

	! ! !

Настройка времени подавления пакета Register и времени проверки пустого пакета Register

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • Настройте время подавления пакета Register на маршрутизаторе B на 20 с. • Настройте время проверки пустого пакета Register на маршрутизаторе B на 2 секунды. • Запустите **show ip pim sparse-mode track**, чтобы отобразить количество пакетов Register
	QTECH(config)#ip pim register-suppression 20 QTECH(config)#ip pim probe-interval 2
Проверка	Отображение количества пакетов Register на маршрутизаторе B. Информация должна отображаться следующим образом:
	QTECH#show ip pim sparse-mode track PIM packet counters track Elapsed time since counters cleared: 04d23h15m received sent Valid PIM packets: 23788 43249 Hello: 13817 23178 Join-Prune: 0 4568 Register: 0 8684 Register-Stop: 4223 0 Assert: 0 0 BSM: 0 6819 C-RP-ADV: 5748 0 PIMDM-Graft: 0 PIMDM-Graft-Ack: 0 PIMDM-State-Refresh: 0 Unknown PIM Type: 0 Errors: Malformed packets: 0 Bad checksums: 0

	Send errors: 0 Packets received with unknown PIM version: 0 QTECH# QTECH#
	Через 18 секунд отобразите количество зарегистрированных пакетов на маршрутизаторе B. Информация должна отображаться следующим образом:
	QTECH#show ip pim sparse-mode track PIM packet counters track Elapsed time since counters cleared: 04d23h17m received sent Valid PIM packets: 23798 43263 Hello: 13820 23184 Join-Prune: 0 4569 Register: 0 8685 Register-Stop: 4224 0 Assert: 0 0 BSM: 0 6820 C-RP-ADV: 5749 0 PIMDM-Graft: 0 PIMDM-Graft-Ack: 0 PIMDM-State-Refresh: 0 Unknown PIM Type: 0 Errors: Malformed packets: 0 Bad checksums: 0 Send errors: 0 Packets received with unknown PIM version: 0 QTECH#

Настройка RP для получения пакетов Register и времени жизни (S, G)

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • Настройте маршрутизатор A для получения пакетов Register, а время жизни (S, G) составляет 60 с. • Запустите команду **show ip pim sparse-mode mrout**, чтобы отобразить количество зарегистрированных пакетов

	QTECH(config)#ip pim rp-register-kat 60
Проверка	После настройки времени жизни убедитесь, что время жизни (S, G) на маршрутизаторе A не превышает 60 с
	QTECH(config)#show ip pim sparse-mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 0 (192.168.1.100, 233.3.3.3) RPF nbr: 192.168.36.90 RPF idx: VLAN 1 SPT bit: 0 Upstream State: NOT JOINED kat expires in 49 seconds 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . . . . . . Joined 0 . . . . . . Asserted 0 . . . . . . Outgoing 0 . . . . . . (192.168.1.100, 233.3.3.3, rpt) RP: 192.168.8.8 RPF nbr: 0.0.0.0 RPF idx: None Upstream State: RPT NOT JOINED

	00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . . . . . . Pruned 0 . . . . . . Outgoing 0 . . . . . . (*, 239.255.255.250) RP: 192.168.8.8 RPF nbr: 0.0.0.0 RPF idx: None Upstream State: JOINED 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . . . . . . Joined 0 . j . . . . . . Asserted 0 . . . . . . FCR: QTECH(config)# QTECH(config)#show ip pi

6.4.4.7. Распространенные ошибки

- Основные функции PIM-SM не настроены или конфигурация не удалась.
- (S, G) пакетов Register не настроены на C-RP или статическом RP, или конфигурация не удалась.
- ACL для ограничения (S, G) пакетов Register не настроен или диапазон (S, G) в этом ACL настроен неправильно.
- Диапазон (S, G) пакетов Register на каждом C-RP или статическом RP не одинаков.

6.4.5. Настройка интервала отправки пакета Join/Prune

6.4.5.1. Эффект конфигурации

Измените интервал отправки пакета Join/Prune для формирования RPT или SPT.

6.4.5.2. Примечания

Необходимо настроить основные функции PIM-SM.

6.4.5.3. Шаги настройки

Настройте интервал для отправки пакета Join/Prune.

6.4.5.4. Проверка

На маршрутизаторе B настройте интервал для отправки пакета Join/Prune как 120 с. Запустите **show ip pim sparse-mode mroute**, чтобы отобразить время жизни записи.

6.4.5.5. Связанные команды

Настройка интервала отправки пакета Join/Prune

Команда	**ip pim jp-timer** *seconds*
Описание параметра	*seconds*: указывает интервал отправки пакета Join/Prune. Измеряется в секундах. Значение варьируется от 1 до 65 535 (по умолчанию 60)
Командный режим	Режим глобальной конфигурации

6.4.5.6. Пример конфигурации

Настройка интервала отправки пакета Join/Prune

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • Настройте интервал для отправки пакета Join/Prune
	QTECH(config)#ip pim jp-timer 120
Проверка	Запустите **show ip pim sparse-mode mroute**, чтобы отобразить максимальное время ожидания пакета Join/Prune
	QTECH(config)#show ip pim sparse-mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 1 (192.168.1.100, 233.3.3.3)

RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 96 seconds
kat expires in 92 seconds
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0 . . . . . .
1 . . . . . .
Joined
0 . . . . . .
1 . . . . . .
Asserted
0 . . . . . .
1 . . . . . .
Outgoing
0 . . . . . .
1 . . o . . . . . .

(192.168.1.100, 233.3.3.3, rpt)
RP: 192.168.8.8
RPF nbr: 192.168.36.89
RPF idx: GigabitEthernet 0/1
Upstream State: RPT NOT JOINED
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0 . . . . . .
1 . . . . . .
Pruned
0 . . . . . .
1 . . . . . .
Outgoing
0 . . . . . .

```
1 . . . . . .

(*, 239.255.255.250)
RP: 192.168.8.8
RPF nbr: 192.168.36.89
RPF idx: GigabitEthernet 0/1
Upstream State: JOINED
jt_timer expires in 119 seconds
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
27 28 29 30 31
Local
0 . . . . i . . . . . .
1 . . . . . .
Joined
0 . . . . . .
1 . . . . . .
Asserted
0 . . . . . .
1 . . . . . .
FCR:

VSU(config)#
```

6.4.5.7. Распространенные ошибки

Основные функции PIM-SM не настроены или конфигурация не удалась.

6.4.6. Настройка маршрутизатора последнего hop-а для переключения с RPT на SPT

6.4.6.1. Эффект конфигурации

Переключиться с RPT на SPT.

6.4.6.2. Примечания

Необходимо настроить основные функции PIM-SM.

6.4.6.3. Шаги настройки

Настройте маршрутизатор последнего hop-а для переключения с RPT на SPT.

6.4.6.4. Проверка

Сначала настройте базовые функции PIM-SM. Настройте DR источника для отправки трафика данных (*, 233.3.3.3), а принимающую сторону — для принудительного

присоединения к группе 233.3.3.3 для формирования RPT. Настройте DR приемника на принудительное переключение с RPT на SPT. Запустите **show running-config**, чтобы отобразить результат.

6.4.6.5. Связанные команды

Включение переключения SPT

Команда	**ip pim spt-threshold** [**group-list** *access-list*]
Описание параметра	**group-list** *access-list*: определяет диапазон адресов группы multicast, разрешенных для переключения SPT с использованием ACL. access-list: поддерживаемое значение находится в диапазоне от 1 до 99 или от 1300 до 1999. Также поддерживается присвоение имени ACL
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если **group-list** *access-list* не указан, всем группам разрешено выполнять переключение SPT

6.4.6.6. Пример конфигурации

Настройка маршрутизатора последнего hop-а для переключения с RPT на SPT

Шаги настройки	• Настройте базовые функции PIM-SM. (пропущено) • Настройте DR источника для отправки трафика данных группы 233.3.3.3. • Настройте DR приемника для приема трафика данных группы 233.3.3.3. • Настройте DR приемника последнего hop-а для переключения с RPT на SPT
	QTECH(config)#ip pim spt-threshold
Проверка	Запустите **show running-config**, чтобы отобразить конфигурацию
	! ! ip pim jp-timer 120 ip pim spt-threshold ip pim rp-candidate Loopback 0 ! ! !

6.5. Мониторинг

6.5.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере важной информации и, таким образом, к прерыванию работы служб.

Описание	Команда
Очищает записи multicast-маршрутизации	**clear ip mroute** { * | *group-address* [*source-address*] }
Очищает счетчики multicast-маршрутов	**clear ip mroute statistics** {* | *group-address* [*source-address*] }
Очищает информацию о динамических RP	**clear ip pim sparse-mode bsr rp-set ***
Очищает счетчики пакетов PIM-SM	**clear ip pim sparse-mode track**

6.5.2. Отображение

Описание	Команда
Отображает подробную информацию о BSR	**show ip pim sparse-mode bsr-router**
Отображает информацию PIM-SM интерфейса	**show ip pim sparse-mode interface** [*interface-type interface-number*] [**detail**]
Отображает локальную информацию IGMP об интерфейсе PIM-SM	**show ip pim sparse-mode local-members** [*interface-type interface-number*]
Отображает информацию о записи multicast-маршрутизации PIM-SM	**show ip pim sparse-mode mroute** [*group-or-source-address* [*group-or-source-address*]]
Отображает информацию о соседях PIM-SM	**show ip pim sparse-mode neighbor** [**detail**]
Отображает информацию о следующем hop-е PIM-SM, полученную от NSM	**show ip pim sparse-mode nexthop**

Описание	Команда
Отображает информацию о RP, соответствующем групповому multicast-адресу	**show ip pim sparse-mode rp-hash** *group-address*
Отображает информацию обо всех RP и группах, которые они обслуживают	**show ip pim sparse-mode rp mapping**
Отображает количество отправленных и полученных пакетов PIM-SM с момента начала статистики	**show ip pim sparse-mode track**

7. НАСТРОЙКА PIM-SMV6

7.1. Обзор

Protocol Independent Multicast (PIM) — это протокол multicast-маршрутизации.

PIM не полагается на конкретный протокол unicast-маршрутизации. Он использует таблицу unicast-маршрутизации, установленную любым протоколом unicast-маршрутизации, для завершения проверки пересылки по обратному пути (RPF) и установления multicast-маршрутов. PIM не требуется передавать и получать обновления маршрутов multicast. Таким образом, накладные расходы PIM намного ниже, чем у других протоколов multicast-маршрутизации.

PIM определяет два режима: режим dense и режим sparse. Protocol Independent Multicast Spare Mode (PIM-SM) применим к различным сетевым средам.

ПРИМЕЧАНИЕ: PIM-SM, работающий на IPv6, называется PIM-SMv6.

7.1.1. Протоколы и стандарты

- RFC4601: Protocol Independent Multicast — режим Sparse (PIM-SM).
- RFC5059: механизм Bootstrap Router (BSR) для Protocol Independent Multicast (PIM).
- RFC3962: Protocol Independent Multicast — протокол режима Dense.
- RFC4607: multicast-рассылка с учетом источника для IP (Source-Specific Multicast for IP).

7.2. Приложения

Приложение	Описание
Реализация ASM с использованием PIM-SMv6	Приемник получает пакеты от любого источника multicast
Реализация SSM с использованием PIM-SMv6	Приемник выбирает источник multicast
Пример применения встроенного RP	Встроенный адрес RP настраивается в адресе группы multicast IPv6
Приложение PIM-SMv6 в среде горячего резервного копирования	Протокол multicast PIM-SMv6 работает в среде горячего резервного копирования

7.2.1. Реализация ASM с использованием PIM-SMv6

7.2.1.1. Сценарий

Услуга multicast предоставляется только в одном домене.

Как показано на следующем Рисунке, приемники получают пакеты от любого источника multicast.

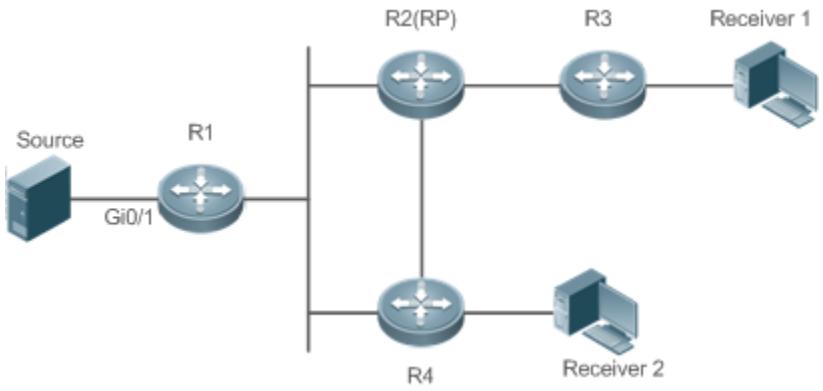

Рисунок 7-1.

R1 напрямую подключен к источнику multicast.

R2 настроен как rendezvous point (RP).

R3 напрямую подключен к приемнику A.

R4 напрямую подключен к приемнику B.

7.2.1.2. Развертывание

- Запустите протокол Open Shortest Path First для IPv6 (OSPFv6) в домене, чтобы реализовать unicast-маршрутизацию.
- Запустите протокол PIM-SMv6 в домене, чтобы реализовать multicast-маршрутизацию.
- Запустите протокол управления группами Интернета версии 6 (IGMPv6) в сегменте сети хоста пользователя, чтобы реализовать управление участниками группы.

7.2.2. Реализация SSM с использованием PIM-SMv6

7.2.2.1. Сценарий

Услуга multicast предоставляется только в одном домене.

Как показано на следующем Рисунке, приемники получают пакеты от определенного источника multicast.

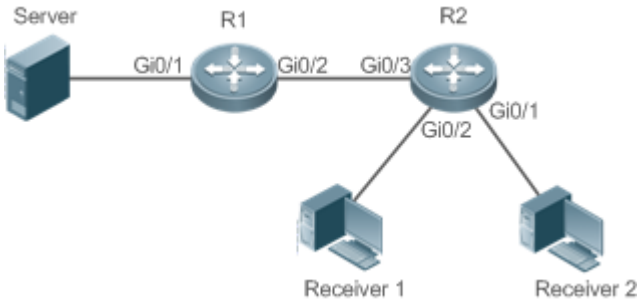

Рисунок 7-2.

R1 напрямую подключен к источнику multicast.

R2 настроен как RP.

R2 напрямую подключен к приемнику A.

R2 напрямую подключен к приемнику B.

7.2.2.2. Развертывание

- Запустите протокол OSPFv6 в домене, чтобы реализовать unicast-маршрутизацию.
- Запустите протокол PIM-SMv6 в домене, чтобы реализовать multicast-маршрутизацию.
- Включите функцию multicast с учетом источника (SSM) протокола PIM-SMv6, чтобы реализовать функцию SSM.
- Запустите протокол управления группами Интернета версии 3 (IGMPv3) в сегменте сети хоста пользователя, чтобы реализовать управление участниками группы.

7.2.3. Пример применения встроенного RP

7.2.3.1. Сценарий

Услуга multicast предоставляется только в одном домене.

Как показано на следующем Рисунке, адрес RP настроен для R2, чтобы маршрутизатор стал встроенным RP.

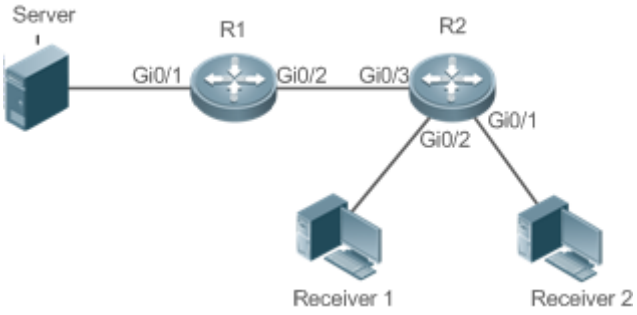

Рисунок 7-3.

R1 напрямую подключен к источнику multicast.

R2 настроен как RP.

R2 напрямую подключен к приемнику A.

R2 напрямую подключен к приемнику B.

R2 настроен как встроенный RP.

7.2.3.2. Развертывание

- Запустите протокол OSPFv6 в домене, чтобы реализовать unicast-маршрутизацию.
- Запустите протокол PIM-SMv6 в домене, чтобы реализовать multicast-маршрутизацию.
- Включите функцию SSM протокола PIM-SMv6, чтобы реализовать функцию SSM.
- Запустите протокол IGMPv3 в сегменте сети хоста пользователя, чтобы реализовать управление участниками группы.
- Настройте адрес RP и встроенный RP на маршрутизаторе R2.

7.2.4. Приложение PIM-SMv6 в среде горячего резервного копирования

7.2.4.1. Сценарий

В среде горячего резервного копирования запустите PIM-SMv6. Устройство выполняет горячее резервное переключение, чтобы гарантировать, что трафик не прерывается.

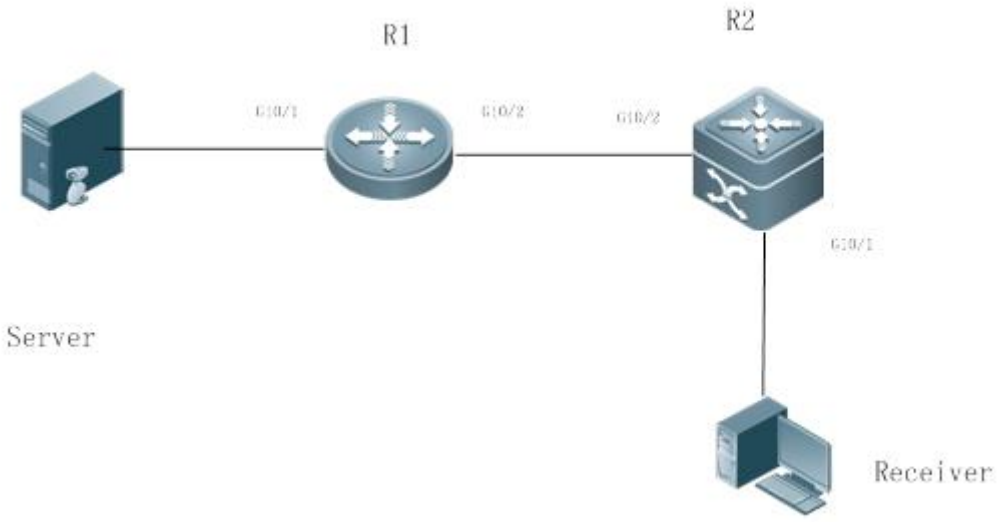

Рисунок 7-4.

R1 подключен к видеосерверу, R2 напрямую подключен к Приемнику, а R2 работает в режиме горячего резервирования.

Протокол multicast уровня 3 работает на маршрутизаторах R1 и R2.

7.2.4.2. Развертывание

- Запустите OSPF на маршрутизаторах R1 и R2, чтобы реализовать unicast-маршрутизацию.
- Запустите PIM-SMv6 на маршрутизаторах R1 и R2, чтобы реализовать multicast-маршрутизацию.
- Заставьте R2 работать в режиме горячего резервного копирования двухузлового (two-node) кластера.

ПРИМЕЧАНИЕ:

R2 может выполнять горячее резервное переключение в среде горячего резервного копирования. В этом случае интервал Query пакетов Hello PIM (значение по умолчанию — 30 секунд) необходимо настроить на маршрутизаторе R2, поскольку таймер keepalive соседа в пакетах Hello PIM маршрутизатора R1 мог истечь (значение по умолчанию в 3,5 раза превышает интервал Query, то есть 105 секунд). Функция multicast в настоящее время опирается на функцию unicast-рассылки, и функция multicast начинает конвергенцию после завершения конвергенции функции unicast-рассылки. Например, время конвергенции плавной перезагрузки (GR) по умолчанию для функции unicast-рассылки составляет 120 секунд. Рекомендуется установить интервал Query пакетов Hello PIM равным 60 секундам. Время keepalive соседа в пакетах PIM Hello составляет 210 секунд. В этом сценарии интервал Query пакетов Hello PIM должен быть установлен со ссылкой на время сходимости GR функции unicast-рассылки, а значение, в 3,5 раза превышающее интервал Query пакетов Hello PIM, должно быть больше, чем время сходимости GR функции

unicast-рассылки. Кроме того, если время конвергенции функции unicast-рассылки велико, интервал передачи пакетов PIM Join/Prune также необходимо скорректировать, поскольку время keepalive пакетов PIM Join/Prune в 3,5 раза превышает интервал передачи пакетов PIM Join/Prune. Время keepalive по умолчанию для пакетов PIM Join/Prune составляет 210 секунд. Если R2 настроен как динамический RP, интервал передачи уведомлений C-RP кандидатом RP (C-RP) также необходимо скорректировать. Интервал передачи по умолчанию составляет 60 секунд, а время keepalive — 2,5-кратный интервал передачи уведомлений C-RP. Например, если время конвергенции функции unicast-рассылки превышает 150 секунд, необходимо настроить интервал передачи уведомлений C-RP. В среде горячего резервного копирования рекомендуется, чтобы интервал Query пакетов PIM Hello был больше значения по умолчанию (30 секунд). В противном случае таймер keepalive соседа в пакетах Hello PIM на стороне peer end истечет во время переключения горячего резервного копирования.

7.3. Функции

7.3.1. Базовые определения

PIM-маршрутизатор и PIM-интерфейс

Маршрутизаторы, на которых включен протокол PIM, называются маршрутизаторами PIM. Интерфейсы, в которых включен протокол PIM, называются интерфейсами PIM.

Multicast-пакеты пересылаются маршрутизаторами PIM. PIM-интерфейсы для приема multicast-пакетов называются upstream-интерфейсами, а PIM-интерфейсы для передачи multicast-пакетов называются downstream-интерфейсами.

Сегменты сети, в которых расположены upstream-интерфейсы, называются upstream сетевыми сегментами. Сегменты сети, в которых расположены downstream-интерфейсы, называются downstream сегментами сети.

Сеть PIM и домен PIM

PIM-маршрутизаторы подключаются через PIM-интерфейсы и образуют сеть PIM.

На некоторых интерфейсах PIM установлены границы, разделяющие большую сеть PIM на несколько доменов PIM. Границы могут отклонять определенные multicast-пакеты или ограничивать передачу сообщений PIM.

Multicast Distribution Tree, DR, RP

Multicast-пакеты передаются из одной точки в несколько точек. Путь пересылки представляет собой древовидную структуру. Этот путь пересылки называется Multicast Distribution Tree (MDT). MDT подразделяются на два типа:

- Rendezvous point tree (RPT): rendezvous point (RP) используется в качестве «корня», а назначенные маршрутизаторы (DR), подключенные к участникам группы, в качестве «листьев».
- Shortest path tree (SPT): используйте DR, подключенный к источнику multicast, в качестве «корня», а RP или DR, подключенные к участникам группы, в качестве «листьев».

DR и RP — это функциональные роли маршрутизаторов PIM.

- RP собирают информацию об источниках multicast и членах групп в сети.
- DR, подключенный к источнику multicast, передает информацию об источнике multicast RP, а DR, подключенные к участникам группы, передают информацию об участниках группы RP.

(*,G), (S,G)

- (*,G): указывает пакеты, переданные из любого источника в группу G, записи маршрутизации, соответствующие пакетам, и путь пересылки (RPT), соответствующий пакетам.
- (S,G): указывает пакеты, переданные из источника S в группу G, записи маршрутизации, соответствующие пакетам, и путь пересылки (SPT), соответствующий пакетам.

ASM, SSM

PIM-SM поддерживает две модели обслуживания multicast: multicast-рассылку с любым источником (ASM) и multicast-рассылку с указанием источника (SSM), которые применимы к различным сегментам адреса multicast.

- ASM: в модели ASM пользовательский хост не может выбрать источник multicast. Хост пользователя присоединяется к группе multicast и получает все пакеты, отправленные из всех источников в группу multicast.
- SSM: в модели SSM пользовательский хост может выбрать источник multicast. Хост пользователя указывает адрес источника при присоединении к группе multicast, а затем получает пакеты только от указанного источника в группу multicast.

ПРИМЕЧАНИЕ: требование модели SSM: необходимо использовать другие сетевые сервиса, чтобы позволить хосту пользователя заранее знать положение источника multicast, чтобы хост пользователя мог выбрать источник multicast.

7.3.2. Обзор

Особенность	Описание
Установление соседских отношений PIM	Отношения соседства устанавливаются между маршрутизаторами PIM для формирования сети PIM
Выбор DR	В сегменте общей сети, подключенном к участникам группы, выбор DR проводится среди соседей PIM для выбора DR, подключенного к участникам группы. В сегменте общей сети, подключенном к источнику multicast, выбор DR проводится среди соседей PIM для выбора DR, подключенного к источнику multicast
Механизм RP	В сети PIM RP статически настраивается или выбирается динамически, так что каждый маршрутизатор PIM знает положение RP
Регистрационная информация об источнике multicast	Когда в сети возникает источник multicast, DR, подключенный к источнику multicast, передает пакет Register на RP, чтобы RP получила информацию об источнике multicast и multicast-пакетах

Особенность	Описание
Создание RPT	Когда участник группы появляется в сети, DR, подключенный к участнику группы, передает пакет Join в направлении RP для установления RPT. Если в сети есть источник multicast, multicast-пакет, передаваемый на RP, может достичь члена группы по RPT
Создание SPT	Когда пакет данных достигает DR, подключенного к участнику группы, DR, подключенный к участнику группы, передает пакет Join в направлении источника multicast для установления SPT. Затем multicast-пакеты пересылаются по SPT
Модели ASM и SSM	PIM-маршрутизаторы предоставляют услуги multicast моделей ASM и SSM. Модель SSM используется для групп в диапазоне адресов SSM, а модель ASM — для других групп

7.3.3. Установление соседских отношений PIM

Отношения соседства устанавливаются между маршрутизаторами PIM для формирования сети PIM. Отношения соседства должны быть установлены между маршрутизаторами PIM до того, как будут обмениваться другими управляющими сообщениями PIM или пересылаться multicast-пакеты.

7.3.3.1. Принцип работы

Сообщение Hello отправляется через интерфейс PIM. Для multicast-пакета для инкапсуляции сообщения Hello адресом назначения является ff02::d (указывает все PIM-маршрутизаторы в одном сегменте сети), исходным адресом является IP-адрес интерфейса PIM и время жизни (TTL) со значением 1.

Сообщения Hello используются для обнаружения соседей, согласования параметров протокола и поддержания отношений соседей.

Обнаружение соседей PIM

PIM-маршрутизаторы в том же сегменте сети получают multicast-пакеты с адресом назначения ff02::d. Таким образом, PIM-маршрутизаторы получают информацию о соседях и устанавливают отношения соседства.

Когда интерфейс PIM включен или обнаруживает нового соседа, сообщение Triggered-Hello-Delay используется для генерации случайного периода времени. В течение этого периода времени интерфейс отправляет пакеты Hello.

Согласование параметров протокола

Сообщение Hello содержит несколько параметров протокола, которые описаны следующим образом:

- DR_Priority: указывает приоритет каждого интерфейса маршрутизатора для выбора DR. Более высокий приоритет означает более высокую вероятность быть избранным DR.
- Holdtime: указывает время ожидания, в течение которого сосед удерживается в состоянии доступности.

- LAN_Delay: указывает задержку передачи сообщения Prune в общем сегменте сети.
- Override-Interval: указывает время prune override, передаваемое в сообщении Hello.

Когда маршрутизатор PIM получает сообщение Prune от upstream-интерфейса, это указывает на то, что в общем сегменте сети существуют другие downstream-интерфейсы. Если маршрутизатору PIM по-прежнему необходимо получать данные multicast, он должен отправить сообщение Prune Override upstream-интерфейсу в течение времени Override-Interval.

LAN_Delay + Override-Interval = PPT (Prune-Pending Timer). После того как маршрутизатор PIM получает сообщение Prune от downstream-интерфейса, он не выполняет pruning немедленно, а ожидает таймаута PPT. По истечении времени PPT маршрутизатор PIM выполняет pruning. Если во время PPT маршрутизатор PIM получает сообщение Prune Override от downstream-интерфейса, он отменяет pruning.

Обслуживание отношений с соседями

Сообщение Hello периодически отправляется между маршрутизаторами PIM. Если пакет Hello не получен от соседа PIM в течение времени Holdtime, сосед считается недоступным и удаляется из списка соседей. Любые изменения в соседях PIM приведут к изменению топологии multicast в сети. Если upstream-сосед или downstream-сосед в MDT недоступен, повторная конвергенция multicast-маршрутизации выполняется снова и MDT переносится.

7.3.3.2. Сопутствующая конфигурация

Включение функции PIM-SMv6 на интерфейсе

По умолчанию функция PIM-SMv6 на интерфейсе отключена.

Запустите команду **ipv6 pim sparse-mode**, чтобы включить или отключить функцию PIM-SMv6 на интерфейсе.

Функция PIM-SMv6 должна быть включена на интерфейсе, чтобы интерфейс участвовал в работе протоколов PIM. Если функция PIM-SMv6 отключена на интерфейсе, который функционирует как DR, статический RP, кандидат-rendezvous point (C-RP) или кандидат-bootstrap router (C-BSR), соответствующая роль протокола не вступает в силу.

Настройка интервала передачи сообщений Hello на интерфейсе

По умолчанию сообщения Hello передаются с интервалом в 30 секунд.

Запустите команду **ipv6 pim query-interval** *seconds*, чтобы настроить интервал передачи сообщений Hello на интерфейсе. Значение варьируется от 1 до 65 535.

Большее значение *interval-seconds* означает больший интервал передачи сообщений Hello, а меньшее значение *interval-seconds* означает меньший интервал передачи сообщений Hello.

7.3.4. Выбор DR

В сегменте общей сети, подключенном к участникам группы, выбор DR проводится среди соседей PIM для выбора DR, подключенного к участникам группы.

В сегменте общей сети, подключенном к источнику multicast, выбор DR проводится среди соседей PIM для выбора DR, подключенного к источнику multicast.

DR передает сообщение Join/Prune в направлении root-узла MDT для напрямую подключенных участников группы или передает данные напрямую подключенного источника multicast в MDT.

7.3.4.1. Принцип работы

IP-адрес соседа и приоритет DR получаются из пакетов Hello соседей во время установления отношений соседства PIM, чтобы выбрать DR.

Ключом к выбору DR являются приоритеты DR и IP-адреса интерфейсов.

Приоритет интерфейса DR

Более высокий приоритет интерфейса DR означает более высокую вероятность того, что маршрутизатор PIM будет успешно выбран в качестве DR во время выборов DR.

IP-адрес интерфейса

Если интерфейсы маршрутизаторов PIM имеют одинаковый приоритет DR во время выбора DR, сравниваются IP-адреса соседей. Больший IP-адрес означает более высокую вероятность того, что маршрутизатор PIM будет успешно выбран в качестве DR.

7.3.4.2. Сопутствующая конфигурация

Настройка IP-адресов интерфейсов

По умолчанию для интерфейсов не настроены IP-адреса.

Запустите команду **ipv6 address**, чтобы установить IP-адрес для интерфейса.

Если PIM-маршрутизаторы имеют одинаковый приоритет DR, маршрутизатор PIM с большим IP-адресом выбирается в качестве DR.

Включение функции PIM-SMv6 на интерфейсе

По умолчанию функция PIM-SMv6 на интерфейсе отключена.

Запустите команду **ipv6 pim sparse-mode**, чтобы включить или отключить функцию PIM-SMv6 на интерфейсе.

Функция PIM-SMv6 должна быть включена на интерфейсе, чтобы интерфейс участвовал в работе протоколов PIM. Если функция PIM-SMv6 отключена на интерфейсе, который функционирует как DR, статический RP, C-RP или C-BSR, соответствующая роль протокола не вступает в силу.

Настройка приоритета DR интерфейса

По умолчанию приоритет DR равен 1.

Запустите команду **ipv6 pim dr-priority** *priority-value*, чтобы настроить приоритет DR интерфейса. Значение приоритета находится в диапазоне от 0 до 4 294 967 294.

Приоритет DR интерфейса используется для выбора DR в напрямую подключенном сегменте сети интерфейса. Большее значение приоритета означает более высокую вероятность того, что маршрутизатор PIM будет выбран в качестве DR.

7.3.5. Механизм BSR

В сети PIM bootstrap router (BSR) периодически генерирует сообщения bootstrap (BSM), включая информацию о серии C-RP и соответствующих групповых адресах. BSM передаются hop за hop-ом во всем домене. PIM-маршрутизаторы по всей сети получают BSM и записывают информацию о C-RP и соответствующих групповых адресах.

7.3.5.1. Принцип работы

В домене PIM-SMv6 настраиваются один или несколько C-BSR, и BSR выбирается из кандидатов BSR в соответствии с определенными правилами.

7.3.5.2. Сопутствующая конфигурация

Настройка C-BSR

По умолчанию C-BSR не настроен.

Запустите команду **ipv6 pim bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority-value*]], чтобы настроить или отменить C-BSR.

C-BSR выбирают глобально уникальный BSR в домене PIM-SM посредством изучения и выбора BSM. BSR передает BSM.

Настройка границы BSR

По умолчанию граница BSR не настроена.

Запустите команду **ipv6 pim bsr-border**, чтобы настроить или отменить границу BSR.

После настройки этой команды для интерфейса интерфейс немедленно отбрасывает полученные BSM и не пересылает BSM, тем самым предотвращая флудинг BSM. Граница BSR не настроена, если эта команда не настроена.

Определение допустимого диапазона BSR

По умолчанию BSM BSR не фильтруются.

Запустите команду **ipv6 pim accept-bsr list** *ipv6_access-list*, чтобы определить или отменить диапазон BSR.

После настройки этой команды определяется допустимый диапазон BSR. Если эта команда не настроена, устройство с включенной функцией PIM-SMv6 будет получать все BSM.

Настройка C-BSR для ограничения диапазона адресов действительных C-RP и диапазона групп multicast, обслуживаемых C-RP

C-BSR получает уведомления от всех C-RP.

Запустите команду **ipv6 pim accept-crp list** *ipv6_access-list*, чтобы настроить фильтрацию уведомлений от C-RP.

После настройки этой команды C-BSR ограничивает диапазон адресов действительных C-RP и диапазон групп multicast, обслуживаемых C-RP. Если эта команда не настроена, C-BSR получает уведомления от всех C-RP.

Настройка C-BSR для приема пакетов C-RP-ADV с счетчиком префиксов, равным 0

По умолчанию C-BSR не получает пакеты C-RP-ADV с счетчиком префикса, равным 0.

Запустите команду **ipv6 pim accept-crp-with-null-group**, чтобы настроить, следует ли получать пакеты C-RP-ADV с счетчиком префикса, равным 0.

После настройки этой команды C-BSR может принимать пакеты C-RP-ADV с счетчиком префиксов, равным 0. Если эта команда не настроена, C-BSR не обрабатывает пакеты C-RP-ADV с счетчиком префиксов, равным 0.

7.3.6. Механизм RP

В сети PIM RP статически настраивается или выбирается динамически, так что каждый маршрутизатор PIM знает положение RP. RP служит root-ом RPT. Установление RPT и пересылка потоков данных RPT должны использовать RP в качестве точки пересылки.

7.3.6.1. Принцип работы

Все PIM-маршрутизаторы в домене PIM должны быть сопоставлены с одним и тем же RP через определенный адрес группы multicast. В сети PIM RP подразделяются на статические и динамические RP.

Статическая RP

В статической конфигурации RP адрес RP настраивается непосредственно на каждом маршрутизаторе PIM, чтобы все PIM-маршрутизаторы в сети PIM знали адрес RP.

Динамическая RP

C-RP также настраиваются в домене PIM-SMv6. Эти C-RP передают пакеты данных, содержащие их адреса и информацию об обслуживаемых ими группах multicast в BSR в unicast-режиме. BSR периодически генерирует BSM, которые содержат информацию о серии C-RP и их групповых адресах. BSM передаются hop за hop-ом во всем домене. Устройства получают и сохраняют эти BSM. DR на принимающей стороне использует алгоритм хеширования для сопоставления адреса группы с C-RP, который может обслуживать группу. Затем может быть определена RP, соответствующая групповому адресу.

7.3.6.2. Сопутствующая конфигурация

Установка статического адреса RP

По умолчанию адрес RP не настроен.

Запустите команду **ipv6 pim rp-address** *ipv6_rp-address* [*ipv6_access-list*], чтобы настроить или отменить статический адрес RP для маршрутизатора PIM.

RP должен быть настроен для реализации ASM в сети PIM-SMv6. Вы можете настроить статический RP или динамический RP.

Если в сети PIM-SMv6 настроен статический RP, конфигурация статического RP на всех устройствах в домене PIM-SMv6 должна быть единообразной, чтобы предотвратить неоднозначность маршрута multicast в домене PIM-SMv6.

Настройка адреса C-RP

По умолчанию адрес C-RP не настроен.

Запустите команду **ipv6 pim rp-candidate** *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *ipv6_access-list*], чтобы настроить или отменить маршрутизатор PIM в качестве C-RP.

C-RP периодически передают уведомления C-RP в BSR. Информация, содержащаяся в этих уведомлениях C-RP, распространяется на все устройства PIM-SMv6 в домене, тем самым обеспечивая уникальность сопоставления RP.

Игнорирование приоритета RP в настройках RP

По умолчанию предпочтение отдается C-RP с более высоким приоритетом.

Запустите команду **ipv6 pim ignore-rp-set-priority**, чтобы указать или игнорировать приоритет RP при выборе RP для группы.

Когда для multicast-адреса необходимо выбрать один RP и несколько RP могут обслуживать этот multicast-адрес, используйте эту команду, если приоритет RP необходимо игнорировать во время сравнения RP. Если эта команда не настроена, приоритет RP будет учитываться во время сравнения RP.

Настройка статической RPпервой

По умолчанию предпочтительным является динамический C-RP.

Запустите команду **ipv6 pim static-rp-preferred**, чтобы сначала выбрать статический RP во время выбора RP.

После настройки этой команды сначала принимается статическая RP. Если эта команда не настроена, сначала принимается C-RP.

Настройка встроенной функции RP

По умолчанию встроенная функция RP включена для всех адресов группы IPv6, в которые встроен адрес RP.

Запустите команду **ipv6 pim rp embedded** [**group-list** *ipv6_acl_name*], чтобы включить встроенную функцию RP.

Встроенная функция RP — это особый механизм обнаружения RP в IPv6 PIM. Этот механизм использует адрес multicast IPv6, в который встроен адрес RP, чтобы позволить устройству multicast напрямую извлекать адрес RP из адреса multicast. По умолчанию встроенная функция RP включена для всех адресов группы IPv6, в которые встроен адрес RP.

7.3.7. Регистрационная информация об источнике multicast

Когда в сети возникает источник multicast, DR, подключенный к источнику multicast, передает пакет Register на RP, чтобы RP получила информацию об источнике multicast и multicast-пакетах.

7.3.7.1. Принцип работы

DR на стороне источника данных получает пакет данных multicast от напрямую подключенного хоста и инкапсулирует данные multicast в сообщение Register. Затем он передает сообщение Register на RP в unicast-режиме. RP генерирует запись (S,G).

Если запись пересылки содержит исходящий интерфейс на RP, RP пересылает инкапсулированный пакет данных на исходящий интерфейс.

Если у RP нет записи пересылки текущей группы, он запускает таймер запуска записи (S,G). По истечении времени таймера RP передает сообщение Register-Stop на DR и удаляет запись. После того, как DR на стороне источника данных получает сообщение Register-Stop, DR передает probing-пакет (пакет проверки) до истечения таймера сообщения Register-Stop.

Если DR не получает сообщение Register-Stop, после истечения таймера DR на стороне источника данных инкапсулирует multicast-данные в сообщение Register и передает их RP в unicast-режиме.

Если DR получает сообщение Register-Stop, он возобновляет задержку и повторно передает probing-пакет до истечения задержки.

7.3.7.2. Сопутствующая конфигурация

Настройка обнаружения доступности пакетов Register RP

По умолчанию доступность RP не обнаружена.

Запустите команду **ipv6 pim register-rp-reachability**, чтобы установить или отменить обнаружение доступности RP.

Если необходимо определить доступность RP для пакета Register, передаваемого от DR к RP, вы можете настроить эту команду. После настройки этой команды доступность RP обнаруживается до того, как DR передает пакет Register на RP. То есть DR запрашивает таблицу unicast-маршрутизации и статическую таблицу multicast-маршрутизации, чтобы проверить, существует ли маршрут, доступный для RP. Если нет, DR не передает пакет Register.

Настройка RP для фильтрации пакетов Register

По умолчанию RP разрешает каждый полученный пакет Register.

Запустите команду **ipv6 pim accept-register** { **list** *ipv6_access-list* [**route-map** *map-name*] | **route-map** *map-name* [**list** *ipv6_access-list*] } для включения или отключения RP для фильтрации полученных пакетов Register.

Чтобы фильтровать полученные пакеты Register на RP, настройте эту команду. Если эта команда не настроена, RP разрешает каждый полученный пакет Register. Если эта команда настроена, обрабатываются только те пакеты Register, адреса источника и групповые адреса которых разрешены ACL. В противном случае пакеты Register отфильтровываются.

Настройка ограничения скорости передачи для пакетов Register

По умолчанию скорость передачи пакетов Register не ограничена.

Запустите команду **ipv6 pim register-rate-limit** *rate*, чтобы настроить, следует ли ограничивать скорость передачи пакетов Register.

Если в этой команде установлено значение **no**, скорость передачи не ограничивается. Эта команда используется для настройки скорости передачи пакетов Register с адреса multicast-группы (S,G), а не скорости передачи пакетов Register всей системы.

Настройка расчета контрольной суммы пакета Register на основе всего пакета Register

По умолчанию контрольная сумма в пакете Register рассчитывается в режиме по умолчанию, указанном в протоколе.

Запустите команду **ipv6 pim register-checksum-wholepkt [group-list** *ipv6_access-list* **]**, чтобы установить длину пакета для расчета контрольной суммы.

Если для расчета контрольной суммы пакета Register используется весь пакет протокола PIM, включая инкапсулированный пакет multicast-данных, используйте эту команду. Если эта команда не настроена, контрольная сумма в пакете Register рассчитывается в режиме по умолчанию, указанном в протоколе.

Настройка исходного адреса пакетов Register

По умолчанию адрес источника пакетов Register использует адрес интерфейса DR, подключенного к источнику multicast.

Запустите команду **ipv6 pim register-source** { *ipv6_local_address* | *interface-type interface-number }* для настройки исходного адреса пакетов Register.

Чтобы настроить адрес источника пакетов Register, передаваемых из DR, используйте эту команду. Если эта команда не настроена или в этой команде установлено значение **no**, в качестве адреса источника пакетов Register используется адрес интерфейса DR, подключенного к источнику multicast. Если используется параметр адреса этой команды, настроенный адрес должен быть доступным unicast-маршрутом. Если используется параметр интерфейса этой команды, этот интерфейс может быть loopback-интерфейсом или интерфейсом других типов, а адрес интерфейса должен быть объявленным unicast-маршрутом.

Настройка времени подавления пакетов Register

Время подавления пакетов Register по умолчанию составляет 60 секунд.

Запустите команду **ipv6 pim register-suppression** *seconds*, чтобы настроить время подавления.

Если эта команда используется для настройки времени подавления пакетов Register, настройка значения на DR изменит время подавления пакетов Register на DR. Если

команда **ipv6 pim rp-register-kat** *seconds* не настроена, определение значения на RP изменит время keepalive на RP.

Настройка времени проверки пустых пакетов Register

Время проверки (probing) по умолчанию составляет 5 секунд.

Запустите команду **ipv6 pim probe-interval** *interval-seconds*, чтобы установить время проверки.

DR источника передает пустой пакет Register в RP в течение определенного интервала до истечения времени подавления пакета Register. Этот интервал является временем проверки. Время проверки по умолчанию составляет 5 секунд.

Настройка значения времени таймера RP KAT

По умолчанию используется значение KAT по умолчанию. Значение KAT по умолчанию = время подавления регистрации x 3 + время обнаружения регистрации.

Запустите команду **ipv6 pim rp-register-kat** *seconds*, чтобы установить время таймера KAT.

Чтобы настроить время keepalive пакетов Register с адреса группы multicast (S,G) на RP, используйте эту команду.

7.3.8. Создание RPT

Когда участник группы появляется в сети, DR, подключенный к участнику группы, передает пакет Join в направлении RP для установления RPT. Если в сети есть источник multicast, multicast-пакет, передаваемый на RP, может достичь члена группы по RPT.

7.3.8.1. Принцип работы

Процесс создания RPT выглядит следующим образом:

1. DR на принимающей стороне получает пакет MLD (*,G)Include report от получателя.
2. Если DR на принимающей стороне не является RP группы G, DR на принимающей стороне передает один пакет (*.G)join в направлении RP. Upstream-устройство, которое получает пакет (*.G)join, передает пакет (*.G)join в направлении RP. Пакет (*.G)join передается hop за hop-ом до тех пор, пока RP группы G не получит пакет (*.G)join, указывающий, что DR на принимающей стороне присоединяется к RPT.
3. Когда хост источника данных передает multicast-данные группе, исходные данные инкапсулируются в сообщение Register и передаются RP в unicast-режиме DR на стороне источника данных. RP декапсулирует сообщение Register, извлекает пакет данных и затем пересылает его каждому участнику группы по RPT.
4. RP передает пакет (S,G)join в DR на стороне источника данных, чтобы присоединиться к SPT этого источника данных.
5. После того как SPT от RP к DR на стороне источника данных установлен, пакеты данных от источника данных передаются на RP по SPT без инкапсуляции.
6. Когда первый пакет multicast-данных достигает RP по SPT, RP передает сообщение Register-Stop DR на стороне источника данных, чтобы позволить DR остановить инкапсуляцию пакетов Register. После того, как DR на стороне источника данных получает сообщение Register-Stop, он не инкапсулирует пакеты Register, а передает пакеты Register на RP по SPT источника данных. RP пересылает пакеты Register каждому участнику группы по RPT.

7.3.8.2. Сопутствующая конфигурация

Настройка интервала передачи пакетов Join/Prune

Интервал передачи пакетов Join/Prune по умолчанию составляет 60 секунд.

Запустите команду **ipv6 pim jp-timer** *seconds*, чтобы установить интервал передачи пакетов Join/Prune.

Чтобы изменить интервал передачи пакетов Join/Prune по умолчанию, настройте эту команду. Если эта команда не настроена, интервал передачи пакетов Join/Prune по умолчанию составляет 60 секунд.

7.3.9. Создание SPT

Когда пакет данных достигает DR, подключенного к участнику группы, DR, подключенный к участнику группы, передает пакет Join в направлении источника multicast для установления SPT. Затем multicast-пакеты пересылаются по SPT, тем самым разгружая RP в RPT и уменьшая количество hop-ов от DR на стороне источника данных к принимающей стороне.

7.3.9.1. Принцип работы

Процесс создания SPT выглядит следующим образом:

DR на принимающей стороне передает пакет (*,G)join в DR на исходящей стороне по SPT. Пакет (*,G)join передается hop за hop-ом до тех пор, пока DR на исходящей стороне не получит пакет (*,G)join, образуя SPT.

7.3.9.2. Сопутствующая конфигурация

По умолчанию переключение SPT отключено.

Запустите команду **ipv6 pim spt-threshold** [**group-list** *ipv6_access-list*], чтобы настроить, следует ли запускать переключение SPT.

После настройки этой команды, когда DR получает пакет (S,G) от первого члена группы, генерируется одно сообщение PIM Join, которое пересылается RP для создания «дерева» SPT. Если **group-list** определен, определенная группа переключается с RPT на SPT. Если в этой команде установлено значение **no** и **group-list** не определен, переключение с RPT на SPT отключается, и устройство перенаправляется на RPT и передает источнику один пакет Prune. Если в этой команде установлено значение **no**, **group-list** определен, а определенный список ACL является настроенным списком ACL, список ACL, связанный со списком групп, отменяется, и всем группам разрешено переключение с RPT на SPT.

7.3.10. Модели ASM и SSM

PIM-SM поддерживает две модели multicast: ASM и SSM. В модели ASM приемник multicast-данных указывает только на присоединение к группе multicast G, но не указывает источник multicast S. В модели SSM приемник multicast-данных может указать как источник multicast S, так и группу multicast G.

ПРИМЕЧАНИЕ: когда модель SSM реализуется через IPv6, необходимо использовать MLDv2 для управления отношениями участников между хостами и устройствами, а PIM-SMv6 необходимо использовать для подключения устройств.

В модели SSM приемник multicast заранее узнает об источнике multicast (S,G) посредством некоторых каналов (таких как получение доступа к серверу или получение объявлений). Когда приемнику multicast необходимо заказать сервис multicast, он напрямую передает пакет MLD(S,G) Join устройству последнего hop-а, например, как показано на следующем Рисунке. Multicast-приемник 1 передает пакет MLD(S,G) Join для утверждения

multicast-сервиса (S,G). После получения пакета MLD(S,G) Join от multicast-приемника устройство последнего hop-а передает пакет PIM(S,G) Join к источнику multicast hop за hop-ом, например, как показано на следующем Рисунке, после, получив пакет MLD(S,G) Join от multicast-приемника 1, R1 передает пакет PIM(S,G) Join на R3, который передает пакет PIM(S,G) Join на R4. В результате устанавливается SPT от multicast-приемника к источнику multicast.

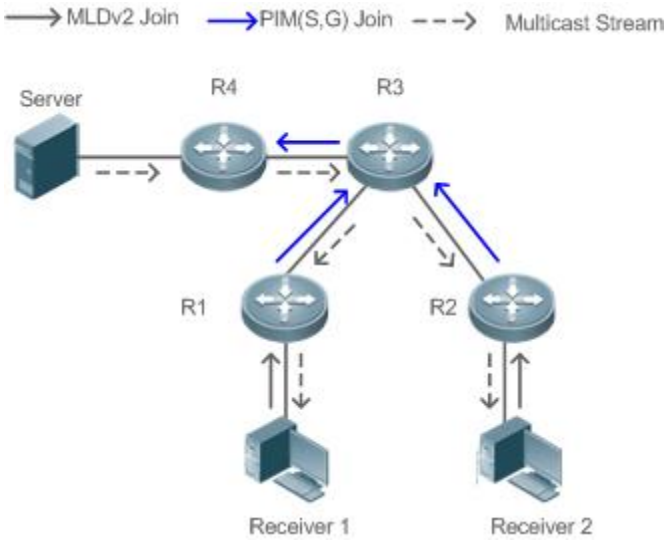

Рисунок 7-5.

Для реализации модели SSM необходимо выполнение следующих условий:

- Приемник multicast заранее узнает информацию об источнике multicast (S,G) посредством некоторых каналов. Приемник multicast инициирует пакет MLD(S,G) Join к желаемому сервису multicast.
- MLDv2 должен быть включен на интерфейсе устройства последнего hop-а, подключенного к приемнику multicast. MLDv1 не поддерживает SSM.
- PIM-SM и SSM должны быть включены на промежуточных устройствах между приемником multicast и источником multicast.

ПРИМЕЧАНИЕ: после включения функции SSM диапазон групп SSM по умолчанию — FF3x::/32. Вы можете запустить команду, чтобы изменить групповой диапазон SSM.

Модель SSM имеет следующие особенности:

- В модели SSM приемник multicast может заранее узнать информацию об источнике multicast посредством некоторых каналов (например, получая объявления или обращаясь к указанному серверу).
- Модель SSM представляет собой определенное подмножество PIM-SM и обрабатывает только сообщения PIM(S,G) Join и PIM(S,G) Prune. Он отбрасывает сообщения, относящиеся к RPT, в пределах диапазона SSM, например сообщения PIM(*,G) Join/Prune. Для пакетов Register в диапазоне SSM он немедленно отвечает пакетом Register-Stop.
- В модели SSM не требуется RP, а также не требуется выбор и распространение сообщений RP. Установленным MDT является SPT в SSM.

7.4. Конфигурация

7.4.1. Настройка основных функций PIM-SMv6

7.4.1.1. Эффект конфигурации

- Создайте сеть PIM для предоставления услуги multicast IPv6 для источников данных и пользовательских терминалов в сети.
- Могут поддерживаться обе или одна из двух моделей обслуживания multicast (ASM и SSM).

7.4.1.2. Примечания

- PIM-SMv6 должен использовать функцию unicast-маршрутизации IPv6.
- Если сеть PIM должна поддерживать multicast-сервис модели SSM, необходимо настроить MLDv3 или сопоставление SSM.

7.4.1.3. Шаги настройки

Включение функции multicast-маршрутизации IPv6

- Обязательный.
- Функция multicast-маршрутизации IPv6 должна быть включена на каждом маршрутизаторе, если не указано иное.

Включение функции PIM-SMv6

- Обязательный.
- Функцию PIM-SMv6 следует включить на следующих интерфейсах, если не указано иное: интерфейсы соединения маршрутизаторов, интерфейс, который работает как статический RP, C-RP или C-BSR, интерфейс для подключения к источнику multicast и интерфейс для подключения к пользовательскому хосту.

Включение пассивного режима PIM-SMv6

- В сети PIM, если интерфейсу необходимо получать только пакеты multicast-данных и ему не требуется участвовать в установлении топологии сети PIM, интерфейс можно настроить для работы в пассивном режиме PIM-SMv6.
- Функция пассивного режима PIM-SMv6 должна быть включена на следующих интерфейсах, если не указано иное: интерфейс для подключения тупикового сетевого устройства к пользовательскому хосту. После настройки пассивного режима PIM-SMv6 этот интерфейс не передает и не принимает пакеты PIM.

Настройка RP

- Если сеть PIM должна поддерживать сервис multicast модели ASM, необходимо настроить RP.
- Существует три метода настройки RP: настройка только статической RP, настройка только динамической RP и настройка статической и динамической RP. Если настроены как статическая RP, так и динамическая RP, динамическая RP является предпочтительной.
- Настройка статической RP: Статическая RP должна быть настроен на каждом маршрутизаторе, если не указано иное.
- Настройка динамической RP. C-RP или C-BSR следует настроить на одном или нескольких маршрутизаторах, если не указано иное.

Включение SSM

- Если сеть PIM должна поддерживать сервис multicast модели SSM, SSM должен быть включен.
- SSM должен быть включен на каждом маршрутизаторе, если не указано иное.

7.4.1.4. Проверка

Сделайте, чтобы источник multicast в сети отправлял пакеты группам в пределах диапазона ASM и SSM, и хост пользователя присоединился к группам.

- Проверьте, может ли хост пользователя успешно получать пакеты из каждой группы.
- Проверьте, созданы ли на маршрутизаторах правильные записи маршрутизации PIM-SMv6.

7.4.1.5. Связанные команды

Включение функции multicast-маршрутизации IPv6

Команда	**ipv6 multicast-routing**
Командный режим	Режим глобальной конфигурации

Включение функции PIM-SMv6

Команда	**ipv6 pim sparse-mode**
Командный режим	Режим настройки интерфейса
Руководство по использованию	Прежде чем включать функцию PIM-SMv6, включите функцию пересылки multicast-маршрутизации в режиме глобальной конфигурации. В противном случае пакеты multicast-данных не могут быть перенаправлены, даже если функция PIM-SMv6 включена. Когда функция PIM-SMv6 включена, MLD автоматически включается на каждом интерфейсе без ручной настройки. Если во время настройки этой команды отображается сообщение «Failed to enable PIM-SMv6 on <interface name>, resource temporarily unavailable, please try again» («Не удалось включить PIM-SMv6 на < interface name>, ресурс временно недоступен, повторите попытку»), попробуйте настроить эту команду еще раз. Если появилось сообщение «PIM-SMv6 Configure failed! VIF limit exceeded in NSM!!!» («Ошибка настройки PIM-SMv6! Превышен лимит VIF в NSM!!!») отображается во время настройки этой команды, настроенное количество multicast-интерфейсов достигает верхнего предела multicast-интерфейсов, которые можно настроить на устройстве. Если функцию PIM-SMv6 по-прежнему необходимо включить на интерфейсе, удалите некоторые ненужные интерфейсы PIM-SMv6 или PIM-DMv6.

	Если интерфейс имеет туннельный тип, только туннель конфигурации 6Over4, туннель конфигурации 6Over4 GRE, туннель конфигурации 6Over6 и туннель 6Over6 GRE поддерживают функцию multicast IPv6. Функцию multicast также можно включить на туннельных интерфейсах, которые не поддерживают функцию multicast, но при этом запросы не отображаются, а multicast-пакеты не принимаются и не передаются. Multicast-туннели могут быть установлены только на портах Ethernet. Встроенные туннели и QoS/ACL для multicast-передачи данных не поддерживаются

Включение функции пассивного режима PIM-SMv6 (PIM-SMv6 PASSIVE)

Команда	**ipv6 pim sparse-mode passive**
Командный режим	Режим настройки интерфейса
Руководство по использованию	Прежде чем включать функцию PIM-SMv6, включите функцию переадресации multicast-маршрутизации в режиме глобальной конфигурации. В противном случае пакеты multicast-данных не могут быть перенаправлены, даже если включена функция пассивного режима PIM-SMv6. Когда функция PIM-SMv6 включена, MLD автоматически включается на каждом интерфейсе без ручной настройки. Интерфейсы с функцией пассивного режима PIM-SMv6 не принимают и не передают пакеты PIM, но могут пересылать multicast-пакеты. Таким образом, режим пассивного режима PIM-SMv6 обычно настраивается на интерфейсе тупикового сетевого устройства, подключенного к пользовательскому хосту, чтобы предотвратить флудинг пакетов Hello PIM уровня 2

Настройка статического RP

Команда	**ipv6 pim rp-address** *ipv6_rp-address* [*ipv6_access-list*]
Описание параметра	*ipv6_rp-address*: указывает IPv6-адрес RP. *ipv6_access-list*: ссылается на список ACL IPv6 для ограничения диапазона адресов группы, обслуживаемого статическим RP. Поддерживается именованный ACL
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Можно настроить статические multicast RP. Статическая RP и C-RP могут сосуществовать. Примечания: 1. Если и механизм BSR, и статическая конфигурация RP эффективны, динамическая конфигурация предпочтительна. 2. Список управления можно использовать для статической настройки адреса RP для нескольких групп multicast (с использованием ACL) или всех групп multicast (без использования ACL), но один статический адрес RP нельзя использовать несколько раз. 3. Если одну и ту же группу обслуживают несколько статических RP, предпочтительно использовать статический RP с большим адресом IPv6. 4. Действуют только multicast-группы с адресами, разрешенными ACL. По умолчанию разрешены все multicast-группы. 5. После завершения настройки статический адрес источника RP будет вставлен в древовидную структуру статической группы RP на основе диапазона групп. Статическая группа multicast в каждом диапазоне групп поддерживает структуру связанного списка одной статической группы RP. Этот связанный список упорядочен по убыванию IPv6-адресов. Если для группового диапазона выбран RP, будет выбран RP с наибольшим адресом IPv6. 6. При удалении статического адреса RP этот адрес удаляется из всех существующих групп, а в качестве адреса RP выбирается адрес из существующей статической древовидной структуры RP

Настройка C-RP

Команда	**ipv6 pim rp-candidate** *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *ipv6_access-list*]
Описание параметра	*interface-type interface-number*: указывает имя интерфейса. Этот адрес интерфейса используется как адрес C-RP. **priority** *priority-value*: определяет приоритет C-RP. Значение варьируется от 0 до 255, значение по умолчанию — 192. **interval** *interval-seconds*: указывает интервал передачи сообщений C-RP в BSR, в секундах. Значение варьируется от 1 до 16 383, значение по умолчанию — 60. **group-list** *ipv6_access-list*: ссылается на список ACL IPv6 для ограничения диапазона адресов группы, обслуживаемого C-RP. Поддерживается именованный ACL
Командный режим	Режим глобальной конфигурации
Руководство по использованию	В протоколе PIM-SMv6 RPT, созданный с помощью multicast-маршрутизации, использует RP в качестве root-узла. После выбора BSR все C-RP периодически передают сообщения C-RP в BSR

	в unicast-режиме, а затем BSR распределяет сообщения по всему домену PIM. Чтобы указать интерфейс в качестве C-RP определенного диапазона группы, включите в эту команду параметр ACL. Обратите внимание, что расчет группового диапазона основан только на разрешенных записях управления доступом (ACE), а запрещенные записи ACE в расчете не участвуют. Если в команде не указан **group-list** *ipv6_access-list*, обслуживаются все группы

Настройка C-BSR

Команда	**ipv6 pim bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority-value*]]
Описание параметра	*interface-type interface-number*: указывает имя интерфейса. Этот адрес интерфейса используется как адрес C-BSR. *hash-mask-length*: указывает длину хэш-маски. Значение варьируется от 0 до 128, значение по умолчанию — 126. *priority-value*: указывает приоритет. Значение варьируется от 0 до 255, значение по умолчанию — 64
Командный режим	Режим глобальной конфигурации
Руководство по использованию	В домене PIM-SMv6 должен существовать уникальный BSR. BSR собирает и публикует информацию о RP. Уникальный известный BSR выбирается из нескольких C-BSR посредством BSM. Все C-BSR считают, что они являются BSR, прежде чем узнают информацию о BSR. Они периодически передают BSM, содержащие адрес BSR и приоритет в домене PIM-SMv6. Эту команду можно использовать, чтобы позволить устройству передавать один BSM всем соседям PIM, используя выделенный адрес BSR. Каждый сосед сравнивает адрес источника BSR с адресом в полученном BSM. Если адрес IPv6 в полученном BSM равен или больше его адреса BSR, сосед сохраняет этот адрес как адрес BSR и пересылает BSM. В противном случае сосед отбрасывает BSM. Текущее устройство считает, что это BSR, пока не получит BSM от другого C-BSR и не узнает, что C-BSR имеет более высокий приоритет (или тот же приоритет, но больший IPv6-адрес)

Включение SSM

Команда	**ipv6 pim ssm** { **default** | **range** *ipv6_access-list* }
Описание параметра	**default**: диапазон адресов группы SSM по умолчанию — FF3x::/32.

	range *ipv6_access-list*: ссылается на список ACL IPv6 для ограничения диапазона адресов группы SSM. Поддерживается именованный ACL
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Чтобы применить SSM в сети PIM-SMv6, необходимо настроить эту команду

Отображение таблицы маршрутизации PIM-SM

Команда	**show ipv6 pim sparse-mode mroute** [*group-or-source-address* [*group-or-source-address*]]
Описание параметра	*group-or-source-address*: указывает адрес группы или адрес источника. Два адреса не могут быть одновременно групповыми адресами или адресами источника
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации и режим конфигурации интерфейса
Руководство по использованию	Каждый раз можно указывать адрес группы, адрес источника или адрес группы и адрес источника. Вы также не можете указать конкретный групповой адрес или адрес источника, но вы не можете указать два групповых адреса или два адреса источника одновременно

7.4.1.6. Пример конфигурации

Создание сервиса multicast IPv6 в сети IPv6 для поддержки ASM и SSM

Сценарий:

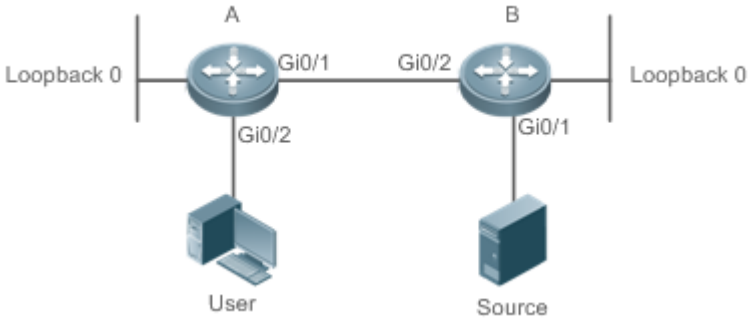

Рисунок 7-6.

Шаги настройки	• Настройте протокол unicast-маршрутизации IPv6 (например, OSPFv6) на маршрутизаторах и убедитесь, что unicast-маршруты loopback-интерфейсов доступны. (пропущено) • Включите функцию multicast-маршрутизации IPv6 на всех маршрутизаторах.

	• Включите функцию PIM-SMv6 на интерфейсах соединения устройств, интерфейсе подключения к пользовательскому хосту и интерфейсе подключения к источнику multicast. • Настройте C-RP и C-BSR на loopback-интерфейсах маршрутизатора A и маршрутизатора B. Включите функцию PIM-SMv6 на loopback-интерфейсах. • Включите SSM на всех маршрутизаторах. • Включите MLDv3 на интерфейсе маршрутизатора для подключения к пользовательскому хосту. (пропущено)
A	switch(config)#ipv6 multicast-routing switch(config)#ipv6 pim ssm default switch(config)#int gi 0/2 switch(config-if-GigabitEthernet 0/2)#ipv6 add 2000::2/64 switch(config-if-GigabitEthernet 0/2)#ipv6 pim sparse-mode switch(config-if-GigabitEthernet 0/2)#exit switch(config)#int gi 0/1 switch(config-if-GigabitEthernet 0/1)#ipv6 add 1000::1/64 switch(config-if-GigabitEthernet 0/1)#ipv6 pim sparse-mode switch(config-if-GigabitEthernet 0/1)#exit switch(config)#int Loopback 0 switch(config-if-Loopback 0)#ipv6 add 3000::5/64 switch(config-if-Loopback 0)#ipv6 pim sparse-mode switch(config-if-Loopback 0)#exit switch(config)#ipv6 pim rp-candidate Loopback 0
B	QTECH(config)#ipv6 multicast-routing QTECH(config)#ipv6 pim ssm default QTECH(config)#int gi 0/2 QTECH(config-if-GigabitEthernet 0/2)#ipv6 add 2000::1/64 QTECH(config-if-GigabitEthernet 0/2)#ipv6 pim sparse-mode QTECH(config-if-GigabitEthernet 0/2)#exit QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)#ipv6 add 1100::1/64 QTECH(config-if-GigabitEthernet 0/1)#ipv6 pim sparse-mode QTECH(config-if-GigabitEthernet 0/1)#exit QTECH(config)#int Loopback 0 QTECH(config-if-Loopback 0)#ipv6 add 5000::5/64 QTECH(config-if-Loopback 0)#ipv6 pim sparse-mode

	QTECH(config-if-Loopback 0)#exit QTECH(config)#ipv6 pim bsr-candidate Loopback 0
Проверка	Сделайте, чтобы источник (2000::2/64) отправлял пакеты на G1(ff16::1) и пользователь присоединился к G1. • Проверьте multicast-пакеты, полученные Пользователем. Пользователь должен иметь возможность получать multicast-пакеты от G1. • Проверьте таблицы маршрутизации PIM-SMv6 на маршрутизаторах A и B. В таблицах маршрутизации PIM-SMv6 должны присутствовать записи
A	switch(config)# show ipv6 pim sparse-mode mroute IPv6 Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 0 (*, ff16::1) RP: 3000::5 RPF nbr: :: RPF idx: None Upstream State: JOINED 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . . i . . . . . . 1 . . . . . . Joined 0 . . . . . . 1 . . . . . . Asserted 0 . . . . . . 1 . . . . . . FCR:

(1100::2, ff16::1)
RPF nbr: fe80::21a:a9ff:fe3a:6355
RPF idx: GigabitEthernet 0/2
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 44 seconds
kat expires in 194 seconds
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0 . . . . . .
1 . . . . . .
Joined
0 . . . . . .
1 . . . . . .
Asserted
0 . . . . . .
1 . . . . . .
Outgoing
0 . . o . . . . . .
1 . . . . . .

(1100::2, ff16::1, rpt)
RP: 3000::5
RPF nbr: ::
RPF idx: None
Upstream State: PRUNED
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31
Local
0 . . . . . .
1 . . . . . .
Pruned
0 . . . . . .
1 . . . . . .

	Outgoing 0 . . o . . . . . . 1 . . . . .
B	QTECH#show ipv6 pim sparse-mode mroute IPv6 Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 0 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 1 (1100::2, ff16::1) RPF nbr: :: RPF idx: None SPT bit: 1 Upstream State: JOINED kat expires in 20 seconds 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . . . . . . Joined 0 . j . . . . . . Asserted 0 . . . . . . Outgoing 0 . o . . . . . . (1100::2, ff16::1, rpt) RP: 3000::5 RPF nbr: fe80::2d0:f8ff:fe22:341b RPF idx: GigabitEthernet 0/2 Upstream State: RPT NOT JOINED 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27

	28 29 30 31 Local 0 . . . . . . Pruned 0 . . . . . . Outgoing 0 . . . . .

7.4.1.7. Распространенные ошибки

- Unicast-маршрутизация IPv6 настроена неправильно.
- На маршрутизаторе не включена multicast-маршрутизация IPv6.
- SSM не включен на маршрутизаторе, или диапазон адресов группы SSM маршрутизатора отличается от диапазона других маршрутизаторов.
- PIM-SMv6 не включен на интерфейсе (например, интерфейсе, указанном как C-RP или C-BSR, или интерфейсе, который функционирует как шлюз пользовательского хоста или источника multicast).
- MLDv3 не включен на интерфейсе, подключенном к пользовательскому хосту.
- В сети не настроен RP.
- На маршрутизаторе не настроен статический RP или настроенный статический RP отличается от такового на других маршрутизаторах.
- C-RP настроен, но в сети не настроен C-BSR.
- Unicast-маршрут к статическому RP, C-RP или C-BSR недоступен.

7.4.2. Настройка параметров соседа PIM

7.4.2.1. Эффект конфигурации

- Согласуйте параметры протокола и настройте параметры в пакете Hello.
- PIM-маршрутизаторы обнаруживают соседей, согласовывают параметры протокола и поддерживают отношения соседства.
- Защитите соседские отношения, чтобы ограничить соседей.

7.4.2.2. Примечания

Необходимо настроить основные функции PIM-SMv6.

7.4.2.3. Шаги настройки

Установите параметры на каждом интерфейсе маршрутизатора PIM, если не указано иное.

7.4.2.4. Проверка

Задайте параметры в пакете Hello на интерфейсе и запустите команду **debug ipv6 pim sparse-mode packet**, чтобы проверить параметры в пакете Hello.

Установите фильтрацию соседей и запустите команду **show ipv6 pim sparse-mode neighbor**, чтобы проверить отношения соседей.

7.4.2.5. Связанные команды

Настройка интервала передачи сообщений Hello

Команда	**ipv6 pim query-interval** *seconds*
Описание параметра	*seconds:* указывает интервал передачи пакетов Hello. Единица измерения — секунды. Значение варьируется от 1 до 65 535, значение по умолчанию — 30
Командный режим	Режим настройки интерфейса
Руководство по использованию	Каждый раз, когда интервал передачи сообщений Hello обновляется, время Holdtime сообщений Hello соответственно обновляется в соответствии со следующим правилом: Время Holdtime сообщений Hello обновляется до 3,5-кратного интервала передачи сообщений Hello. Если интервал передачи сообщений Hello, умноженный на 3,5, превышает 65 535, интервал передачи сообщений Hello принудительно обновляется до 18 725

Настройка задержки Propagation Delay сообщений Hello

Команда	**Ipv6 pim propagation-delay** *milliseconds*
Описание параметра	*milliseconds*: единица измерения — миллисекунды. Значение варьируется от 1 до 32 767, значение по умолчанию — 500
Командный режим	Режим настройки интерфейса
Руководство по использованию	Изменение propagation delay или задержки prune override повлияет на интервал J/P-override-interval. Согласно протоколу, интервал J/P-override-interval должен быть меньше времени Holdtime пакетов Join-Prune. В противном случае произойдет кратковременное прерывание потока. Это должно поддерживаться и гарантироваться сетевыми администраторами

Настройка интервала Prune Override для сообщений Hello

Команда	**ipv6 pim override-interval** *milliseconds*
Описание параметра	*milliseconds*: единица измерения — миллисекунды. Значение варьируется от 1 до 65 535, значение по умолчанию — 2500
Командный режим	Режим настройки интерфейса

Руководство по использованию	Изменение propagation delay или задержки prune override повлияет на интервал J/P-override-interval. Согласно протоколу, интервал J/P-override-interval должен быть меньше времени Holdtime пакетов Join-Prune. В противном случае произойдет кратковременное прерывание потока

Настройка возможности подавления присоединения интерфейса для сообщений Hello

Команда	**ipv6 pim neighbor-tracking**
Командный режим	Режим настройки интерфейса
Руководство по использованию	Когда функция подавления присоединения интерфейса включена и локальному маршрутизатору необходимо передать пакет Join upstream-соседу, пакет Join локального маршрутизатора подавляется и не передается, если локальный маршрутизатор получает пакет Join от соседа к upstream-маршрутизатору. Если функция подавления присоединения интерфейса отключена, локальный маршрутизатор передает пакет Join. Когда возможность подавления присоединения downstream-приемника отключена, upstream-сосед может точно узнать количество приемников, подключенных к downstream-соседу, через полученный пакет Join, тем самым реализуя отслеживание соседей

Настройка задержки отправки сообщений Hello

Команда	**Ipv6 pim triggered-hello-delay** *seconds*
Описание параметра	*seconds*: единица измерения — секунды. Значение варьируется от 1 до 5, значение по умолчанию — 5
Командный режим	Режим настройки интерфейса
Руководство по использованию	Когда интерфейс включен или обнаруживает нового соседа, сообщение Triggered-Hello-Delay используется для генерации случайного периода времени. В течение этого периода времени интерфейс отправляет пакеты Hello

Настройка приоритета DR для сообщений Hello

Команда	**Ipv6 pim dr-priority** *priority-value*
Описание параметра	*priority-value*: указывает приоритет. Большее значение означает более высокий приоритет. Значение находится в диапазоне от 0 до 4 294 967 294, значение по умолчанию — 1

Командный режим	Режим настройки интерфейса
Руководство по использованию	Процесс выбора DR выглядит следующим образом: Параметр приоритета устанавливается для пакетов Hello устройств в одной локальной сети. Приоритет сравнивается для выбора DR. Устройство с более высоким приоритетом становится DR. Если несколько устройств имеют один и тот же приоритет, устройство с большим IP-адресом является DR. Если параметр приоритета не установлен для пакетов Hello устройства в локальной сети, устройство с большим IP-адресом выбирается в качестве DR в локальной сети

Настройка фильтрации соседей

Команда	**ipv6 pim neighbor-filter** *ipv6_access-list*
Описание параметра	*ipv6_access-list*: ссылается на список ACL IPv6 для ограничения диапазона адресов соседей
Командный режим	Режим настройки интерфейса
Руководство по использованию	Эту команду можно использовать для фильтрации соседей, чтобы повысить безопасность сети PIM и ограничить диапазон адресов допустимых соседей. Если сосед отклонен ACL, PIM-SMv6 не будет устанавливать peering-отношения с этим соседом или приостанавливать peering-отношения с этим соседом

Отображение информации о соседях интерфейса

Команда	**show ipv6 pim sparse-mode neighbor** [**detail**]
Описание параметра	**detail**: отображает подробно детали
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации и режим конфигурации интерфейса

7.4.2.6. Пример конфигурации

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Установите интервал передачи пакетов Hello PIM-SMv6 на 50 секунд. • Установите задержку propagation delay пакетов Hello PIM-SMv6 на 400 миллисекунд.

	• Установите интервал prune override пакетов Hello PIM-SMv6 на 3000 миллисекунд. • Настройте возможность подавления присоединения интерфейса для сообщений Hello PIM-SMv6. • Установите задержку отправки сообщений Hello для PIM-SMv6 на 3 секунды. • Установите приоритет DR сообщений Hello PIM-SMv6 на 5
	switch # configure terminal switch (config)#int gi 0/1 switch (config-if-GigabitEthernet 0/1)#ipv6 pim query-interval 50 switch (config-if-GigabitEthernet 0/1)#ipv6 pim propagation-delay 400 switch (config-if-GigabitEthernet 0/1)#ipv6 pim override-interval 3000 switch (config-if-GigabitEthernet 0/1)#ipv6 pim triggered-hello-delay 3 switch (config-if-GigabitEthernet 0/1)# ipv6 pim dr-priority 5
Проверка	Запустите команду **debug ipv6 pim sparse-mode packet**, чтобы проверить параметры в пакете Hello
	switch # debug ipv6 pim sparse-mode packet *Jan 2 02:37:55: %7: Hello send to GigabitEthernet 0/2 *Jan 2 02:37:55: %7: Send Hello message *Jan 2 02:37:55: %7: Holdtime: 175 *Jan 2 02:37:55: %7: T-bit: off *Jan 2 02:37:55: %7: Propagation delay: 400 *Jan 2 02:37:55: %7: Override interval: 3000 *Jan 2 02:37:55: %7: DR priority: 5 *Jan 2 02:37:55: %7: Gen ID: 99572792 *Jan 2 02:37:55: %7: Secondary Addresses: *Jan 2 02:37:55: %7: 2000::2
Шаги настройки	Настройте фильтрацию соседей на интерфейсе для получения пакетов соседей с адресом (8000::1/64)
	switch(config-if-GigabitEthernet 0/2)#ipv6 pim neighbor-filter acl % access-list acl not exist switch(config-if-GigabitEthernet 0/2)#exit switch(config)#ipv6 access-list acl switch(config-ipv6-acl)#permit ipv6 8000::1/64 any

Проверка	Прежде чем настраивать фильтрацию соседей, отобразите информацию о соседях
	switch#show ipv6 pim sparse-mode neighbor Neighbor Address Interface Uptime/Expires DR Pri/Mode fe80::21a:a9ff:fe3a:6355 GigabitEthernet 0/2 00:32:29/00:01:16 1 /
Проверка	После настройки фильтрации соседей информация о соседях пуста
	switch#show ipv6 pim sparse-mode neighbor

7.4.2.7. Распространенные ошибки

Основные функции PIM-SMv6 не настроены или не могут быть настроены.

7.4.3. Настройка параметров BSR

7.4.3.1. Эффект конфигурации

Ограничьте диапазон действия BSM.

7.4.3.2. Примечания

- Необходимо настроить основные функции PIM-SMv6.
- Необходимо настроить C-RP и C-BSR.
- Граница должна быть настроена на интерфейсе между доменами.

7.4.3.3. Шаги настройки

Настройка границы

- Граница должна быть настроена, если имеется несколько доменов.
- Настройте границу интерфейса между двумя доменами.

Настройка маршрутизатора PIM для ограничения BSM

- Опционально.
- Эту настройку можно выполнить на маршрутизаторе PIM, если не указано иное.

Настройка C-BSR для ограничения диапазона C-PR

- Опционально.
- Эту конфигурацию можно выполнить на всех C-BSR, если не указано иное.

Настройка C-BSR для приема пакетов C-RP-ADV с счетчиком префиксов, равным 0

- Опционально.
- Эту конфигурацию можно выполнить на всех C-BSR, если не указано иное.

7.4.3.4. Проверка

Проверка границы

Включите базовые функции PIM-SMv6, настройте два маршрутизатора в разных доменах и настройте маршрутизатор B как C-BSR. Маршрутизатор A обычно может получать BSM.

Установите общую границу между маршрутизаторами A и B в качестве граничного интерфейса. Маршрутизатор A не может получать BSM.

Проверка маршрутизатора PIM для ограничения BSM

Включите базовые функции PIM-SMv6 и настройте маршрутизатор B как C-BSR. Маршрутизатор A обычно может получать BSM. Ограничьте диапазон C-BSR на маршрутизаторе A. Маршрутизатор A не может принимать BSM.

Проверка C-BSR для ограничения диапазона C-PR

Включите базовые функции PIM-SMv6, установите маршрутизатор B как C-BSR, установите маршрутизатор A как C-RP и ограничьте диапазон C-RP на C-BSR. Маршрутизатор B не может получать пакеты от C-RP.

7.4.3.5. Связанные команды

Настройка границы BSR

Команда	**ipv6 pim bsr-border**
Командный режим	Режим настройки интерфейса
Руководство по использованию	Границу BSR можно настроить на интерфейсе, чтобы ограничить флудинг BSM. Когда этот интерфейс получает BSM, он немедленно отбрасывает их, и BSM не пересылаются этим интерфейсом

Настройка маршрутизатора PIM для ограничения BSM

Команда	**ipv6 pim accept-bsr list** *ipv6_access-list*
Описание параметра	**list** *ipv6_access-list*: ссылается на список ACL IPv6 для ограничения диапазона адресов BSR. Поддерживается именованный ACL
Командный режим	Режим глобальной конфигурации

Настройка C-BSR для ограничения диапазона C-PR

Команда	**ipv6 pim accept-crp list** *ipv6_access-list*
Описание параметра	**list** *ipv6_access-list*: ссылается на список ACL IPv6 для ограничения диапазона адресов C-RP и диапазона адресов группы, обслуживаемых C-RP. Поддерживается именованный ACL
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Настройте эту команду на C-BSR. Когда этот C-BSR выбран в качестве BSR, он может ограничить диапазон адресов действующего C-RP и диапазон групп multicast, обслуживаемых C-RP

Отображение BSM

Команда	**show ipv6 pim sparse-mode bsr-router**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации и режим конфигурации интерфейса

Отображение всех RP, настроенных на локальном устройстве, и групп multicast, обслуживаемых этими RP.

Команда	**show ipv6 pim sparse-mode rp mapping**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации и режим конфигурации интерфейса

7.4.3.6. Пример конфигурации

Настройка границы BSR

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Настройте границу BSR на соединительном интерфейсе между маршрутизаторами B и A
	QTECH(config-if-GigabitEthernet 0/2)#ipv6 pim bsr-border
Проверка	До настройки границы BSR информация BSM маршрутизатора A отображается следующим образом:
	switch#show ipv6 pim sparse-mode bsr-router PIMv2 Bootstrap information BSR address: 5000::5 Uptime: 00:05:42, BSR Priority: 64, Hash mask length: 126 Expires: 00:01:28 Role: Non-candidate BSR Priority: 0, Hash mask length: 126 State: Accept Preferred Candidate RP: 3000::5(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:24 switch#
	ПРИМЕЧАНИЕ: кандидат RP: указывает все C-RP, настроенные на локальном маршрутизаторе, за исключением других маршрутизаторов

	После настройки границы BSR информация BSM маршрутизатора A отображается следующим образом:
	switch#show ipv6 pim sparse-mode bsr-router Candidate RP: 3000::5(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:53

Настройка маршрутизатора PIM для ограничения диапазона исходных адресов BSM до (8000::5/64)

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Настройте маршрутизатор PIM A для ограничения BSM. Ограниченный диапазон адресов источника — (8000::5/64)
	switch(config)#ipv6 access-list acl switch(config-ipv6-acl)#permit ipv6 8000::5/64 any switch(config-ipv6-acl)#exit switch(config)#ipv6 pim accept-crp list acl
Проверка	До настройки ограничения BSM информация BSM маршрутизатора A отображается следующим образом:
	switch#show ipv6 pim sparse-mode bsr-router PIMv2 Bootstrap information BSR address: 5000::5 Uptime: 00:05:42, BSR Priority: 64, Hash mask length: 126 Expires: 00:01:28 Role: Non-candidate BSR Priority: 0, Hash mask length: 126 State: Accept Preferred Candidate RP: 3000::5(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:24 switch#
	После настройки ограничения BSM информация BSM маршрутизатора A отображается следующим образом:

	switch#show ipv6 pim sparse-mode bsr-router Candidate RP: 3000::5(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:34

Настройка C-BSR для ограничения диапазона исходных адресов пакетов C-PR до (9000::5/64)

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Настройте маршрутизатор B для ограничения пакетов C-RP. Ограниченный диапазон адресов источника — (9000::5/64)
	QTECH(config)#ipv6 access-list acl QTECH(config-ipv6-acl)#permit ipv6 9000::5/64 any QTECH(config-ipv6-acl)#exit QTECH(config)#ipv6 pim accept-crp list acl
Проверка	До настройки фильтрации пакетов C-RP информация обо всех группах RP на маршрутизаторе B отображается следующим образом:
	QTECH#show ipv6 pim sparse-mode rp mapping PIM Group-to-RP Mappings This system is the Bootstrap Router (v2) Group(s): ff00::/8 RP: 3000::5(Not self) Info source: 3000::5, via bootstrap, priority 192 Uptime: 00:02:26, expires: 00:02:08 QTECH#
	После настройки фильтрации пакетов C-RP информация обо всех группах RP на маршрутизаторе B отображается следующим образом:
	QTECH#show ipv6 pim sparse-mode rp mapping PIM Group-to-RP Mappings This system is the Bootstrap Router (v2)

Настройка статической RP первой

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Установите адрес интерфейса Loopback0 маршрутизатора A на 3000::5. (пропущено) • Установите адрес интерфейса Loopback1 маршрутизатора A равным 4000::5. (пропущено) • Установите статический адрес маршрутизатора A на 3300::5. (пропущено) • Установите статический адрес маршрутизатора B на 3300::5. • Настройте статический RP первым на маршрутизаторе A
	switch(config)#ipv6 pim rp-address 3300::5 switch(config)#ipv6 pim static-rp-preferred
Проверка	Прежде чем настроить статический RP первым, отобразите информацию о RP, соответствующем FF16::1
	switch#show ipv6 pim sparse-mode rp ff16::1 RP: 4000::5 Info source: 5000::5, via bootstrap PIMv2 Hash Value 126 RP 4000::5, via bootstrap, priority 56, hash value 892666309 RP 3000::5, via bootstrap, priority 200, hash value 1161101765 RP 3300::5, static (hash value 204800453 not used)
Проверка	После настройки статического RP первым отобразите информацию о RP, соответствующем FF16::1
	switch(config)#show ipv6 pim sparse-mode rp ff16::1 RP: 3300::5 (Static) PIMv2 STATIC RP PREFERRED PIMv2 Hash Value 126 RP 4000::5, via bootstrap, priority 56, hash value 892666309 RP 3000::5, via bootstrap, priority 200, hash value 1161101765 RP 3300::5, static (hash value 204800453 not used) switch(config)#

7.4.3.7. Распространенные ошибки

- Основные функции PIM-SMv6 не настроены или не могут быть настроены.
- C-BSR не настроен.
- Граница BSR не настроена на интерфейсе между разными доменами.

7.4.4. Настройка параметров RP и DR

7.4.4.1. Эффект конфигурации

- Настройте игнорирование приоритета C-RP для повторного выбора RP.
- Настройте DR на стороне источника данных, чтобы определить доступность RP.
- Ограничьте адрес группы multicast (S,G) источника данных, чтобы модель ASM предоставляла сервис multicast только для пакетов multicast в пределах допустимого диапазона.
- Настройте ограничение скорости для DR на стороне источника данных для передачи пакетов Register.
- Настройте длину контрольной суммы пакетов Register.
- Настройте адрес источника пакетов Register.
- Настройте время подавления пакетов Register.
- Настройте время проверки пустых пакетов.
- Настройте TTL пакетов Register, полученных RP с адреса группы multicast (S,G).
- Сначала настройте статический RP.

7.4.4.2. Примечания

Необходимо настроить основные функции PIM-SMv6.

7.4.4.3. Шаги настройки

Настройка игнорирования приоритета C-RP для повторного выбора RP

- Опционально.
- Игнорирование приоритета C-RP можно включить на каждом маршрутизаторе, если не указано иное.

Настройка DR на стороне источника данных для определения доступности RP

- Опционально.
- Обнаружение доступности можно включить на DR, который напрямую подключен к источнику данных, если не указано иное.

Ограничение диапазона адресов (S,G) пакетов Register на стороне источника данных

- Опционально.
- Диапазон адресов (S,G) пакетов Register на стороне источника данных может быть ограничен на всех маршрутизаторах, которые функционируют как C-RP или статические RP, если не указано иное.

Ограничение скорости DR на стороне источника данных для передачи пакетов Register

- Опционально.

- Ограничение скорости передачи пакетов Register может быть включено на DR, который напрямую подключен к источнику данных, если не указано иное.

Настройка длины контрольной суммы пакетов Register

- Опционально.
- Длина контрольной суммы пакетов Register может быть настроена на всех C-RP или статических RP, если не указано иное.

Настройка исходного адреса пакетов Register

- Опционально.
- Адрес источника пакетов Register можно настроить на DR, который напрямую подключен к источнику данных, если не указано иное.

Настройка времени подавления пакетов Register

- Опционально.
- Время подавления пакетов Register можно настроить на DR, который напрямую подключен к источнику данных, если не указано иное.

Настройка времени проверки пустых пакетов

- Опционально.
- Время проверки пустых пакетов можно настроить на DR, который напрямую подключен к источнику данных, если не указано иное.

Настройка TTL пакетов Register, полученных RP с адреса multicast-группы (S,G)

- Опционально.
- TTL пакетов Register из адреса группы multicast (S,G) можно настроить на всех маршрутизаторах, которые функционируют как C-RP или статические RP, если не указано иное.

Настройка статического RP первым

- Опционально.
- Статический RP можно настроить первым на всех маршрутизаторах, если не указано иное.

7.4.4.4. Проверка

Проверка игнорирования приоритета C-RP

Установите адрес 3000::5 и приоритет 200 для интерфейса Loopback0 на маршрутизаторе A. Установите адрес 4000: : 5 и приоритет 56 для интерфейса Loopback1 на маршрутизаторе A. Установите адрес C-BSR на 5000: : 5 на Маршрутизатор B.

- Запустите команду **show ipv6 pim sparse-mode rp** ff16::2, чтобы отобразить информацию о RP, который обслуживает текущую группу.

Проверка DR на стороне источника данных для определения доступности RP

Установите адрес 3000::5 и приоритет 200 для интерфейса Loopback0 на маршрутизаторе A. Установите адрес 4000: : 5 и приоритет 56 для интерфейса Loopback1 на маршрутизаторе A. Установите адрес C-BSR на 5000: : 5 на Маршрутизатор B. Настройте обнаружение доступности RP на маршрутизаторе B.

- Запустите команду **show running-config**, чтобы проверить, настроено ли обнаружение доступности RP.

Проверка ограничения диапазона адресов (S,G) пакетов Register на стороне источника данных

Установите адрес 3000::5 и приоритет 200 для интерфейса Loopback0 на маршрутизаторе A. Установите адрес 4000: : 5 и приоритет 56 для интерфейса Loopback1 на маршрутизаторе A. Установите адрес C-BSR на 5000: : 5 на Маршрутизатор B. Адрес multicast-группы — FF16::2. Настройте маршрутизатор A на получение пакетов только от источника multicast с адресом источника (1300::1/64).

- Запустите команду **show ip pim sparse-mode mroute**, чтобы отобразить записи (S,G).

Проверка ограничения скорости для DR на стороне источника данных для передачи пакетов Register

Установите скорость передачи пакетов Register для маршрутизатора B, а затем запустите команду **show ip pim sparsemode track**, чтобы проверить количество переданных пакетов Register для подтверждения.

Проверка длины контрольной суммы пакетов Register

Настройте маршрутизатор A на проверку пакета Register на основе всего пакета, а не только на основе заголовка пакета и заголовка пакета Register. Запустите команду **show running-config**, чтобы проверить конфигурацию.

Проверка исходного адреса пакетов Register

Настройте адрес источника пакетов Register на маршрутизаторе B и запустите команду **show running-config**, чтобы проверить конфигурацию на маршрутизаторе A.

Проверка времени подавления и времени проверки пакетов Register

Настройте время подавления и время проверки пакетов Register на маршрутизаторе B и запустите команду **show running-config**, чтобы проверить конфигурацию.

Проверка TTL пакетов Register, полученных RP от адреса multicast-группы (S,G)

Настройте TTL пакетов Register из адреса multicast-группы (S,G) на маршрутизаторе A и запустите команду **show ip pim sparse-mode mroute**, чтобы отобразить максимальный TTL (S,G).

Проверьте статический RP первым

Настройте статический RP и C-RP на маршрутизаторе A, сначала настройте статический RP, а затем запустите команду **show ipv6 pim sparse-mode rp** ff16::2, чтобы отобразить информацию о текущем RP.

7.4.4.5. Связанные команды

Игнорирование приоритета C-RP

Команда	**ipv6 pim ignore-rp-set-priority**
Командный режим	Режим глобальной конфигурации

Отображение информации о RP, обслуживающем группу

Команда	**show ipv6 pim sparse-mode rp-hash** *group-address*
Описание параметра	*group-address*: указывает адрес спарсенной группы
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации и режим конфигурации интерфейса

Настройка DR, напрямую подключенного к источнику данных, для определения доступности RP

Команда	**ipv6 pim register-rp-reachability**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После настройки этой команды доступность RP определяется до передачи пакетов Register. Если RP доступен, передаются пакеты Register. Если RP недоступен, пакеты Register не передаются

Ограничение диапазона адресов (S,G) пакетов Register на стороне источника данных

Команда	**ipv6 pim accept-register** { **list** *ipv6_access-list* [**route-map** *map-name*] | **route-map** *map-name* [**list** *ipv6_access-list*] }
Описание параметра	**list** *ipv6_access-list*: ссылается на расширенный список ACL IP для ограничения диапазона адресов (S,G). Диапазон значений: 100–199, 2000–2699 и имя. **route-map** *map-name*: использует карту маршрутов для ограничения диапазона адресов (S,G)
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После настройки этой команды при получении пакета Register от неавторизованного источника RP немедленно возвращает пакет Register-Stop

Отображение записей multicast-маршрутизации

Команда	**show ipv6 pim sparse-mode mroute** [*group-or-source-address* [*group-or-source-address*]]
Описание параметра	*group-or-source-address*: указывает адрес группы или адрес источника. Два адреса не могут быть одновременно адресами группы или адресами источника

Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации и режим конфигурации интерфейса
Руководство по использованию	Каждый раз можно указывать групповой адрес, адрес источника или оба адреса. Вы также не можете указать конкретный групповой адрес или адрес источника, но вы не можете указать два групповых адреса или два адреса источника одновременно

Настройка ограничения скорости для DR для передачи пакетов Register

Команда	**ipv6 pim register-rate-limit** *rate*
Описание параметра	*rate*: указывает количество пакетов Register, которые разрешено передавать в секунду. Значение варьируется от 1 до 65 535
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для настройки скорости передачи пакетов Register с адреса multicast-группы (S,G), а не пакетов Register всей системы. После настройки этой команды нагрузка на исходные DR и RP будет разгружена и будут передаваться пакеты Register, скорость которых не превышает лимит

Отображение статистики по пакетам PIM

Команда	**show ipv6 pim sparse-mode track**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации и режим конфигурации интерфейса
Руководство по использованию	При запуске системы сначала устанавливается момент начала статистики. Каждый раз, когда вызывается **clear ip pim sparse-mode track**, момент начала статистики устанавливается снова, а счетчик пакетов PIM очищается

Настройка расчета контрольной суммы пакета Register на основе всего пакета

Команда	**ipv6 pim register-checksum-wholepkt** [**group-list** *ipv6_access-list*]
Описание параметра	**group-list** *ipv6_access-list*: использует ACL для ограничения адресов группы, использующих эту конфигурацию. access-list: поддерживает цифры <1,99> и <1300,1999>. Поддерживается именованный ACL
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Устройство вычисляет контрольную сумму пакета Register на основе всего пакета протокола PIM, включая инкапсулированный пакет multicast-данных, а не на основе заголовка PIM пакета Register. Если в этой команде не указан **group-list** *ipv6_access-list*, эта конфигурация применяется ко всем групповым адресам

Настройка адреса источника пакетов Register

Команда	**ipv6 pim register-source** { *ipv6_local_address* | *interface-type interface-number* }
Описание параметра	*ipv6_local_address*: указывает адрес IPv6 в качестве адреса источника для пакетов Register. *interface-type interface-number*: указывает IPv6-адрес интерфейса в качестве адреса источника пакетов Register
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Настроенный адрес должен быть доступен. Когда RP получает пакет Register, он передает пакет Register-Stop с IPv6-адресом источника пакета Register в качестве адреса назначения. PIM-SMv6 не требуется включать на связанных интерфейсах

Настройка времени подавления пакетов Register

Команда	**ipv6 pim register-suppression** *seconds*
Описание параметра	*seconds*: указывает время подавления пакетов Register. Единица измерения — секунды. Значение варьируется от 1 до 65 535, значение по умолчанию — 60
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Настройка этого значения на DR изменит время подавления пакетов Register, определенных на DR. Если команда **ipv6 pim rp-register-kat** не настроена, настройка этого значения на RP изменит время keepalive RP

Настройка времени проверки пакетов Register

Команда	**ipv6 pim probe-interval** *seconds*
Описание параметра	*seconds*: указывает время проверки пакетов Register. Единица измерения — секунды. Значение варьируется от 1 до 65 535, значение по умолчанию — 5

Командный режим	Режим глобальной конфигурации
Руководство по использованию	Время проверки пакетов Register — это интервал, в течение которого DR источника передает пустой пакет Register на RP до истечения времени подавления пакетов Register. Время проверки пакетов Register не может превышать половину времени подавления пакетов Register. В противном случае произойдет сбой настройки и появится предупреждение. Кроме того, время подавления пакетов Register, умноженное на три, плюс время проверки пакетов Register, не может превышать 65 535. В противном случае будет отображено предупреждение

Настройка интервала KAT на RP

Команда	**Ipv6 pim rp-register-kat** *seconds*
Описание параметра	*seconds*: указывает время таймера KAT. Единица измерения — секунды. Значение находится в диапазоне от 1 до 65 535, значение по умолчанию — 210
Командный режим	Режим глобальной конфигурации

Настройка статической RP первой

Команда	**ipv6 pim static-rp-preferred**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После настройки этой команды приоритет статической RP выше, чем у RP, выбранной с помощью механизма BSR

7.4.4.6. Пример конфигурации

Настройка того, учитывается ли приоритет C-RP при сопоставлении группы с RP (Group-to-RP)

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Установите адрес 3000::5 и приоритет 200 для интерфейса Loopback0 на маршрутизаторе A. (Пропущено) • Установите адрес 4000: : 5 и приоритет 56 для интерфейса Loopback1 на маршрутизаторе A. (Пропущено) • Установите адрес C-BSR на 5000: : 5 на маршрутизаторе B. (Пропущено) • Отобразите группу, соответствующую FF16::1.

	• Настройте игнорирование приоритета C-RP на маршрутизаторе B
	switch#configure terminal QTECH(config)# ipv6 pim ignore-rp-set-priority
Проверка	Прежде чем будет настроено игнорирование приоритета C-RP, отображается следующая информация:
	switch(config)#show ipv6 pim sparse-mode rp FF16::1 RP: 4000::5 Info source: 5000::5, via bootstrap PIMv2 Hash Value 126 RP 4000::5, via bootstrap, priority 56, hash value 892666309 RP 3000::5, via bootstrap, priority 200, hash value 1161101765
	После настройки игнорирования приоритета C-RP отображается следующая информация:
	switch(config)#show ipv6 pim sparse-mode rp FF16::1 RP: 3000::5 Info source: 5000::5, via bootstrap

Настройка обнаружения доступности RP, напрямую подключенной к источнику данных

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Настройте обнаружение доступности RP, напрямую подключенной к источнику данных
	QTECH(config)#ipv6 pim register-rp-reachability
Проверка	Запустите команду **show running-config**, чтобы проверить конфигурацию. Отображается следующая информация:
	QTECH(config)#show running-config ! ! ! ipv6 pim register-rp-reachability ipv6 pim bsr-candidate Loopback 0 !

	!

Ограничение диапазона адресов (S,G) пакетов Register на стороне источника данных

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Настройте маршрутизатор A на фильтрацию пакетов по адресу источника и прием пакетов только с адреса источника (1300::1/64)
	switch(config)#ipv6 pim accept-register list acl % access-list 101 not exist switch(config)#ipv6 access-list acl switch(config-ipv6-acl)#permit ipv6 1300::1/64 any switch(config-ipv6-acl)#exit
Проверка	Прежде чем диапазон адресов (S,G) для пакетов Register на стороне источника данных будет ограничен, запустите команду **show ipv6 pim sparse-mode mroute**, чтобы отобразить записи multicast. Запись (S,G) и запись (S,G,RPT) существуют
	switch#show ipv6 pim sparse-mode mroute IPv6 Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 0 (*, ff16::1) RP: 4000::5 RPF nbr: :: RPF idx: None Upstream State: JOINED 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . . . i . . . . . . 1 . . . . .

	Joined 0 . . . . . . 1 . . . . . . Asserted 0 . . . . . . 1 . . . . . . FCR: (1100::2, ff16::1) RPF nbr: fe80::21a:a9ff:fe3a:6355 RPF idx: GigabitEthernet 0/2 SPT bit: 1 Upstream State: JOINED jt_timer expires in 36 seconds kat expires in 191 seconds 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local
	После ограничения диапазона адресов (S,G) для пакетов Register на стороне источника данных запустите команду **show ipv6 pim sparse-mode mroute**, чтобы отобразить записи multicast. Запись (S,G) и запись (S,G,RPT) существуют
	switch#show ipv6 pim sparse-mode mroute IPv6 Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 0 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 0 (*, ff16::1) RP: 4000::5 RPF nbr: :: RPF idx: None

	Upstream State: JOINED 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . . . i . . . . . . 1 . . . . . . Joined 0 . . . . . . 1 . . . . . . Asserted 0 . . . . . . 1 . . . . . . FCR: (1100::2, ff16::1, rpt) RP: 4000::5 RPF nbr: :: RPF idx: None Upstream State: PRUNED 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . . . . . .

Ограничение скорости DR на стороне источника данных для передачи пакетов Register

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Проверьте количество пакетов PIM, переданных маршрутизатором B. • Через секунду проверьте количество пакетов PIM, переданных маршрутизатором B. • Установите скорость передачи пакетов Register для маршрутизатора B. • Через секунду проверьте количество пакетов PIM, переданных маршрутизатором B
	QTECH(config)#ipv6 pim register-rate-limit 1

Проверка	Прежде чем настраивать ограничение скорости, проверьте количество пакетов PIM, переданных DR. Отображается следующая информация:
	QTECH#show ipv6 pim sparse-mode track PIMv6 packet counters track Elapsed time since counters cleared: 17:14:54 received sent Valid PIMv6 packets: 5064 7727 Hello: 1329 4057 Join-Prune: 863 0 Register: 0 2636 Register-Stop: 975 0 Assert: 0 0 BSM: 0 1034 C-RP-ADV: 1897 0 PIMDM-Graft: 0 PIMDM-Graft-Ack: 0 PIMDM-State-Refresh: 0 Unknown PIM Type: 0 Errors: Malformed packets: 0 Bad checksums: 0 Send errors: 5 Packets received with unknown PIM version: 0
	Прежде чем настраивать ограничение скорости, проверьте количество пакетов PIM, переданных DR, через секунду. Отображается следующая информация:
	QTECH#show ipv6 pim sparse-mode track PIMv6 packet counters track Elapsed time since counters cleared: 17:14:55 received sent Valid PIMv6 packets: 5064 7727 Hello: 1335 4063 Join-Prune: 866 0 Register: 0 2639

	Register-Stop: 978 0 Assert: 0 0 BSM: 0 1035 C-RP-ADV: 1897 0 PIMDM-Graft: 0 PIMDM-Graft-Ack: 0 PIMDM-State-Refresh: 0 Unknown PIM Type: 0 Errors: Malformed packets: 0 Bad checksums: 0 Send errors: 5 Packets received with unknown PIM version: 0
	После настройки ограничения скорости проверьте количество пакетов PIM, переданных DR. Отображается следующая информация:
	QTECH#show ipv6 pim sparse-mode track PIMv6 packet counters track Elapsed time since counters cleared: 17:14:56 received sent Valid PIMv6 packets: 5064 7727 Hello: 1341 4069 Join-Prune: 869 0 Register: 0 2640 Register-Stop: 979 0 Assert: 0 0 BSM: 0 1036 C-RP-ADV: 1897 0 PIMDM-Graft: 0 PIMDM-Graft-Ack: 0 PIMDM-State-Refresh: 0 Unknown PIM Type: 0 Errors: Malformed packets: 0

	Bad checksums: 0 Send errors: 5 Packets received with unknown PIM version: 0

Настройка длины контрольной суммы пакетов Register

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Настройте расчет контрольной суммы пакета Register на основе всего пакета на маршрутизаторе A. • Запустите команду **show running-config**, чтобы проверить конфигурацию
	switch(config)#ipv6 pim register-checksum-wholepkt switch(config)#show running-config
Проверка	Проверьте конфигурацию маршрутизатора A. Конфигурация отображается следующим образом:
	! ! ipv6 pim register-checksum-wholepkt ipv6 pim rp-candidate Loopback 0 priority 200 ipv6 pim rp-candidate Loopback 1 priority 56 ipv6 pim ssm default ! !

Настройка адреса источника пакетов Register

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Установите адрес источника интерфейса Loopback1 на 5500::5/64 на маршрутизаторе B. (Пропущено) • Установите адрес источника пакетов Register на адрес интерфейса Loopback2 на маршрутизаторе B. (Пропущено) • Запустите команду **show running-config**, чтобы проверить конфигурацию
	QTECH(config)#ipv6 pim register-source Loopback 1
Проверка	Проверьте конфигурацию маршрутизатора B
	! !

	ipv6 pim register-source Loopback 1 ipv6 pim register-rate-limit 1 ipv6 pim bsr-candidate Loopback 0 !

Настройка времени подавления и времени проверки пакетов Register

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Установите время подавления на 20 секунд на маршрутизаторе B. • Установите время проверки на 2 секунды на маршрутизаторе B. • Запустите команду **show running-config**, чтобы проверить конфигурацию
	QTECH(config)#ipv6 pim register-suppression 20 QTECH(config)#ipv6 pim probe-interval 2 QTECH(config)# show ip pim sparse-mode track
Проверка	Проверьте конфигурацию маршрутизатора B
	! ipv6 pim register-source Loopback 1 ipv6 pim register-rate-limit 1 ipv6 pim register-suppression 20 ipv6 pim probe-interval 2 ipv6 pim bsr-candidate Loopback 0 ! !

Настройка TTL пакетов Register, полученных RP с адреса multicast-группы (S,G)

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Установите TTL пакетов Register, полученных маршрутизатором A от адреса группы multicast (S,G), равным 60 секундам. • Запустите команду **show ip pim sparse-mode mroute**, чтобы проверить количество пакетов Register
	QTECH(config)#ip pim rp-register-kat 60
Проверка	После настройки TTL проверьте TTL пакетов Register с адреса группы multicast (S,G) на маршрутизаторе A. TTL не превышает 60 секунд
	switch(config)#show ipv6 pim sparse-mode mroute

```
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
REG Entries: 0

(1100::2, ff16::1)
RPF nbr: fe80::21a:a9ff:fe3a:6355
RPF idx: GigabitEthernet 0/2
SPT bit: 0
Upstream State: NOT JOINED
kat expires in 60 seconds
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
27 28 29 30 31
Local
0 . . . . . .
1 . . . . . .
Joined
0 . . . . . .
1 . . . . . .
Asserted
0 . . . . . .
1 . . . . . .
Outgoing
0 . . . . . .
1 . . . . . .

(1100::2, ff16::1, rpt)
RP: 4000::5
RPF nbr: ::
RPF idx: None
```

7.4.4.7. Распространенные ошибки

- Основные функции PIM-SMv6 не настроены или не могут быть настроены.

- Диапазон адресов (S,G) пакетов Register на стороне источника данных не ограничен или не может быть настроен на C-RP или статической RP.
- Если диапазон адресов (S,G) пакетов Register на стороне источника данных ограничен, указанный список ACL не настроен или диапазон адресов источника/группы, разрешенный ACL, настроен неправильно.
- Диапазоны адресов источника/группы, разрешенные C-RP или статическими RP, несовместимы.

7.4.5. Настройка интервала передачи пакетов Join/Prune

7.4.5.1. Эффект конфигурации

Измените интервал передачи пакетов Join/Prune, чтобы сформировать RPT или SPT.

7.4.5.2. Примечания

Необходимо настроить основные функции PIM-SMv6.

7.4.5.3. Шаги настройки

Настройте интервал передачи пакетов Join/Prune.

7.4.5.4. Проверка

Установите интервал передачи пакетов Join/Prune на 120 секунд на маршрутизаторе B. Запустите команду **show ipv6 pim sparse-mode mroute**, чтобы проверить значение TTL записи.

7.4.5.5. Связанные команды

Настройка интервала передачи пакетов Join/Prune

Команда	**ipv6 pim jp-timer** *seconds*
Описание параметра	*seconds*: указывает интервал передачи пакетов Join/Prune. Единица измерения — секунды. Значение варьируется от 1 до 65 535, значение по умолчанию — 60
Командный режим	Режим глобальной конфигурации

7.4.5.6. Пример конфигурации

Настройка интервала передачи пакетов Join/Prune на маршрутизаторе

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Настройте интервал передачи пакетов Join/Prune на маршрутизаторе
	QTECH(config)#ip pim jp-timer 120
Проверка	Запустите команду **show ipv6 pim sparse-mode mroute**, чтобы проверить запись. Время передачи пакетов Join/Prune не превышает 120

```
switch(config)#show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
REG Entries: 0

(*, ff16::1)
RP: 4000::5
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
27 28 29 30 31
Local
0 . . . i . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Joined
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
FCR:

(1100::2, ff16::1)
RPF nbr: fe80::21a:a9ff:fe3a:6355
RPF idx: GigabitEthernet 0/2
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 116 seconds
kat expires in 59 seconds
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
```

	27 28 29 30 31 Local 0 . . . . .

7.4.5.7. Распространенные ошибки

Основные функции PIM-SMv6 не настроены или не могут быть настроены.

7.4.6. Настройка устройства Last-Hop для переключения с RPT на SPT

7.4.6.1. Эффект конфигурации

Переключите устройство Last-Hop с RPT на SPT.

7.4.6.2. Примечания

Необходимо настроить основные функции PIM-SMv6.

7.4.6.3. Шаги настройки

Настройте устройство Last-Hop для переключения с RPT на SPT.

7.4.6.4. Проверка

Настройте базовые функции PIM-SMv6, сделайте, чтобы DR на стороне источника данных передавал потоки данных в группу FF16::1, и приемник принудительно присоединился к группе FF16::1 для формирования RPT. DR на принимающей стороне принудительно выполняет переключение с RPT на SPT. Проверьте конфигурацию RP.

7.4.6.5. Связанные команды

Включение функции коммутации SPT

Команда	**ipv6 pim spt-threshold** [**group-list** *ipv6_access-list*]
Описание параметра	**group-list** *ipv6_access-list*: ссылается на список ACL IPv6 для ограничения диапазона адресов группы, позволяющего коммутацию SPT. ipv6_access-list: поддерживается именованный ACL
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если в этой команде не указан параметр **group-list** *ipv6_access-list*, всем multicast-группам разрешено осуществлять коммутацию SPT
	Если в этой команде установлено значение **no**, переносится список групп, а переносимый список ACL является настроенным ACL, ограничение ACL, связанное со списком групп, отменяется, и всем группам разрешается переключаться с RPT на SPT

7.4.6.6. Пример конфигурации

Настройка устройства Last-Hop для переключения с RPT на SPT

Шаги настройки	• Настройте базовые функции PIM-SMv6. (пропущено) • Сделайте, чтобы DR на стороне источника данных передавал кодовые потоки в группу FF16::1. • Сделайте, чтобы DR на принимающей стороне получал потоки кода из группы FF16::1. • Настройте устройство Last-Hop для переключения с RPT на SPT на DR на принимающей стороне
	switch(config)#ipv6 pim spt-threshold
Проверка	Запустите команду **show running-config**, чтобы проверить конфигурацию
	switch(config)#show running-config ! ! ip pim jp-timer 120 ip pim spt-threshold ip pim rp-candidate Loopback 0 ! !

7.5. Мониторинг

7.5.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере важной информации и, таким образом, к прерыванию работы служб.

Описание	Команда
Очищает информацию о динамической RP	**clear ipv6 pim sparse-mode bsr rp-set ***
Снова устанавливает время начала статистики пакетов и очищает счетчик пакетов PIMv6	**clear ipv6 pim sparse-mode track**

7.5.2. Отображение

Описание	Команда
Отображает подробную информацию о BSR	**show ipv6 pim sparse-mode bsr-router**
Отображает информацию PIM-SM об интерфейсе	**show ipv6 pim sparse-mode interface** [*interface-type interface-number*] [**detail**]
Отображает локальную информацию MLD об интерфейсе PIM-SMv6	**show ipv6 pim sparse-mode local-members** [*interface-type interface-number*]
Отображает информацию о маршрутизации PIM-SMv6	**show ipv6 pim sparse-mode mroute** [*group-or-source-address* [*group-or-source-address*]]
Отображает информацию о соседе PIM-SMv6	**show ipv6 pim sparse-mode neighbor** [**detail**]
Отображает информацию, относящуюся к следующему hop-у, включая идентификатор интерфейса следующего hop-а, адрес и метрику	**show ipv6 pim sparse-mode nexthop**
Отображает все RP, настроенные на локальном устройстве, и группы, обслуживаемые этими RP	**show ipv6 pim sparse-mode rp mapping**
Отображает информацию о RP, обслуживающей групповой адрес	**show ipv6 pim sparse-mode rp-hash** *ipv6-group-address*
Отображает количество переданных и полученных пакетов PIM с момента начала статистики до текущего времени	**show ipv6 pim sparse-mode track**

8. НАСТРОЙКА MSDP

8.1. Обзор

Протокол обнаружения источника multicast используется для подключения нескольких rendezvous point (RP) в сети и совместного использования информации об источнике multicast между этими RP.

- Используйте MSDP между несколькими доменами Protocol Independent Multicast - Sparse-Mode (PIM-SM), чтобы совместно использовать информацию об источнике multicast этих доменов PIM-SM для реализации междоменной multicast.
- Используйте MSDP в домене PIM-SM для совместного использования информации об источнике multicast нескольких RP для реализации Anycast-RP.

8.1.1. Протоколы и стандарты

- RFC3618: Multicast Source Discovery Protocol (MSDP).

8.2. Приложения

Приложение	Описание
Междоменный multicast	Подключает несколько AS, делится ресурсами multicast между автономными системами (AS) и предоставляет услуги multicast между AS
Anycast-RP	Делится информацией об источнике multicast между несколькими RP в одной AS

8.2.1. Междоменный multicast

8.2.1.1. Сценарий

Подключите несколько AS, запустите PPIM-SM внутри AS и установите peer-отношения MSDP между RP разных AS.

Как показано на Рисунке 8-1, DR 1 подключен к регистрам источника multicast с RP 1 в локальном домене. DR 2, подключенный к хосту-участнику группы, запускает Join к RP 2 в локальном домене. RP 1 использует сообщение SA для уведомления RP 2 об источнике multicast. RP 2 продолжает инициировать присоединение (Join) с источником multicast для построения Multicast Distribution Tree (MDT).

Междоменный multicast позволяет хостам-участникам группы применять multicast-потоки через AS.

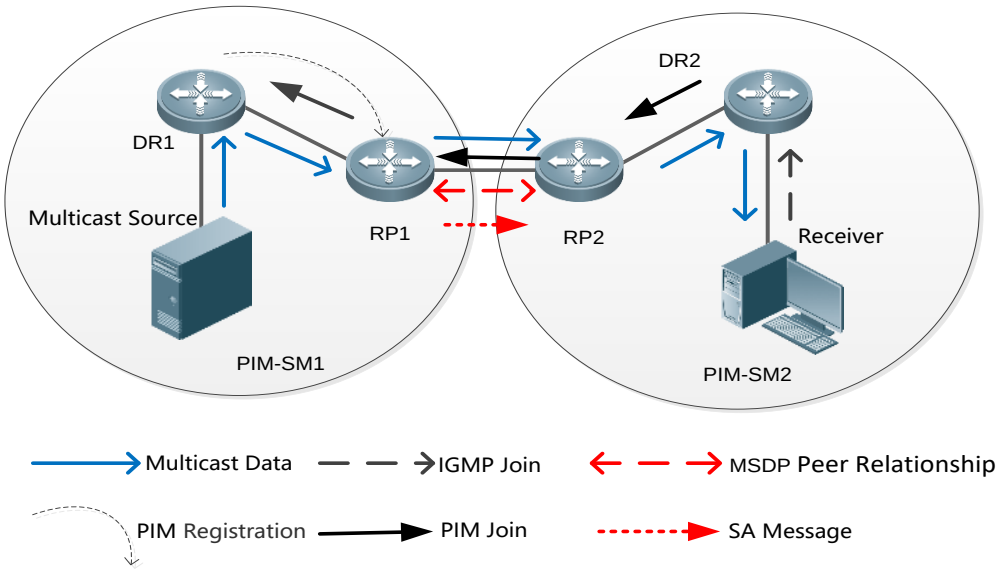

Рисунок 8-1.

8.2.1.2. Развертывание

- Запустите Open Shortest Path First (OSPF) в каждой AS и запустите протокол Border Gateway (BGP) между AS для реализации междоменной unicast-рассылки.
- Запустите PIM-SM внутри каждой AS и запустите MSDP между AS для реализации междоменного multicast.

8.2.2. Anycast-RP

8.2.2.1. Сценарий

PIM-SM работает внутри каждой AS. Существует несколько RP, которые используют один и тот же адрес RP и обслуживают одну и ту же группу. Между этими RP устанавливаются peer-отношения MSDP.

Как показано на Рисунке 8-2, DR 1 подключен к регистрам источника multicast с ближайшим RP 1 в локальном домене. DR 2, подключенный к хосту-участнику группы, запускает присоединение с ближайшим RP 2. RP 1 использует сообщение SA для уведомления RP 2 об источнике multicast. RP 2 продолжает инициировать присоединение с источником multicast для создания MDT.

Anycast-RP обеспечивает резервирование и балансировку нагрузки для RP, а также помогает ускорить конвергенцию multicast-маршрутов.

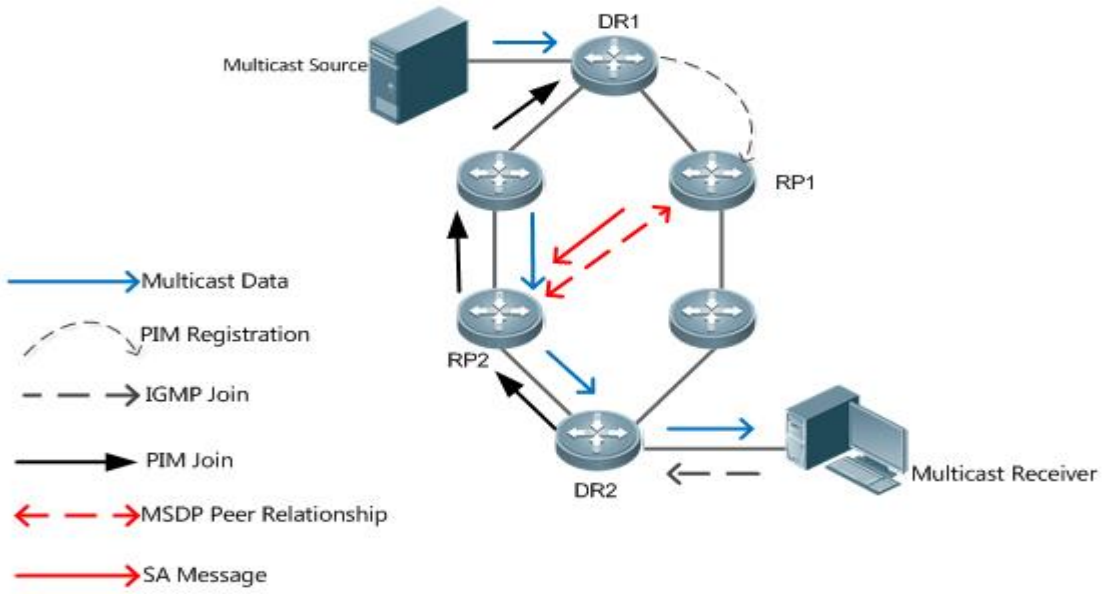

Рисунок 8-2.

8.2.2.2. Развертывание

- Запустите OSPF в каждой AS, чтобы реализовать unicast-передачу внутри домена (intra-domain unicast).
- Запустите PIM-SM в каждой AS для реализации внутридоменного multicast.
- Запустите MSDP между RP, чтобы поделиться информацией об источнике multicast.

8.3. Функции

Функция	Описание
Установление peer-отношений MSDP	Подключите несколько RP для совместного использования информации об источнике multicast
Получение и пересылка сообщений SA	Предотвратите переполнение SA и подавите штормы SA

8.3.1. Установление peer-отношений MSDP

8.3.1.1. Принцип работы

Настройте одну или несколько пар peer-узлов MDSP в сети для подключения RP, тем самым уведомляя другие RP об информации об источнике multicast на RP.

Используйте TCP-соединение между peer-ами MDSP через порт 639. Если доступен unicast-маршрут, можно установить peer-отношения MSDP.

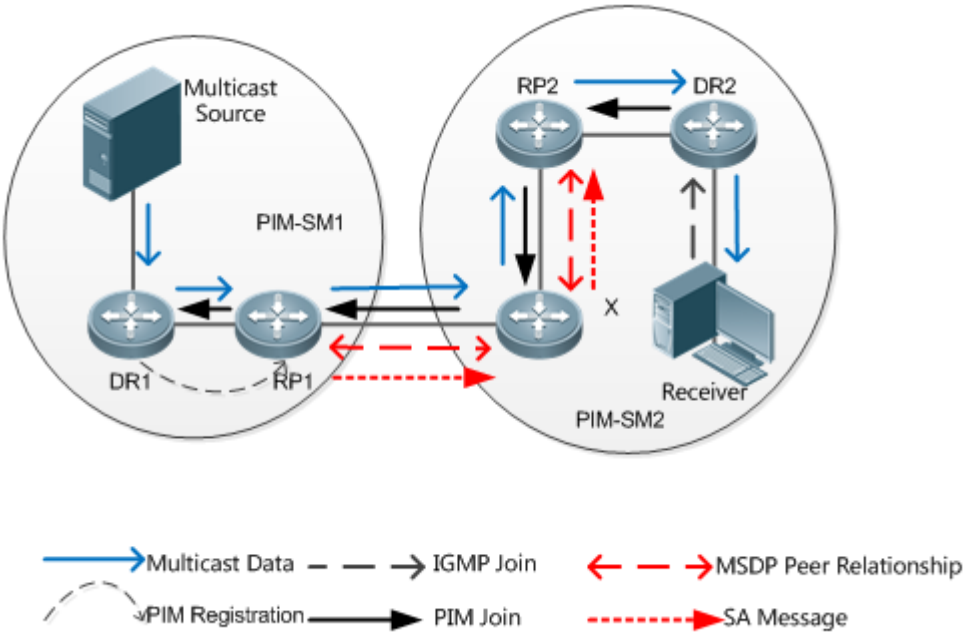

Рисунок 8-3.

RP подключен к источнику multicast

Настройте peer-узел MSDP на RP, подключенном к источнику multicast. Затем этот RP может использовать сообщения SA для отправки информации о локальном источнике multicast другим RP.

Как показано на Рисунке 8-3 DR 1 регистрирует информацию об источнике multicast с помощью RP 1. Когда между RP 1 и RP 2 устанавливаются peer-отношения, RP 1 отправляет информацию об источнике multicast в X.

Пересылка сообщений SA

Non-RP также могут выступать в качестве peer-узлов MSDP, но пересылают только сообщения SA.

Как показано на Рисунке 8-3, X пересылает сообщения SA, отправленные с RP 1 на RP 2. Таким образом, информация об источнике multicast передается на RP 2.

RP подключен к приемнику multicast

Настройте peer-узел MSDP на RP, подключенном к приемнику multicast. Затем этот RP может инициировать присоединение к источнику multicast на основе полученного сообщения SA.

Как показано на Рисунке 8-3, DR 2 запускает соединение с RP 2. Поскольку RP 2 уже получает информацию об источнике multicast, RP 2 продолжает инициировать присоединение с источником multicast, тем самым устанавливая MDT от DR 1 к DR 2.

8.3.2. Получение и пересылка сообщений SA

8.3.2.1. Принцип работы

Сообщение SA содержит адрес источника multicast, адрес группы multicast и адрес RP. Адрес RP — это IP-адрес RP, под которым зарегистрирован источник multicast.

- RP инкапсулирует локально зарегистрированную информацию об источнике multicast в сообщении SA и отправляет сообщение всем своим peer-ам MSDP.

- При получении сообщения SA каждый peer MSDP выполняет проверку Peer-RPF, сравнивает SA-Cache и сопоставляет сообщение SA с правилами фильтрации входящего и исходящего трафика SA. Если сообщение SA проходит проверку Peer-RPF, не существует в SA-Cache SA и соответствует правилам исходящей фильтрации, это сообщение SA пересылается другим peer-ам MSDP.

ПРИМЕЧАНИЕ: сообщения запроса SA и ответа SA также используются между peer-ами MSDP для передачи исходной информации конкретной группы.

Проверка Peer-RPF

Любое сообщение SA, поступающее от peer-а MSDP (адрес: N), будет проверено следующим образом:

ПРИМЕЧАНИЕ: оцените, проходит ли сообщение SA проверку Peer-RPF, в следующей последовательности. Как только сообщение SA пройдет проверку Peer-RPF, примите сообщение SA; в противном случае отбросьте сообщение SA.

1. Если N является членом mesh-группы, сообщение SA проходит проверку Peer-RPF; в противном случае перейдите к шагу 2.
2. Если N является единственным активным peer-ом MSDP на локальном устройстве, сообщение SA проходит проверку Peer-RPF; в противном случае перейдите к шагу 3.
3. Если N — это адрес RP в сообщении SA, сообщение SA проходит проверку Peer-RPF; в противном случае перейдите к шагу 4.
4. Если на локальном устройстве существует маршрут EBGP к адресу RP в сообщении SA и следующий hop этого маршрута является N, сообщение SA проходит проверку Peer-RPF; в противном случае перейдите к шагу 5.
5. Если на локальном устройстве существует оптимальный маршрут к адресу RP в сообщении SA, проверьте следующее:

- Если этот оптимальный маршрут является маршрутом с вектором расстояния (например, маршрутом BGP/RIP), и этот маршрутизатор объявлен N, сообщение SA проходит проверку Peer-RPF.
- Если этот оптимальный маршрут является маршрутом состояния канала (например, маршрут OSPF/IS-IS), а следующим hop-ом этого маршрутизатора является N, сообщение SA проходит проверку Peer-RPF.
- В противном случае перейдите к шагу 6.

6. Если на локальном устройстве существует оптимальный маршрут к адресу RP в сообщении SA, и этот маршрут является маршрутом MBGP/BGP, извлеките ближайший AS из AS-Path этого маршрута MBGP/BGP. Если локальное устройство имеет несколько peer-узлов MSDP в этой AS и N — peer-узел MSDP с наибольшим IP-адресом или N — единственный peer-узел MSDP в этой AS, сообщение SA проходит проверку Peer-RPF; в противном случае перейдите к шагу 7.
7. Если N является peer-узлом MSDP по умолчанию, сообщение SA проходит проверку Peer-RPF; в противном случае перейдите к шагу 8.
8. Сообщение SA не проходит проверку Peer-RPF.

Проверка Peer-RPF помогает предотвратить образование петель и переполнение SA.

Mesh-группа

В mesh-группе peer-отношения MSDP устанавливаются для каждых двух участников.

- Для сообщений SA, поступающих от объектов за пределами mesh-группы, после прохождения проверки Peer-RPF и сравнения SA-Cache эти сообщения SA пересылаются другим участникам группы.

- Сообщения SA внутри группы больше не пересылаются другим участникам группы.

Mesh-группа помогает уменьшить количество сообщений SA.

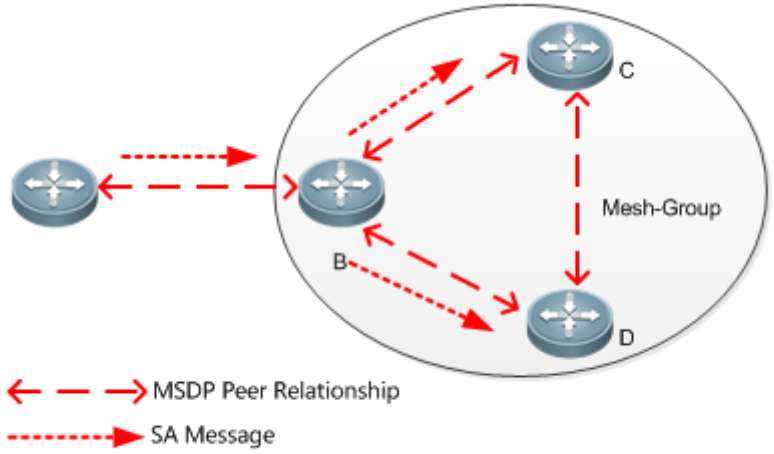

Рисунок 8-4.

SA Cache (Кеш SA)

Кеш SA используется для буферизации статуса сообщения SA. Сообщения SA с истекшим сроком действия будут удалены.

Когда peer-узел MSDP получает сообщение SA, если это сообщение не существует в кеше SA и проходит проверку Peer-RPF, сообщение сохраняется в кеше SA. Если это сообщение уже существует в кеше SA, оно игнорируется. Это помогает подавить штормы SA.

Когда peer-узел MSDP получает сообщение SA, если это сообщение уже существует в кеше SA, на сообщение немедленно отправляется ответ. Это помогает повысить эффективность протокола.

8.4. Конфигурация

Элемент конфигурации	Описание и команда	
Настройка междоменного multicast	Эта конфигурация является обязательной в сценарии междоменного multicast	
	ip msdp peer *peer-address* **connect-source** *interface-type interface-number*	Устанавливает peer-отношения MSDP
Настройка Anycast-RP	Эта конфигурация является обязательной в сценарии Anycast-RP	
	ip msdp peer *peer-address* **connect-source** *interface-type interface-number*	Устанавливает peer-отношения MSDP

Элемент конфигурации	Описание и команда	
Настройка Anycast-RP	**ip msdp originator-id** *interface-type interface-number*	Изменяет адрес RP в сообщении SA
Настройка Green Channel проверки Peer-RPF	Опционально. Он используется для того, чтобы сообщение SA успешно прошло проверку Peer-RPF	
	ip msdp default-peer *peer-address* [**prefix-list** *prefix-list-name*]	Настраивает peer-узел MSDP по умолчанию
	ip msdp mesh-group *mesh-name peer-address*	Настраивает mesh-группу MSDP
Включение мер безопасности	Опционально. Он используется для предотвращения незаконных TCP-соединений и подавления штормов SA	
	ip msdp password peer *peer-address* [*encryption-type*] *string*	Включает шифрование TCP MD5
	ip msdp sa-limit *peer-address sa-limit*	Ограничивает количество сообщений SA в кеше SA
Ограничение broadcast-а сообщений SA	Опционально. Он используется для ограничения выпуска, получения и пересылки сообщений SA	
	ip msdp redistribute [**list** *access-list*] [**route-map** *route-map*]	Фильтрует исходную информацию, распространяемую локально
	ip msdp filter-sa-request *peer-address*[**list** *access-list*]	Фильтрует полученные запросы SA
	ip msdp sa-filter in *peer-address* [**list** *access-list*] [**route–map** *route-map*] [**rp-list** *rp-access-list*] [**rp-route-map** *rp-route-map*]	Фильтрует полученные сообщения SA
	ip msdp sa-filter out *peer-address* [**list** *access-list*] [**route–map** *route-map*] [**rp-list** *rp-access-list*] [**rp-route-map** *rp-route-map*]	Фильтрует отправленные сообщения SA

Элемент конфигурации	Описание и команда	
Управление peer-ами MSDP	Опционально. Он используется для удобного управления peer-отношениями MSDP	
	ip msdp description *peer-address text*	Добавляет описание к peer-у MSDP
	ip msdp shutdown *peer-address*	Отключает peer-узел MSDP
Изменение параметров протокола	Опционально. Не рекомендуется изменять значения параметров протокола по умолчанию	
	ip msdp timer *interval*	Изменяет интервал повторного подключения TCP
	ip msdp ttl-threshold *peer-addressttl-value*	Изменяет значение TTL пакета multicast-данных, содержащегося в сообщении SA

8.4.1. Настройка междоменного multicast

8.4.1.1. Эффект конфигурации

Установите peer-отношения MSDP между несколькими AS, чтобы хосты-участники группы могли принимать multicast-потоки между AS.

8.4.1.2. Примечания

- Unicast-маршрут между AC (inter-AC) должен быть доступен.
- Запустите PIM-SM в каждой AS и настройте границу BSR.

8.4.1.3. Шаги настройки

Установление peer-отношений MSDP

- Обязательный.
- Установите peer-отношения между RP соответствующего домена PIM multicast.
- Установите peer-отношения MSDP между устройствами EBGP разных AS.
- Установите peer-отношения MSDP между RP и устройством EBGP в каждой AS.

Команда	**ip msdp peer** *peer-address* **connect-source** *interface-type interface-number*
Описание параметра	*peer-address*: указывает IP-адрес удаленного peer-а. *interface-type interface-number*: указывает локальный интерфейс, который используется для установления TCP-соединения с удаленным peer-ом
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Peer-отношения являются двунаправленными. Поэтому эту команду необходимо настроить с обеих сторон. IP-адрес и локальный интерфейс peer-а MSDP должны быть такими же, как у peer-а EBGP. Чтобы гарантировать, что сообщения SA могут успешно пройти проверку Peer-RPF, рекомендуется: • Настройте mesh-группу. • Настройте peer-узел MSDP по умолчанию

8.4.1.4. Проверка

Отправьте пакет из источника (S), близкого к RP, в группу (G) и разрешите хосту, расположенному рядом с другим RP, присоединиться к G.

- Убедитесь, что хост может получить пакет (S, G).
- Запустите команду **show ip msdp summary** на RP в другой AS, чтобы отобразить состояние peer-а MSDP.
- Запустите команду **show ip msdp sa-cache** на RP в другой AS, чтобы отобразить полученную информацию об источнике MSDP.

Отображение полученной информации источника MSDP

Команда	**show ip msdp sa-cache**
Командный режим	Привилегированный режим, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если адрес не указан, вся информация (S, G) отображается по умолчанию. Если указан адрес, устройство проверяет, является ли этот адрес адресом unicast или multicast. Если адрес является адресом unicast, этот адрес рассматривается как источник multicast (S), и будет отображаться вся информация (S, G), в которой источником multicast является S. Если адрес является адресом multicast, этот адрес рассматривается как группа multicast (G), и будет отображаться вся информация (S, G), в которой группа multicast имеет значение G. Если

	этот адрес не является ни unicast, ни multicast, информация не отображается. Если указаны два адреса, один адрес рассматривается как источник multicast (S), а другой — как группа multicast (G). Если один адрес является адресом unicast, а другой адрес — адресом группы multicast, никакая информация не отображается
	QTECH# show ip msdp sa-cache MSDP Source-Active Cache: 2 entries (200.200.200.200, 227.1.2.2), RP: 20.20.20.20, (M)BGP/AS 100, 04:17:09/00:02:05, Peer 200.200.200.2 Learned from peer 200.200.200.2, RPF peer 200.200.200.2, SAs received: 277, Encapsulated data received: 0 (200.200.200.200, 227.1.2.3), RP: 20.20.20.20, (M)BGP/AS 100, 04:17:09/00:02:05, Peer 200.200.200.2 Learned from peer 200.200.200.2, RPF peer 200.200.200.2, SAs received: 277, Encapsulated data received: 0

Отображение краткой информации о peer-ах MSDP

Команда	**show ip msdp summary**
Командный режим	Привилегированный режим, режим глобальной конфигурации или режим конфигурации интерфейса
	QTECH# show ip msdp summary Msdp Peer Status Summary Peer Address As State Uptime/Downtime Reset-Count Sa-Count Peer-description 200.200.200.2 100 Up 04:22:11 10 6616 No description 200.200.200.3 100 Down 19:17:13 4 0 peer-A

8.4.1.5. Пример конфигурации

Настройка междоменной multicast

Сценарий:

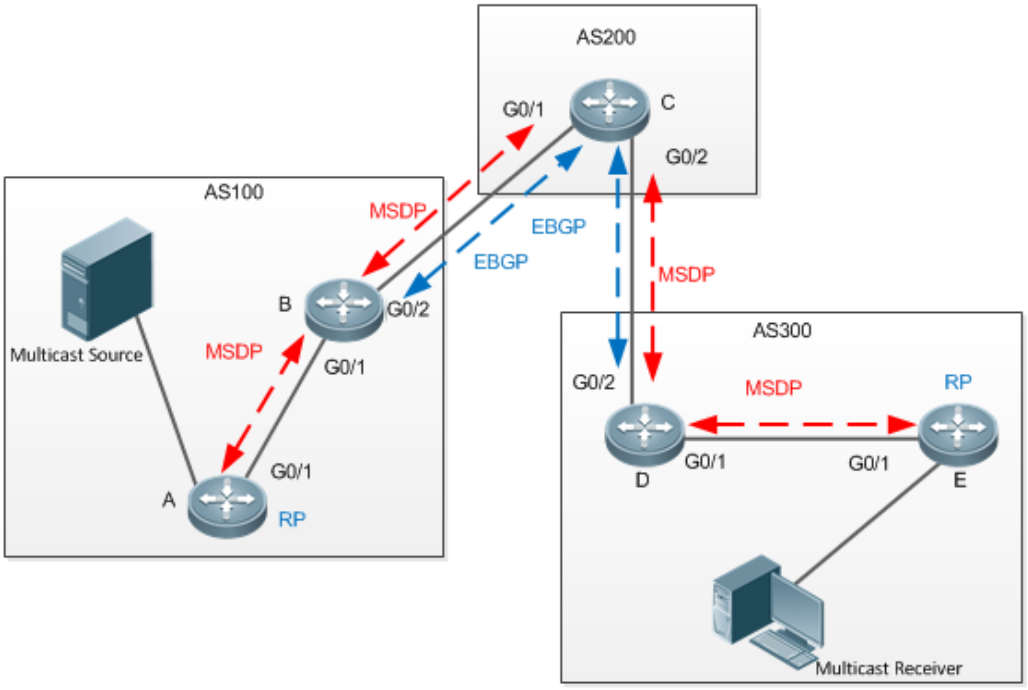

Рисунок 8-5.

В следующей таблице перечислены интерфейсы и IP-адреса различных устройств:

Устрой-ство	Интерфейс	IP-адрес	Примечание
A	G0/1	100.100.100.1/24	
	Loopback0	10.10.10.10/32	Адрес RP, который используется для установления соединения MSDP
B	G0/1	100.100.100.2/24	
	G0/2	1.1.1.1/24	Граница BSR
	Loopback0	20.20.20.20/32	Используется для установления соединений EBGP и MSDP
C	G0/1	1.1.1.2/24	Граница BSR
	G0/2	2.2.2.1/24	Граница BSR

		Loopback0	30.30.30.30/32	Используется для установления соединений EBGP и MSDP
	D	G0/2	2.2.2.2/24	Граница BSR
		G0/1	3.3.3.1/24	
		Loopback0	40.40.40.40/32	Используется для установления соединений EBGP и MSDP
	E	G0/1	3.3.3.2/24	
		Loopback0	50.50.50.50/32	Адрес RP, который используется для установления соединения MSDP.
Шаги настройки	• Настройте IP-адреса интерфейсов. • Включите OSPF в каждой AS. Настройте peer-отношения EBGP между AS 200 и AS 100, а также между AS 200 и AS 300. Познакомьте BGP с OSPF. • Включите PIM-SM в каждой AS, настройте C-BSR и C-RP, а также настройте границу BSR. • Установите peer-отношения MSDP между peer-ами EBGP, а также между peerами RP и EBGP. **ПРИМЕЧАНИЕ:** IP-адрес и локальный интерфейс peer-а MSDP должны быть такими же, как у peer-а EBGP			
A	A#configure terminal A(config)#ip multicast-routing A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)#interface loopback 0 A(config-if-loopback 0)#ip pim sparse-mode A(config-if-loopback 0)# exit A(config)#ip pim rp-candidate loopback 0 A(config)#ip pim bsr-candidate loopback 0 A(config)#ip msdp peer 10.10.10.10 connect-source loopback 0			
B	B#configure terminal B(config)#ip multicast-routing			

	B(config)#interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ip pim sparse-mode B(config-if-GigabitEthernet 0/1)# exit B(config)#interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)#ip pim sparse-mode B(config-if-GigabitEthernet 0/2)#ip pim bsr-border B(config-if-GigabitEthernet 0/2)# exit B(config)#interface loopback 0 B(config-if-loopback 0)#ip pim sparse-mode B(config-if-loopback 0)# exit B(config)#ip msdp peer 10.10.10.10 connect-source loopback 0 B(config)#ip msdp peer 30.30.30.30 connect-source loopback 0
C	C#configure terminal C(config)#ip multicast-routing C(config)#interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)#ip pim sparse-mode C(config-if-GigabitEthernet 0/1)#ip pim bsr-border C(config-if-GigabitEthernet 0/1)# exit C(config)#interface GigabitEthernet 0/2 C(config-if-GigabitEthernet 0/2)#ip pim sparse-mode C(config-if-GigabitEthernet 0/2)#ip pim bsr-border C(config-if-GigabitEthernet 0/2)# exit C(config)#interface loopback 0 C(config-if-loopback 0)#ip pim sparse-mode C(config-if-loopback 0)# exit C(config)#ip msdp peer 20.20.20.20 connect-source loopback 0 C(config)#ip msdp peer 40.40.40.40 connect-source loopback 0
D	D#configure terminal D(config)#ip multicast-routing D(config)# ip pim ssmdefault D(config)#interface GigabitEthernet 0/1 D(config-if-GigabitEthernet 0/1)#ip pim sparse-mode D(config-if-GigabitEthernet 0/1)# exit D(config)#interface GigabitEthernet 0/2 D(config-if-GigabitEthernet 0/2)#ip pim sparse-mode

	D(config-if-GigabitEthernet 0/2)#ip pim bsr-border D(config-if-GigabitEthernet 0/2)# exit D(config)#interface loopback 0 D(config-if-loopback 0)#ip pim sparse-mode D(config-if-loopback 0)# exit D(config)#ip msdp peer 30.30.30.30 connect-source loopback 0 D(config)#ip msdp peer 50.50.50.50 connect-source loopback 0
E	E#configure terminal E(config)#ip multicast-routing E(config)#interface GigabitEthernet 0/1 E(config-if-GigabitEthernet 0/1)#ip pim sparse-mode E(config-if-GigabitEthernet 0/1)# exit E(config)#interface loopback 0 E(config-if-loopback 0)#ip pim sparse-mode E(config-if-loopback 0)# exit E(config)#ip pim rp-candidate loopback 0 E(config)#ip pim bsr-candidate loopback 0 E(config)#ip msdp peer 50.50.50.50 connect-source loopback 0
Проверка	Используйте источник multicast для отправки пакета (200.200.200.200,225.1.1.1) и разрешите хосту присоединиться к группе 225.1.1.1. • Убедитесь, что хост получил этот пакет. • На устройстве C проверьте состояние и сообщение SA peer-a MSDP
D	D# show ip msdp summarywww.qtech.ru Msdp Peer Status Summary Peer Address As State Uptime/Downtime Reset-Count SA-Count PeerDescription 30.30.30.30 200 Up 00:01:420 1 No description D# show ip msdp sa-cache MSDP Source-Active Cache: 1 entries (200.200.200.200,225.1.1.1),RP:10.10.10.10,(M)BGP/AS 100, 00:00:18/00:01:57, Peer 30.30.30.30 Learned from peer 30.30.30.30, RPF peer 30.30.30.30, SAs received: 1, Encapsulated data received: 1

8.4.1.6. Распространенные ошибки

- Граница BSR не настроена или настроена на неправильном интерфейсе.
- PIM-SM не включен на локальном интерфейсе, используемом для установления peer-соединения MSDP, или на интерфейсе IP-адреса peer-а.
- Сообщения SA не могут пройти проверку Peer-RPF.

8.4.2. Настройка Anycast-RP

8.4.2.1. Эффект конфигурации

Установите peer-отношения MSDP внутри AS, чтобы обеспечить резервирование и балансировку нагрузки для RP.

8.4.2.2. Примечания

- Unicast-маршрут между AC должен быть доступен.
- PIM-SM должен работать в AS, и необходимо настроить несколько RP, использующих одни и те же IP-адреса.
- C-RP и C-BSR нельзя настроить на одном и том же интерфейсе.

8.4.2.3. Шаги настройки

Установление peer-отношений MSDP

- Обязательный.
- Настройте следующую команду на каждой RP одной и той же AS, чтобы установить peer-отношения MSDP с каждой из других RP:

Команда	**ip msdp peer** *peer-address* **connect-source** *interface-type interface-number*
Описание параметра	*peer-address*: указывает IP-адрес удаленного peer-а. *interface-type interface-number*: указывает локальный интерфейс, который используется для установления TCP-соединения с удаленным peer-ом
По умолчанию	Peer-отношения MSDP не установлены
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Peer-отношения являются двунаправленными. Поэтому эту команду необходимо настроить с обеих сторон. Чтобы гарантировать, что сообщения SA могут успешно пройти проверку Peer-RPF, рекомендуется настроить mesh-группу

Изменение адреса RP в сообщении SA

- Обязательный.
- Настройте следующую команду на каждой RP одной и той же AS:

Команда	**ip msdp originator-id** *interface-type interface-number*
Описание параметра	*interface-type interface-number*: использует IP-адрес этого интерфейса в качестве адреса RP в сообщении SA
По умолчанию	По умолчанию адрес RP в сообщении SA не изменяется
Командный режим	Режим глобальной конфигурации
Руководство по использованию	В сценарии применения Anycast-RP адреса RP на всех устройствах RP одинаковы. Если адрес RP в сообщении SA не изменен, устройство RP может определить, что это сообщение SA отправлено само по себе, и, следовательно, отбросить это сообщение. Поэтому вам необходимо настроить разные адреса RP для сообщений SA, отправляемых разными устройствами RP

8.4.2.4. Проверка

Отправьте пакет из источника (S), близкого к RP, в группу (G) и разрешите хосту, расположенному рядом с другой RP, присоединиться к G.

- Убедитесь, что хост может получить пакет (S, G).
- Запустите команду **show ip msdp sa-cache** на RP в другой AS, чтобы отобразить полученную информацию об источнике MSDP.

Отображение полученной исходной информации MSDP

Команда	**show ip msdp sa-cache**
Командный режим	Привилегированный режим, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если адрес не указан, вся информация (S, G) отображается по умолчанию. Если указан адрес, устройство проверяет, является ли этот адрес адресом unicast или multicast. Если адрес является адресом unicast, этот адрес рассматривается как источник multicast (S), и будет отображаться вся информация (S, G), в которой источником multicast является S. Если адрес является адресом multicast, этот адрес рассматривается как группа multicast (G), и будет отображаться вся информация (S, G), в которой группа multicast имеет значение G. Если этот адрес не является ни unicast, ни multicast, никакая информация не отображается. Если указаны два адреса, один адрес рассматривается как источник multicast (S), а другой — как группа multicast (G). Если один адрес является адресом unicast, а другой адрес — адресом группы multicast, никакая информация не отображается

	QTECH# show ip msdp sa-cache MSDP Source-Active Cache: 2 entries (200.200.200.200, 227.1.2.2), RP: 20.20.20.20, (M)BGP/AS 100, 04:17:09/00:02:05, Peer 200.200.200.2 Learned from peer 200.200.200.2, RPF peer 200.200.200.2, SAs received: 277, Encapsulated data received: 0 (200.200.200.200, 227.1.2.3), RP: 20.20.20.20, (M)BGP/AS 100, 04:17:09/00:02:05, Peer 200.200.200.2 Learned from peer 200.200.200.2, RPF peer 200.200.200.2, SAs received: 277, Encapsulated data received: 0

8.4.2.5. Пример конфигурации

Совместное использование исходной информации между Anycast-RP в том же multicast-домене

Сценарий:

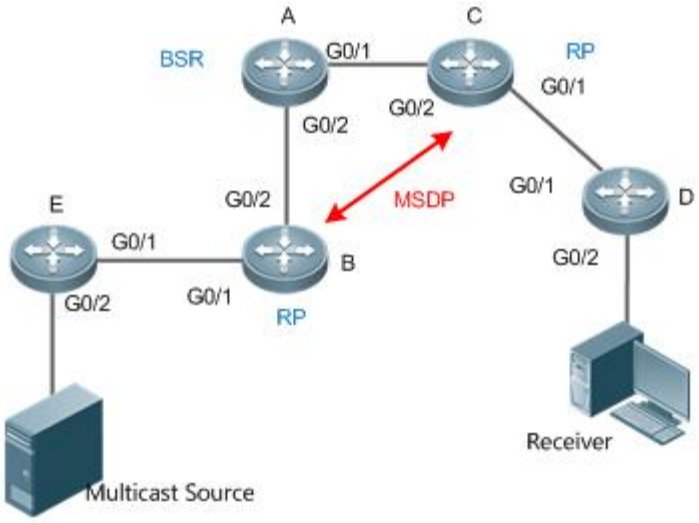

Рисунок 8-6.

	В следующей таблице перечислены интерфейсы и IP-адреса различных устройств:

Устрой-ство	Интерфейс	IP-адрес	Примечание
A	G0/2	2.2.2.1/24	

		G0/1	1.1.1.1/24	
		Loopback0	100.100.100.100/32	C-BSR настроен на этом интерфейсе
	B	G0/2	2.2.2.2/24	
		G0/1	3.3.3.1/24	
		Loopback1	20.20.20.20/32	Используется для установления соединения MSDP и изменения адреса RP в сообщении SA
		Loopback0	10.10.10.10/32	C-RP настроен на этом интерфейсе
	C	G0/2	1.1.1.2/24	
		G0/1	4.4.4.1/24	
		Loopback1	30.30.30.30/32	Используется для установления соединения MSDP и изменения адреса RP в сообщении SA
		Loopback0	10.10.10.10/32	C-RP настроен на этом интерфейсе
	D	G0/1	4.4.4.2/24	
		G0/2	5.5.5.1/24	
	E	G0/1	3.3.3.2/24	
		G0/2	6.6.6.1/24	
Шаги настройки	• Настройте IP-адреса интерфейсов. • Включите OSPF в AS. • Включите PIM-SM в AS и настройте C-BSR и C-RP. • Установите peer-отношения MSDP между RP и измените адрес RP в сообщении SA. • Настройте mesh-группу			

A	A#configure terminal A(config)#ip multicast-routing A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)#interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#ip pim sparse-mode A(config-if-GigabitEthernet 0/2)# exit A(config)#interface loopback 0 A(config-if-loopback 0)#ip pim sparse-mode A(config-if-loopback 0)# exit A(config)#ip pim bsr-candidate loopback0
B	B#configure terminal B(config)#ip multicast-routing B(config)#interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ip pim sparse-mode B(config-if-GigabitEthernet 0/1)# exit B(config)#interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)#ip pim sparse-mode B(config-if-GigabitEthernet 0/2)# exit B(config)#interface loopback 0 B(config-if-loopback 0)#ip pim sparse-mode B(config-if-loopback 0)# exit B(config)#interface loopback 1 B(config-if-loopback 1)#ip pim sparse-mode B(config-if-loopback 1)# exit B(config)#ip pim rp-candidate loopback 0 B(config)#ip msdp peer 30.30.30.30 connect-source loopback 1 B(config)# ip msdp originator-id loopback 1 B(config)#ip msdp mesh-group mesh-name 30.30.30.30
C	C#configure terminal C(config)#ip multicast-routing C(config)#interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)#ip pim sparse-mode C(config-if-GigabitEthernet 0/1)# exit

	C(config)#interface GigabitEthernet 0/2 C(config-if-GigabitEthernet 0/2)#ip pim sparse-mode C(config-if-GigabitEthernet 0/2)# exit C(config)#interface loopback 0 C(config-if-loopback 0)#ip pim sparse-mode C(config-if-loopback 0)# exit C(config)#interface loopback 1 C(config-if-loopback 1)#ip pim sparse-mode C(config-if-loopback 1)# exit C(config)#ip pim rp-candidate loopback 0 C(config)#ip msdp peer 20.20.20.20 connect-source loopback 1 C(config)# ip msdp originator-id loopback 1 C(config)#ip msdp mesh-group mesh-name 20.20.20.20
D	D#configure terminal D(config)#ip multicast-routing D(config)#interface GigabitEthernet 0/1 D(config-if-GigabitEthernet 0/1)#ip pim sparse-mode D(config-if-GigabitEthernet 0/1)# exit D(config)#interface GigabitEthernet 0/2 D(config-if-GigabitEthernet 0/2)#ip pim sparse-mode D(config-if-GigabitEthernet 0/2)# exit
E	E#configure terminal E(config)#ip multicast-routing E(config)#interface GigabitEthernet 0/1 E(config-if-GigabitEthernet 0/1)#ip pim sparse-mode E(config-if-GigabitEthernet 0/1)# exit E(config)#interface GigabitEthernet 0/2 E(config-if-GigabitEthernet 0/2)#ip pim sparse-mode E(config-if-GigabitEthernet 0/2)# exit
Проверка	Используйте источник multicast для отправки пакета (6.6.6.6,225.1.1.1) и разрешите хосту присоединиться к группе 225.1.1.1. • Убедитесь, что хост получил этот пакет. • На устройстве C проверьте состояние и сообщение SA peer-a MSDP
C	C# show ip msdp summary

	Msdp Peer Status Summary Peer Address As SA-Count State Uptime/Downtime Reset-Count Peer Description 20.20.20.20 Unknown Up 00:01:420 1 No description C# show ip msdp sa-cache MSDP Source-Active Cache: 1 entries (6.6.6.6,225.1.1.1),RP:10.10.10.10,(M)BGP/AS unknown, 00:00:18/00:01:57, Peer 20.20.20.20 Learned from peer 20.20.20.20, RPF peer 20.20.20.20,

8.4.2.6. Распространенные ошибки

- C-BSR и C-RP настроены на одном и том же интерфейсе.
- Адрес RP в сообщении SA не изменяется.
- Сообщения SA не могут пройти проверку Peer-RPF.

8.4.3. Настройка Green Channel проверки Peer-RPF

8.4.3.1. Эффект конфигурации

Настройте Green Channel проверки Peer-RPF, чтобы все сообщения SA, отправленные от указанного peer-a MSDP, могли пройти проверку Peer-RPF.

Настройте mesh-группу MSDP так, чтобы все сообщения SA, отправленные от участников mesh-группы, могли пройти проверку Peer-RPF.

8.4.3.2. Примечания

Между устройствами должны быть установлены peer-отношения MSDP.

8.4.3.3. Шаги настройки

Настройка peer-a MSDP по умолчанию

- Опционально.
- Если на peer-е MSDP нет необходимости выполнять проверку Peer-RPF для сообщений SA, отправленных от указанного peer-a, настройте этот peer как peer по умолчанию.

Команда	**ip msdp default-peer** *peer-address* [**prefix-list** *prefix-list-name*]
Описание параметра	*peer-address*: указывает IP-адрес удаленного peer-a. **prefix-list** *prefix-list-name*: определяет список префиксов, который используется для ограничения RP, инициирующих сообщения SA
По умолчанию	По умолчанию peer не настроен

Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если команда не содержит **prefix-list** *prefix-list-name*, принимаются все сообщения SA. Если команда содержит **prefix-list** *prefix-list-name*, но указанный список префиксов не существует, все сообщения SA принимаются. Если команда содержит **prefix-list** *prefix-list-name* и указанный список префиксов существует, принимаются только сообщения SA, инициированные RP, указанными в этом списке префиксов

Создание Mesh-группы

- Опционально.
- Если среди нескольких peer-узлов MSDP сообщения SA, поступающие от любого из этих peer-узлов, по умолчанию проходят проверку Peer-RPF, вы можете добавить эти peer-узлы в mesh-группу.

Команда	**ip msdp mesh-group** *mesh-name peer-address*
Описание параметра	*mesh-name*: указывает имя mesh-группы. Имя чувствительно к регистру. *peer-address*: указывает IP-адрес узла MSDP, который будет добавлен в mesh-группу
По умолчанию	По умолчанию mesh-группа не настроена
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Peer-отношения MSDP должны быть установлены между каждыми двумя peer-ами MSDP, добавленными в одну и ту же mesh-группу. Все сообщения SA, отправленные участниками mesh-группы, могут пройти проверку Peer-RPF

8.4.3.4. Проверка

- Проверьте, могут ли сообщения SA, отправленные peer-ом по умолчанию, пройти проверку Peer-RPF.
- Проверьте конфигурацию mesh-группы и проверьте, могут ли все сообщения SA, отправленные участниками mesh-группы, пройти проверку Peer-RPF.

Отображение информации о проверке Peer-RPF указанного peer-а MSDP

Команда	**show ip msdp rpf-peer** *ip-address*
Описание параметра	*peer-address*: указывает IP-адрес инициатора сообщения SA

Командный режим	Привилегированный режим, режим глобальной конфигурации или режим конфигурации интерфейса
	QTECH# show ip msdp rpf-peer 1.1.1.1 RPF peer information for 1.1.1.1 RPF peer: 200.200.200.2www.qtech.ru RPF rule: Peer is only active peer RPF route/mask: Not-used RPF type: Not-used

Отображение конфигурации Mesh-группы

Команда	**show ip msdp mesh-group**
Командный режим	Привилегированный режим, режим глобальной конфигурации или режим конфигурации интерфейса
	QTECH# show ip msdp mesh-group MSDP peers in each Mesh-group, <Mesh-group name>:<# peers> msdp-mesh: 1.1.1.2 1.1.1.3

8.4.3.5. Пример конфигурации

Настройка проверки Peer-RPF и Mesh-группы

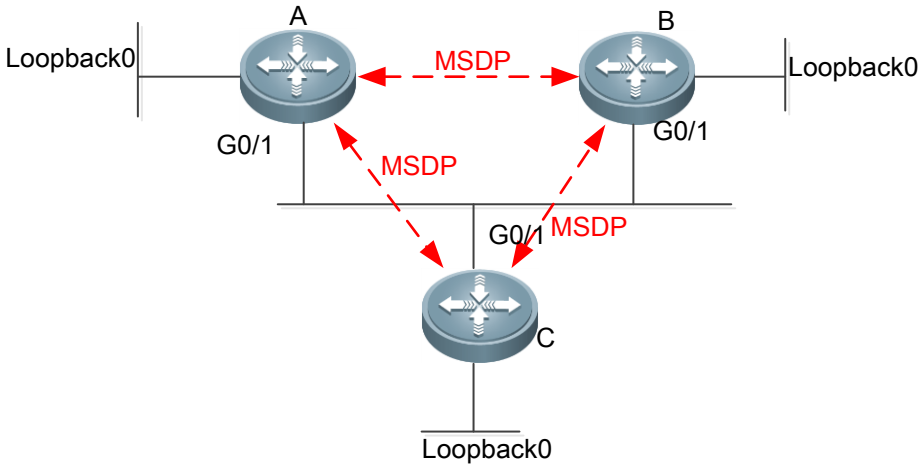

Рисунок 8-7.

В следующей таблице перечислены интерфейсы и IP-адреса различных устройств:

Устройство	Интерфейс	IP-адрес	Примечание
A	G0/1	20.0.0.3/24	
	Loopback0	10.1.1.1/24	
B	G0/1	20.0.0.4/24	
	Loopback0	40.0.0.1/24	
	G0/1	20.0.0.222/24	
	Loopback0	30.0.0.2/24	

Шаги настройки

- Настройте IP-адреса интерфейсов.
- Включите OSPF в AS.
- Установите peer-отношения MSDP между A и B, а также между A и C.
- Включите PIM-SM на интерфейсе G0/1 устройства C.
- Перед настройкой на устройстве A есть два активных peer-а MSDP, но неизвестно, какой из них следует выбрать в качестве peer-а RPF. Поэтому отобразите информацию о peer-е RPF. Отображается «RPF peer does not exist» («Peer RPF не существует»).
- Настройте peer MSDP по умолчанию и проверьте, успешна ли конфигурация.
- Настройте mesh-группу

A

```
A#configure terminal
A(config)#ip msdp peer 20.0.0.4 connect-source gi0/1
A(config)#ip msdp peer 30.0.0.2 connect-source loopback 0
```

B

```
B #configure terminal
B(config)#ip msdp peer 20.0.0.3 connect-source gi0/1
```

C

```
C#configure terminal
C(config)#ip msdp peer 10.0.0.1 connect-source loopback 0
C(config)#interface GigabitEthernet 0/1
C(config-if-GigabitEthernet 0/1)#ip pim sparse-mode
C(config-if-GigabitEthernet 0/1)# exit
```

- Перед настройкой на устройстве A есть два активных peer-а MSDP, но неизвестно, какой из них следует выбрать в качестве peer-а RPF.

	Поэтому отобразите информацию о peer-е RPF. Отображается «RPF peer does not exist» («Peer RPF не существует»). • Настройте peer MSDP по умолчанию. Затем отобразите информацию о peer-е RPF. Отобразится сообщение "Peer is best default peer" («Лучший peer — это peer по умолчанию»)
A	A#configure terminal A(config)#ip msdp default-peer 30.0.0.2 • Отмените peer по умолчанию и отправьте информацию об источнике multicast на устройство C. Информация отображается на устройстве A, указывая, что сообщение SA получено, но не проходит проверку Peer-RPF. • На устройстве A добавьте 30.0.0.2 в mesh-группу. Затем устройство A сможет нормально получить сообщение SA
A	A#configure terminal A(config)#no ip msdp default-peer 30.0.0.2
A	A#configure terminal A(config)#ip msdp mesh-group first 30.0.0.2

8.4.4. Включение мер безопасности

8.4.4.1. Эффект конфигурации

Включите шифрование MD5 для TCP-соединений между peer-ами MSDP, чтобы предотвратить незаконные TCP-соединения.

Ограничьте количество сообщений SA в кеше SA указанного peer-а MSDP, чтобы подавить штормы SA.

8.4.4.2. Примечания

Между устройствами должны быть установлены peer-отношения MSDP.

8.4.4.3. Шаги настройки

Настройка шифрования MD5 в TCP-соединениях между узлами MSDP

- Опционально.
- Настройте согласованное шифрование MD5 на peer-ах MSDP, которым требуется шифрование.

Команда	**ip msdp password peer** *peer-address* [*encryption-type*] *string*
Описание параметра	*peer-address*: указывает IP-адрес удаленного peer-а. *encryption-type*: указывает уровень шифрования. В настоящее время поддерживаются только уровни от 0 до 7. 0 — самый низкий уровень, а 7 — самый высокий уровень. Значение по умолчанию — 0. *string*: указывает шифр, используемый для аутентификации TCP MD5

По умолчанию	По умолчанию шифрование MD5 не настроено
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Чтобы аутентифицировать идентификатор peer-a MSDP, включите шифрование MD5 в TCP-соединении, установленном с этим peer-ом MSDP. Peer MSDP должен иметь согласованную конфигурацию и шифр должен быть одинаковым; в противном случае соединение не будет установлено. Если конфигурация или шифр изменяются, локальное устройство не останавливает текущий сеанс и попытается использовать новый шифр для сохранения текущего сеанса до истечения времени тайм-аута. Если уровень шифрования установлен на 7, длина зашифрованного текста должна быть четным числом, равным или превышающим 4; в противном случае конфигурация завершится неудачно

Ограничение количества сообщений SA в кеше SA указанного peer-a MSDP

- Необязательный.
- Выполните эту настройку, если вам нужно ограничить количество сообщений SA в кеше SA указанного peer-a MSDP.

Команда	**ip msdp sa-limit** *peer-address sa-limit*
Описание параметра	*peer-address*: указывает IP-адрес удаленного peer-a. *sa-limit*: указывает максимальное количество сообщений SA в кеше SA
По умолчанию	Значение по умолчанию — 1024
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Peer-отношения MSDP должны быть установлены между каждыми двумя peer-ами MSDP, добавленными в одну и ту же mesh-группу. Предположим, что количество сообщений SA в кеше SA уже превышает лимит. После завершения настройки количество сообщений SA в кеше SA не превышает лимит

8.4.4.4. Проверка

- Проверьте соединение между peer-ами, на которых настроено шифрование MD5.
- Отправьте количество пакетов с информацией об источнике, превышающее лимит, peer-у, для которого настроено максимальное количество сообщений SA в кеше SA. Проверьте, можно ли изучить всю исходную информацию.

Отображение количества сообщений SA, полученных от указанного peer-а

Команда	**show ip msdp count**
Командный режим	Привилегированный режим, режим глобальной конфигурации или режим конфигурации интерфейса
	QTECH# **show ip msdp count** SA State per Peer Counters, <Peer>: <# SA learned> 1.1.1.2 : 0 100.100.100.14 : 0 100.100.100.15 : 0 100.100.100.200: 0 200.200.200.2 : 2 200.200.200.3 : 0 200.200.200.6 : 0 200.200.200.13 : 0 200.200.200.66 : 0 SA State per ASN Counters, <asn>: <# sources>/<# groups> Total entries: 2 100: 1/2

8.4.4.5. Пример конфигурации

Настройка шифрования MD5 на peer-е MSDP и ограничение количества сообщений SA, отправляемых этим peer-ом MSDP в кеше SA

Сценарий:

Рисунок 8-8.

Шаги настройки	• Установите peer-отношения MSDP между A и B. • Настройте шифрование MD5 на устройстве A. • По истечении времени ожидания MSDP настройте шифр MD5 peer-а на устройстве B, который совпадает с шифром на устройстве A. Затем сеанс повторно подключается. • На устройстве A установите максимальное количество сообщений SA, отправленных peer-ом 20.0.0.4 в кеше SA, равным 10
A	A#configure

	A(config)# ip msdp password peer 20.0.0.4 0 1234567 A(config)# ip msdp sa-limit 20.0.0.4 10
B	B#configure B(config)# ip msdp password peer 20.0.0.4 0 1234567
Проверка	• Установите peer-отношения MSDP между A и B. • Настройте шифрование MD5 на устройстве A. • По истечении времени ожидания MSDP настройте шифр MD5 peer-a на устройстве B, который совпадает с шифром на устройстве A. Затем сеанс повторно подключается. • На устройстве A установите максимальное количество сообщений SA, отправленных peer-ом 20.0.0.4 в кеше SA, равным 10. • После того, как MD5 настроен на устройстве A, но не настроен на устройстве B, отобразится сообщение, указывающее на сбой шифрования MD5. В это время peer MSDP находится в состоянии DOWN. • Через некоторое время после настройки MD5 на устройстве B peer MSDP находится в состоянии DOWN. • Отправьте 20 исходных пакетов multicast на устройство B. На устройстве A отобразится сообщение, указывающее, что количество сообщений SA превышает лимит
A	A# debug ip msdp sa-cache A# show ip msdp count

8.4.5. Ограничение broadcast-а сообщений SA

8.4.5.1. Эффект конфигурации

Настройте правила фильтрации сообщений SA таким образом, чтобы ограничить broadcast сообщений SA.

8.4.5.2. Примечания

Между устройствами должны быть установлены peer-отношения MSDP.

8.4.5.3. Шаги настройки

Фильтрация информации источника, распространяемой локально

- Опционально.
- Настройте правило фильтрации выпуска SA на устройстве MSDP, где необходимо ограничить выпуск (релиз) информации SA.

Команда	**ip msdp redistribute** [**list** *access-list*] [**route-map** *route-map*]
Описание параметра	**list** *access-list*: указывает список управления доступом (ACL), используемый для управления диапазонами S и G.

	route-map *route-map*: указывает карту маршрутов, используемую для управления диапазонами S и G
По умолчанию	По умолчанию ни одно правило не настроено для фильтрации локально выпускаемой информации SA
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После настройки этой команды в MSDP можно вводить только принятую информацию (S, G) (поступающую из локального домена или других доменов). Если команда содержит **list** *access-list*, может быть выпущена только информация (S, G), соответствующая этому ACL. Если команда содержит **route-map** *route-map*, может быть выпущена только информация (S, G), соответствующая этой карте маршрута. Если команда содержит оба параметра, может быть выпущена только информация (S, G), соответствующая ACL и карте маршрутов. Если команда не содержит каких-либо параметров, информация (S, G) не выпускается

Фильтрация полученных запросов SA

- Опционально.
- Выполните эту настройку на устройстве MSDP, где необходимо ограничить ответ на запросы SA.

Команда	**ip msdp filter-sa-request** *peer-address*[**list** *access-list*]
Описание параметра	*peer-address*: указывает IP-адрес удаленного peer-a. **list** *access-list*: указывает список ACL, используемый для управления диапазоном группового адреса
По умолчанию	По умолчанию, ни одно правило не настроено для фильтрации полученных запросов SA
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду, если вам нужно контролировать запросы SA, которые могут быть приняты и на которые можно ответить. Если команда не содержит **list** *access-list*, все запросы SA будут игнорироваться. Если команда содержит **list** *access-list*, но этот AC не существует, все запросы SA будут игнорироваться.

	Если команда содержит **list** *access-list* и этот AC существует, будут приниматься только запросы SA, разрешенные ACL, а остальные игнорируются

Фильтрация полученных сообщений SA

- Опционально.
- Выполните эту настройку на устройстве MSDP, где входящая информация SA должна быть ограничена.

Команда	**ip msdp sa-filter in** *peer-address* [**list** *access-list*] [**route–map** *route-map*] [**rp-list** *rp-access-list*] [**rp-route-map** *rp-route-map*]
Описание параметра	*peer-address*: указывает IP-адрес удаленного peer-a. **list** *access-list*: указывает номер или имя расширенного IP ACL указанного (S, G). Он используется для управления информацией об источнике multicast (S, G), которой разрешено пройти. **route-map** *route-map*: указывает название указанной карты маршрутов (S, G). Информацию об источнике multicast (S, G) разрешается передавать только в том случае, если путь AS маршрута на S соответствует пути AS на карте маршрутов. **rp-list** *rp-access-list*: указывает номер или имя стандартного ACL указанной RP. Он используется для управления RP, из которых разрешена передача исходной multicast-информации (S, G). **rp-route-map** *rp-route-map*: указывает имя карты маршрутов указанной RP. Информацию об источнике multicast (S, G) разрешено передавать только в том случае, если путь AS маршрута на RP соответствует пути AS в карте маршрута
По умолчанию	По умолчанию ни одно правило не настроено для фильтрации входящих сообщений SA
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если эта команда настроена, но не указаны ACL или карта маршрутов, все входящие сообщения SA будут фильтроваться. Если указано только одно ключевое слово (**list** или **route-map**) и каждая запись источника multicast (S, G) в сообщении SA соответствует правилу, указанному ключевым словом, то будет получена запись источника multicast (S, G). Если любой **rp-list** или **rp-route-map** указан, и адрес RP, содержащийся в сообщении SA, соответствует правилу, указанному этим ключевым словом, это сообщение SA будет получено. Если два или более ключевых слов (включая **list, route-map, rp-list** и **rp-route-map**), может быть получена только запись источника multicast (S, G) в сообщении SA, которая соответствует правилам, заданным всеми доступными ключевыми словами

Фильтрация отправленных сообщений SA

- Опционально.
- Выполните эту настройку на устройстве MSDP, где необходимо ограничить исходящую информацию SA.

Команда	**ip msdp sa-filter out** *peer-address* [**list** *access-list*] [**route–map** *route-map*] [**rp-list** *rp-access-list*] [**rp-route-map** *rp-route-map*]
Описание параметра	*peer-address*: указывает IP-адрес удаленного peer-а. **list** *access-list*: указывает номер или имя расширенного IP ACL указанного (S, G). Он используется для управления информацией об источнике multicast (S, G), которой разрешено пройти. **route-map** *route-map*: указывает название указанной карты маршрутов (S, G). Информацию об источнике multicast (S, G) разрешается передавать только в том случае, если путь AS маршрута на S соответствует пути AS на карте маршрутов. **rp-list** *rp-access-list*: указывает номер или имя стандартного списка управления доступом указанной RP. Он используется для управления RP, из которых разрешена передача исходной multicast-информации (S, G). **rp-route-map** *rp-route-map*: указывает имя карты маршрутов указанной RP. Информацию об источнике multicast (S, G) разрешено передавать только в том случае, если путь AS маршрута на RP соответствует пути AS в карте маршрута
По умолчанию	По умолчанию ни одно правило не настроено для фильтрации исходящих сообщений SA
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если эта команда настроена, но не указаны ACL или карта маршрутов, сообщение SA не будет отправлено этому peer-у MSDP. Если указано только одно из ключевых слов (включая **list, route-map, rp-list** и **rp-route-map**), любая запись источника multicast (S, G), соответствующая правилу, указанному в ключевом слове, будет перенаправлена этому peer-у MSDP. Если указаны два или более ключевых слов (включая **list, route-map, rp-list** и **rp-route-map**), любая запись источника multicast (S, G), которая соответствует правилам, заданным всеми доступными ключевыми словами, будет перенаправлена этому peer-у MSDP

8.4.5.4. Проверка

- Проверьте, соответствуют ли сообщения SA, инициированные локальным устройством, правилам фильтрации.
- Проверьте, соответствуют ли сообщения SA, полученные локальным устройством, правилам фильтрации.

Отображение сообщений SA, инициированных локальным устройством

Команда	**show ip msdp sa-originated**
Командный режим	Привилегированный режим, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если локальное устройство является RP PIM-SM, информация об источнике multicast (S, G) зарегистрирована на RP, а peer MSDP настроен на локальном устройстве, вы можете запустить эту команду для отображения (S, G) информации, инициированной локальным устройством. Информация (S, G), отображаемая этой командой, соответствует критериям, заданным командой **ip msdp redistribute**, но такая информация (S, G) может быть отправлена peer-у MSDP только тогда, когда информация соответствует правилам фильтрации исходящей информации SA, заданным командой **ip msdp sa-filter out**
	QTECH# show ip msdp sa-originated MSDP Source-Active Originated: 5 entries (192.168.23.78, 225.0.0.1), RP: 192.168.23.249 (192.168.23.79, 225.0.0.2), RP: 192.168.23.249 (192.168.23.80, 225.0.0.3), RP: 192.168.23.249 (192.168.23.81, 225.0.0.4), RP: 192.168.23.249 (192.168.23.82, 225.0.0.5), RP: 192.168.23.249

8.4.5.5. Пример конфигурации

Настройка правил фильтрации входящих или исходящих сообщений SA

Сценарий:

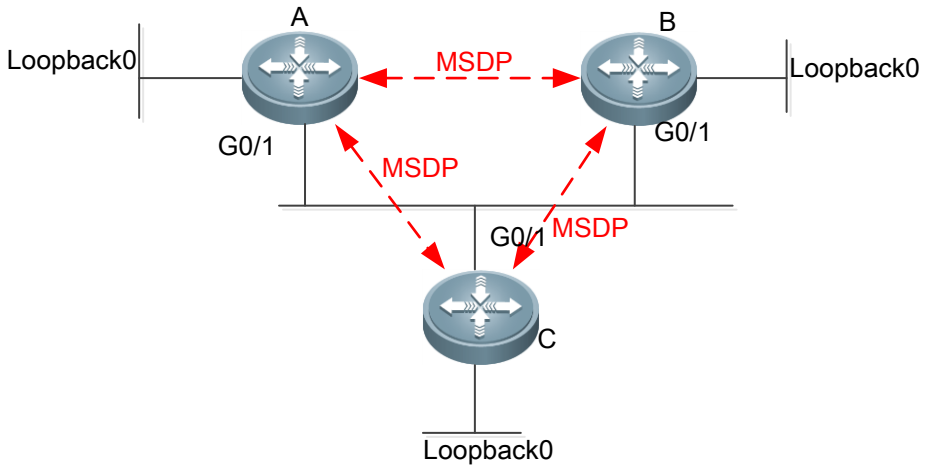

Рисунок 8-9.

<table>
<tr><td></td><td>В следующей таблице перечислены интерфейсы и IP-адреса различных устройств:
<table>
<tr><th>Устрой-ство</th><th>Интерфейс</th><th>IP-адрес</th><th>Примечание</th></tr>
<tr><td rowspan="2">A</td><td>G0/1</td><td>20.0.0.3/24</td><td></td></tr>
<tr><td>Loopback0</td><td>10.1.1.1/24</td><td></td></tr>
<tr><td rowspan="4">B</td><td>G0/1</td><td>20.0.0.4/24</td><td></td></tr>
<tr><td>Loopback0</td><td>40.0.0.1/24</td><td></td></tr>
<tr><td>G0/1</td><td>20.0.0.222/24</td><td></td></tr>
<tr><td>Loopback0</td><td>30.0.0.2/24</td><td></td></tr>
</table></td></tr>
<tr><td>Шаги настройки</td><td>• Завершите базовую настройку, как описано в разделе Настройка Green Channel проверки Peer-RPF.
• Настройте правила фильтрации входящих сообщений SA на устройстве A.
• Настройте правила фильтрации исходящих сообщений SA на устройстве A.
• Отправьте информацию об источнике multicast на устройство C</td></tr>
<tr><td>A</td><td>A#configure
A(config)# ip msdp sa-filter in 30.0.0.2
A(config)# ip msdp sa-filter in 30.0.0.2 list 100
A(config)# ip access-list extended 100
A(config-ext-nacl)# permit ip host 20.0.0.100 host 225.0.0.1
A(config)# ip msdp sa-filter in 30.0.0.2 rp-list rp-acl-1
A(config)# ip access-list standard rp-acl-1
A(config-std-nacl) # permit host 20.0.0.221
A(config)# ip msdp sa-filter in 30.0.0.2 rp-route-map rp-rm-1
A(config)# route-map rp-rm-1
A(config-route-map)#match as-path 1
A(config)# ip as-path access-list 1 permit 2
A#configure
A(config)# ip msdp sa-filter out 30.0.0.2
A(config)# ip msdp sa-filter out 30.0.0.2 list 101</td></tr>
</table>

	A(config)# ip access-list extended 101 A(config-ext-nacl)# permit ip host 20.0.0.100 host 225.0.0.1 A(config)# ip msdp sa-filter out 30.0.0.2 rp-list rp-acl-2 A(config)# ip access-list standard rp-acl-2 A(config-std-nacl) # permit host 20.0.0.221 A(config)# ip msdp sa-filter out 30.0.0.2 rp-route-map rp-rm-2 A(config)# route-map rp-rm-1 A(config-route-map)#match as-path 1 A(config)# ip as-path access-list 1 permit 2
Проверка	• Отправьте информацию об источнике multicast на устройство C в различных сценариях. • На устройстве A проверьте, соответствует ли полученная информация об источнике multicast входящим требованиям. • На устройстве B проверьте, соответствует ли полученная информация об источнике multicast исходящим требованиям
A	A#show ip msdp sa-cache
B	B#show ip msdp sa-cache
C	B#show ip msdp sa-originated

8.4.6. Управление peer-ами MSDP

8.4.6.1. Эффект конфигурации

Управляйте peer-ами MSDP, добавляя описания к указанному MSDP или сбрасывая peer MSDP.

8.4.6.2. Примечания

Peer-ы MSDP должны быть созданы заранее.

8.4.6.3. Шаги настройки

Настройка описания для peer-а MSDP

- Опционально.
- Выполните эту настройку на peer-е MSDP, которым необходимо управлять.

Команда	**ip msdp description** *peer-address text*
Описание параметра	*peer-address*: указывает IP-адрес удаленного peer-а. *text*: указывает строку, описывающую peer MSDP
По умолчанию	По умолчанию информация описания peer-а MSDP не настроена

Командный режим	Режим глобальной конфигурации

Отключения peer-a MSDP

- Необязательный.
- Выполните эту настройку, если необходимо временно отключить соединение с указанным peer-ом.

Команда	**ip msdp shutdown** *peer-address*
Описание параметра	*peer-address*: указывает IP-адрес peer-a MSDP
По умолчанию	По умолчанию peer MSDP не отключается
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда отключает только соединение TCP с peer-ом MSDP, но не удаляет этот peer MSDP или конфигурацию этого peer-a MSDP

8.4.6.4. Проверка

- Отобразите информацию об указанном peer-е MSDP и проверьте, соответствуют ли описание и статус peer-a требованиям.

Отображение информации об указанном peer-е MSDP

Команда	**show ip msdp peer** [*peer-address*]
Командный режим	Привилегированный режим, режим глобальной конфигурации или режим конфигурации интерфейса
	QTECH#show ip msdp peer 20.0.0.1 MSDP PEER 20.0.0.1 (No description), AS unknown Connection status: State: Listen, Resets: 1, Connection source: GigabitEthernet 0/1 (20.0.0.2) Uptime(Downtime): 00:00:25, Message sent/received: 13/19 Input messages discarded: 0 Connection and counters cleared 00:13:25 ago Local Address of connection: 20.0.0.2 MD5 signature protection on MSDP TCP connection: enabled SA Filtering: Input (S,G) Access-list filter: None

	Input (S,G) route-map filter: None Input RP Access-list filter: None Input RP Route-map filter: None Output (S,G) Access-list filter: None Output (S,G) Route-map filter: None Output RP Access-list filter: None Output RP Route-map filter: None SA-Requests: Input filter: None Peer ttl threshold: 0 SAs learned from this peer: 2, SAs limit: No-limit Message counters: SA messages discarded: 0 SA messages in/out: 13/0 SA Requests discarded/in: 0/0 SA Responses out: 0 Data Packets in/out: 6/0

8.4.6.5. Пример конфигурации

Настройка описания peer-а MSDP и закрытие соединения с этим peer-ом

Сценарий:

Рисунок 8-10.

Шаги настройки	• Установите peer-отношения MSDP между устройством A и устройством B. • Настройте описание «peer-router-B» для peer-а 20.0.0.4 на устройстве A. • Подождите 60 и закройте соединение с peer-ом MSDP 20.0.0.4 на устройстве A
A	A#configure A(config)# ip msdp peer 20.0.0.4 connect-source gi0/1 A(config)# ip msdp description 20.0.0.4 peer-router-B A(config)# end

	A# show ip msdp peer 20.0.0.4 …… A#configure A(config)# ip msdp shutdown 20.0.0.4 A(config)# show ip msdp peer 20.0.0.4
B	B# configure B(config)# ip msdp peer 20.0.0.3 connect-source gi0/1 B(config)# end
Проверка	Запустите команду **show ip msdp peer** [*peer-address*], чтобы отобразить краткую информацию об указанном peer-е, включая описание и состояние соединения этого peer-а MSDP
A	A# show ip msdp peer 20.0.0.4

8.4.7. Изменение параметров протокола

8.4.7.1. Эффект конфигурации

Управляйте peer-ами MSDP, добавляя описания к указанному MSDP или сбрасывая peer MSDP.

8.4.7.2. Примечания

Peer-ы MSDP должны быть созданы заранее.

8.4.7.3. Шаги настройки

Настройка интервала повторного подключения TCP peer-а MSDP

- Опционально.
- Выполните эту настройку на устройстве, где необходимо изменить интервал повторного подключения TCP peer-а MSDP.

Команда	**ip msdp timer** *interval*
Описание параметра	*interval*: указывает интервал повторного подключения TCP. Единицы измерения секунды. Значение варьируется от 1 до 60. Значение по умолчанию — 30
По умолчанию	По умолчанию интервал повторного подключения составляет 30 секунд
Командный режим	Режим глобальной конфигурации

Руководство по использованию	В течение интервала повторного подключения TCP peer MSDP на стороне proactive-соединения можно инициировать не более одного TCP-соединения. В некоторых сценариях применения можно сократить интервал повторного подключения TCP, чтобы ускорить конвергенцию peer-отношений MSDP

Настройка TTL multicast-пакета, содержащегося в сообщении SA

- Опционально.
- Выполните эту настройку на устройстве MSDP, где передача multicast-пакетов между RP должна быть ограничена.

Команда	**ip msdp ttl-threshold** *peer-address ttl-value*
Описание параметра	*peer-address*: указывает IP-адрес peer-а MSDP. *peer-address ttl-value*: указывает значение TTL. Значение находится в диапазоне от 0 до 255. Значение по умолчанию — 0
По умолчанию	По умолчанию значение TTL multicast-пакета, содержащегося в сообщении SA, не ограничено
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда ограничивает отправку multicast-пакета, инкапсулированного в сообщение SA. Multicast-пакет отправляется peer-у MSDP только в том случае, если значение TTL в IP-заголовке пакета multicast равно или превышает заданный порог TTL. Если значение TTL в IP-заголовке multicast-пакета меньше заданного порога TTL, multicast-пакет будет удален из сообщения SA и отброшен до того, как сообщение SA будет отправлено peer-у MSDP. Эта команда влияет на отправку multicast-пакета в сообщении SA, но не влияет на отправку информации об источнике multicast (S, G) в сообщении SA

Настройка емкости peer-а MSDP, поддерживаемой устройством

- Опционально.
- Если емкость по умолчанию (64 peer-а MSDP) недостаточна для поддержки приложений, вы можете изменить емкость устройства.

Команда	**ip msdp peer-limit** *peer-limit*
Описание параметра	*peer-limit*: указывает максимальное количество peer-ов MSDP, которые можно настроить. Значение варьируется от 1 до 128. Значение по умолчанию — 64
По умолчанию	По умолчанию можно настроить не более 64 узлов

Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для настройки максимального количества peer-ов MSDP, поддерживаемых устройством. Если при настройке этой команды количество peer-ов MSDP на устройстве превышает настраиваемое значение, отобразится запрос, и настройка завершится сбоем. Конфигурация может быть успешной только после удаления лишних peer-ов

Настройка емкости кеша SA, поддерживаемой устройством

- Опционально.
- Выполните эту настройку на устройстве, на котором необходимо настроить емкость кеша SA.

Команда	**ip msdp global-sa-limit** *sa-liit*
Описание параметра	*sa-liit*: указывает максимальную емкость кеша SA, поддерживаемую устройством. Значение варьируется от 1 до 4096. Значение по умолчанию — 1024
По умолчанию	По умолчанию кеш SA поддерживает 1024 сообщений SA
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для настройки емкости кеша SA устройства. Рекомендуется настроить эту команду, когда устройство запускается. Если емкость увеличивается во время работы MSDP, эта настройка не влияет на кеш SA, который изначально был изучен. Если емкость увеличивается во время работы MSDP, все кеши SA, которые первоначально были изучены с других устройств, или кеши SA, инициированные локальными устройствами, должны быть удалены и повторно изучены

8.4.7.4. Проверка

Завершите соединение с peer-ом MSDP. По истечении интервала повторного подключения проверьте, находится ли peer MSDP снова в состоянии UP.

8.4.7.5. Пример конфигурации

Установка интервала переподключения peer-a MSDP на 20 с

Сценарий:

Рисунок 8-11.

Шаги настройки	Установите peer-отношения MSDP между устройством A и устройством B. На устройстве A установите интервал повторного подключения peer-a MSDP равным 20 с
A	A#configure A(config)# ip msdp peer 20.0.0.4 connect-source gi0/1 A(config)# ip msdp description 20.0.0.4 peer-router-B A(config)# end A# show ip msdp peer 20.0.0.4 …… A#configure A(config)# ip msdp timer 20 A(config)# end
B	B# configure B(config)# ip msdp peer 20.0.0.3 connect-source gi0/1 B(config)# end
Проверка	• На устройстве B выключите и немедленно повторно подключитесь к peer-у MSDP. • Проверьте, находится ли peer MSDP в состоянии UP в течение 20 с
A	A#debug ip msdp timer
B	B# configure B(config)# show ip msdp peer 20.0.0.3

8.5. Мониторинг

8.5.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере важной информации и, таким образом, к прерыванию работы служб.

Описание	Команда
Сбрасывает TCP-соединение с указанным peer-ом MSDP	**clear ip msdp peer** *peer-address*
Очищает кеш SA	**clear ip msdp sa-cache** [*group-address*]
Очищает статистику узлов MSDP	**clear ip msdp statistics** [*peer-address*]

8.5.2. Отображение

Описание	Команда
Отображает количество источников и количество групп, созданных сообщениями SA	**show ip msdp count** [*as-number*]
Отображает информацию о mesh-группе	**show ip msdp mesh-group**
Отображает подробную информацию о peer-ах MSDP	**show ip msdp peer** [*peer-address*]
Отображает информацию о peer-е MSDP RPF, соответствующем указанному адресу инициатора	**show ip msdp rpf-peer** *ip-address*
Отображает изученную информацию (S, G)	**show ip msdpsa-cache** [*group-address* | *source-address*] [*group-address*| *source-address*] [*as-number*]
Отображает информацию (S, G), инициированную локальным устройством	**show ip msdpsa-originated**
Отображает краткую информацию обо всех peer-ах MSDP	**show ip msdp summary**

8.5.2.1. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Поэтому отключайте отладку сразу после использования.

Описание	Команда
Отладка peer-ов MSDP	**debug ip msdp peer**

9. НАСТРОЙКА IGMP SNOOPING

9.1. Обзор

Internet Group Management Protocol (IGMP) snooping — это механизм изучения IP multicast-маршрутизации. Он используется для управления и контроля пересылки multicast IP-трафика внутри VLAN, реализуя multicast-рассылку уровня 2.

Как показано на следующем Рисунке, когда устройство уровня 2 не выполняет IGMP snooping, multicast IP-пакеты передаются внутри VLAN; когда устройство уровня 2 выполняет IGMP snooping, multicast IP-пакеты передаются только участникам профиля.

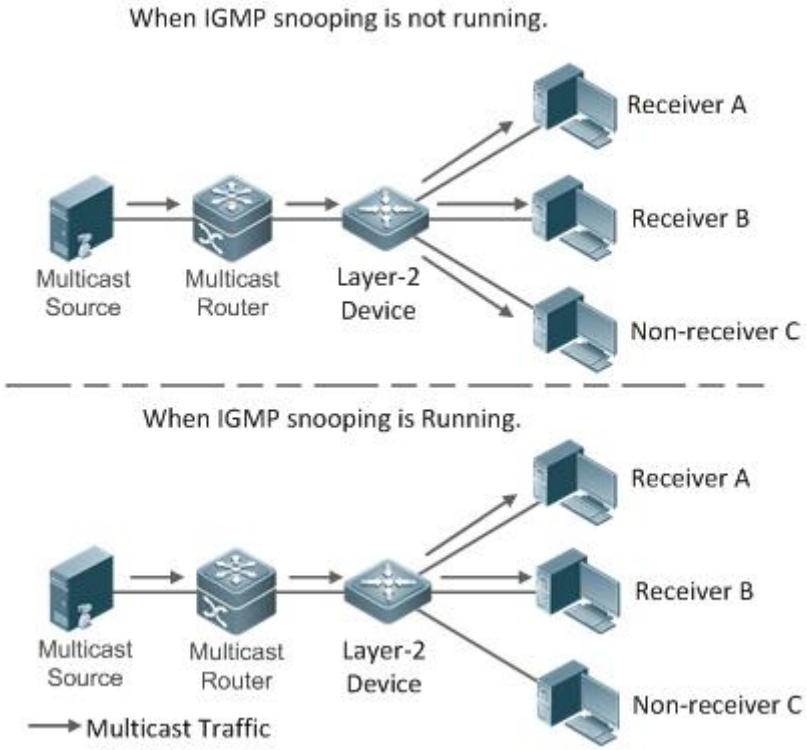

Рисунок 9-1. Сетевая топология IP multicast-пересылки внутри VLAN до и после запуска IGMP Snooping на устройстве уровня 2

9.1.1. Протоколы и стандарты

RFC4541: рекомендации для Snooping коммутаторам Internet Group Management Protocol (IGMP) и Multicast Listener Discovery (MLD).

9.2. Приложения

Приложение	Описание
Управление multicast-ом уровня 2	Обеспечивает точную пересылку multicast-пакетов уровня 2, чтобы избежать флудинга на этом уровне
Общие сервисы multicast (multicast-VLAN)	Несколько пользователей могут совместно использовать multicast-трафик одной и той же VLAN

Приложение	Описание
Премиум-каналы и предварительный просмотр	Управляет диапазоном адресов multicast, которые позволяют пользователю запрашивать и обеспечивает предварительный просмотр профилей, которые запрещено запрашивать

9.2.1. Управление multicast-ом уровня 2

9.2.1.1. Сценарий

Как показано на следующем Рисунке, multicast-пакеты передаются пользователям через коммутатор уровня 2. Когда управление multicast-рассылкой уровня 2 не выполняется, а именно, когда не реализовано IGMP snooping, multicast-пакеты рассылаются всем пользователям, включая тех, кто не должен получать эти пакеты. После реализации IGMP snooping multicast-пакеты из профиля IP multicast-маршрутизации больше не будут транслироваться внутри VLAN, а будут передаваться назначенным получателям.

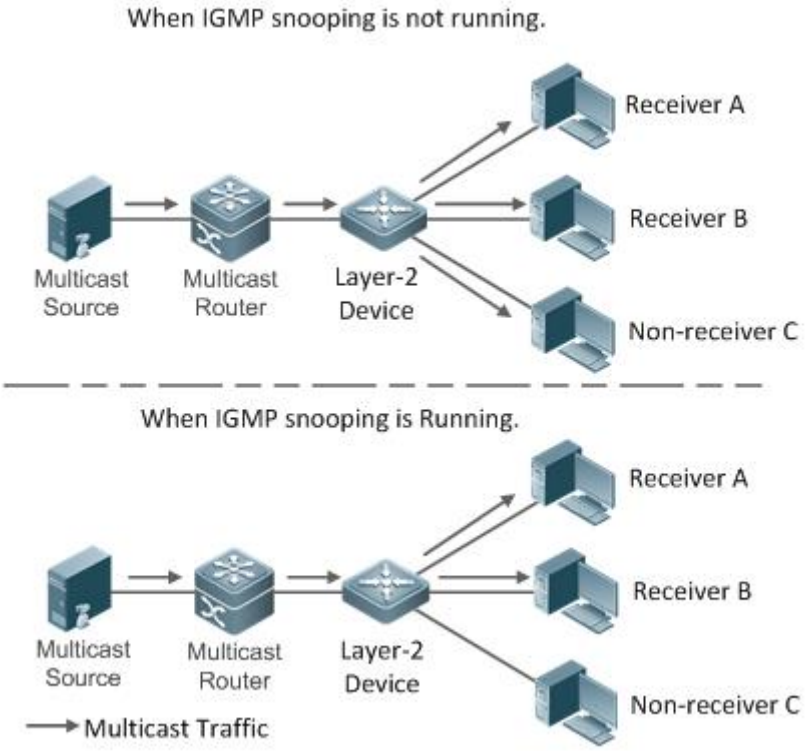

Рисунок 9-2. Сетевая топология реализации управления multicast-рассылкой уровня 2 (multicast VLAN)

9.2.1.2. Развертывание

Настройте базовые функции IGMP snooping.

9.2.2. Общие сервисы multicast (multicast-VLAN)

9.2.2.1. Сценарий

В режиме Shared VLAN Group Learning (SVGL) или режиме IVGL-SVGL (IVGL Independent VLAN Group Learning) устройство, выполняющее IGMP snooping, может предоставлять общие сервисы multicast (или сервисы multicast VLAN) пользователям VLAN. Обычно эта функция используется для предоставления одних и тех же сервисов video-on-demand (VOD) нескольким пользователям VLAN.

На следующем Рисунке показана работа устройства multicast уровня 2 в режиме SVGL IGMP snooping. Маршрутизатор multicast отправляет multicast-пакет в VLAN 1, а устройство multicast уровня 2 автоматически передает пакет в VLAN 1, VLAN 2 и VLAN 3. Таким образом, сервисы multicast VLAN 1 совместно используются VLAN 2 и VLAN. 3.

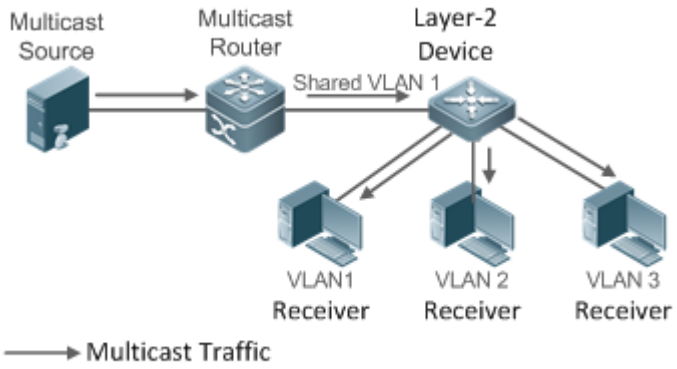

Рисунок 9-3. Сетевая топология общих сервисов multicast (multicast VLAN)

ПРИМЕЧАНИЕ: если multicast-устройство уровня 2 работает в режиме IVGL, маршрутизатор должен отправить пакет в каждую VLAN, что приводит к потере пропускной способности и нагрузке на multicast-устройство уровня 2.

9.2.2.2. Развертывание

Настройте базовые функции IGMP snooping (в режиме SVGL или режиме IVGL-SVG).

9.2.3. Премиум-каналы и предварительный просмотр

9.2.3.1. Сценарий

В приложении VOD, ограничивая диапазон адресов multicast, к которым может получить доступ пользовательский хост, пользователи, не внесщие оплату, не смогут смотреть премиум-каналы. Тем не менее сервис предварительного просмотра предлагается пользователям, не внесшим оплату, прежде чем они решат, платить ли за нее.

Пользователи могут просматривать премиум-канал в течение определенного периода времени (например, 1 минуты) после запроса.

9.2.3.2. Развертывание

- Настройте базовые функции IGMP snooping (в любом рабочем режиме).
- Настройте диапазон адресов multicast, к которым может получить доступ пользователь.

- Включите функцию предварительного просмотра для профилей VOD, доступ к которым запрещен.

9.3. Функции

9.3.1. Базовые определения

Порты multicast-маршрутизатора и порты-участники

ПРИМЕЧАНИЕ: IGMP snooping основано на VLAN. Задействованные порты относятся к портам-участникам VLAN.

Устройство, выполняющее IGMP snooping, идентифицирует порты во VLAN как порты multicast-маршрутизатора или порты-участники, чтобы управлять и контролировать пересылку multicast IP-трафика внутри VLAN. Как показано на следующем Рисунке, когда IGMP snooping запускается на устройстве уровня 2, multicast-трафик поступает в порт multicast-маршрутизатора и выходит из портов-участников.

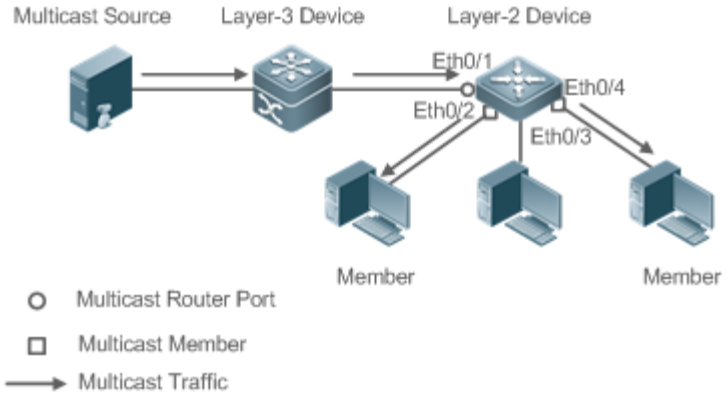

Рисунок 9-4. Сетевая топология двух портов IGMP snooping

- Порт маршрутизатора multicast: расположение источника multicast определяется портом устройства multicast уровня 2, которое подключено к маршрутизатору multicast (устройство multicast уровня 3). Прослушивая пакеты IGMP, устройство multicast уровня 2 может автоматически определять порт multicast-маршрутизатора и динамически поддерживать порт. Он также позволяет пользователям настраивать статический порт маршрутизатора.
- Порт-участник: порт находится на multicast-устройстве уровня 2 и подключен к хостам-участникам. Он направляет участников профиля. Его также называют Listener-порт. Прослушивая пакеты IGMP, устройство multicast уровня 2 может автоматически определять порт-участник и динамически поддерживать порт. Это также позволяет пользователям настраивать статический порт-участник.

Запись пересылки IGMP Snooping

Устройство, выполняющее IGMP snooping, пересылает multicast IP-пакеты в соответствии с записью пересылки IGMP snooping.

Запись пересылки IGMP snooping включает в себя следующие элементы: адрес источника (S), адрес профиля (G), идентификатор VLAN (VLAN_ID), порт multicast-маршрутизатора и порт-участник. Это указывает на то, что пакеты необходимых функций (включая S, G и VLAN_ID) должны входить в порт multicast-маршрутизатора и выходить из порта-участника. Запись пересылки IGMP snooping идентифицируется с использованием группы из S, G и VLAN_ID.

Чтобы отобразить запись о пересылке IGMP snooping, выполните команду **show ip igmp snooping gda-table**.

9.3.2. Обзор

Особенность	Описание
Прослушивание пакетов IGMP	Обнаруживает и идентифицирует порт маршрутизатора и порт-участник для создания и обслуживания записей пересылки IGMP snooping
Режимы работы IGMP Snooping	Предоставляет независимые или совместные сервисы multicast для пользовательской VLAN
Управление безопасностью IGMP	Управляет объемом и нагрузкой сервиса multicast для предотвращения нелегального multicast-трафика
IGMP-профиль	Определяет диапазон адресов multicast, которые разрешают или запрещают запросы пользователей на обращение к другим функциям
IGMP QinQ	Устанавливает режим пересылки multicast-пакетов на интерфейсе QinQ
IGMP Querier	В сети без устройства multicast уровня 3 устройство multicast уровня 2 действует как IGMP querier

9.3.3. Прослушивание пакетов IGMP

Устройство, выполняющее IGMP snooping, анализирует полученные пакеты IGMP, находит и идентифицирует порт маршрутизатора и порт-участник, используя эти пакеты, тем самым создавая и обслуживая запись IGMP snooping.

9.3.3.1. Принцип работы

Устройство, выполняющее IGMP snooping, может идентифицировать и обрабатывать следующие типы пакетов IGMP:

Пакеты Query

ПРИМЕЧАНИЕ: IGMP querier периодически отправляет пакеты General Query. Когда IGMP querier получает пакеты Leave, он отправляет пакеты Group-Specific Query.

Когда устройство, выполняющее IGMP snooping, получает пакеты Query, оно выполняет следующие операции внутри VLAN:

- Пересылайте пакеты Query IGMP на все порты (кроме порта приема этих пакетов).
- Если принимающий порт является портом динамического маршрутизатора, сбрасывается таймер устаревания. По истечении времени таймера порт больше не будет использоваться в качестве порта динамического маршрутизатора.
- Если принимающий порт не является портом динамического маршрутизатора, используйте его как порт динамического маршрутизатора и включите таймер

устаревания. По истечении времени таймера порт больше не будет использоваться в качестве порта динамического маршрутизатора.

- Для General Query сбрасывается таймер устаревания для всех динамических портов-участников. По истечении времени таймера порт больше не будет использоваться в качестве динамического порта для general-группы. По умолчанию максимальное время ответа, передаваемое пакетами Query IGMP, используется в качестве времени ожидания таймера устаревания. Если запущено **ip igmp snooping query-max-response-time**, отображаемое время используется как время ожидания таймера устаревания.
- Для назначенных пакетов Query сбрасывается таймер устаревания для всех динамических портов-участников назначенного профиля. По истечении времени таймера порт больше не будет использоваться в качестве динамического порта-участника назначенного профиля. По умолчанию максимальное время ответа, передаваемое пакетами Query IGMP, используется в качестве времени ожидания таймера устаревания. Если запущено **ip igmp snooping query-max-responsetime**, отображаемое время используется как время ожидания таймера устаревания.
- Если динамическое изучение порта маршрутизатора отключено, IGMP snooping не будет изучать порт динамического маршрутизатора.

Пакеты Report

ПРИМЕЧАНИЕ: когда хост-участник получает Query, он отвечает на него пакетом Report. Если хост запросит присоединение к профилю, он также отправит Report.

ПРИМЕЧАНИЕ: IGMP по умолчанию обрабатывает пакеты IGMPv1 и IGMPv2. Для пакетов Report IGMPv3: Продукты QTECH обрабатывают только информацию о группе, содержащуюся в пакетах.

Когда устройство, выполняющее IGMP snooping, получает пакеты Report, оно выполняет следующие операции внутри VLAN:

- Пересылайте пакеты Report со всех портов маршрутизатора. После выполнения команды **ip igmp snooping suppression enable** в одном цикле Query IGMP будет пересылаться только первый Report, полученный каждым профилем.
- Если порт, на котором принимаются пакеты Report, является динамическим портом-участником, сбросьте таймер устаревания. По истечении времени таймера порт больше не будет использоваться в качестве динамического порта-участника назначенного профиля.
- Если порт, на котором принимаются пакеты Report, не является динамическим портом-участником, используйте его как динамический порт-участник и включите таймер устаревания. По истечении времени таймера порт больше не будет использоваться в качестве динамического порта-участника назначенного профиля.

Пакеты Leave

ПРИМЕЧАНИЕ: если хост запрашивает выход из профиля, он отправит пакет Leave.

Когда устройство, выполняющее IGMP snooping, получает пакеты Leave, оно выполняет следующие операции внутри VLAN:

- Пересылает пакеты Leave со всех портов маршрутизатора.
- Если порт, на котором принимаются пакеты Leave, является динамическим портом-участником и функция Leave включена, порт будет немедленно удален из записи пересылки IGMP snooping назначенного профиля и больше не будет использоваться в качестве динамического порта-участника.

- Если порт, на котором принимаются пакеты Leave, является динамическим портом-участником и функция Leave отключена, состояние порта должно сохраняться.

9.3.3.2. Сопутствующая конфигурация

Настройка статический порта маршрутизатора

Запустите команду **ip igmp snooping vlan mrouter interface**, чтобы настроить статический порт маршрутизатора.

Настройка статического порта-участника

Запустите команду **ip igmp snooping vlan static interface**, чтобы настроить статический порт-участник.

Включение подавления Report-ов

По умолчанию подавление Report-ов отключено.

Запустите команду **ip igmp snooping suppression enable**, чтобы включить подавление Report-ов.

После включения подавления Report-ов в одном цикле Query IGMP будет пересылаться только первый пакет Report, полученный каждым профилем. Исходный MAC-адрес пересылаемого Report-а будет изменен на MAC-адрес устройства.

Включение немедленного выхода (Immediate Leave)

По умолчанию Immediate Leave отключен.

Запустите команду **ip igmp snooping fast-leave enable**, чтобы включить Immediate Leave.

Включение динамического изучения порта маршрутизатора

Динамическое изучение портов маршрутизатора включено по умолчанию.

Запустите команду **no ip igmp snooping mrouter learn pim-dvmrp**, чтобы отключить динамическое изучение порта маршрутизатора.

Запустите команду **no ip igmp snooping vlan** *vid* **mrouter learn pim-dvmrp**, чтобы отключить динамическое изучение портов маршрутизатора для назначенных VLAN.

Настройка времени устаревания порта динамического маршрутизатора

Время устаревания по умолчанию составляет 300 с.

Когда порт динамического маршрутизатора получает пакет Query, таймер устаревания порта включается или сбрасывается; если время устаревания не настроено, в качестве времени устаревания используется максимальное время ответа, переносимое пакетом Query.

Запустите **ip igmp snooping dyn-mr-aging-time**, чтобы настроить время устаревания порта динамического маршрутизатора.

Настройка времени устаревания динамического порта-участника

Время устаревания по умолчанию составляет 260 с.

Когда динамический порт-участник получает пакет Query, таймер устаревания порта включается или сбрасывается, а время устаревания представляет собой максимальное время ответа, переносимое пакетом Query.

Когда динамический порт-участник получает пакет Report, таймер устаревания порта включается или сбрасывается, а время устаревания представляет собой максимальное время ответа динамического порта-участника.

Запустите **ip igmp snooping host-aging-time**, чтобы настроить время устаревания динамического порта-участника.

Настройка максимального времени ответа пакета Query

Максимальное время ответа пакета Query не настроено по умолчанию, и используется максимальное время ответа, переносимое пакетом Query.

Запустите **ip igmp snooping query-max-response-time**, чтобы настроить максимальное время ответа пакета Query.

9.3.4. Режимы работы IGMP Snooping

Устройство, работающее в трех режимах (IVGL, SVGL и IVGL-SVGL) IGMP snooping, может предоставлять независимые сервисы multicast или совместные сервисы multicast для пользовательской VLAN.

9.3.4.1. Принцип работы

IVGL

В режиме IVGL устройство, выполняющее IGMP snooping, может предоставлять независимые сервисы multicast каждой пользовательской VLAN.

Независимые сервисы multicast указывают, что multicast-трафик может пересылаться только в пределах той VLAN, к которой он принадлежит, и пользовательский хост может подписаться на multicast-трафик в той VLAN, к которой принадлежит хост.

SVGL

В режиме SVGL устройство, выполняющее IGMP snooping, может предоставлять совместные сервисы multicast пользовательской VLAN.

Совместные сервисы multicast могут предоставляться только в Shared VLAN и sub VLAN, и используются адреса multicast SVGL. В Shared VLAN multicast-трафик в диапазоне адресов multicast SVGL пересылается в sub VLAN, и пользовательские хосты внутри sub VLAN подписываются на такой multicast-трафик из Shared VLAN.

- В Shared VLAN и sub VLAN совместные сервисы multicast будут предоставляться для multicast-трафика в диапазоне адресов multicast SVGL. Другой multicast-трафик будет отброшен.
- Другие VLAN (кроме Shared VLAN и sub VLAN) применяются к независимым сервисам multicast.

ПРИМЕЧАНИЕ: когда для пользовательской VLAN установлена Shared VLAN или sub VLAN, предоставляются совместные сервисы multicast. Когда пользовательская VLAN настроена на другие VLAN, предоставляются независимые сервисы multicast.

IVGL-SVGL

Режим IVGL-SVGL также называется гибридным режимом. В этом режиме устройство, выполняющее IGMP snooping, может предоставлять как совместные, так и независимые сервисы multicast пользовательской VLAN.

- В Shared VLAN и sub VLAN сервисы multicast будут предоставляться multicast-трафику в профиле SVGL. Для остального multicast-трафика будут предоставляться независимые сервисы multicast.
- Другие VLAN (кроме Shared VLAN и sub VLAN) применяются к независимым сервисам multicast.

ПРИМЕЧАНИЕ: когда пользовательская VLAN настроена как Shared VLAN или sub VLAN, доступны как совместные сервисы multicast, так и независимые сервиса multicast. Если

пользовательская VLAN настроена как VLAN, отличная от Shared VLAN и sub VLAN, доступны только независимые сервисы multicast.

9.3.4.2. Сопутствующая конфигурация

Включение IGMP Snooping и выбор режима работы

IGMP snooping отключено по умолчанию.

Запустите команду **ip igmp snooping ivgl**, чтобы включить IGMP snooping в режиме IVGL.

Запустите команду **ip igmp snooping svgl**, чтобы включить IGMP snooping в режиме SVGL.

Запустите команду **ip igmp snooping ivgl-svgl**, чтобы включить IGMP snooping в режиме IVGL-SVGL.

При включении IGMP snooping необходимо указать рабочий режим, а именно, должен быть выбран один из предыдущих рабочих режимов.

Настройка Shared VLAN

По умолчанию Shared VLAN является VLAN 1.

Запустите команду **ip igmp snooping svgl vlan**, чтобы назначить VLAN как Shared VLAN.

В режимах SVGL и IVGL-SVGL только одна VLAN может быть настроена как Shared VLAN.

Настройка sub VLAN

По умолчанию sub VLAN является любая VLAN, кроме Shared VLAN.

Запустите команду **ip igmp snooping svgl subvlan**, чтобы назначить VLAN в качестве sub VLAN.

В режимах SVGL и IVGL-SVGL количество sub VLAN не ограничено.

Настройка профиля SVGL

Нет настроек по умолчанию.

Запустите команду **ip igmp snooping svgl profile** *profile_num*, чтобы настроить диапазон адресов профиля SVGL.

ПРИМЕЧАНИЕ: в режиме SVGL и режиме IVGL-SVGL необходимо настроить диапазон профиля SVGL; в противном случае совместные сервисы multicast не могут быть предоставлены.

9.3.5. Управление безопасностью IGMP

Устройство, выполняющее IGMP snooping, может контролировать объем и нагрузку сервиса multicast, а также эффективно предотвращает незаконный multicast-трафик.

9.3.5.1. Принцип работы

Настройка фильтрации профилей по требованию пользователя

Настроив список профилей, к которым может получить доступ пользователь, вы можете настроить объем сервиса multicast, чтобы гарантировать интерес операторов и предотвратить незаконный multicast-трафик.

Чтобы включить эту функцию, вам следует использовать профиль, чтобы определить диапазон адресов multicast, к которым разрешен доступ.

- Когда профиль применяется к VLAN, вы можете определить адреса multicast, к которым пользователю разрешен доступ внутри VLAN.
- Когда профиль применяется к интерфейсу, вы можете определить адреса multicast, к которым пользователю разрешен доступ через порт.

Предварительный просмотр multicast

Если поставщик сервисов хочет разрешить пользователям просматривать некоторый multicast видеотрафик, к которому запрещается доступ пользователей, и остановить multicast видеотрафик после достижения продолжительности предварительного просмотра, должна быть предусмотрена функция multicast предварительного просмотра на основе пользователя. Функция предварительного просмотра multicast используется вместе с контролем разрешений multicast. Например, в приложении видеоадминистратор контролирует некоторые премиум-каналы, запуская команду **ip igmp profile** на порту или VLAN. Таким образом, отписавшиеся пользователи не смогут смотреть эти каналы по запросу. Если пользователи хотят просмотреть каналы до того, как они решат, платить за просмотр или нет, можно включить функцию multicast предварительного просмотра, позволяющую пользователям без оплаты просматривать премиум-каналы в течение определенного периода времени (например, 1 минуты).

Управление максимальным количеством профилей, разрешенных для одновременного запроса

Если одновременно запрашивается слишком много multicast-трафика, устройство будет сильно нагружено. Настройка максимального количества профилей, разрешенных для одновременного запроса, может гарантировать пропускную способность.

- Вы можете глобально ограничить количество профилей, разрешенных для одновременного запроса.
- Вы также можете ограничить количество профилей, разрешенных для одновременных запросов на порту.

Управление входом multicast-трафика

Запустив команду **ip igmp snooping source-check port**, чтобы включить проверку порта источника, вы можете ограничить ввод multicast-трафика для предотвращения нелегального трафика.

- Если проверка порта источника включена, легальным считается только multicast-трафик, поступающий с порта маршрутизатора; трафик из других портов считается нелегальным и будет отброшен.
- Когда проверка порта источника отключена, трафик, поступающий с любого порта, считается легальным.

Настройка проверки IP-адреса источника для multicast-трафика

Включив проверку IP-адреса источника, вы можете ограничить IP-адрес multicast-трафика, чтобы предотвратить незаконный трафик.

Проверка IP-адреса источника включает проверку исходных IP-адресов определенных профилей и профилей по умолчанию.

- Проверка исходных IP-адресов профилей по умолчанию (также называемая исходной проверкой сервера по умолчанию): указывает исходные IP-адреса для всех профилей multicast во всех VLAN. Легальным считается только multicast-трафик, IP-адрес источника которого совпадает с заданным.
- Проверка исходных IP-адресов определенных профилей (также называемая limit-ipmc): указывает исходные IP-адреса для определенных профилей multicast в определенных VLAN. Среди multicast-трафика, полученного от конкретных профилей multicast внутри VLAN, только тот, у которого IP-адрес источника совпадает с заданным, считается легальным и будет пересылаться устройством multicast; другой трафик будет отброшен.

9.3.5.2. Сопутствующая конфигурация

Настройка фильтрации профилей

По умолчанию профили не фильтруются и разрешают доступ пользователей.

Чтобы отфильтровать профили multicast, запустите команду **ip igmp snooping filter** в режиме конфигурации интерфейса или режиме глобальной конфигурации.

Включение предварительного просмотра

Предварительный просмотр не включен по умолчанию.

Запустите команду **ip igmp snooping preview**, чтобы включить предварительный просмотр и ограничить диапазон профилей, разрешенных для предварительного просмотра multicast.

Запустите **ip igmp snooping preview interval**, чтобы установить продолжительность предварительного просмотра multicast.

Настройка максимального количества профилей, разрешенных для одновременного запроса на порту

По умолчанию количество профилей, разрешенных для одновременного запроса, не ограничено.

Запустите команду **ip igmp snooping max-groups**, чтобы настроить максимальное количество профилей, разрешенных для одновременного запроса.

Настройка максимального количества профилей multicast, разрешенных глобально

По умолчанию максимальное количество профилей multicast, разрешенное в глобальном масштабе, составляет 65 536.

Запустите команду **ip igmp snooping l2-entry-limit**, чтобы настроить максимальное количество профилей multicast, разрешенных глобально.

Включение проверки порта источника

По умолчанию проверка порта источника не настроена.

Запустите команду **ip igmp snooping source-check port**, чтобы включить проверку порта источника.

Включение проверки IP-адреса источника

По умолчанию проверка IP-адреса источника отключена.

- Запустите команду **ip igmp snooping source-check default-server** *address*, чтобы включить проверку IP-адреса источника и указать IP-адрес источника по умолчанию (применимо к любому профилю любой VLAN).
- (Необязательно) Запустите команду **ip igmp snooping limit-ipmc vlan** *vid* **address** *group-address* **server** *sourceaddress*, чтобы указать конкретный IP-адрес источника для определенного профиля конкретной VLAN (применимо к определенному профилю конкретной VLAN).

Сначала необходимо включить проверку IP-адреса источника, чтобы указать адрес источника по умолчанию, а затем можно указать конкретный адрес источника для определенного профиля конкретной VLAN. Если адрес источника указан для определенного профиля конкретной VLAN, multicast-трафик определенного профиля будет проверять адрес источника, указанный этой командой. Другой multicast-трафик будет проверять адреса источника по умолчанию.

9.3.6. IGMP-профиль

Профиль multicast используется для определения диапазона адресов multicast, которые разрешают или запрещают пользователю запросить ссылку на другие функции.

9.3.6.1. Принцип работы

Профиль используется для определения диапазона адресов multicast.

Когда режим SVGL включен, профиль SVGL используется для определения диапазона адресов multicast SVGL.

Когда фильтр multicast настроен на интерфейсе, профиль используется для определения диапазона адресов multicast, которые разрешают или запрещают запросы пользователя в интерфейсе.

Когда настроен фильтр VLAN, профиль используется для определения диапазона адресов multicast, которые разрешают или запрещают запросы пользователей внутри VLAN.

Когда функция предварительного просмотра включена, профиль используется для определения диапазона адресов multicast, разрешенных для предварительного просмотра.

9.3.6.2. Сопутствующая конфигурация

Настройка профиля

Конфигурация по умолчанию:

- Создайте профиль, который по умолчанию **deny** (запрещен).

Шаги настройки:

- Запустите команду **ip igmp profile** *profile-number*, чтобы создать профиль.
- Запустите команду **range** *low-address high_address*, чтобы определить диапазон адресов multicast. Для каждого профиля настроено несколько диапазонов адресов.
- (Необязательно) Запустите команду **permit** или **deny**, чтобы разрешить или отклонить запрос пользователя (по умолчанию **deny**). Для каждого профиля можно настроить только одну команду **permit** или **deny**.

9.3.7. IGMP QinQ

9.3.7.1. Принцип работы

На устройстве с включенным IGMP snooping и настроенным портом dot1q-tunnel (QinQ) IGMP snooping будет обрабатывать пакеты IGMP, полученные портом QinQ, используя следующие два подхода:

- Подход 1. Создайте запись multicast во VLAN, где расположены пакеты IGMP. Пересылка пакетов IGMP во VLAN, где эти пакеты расположены, называется прозрачной передачей. Например, предположим, что для устройства включено IGMP snooping, порт A обозначен как порт QinQ, VLAN по умолчанию для этого порта — VLAN 1, и он разрешает прохождение пакетов VLAN 1 и VLAN 10. Когда пакет Query multicast отправляется из VLAN 10 на порт A, IGMP snooping устанавливает запись multicast для VLAN 10 и пересылает пакет Query multicast на порт маршрутизатора VLAN 10.
- Подход 2. Создайте запись multicast во VLAN по умолчанию порта QinQ. Инкапсулируйте multicast-пакет с помощью тега VLAN виртуальной локальной сети по умолчанию, в которой расположен порт QinQ, и пересылайте пакет в

пределах VLAN по умолчанию. Например, предположим, что для устройства включено IGMP snooping, порт A обозначен как порт QinQ, VLAN по умолчанию для этого порта — VLAN 1, и он разрешает прохождение пакетов VLAN 1 и VLAN 10. Когда пакет Query multicast отправляется из VLAN 10 на порт A, IGMP snooping устанавливает запись multicast для VLAN 1, инкапсулирует пакет Query multicast с тегом VLAN 1 и пересылает пакет на порт маршрутизатора VLAN 1.

9.3.7.2. Сопутствующая конфигурация

Настройка QinQ

По умолчанию IGMP snooping работает в режиме, указанном в подходе 2.

Запустите команду **ip igmp snooping tunnel**, чтобы реализовать подход 1.

9.3.8. IGMP Querier

В сети с устройством multicast уровня 3 это устройство multicast уровня 3 действует как IGMP querier. В этом случае устройству уровня 2 достаточно только прослушивать пакеты IGMP, чтобы установить и обслуживать запись пересылки, реализуя multicast-рассылку уровня 2.

В сети без устройства multicast уровня 3 устройство multicast уровня 2 должно быть настроено с функцией IGMP querier, чтобы устройство могло прослушивать пакеты IGMP. В этом случае устройству уровня 2 необходимо действовать как IGMP querier, а также прослушивать пакеты IGMP, чтобы установить и поддерживать запись пересылки для реализации multicast уровня 2.

9.3.8.1. Принцип работы

Устройство уровня 2 действует как IGMP querier, периодически отправляя пакеты Query IGMP, прослушивая и обслуживая пакеты Report IGMP, на которые отвечает пользователь, а также создает запись multicast-пересылки уровня 2. Вы можете настроить соответствующие параметры пакетов Query, отправляемых IGMP querier, посредством конфигурации.

Когда устройство получает пакет Protocol-Independent Multicast (PIM) или Distance Vector Multicast Routing Protocol (DVMRP), оно считает, что в сети существует маршрутизатор multicast, который будет действовать как IGMP querier, и отключает функцию querier. Таким образом, маршрутизация IGMP не будет затронута.

Когда устройство получает пакеты Query IGMP от других устройств, оно будет конкурировать с другими устройствами за IGMP querier.

Включение функции Querier

Вы можете включить querier для конкретной VLAN или для всех VLAN.

Только когда функция глобального querier включена, запросы для определенных VLAN могут вступить в силу.

Указание версии IGMP для Querier

Версия IGMP, используемая для отправки пакетов Query, может быть настроена как IGMPv1 или IGMPv2.

Настройка IP-адреса источника Querier

Вы можете настроить IP-адрес источника пакета Query, отправленного querier, на основе VLAN.

Если IP-адрес источника querier не настроен, querier не вступит в силу.

Настройка интервала запроса Querier

Вы можете настроить интервалы отправки глобальных пакетов Query на основе разных querier-ов в разных VLAN.

Настройка максимального времени ответа пакета Query

Вы можете настроить максимальное время ответа, передаваемое пакетом Query, отправленным querier. Поскольку IGMPv1 не поддерживает передачу максимального времени ответа пакетом Query, эта конфигурация не вступает в силу, когда querier использует IGMPv1. Вы можете настроить разное максимальное время ответа для querier-ов в разных VLAN.

Настройка времени устаревания Querier

Если в сети существуют другие запросы IGMP, существующее устройство будет конкурировать с другими querier-ами. Если существующее устройство не может быть выбрано и находится в состоянии non-querier, таймер устаревания querier-а будет включен. По истечении времени таймера другие querier-ы в сети считаются истекшими, и существующее устройство будет возобновлено в качестве querier.

9.3.8.2. Сопутствующая конфигурация

Включение функции Querier

По умолчанию функция querier устройства отключена.

Запустите команду **ip igmp snooping querier**, чтобы включить функцию глобального querier.

Запустите команду **ip igmp snooping vlan** *num* **querier**, чтобы включить функцию querier для определенных VLAN.

Указание версии IGMP для Querier

По умолчанию querier использует IGMPv2.

Запустите команду **ip igmp snooping querier version**, чтобы настроить глобальную версию querier.

Запустите команду **ip igmp snooping vlan querier version**, чтобы указать версию querier для конкретных VLAN.

Настройка IP-адреса источника Querier

По умолчанию IP-адрес источника Querier равен 0.

Запустите команду **ip igmp snooping querier address**, чтобы включить глобальные IP-адреса источника querier-ов.

Запустите команду **ip igmp snooping vlan querier address**, чтобы указать IP-адреса источника querier-ов в определенных VLAN.

Настройка Query интервала Querier-а

По умолчанию интервал Query составляет 60 секунд.

Запустите команду **ip igmp snooping querier query-interval**, чтобы включить глобальный интервал Query для querier-ов.

Запустите **ip igmp snooping vlan querier query-interval**, чтобы указать глобальный интервал Query для querier-ов в определенных VLAN.

Настройка максимального времени ответа пакета Query

По умолчанию максимальное время ответа пакета Query составляет 10 с.

Запустите команду **ip igmp snooping querier max-response-time**, чтобы настроить максимальное время ответа пакетов Query, отправляемых глобальными querier-ами.

Запустите команду **ip igmp snooping vlan querier max-response-time**, чтобы указать максимальное время ответа пакетов Query, отправленных querier-ами в определенных VLAN.

Настройка времени устаревания Querier

По умолчанию время устаревания querier-а составляет 125 с.

Запустите команду **ip igmp snooping querier max-response-time**, чтобы настроить время устаревания глобальных querier-ов.

Запустите команду **ip igmp snooping vlan querier max-response-time**, чтобы настроить время устаревания querier-ов в определенных VLAN.

9.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций IGMP snooping (режим IVGL)	Должен быть выбран любой из режимов IVGL, SVGL и IVGL-SVGL	
	ip igmp snooping ivgl	Включает глобальное IGMP snooping в режиме IVGL
	no ip igmp snooping vlan *num*	Отключает IGMP snooping для VLAN
Настройка основных функций IGMP snooping (режим SVGL)	Должен быть выбран любой из режимов IVGL, SVGL и IVGL-SVGL. Он используется для включения IGMP snooping в режиме SVGL	
	ip igmp snooping svgl	Включает глобальное IGMP snooping в режиме IVGL
	no ip igmp snooping vlan *num*	Отключает IGMP snooping для VLAN
	ip igmp snooping svgl profile *profile_num*	Настраивает профиль SVGL
	ip igmp snooping svgl vlan	Указывает SVGL Shared VLAN
	ip igmp snooping svgl subvlan	Указывает SVGL sub VLAN

Конфигурация	Описание и команда	
Настройка основных функций IGMP snooping (режим IVGL-SVGL)	Должен быть выбран любой из режимов IVGL, SVGL и IVGL-SVGL. Он используется для включения IGMP snooping в режиме IVGL-SVGL	
	ip igmp snooping ivgl-svgl	Включает глобальное IGMP snooping в режиме IVGL-SVGL
	no ip igmp snooping vlan *num*	Отключает IGMP snooping для VLAN
	ip igmp snooping svgl profile *profile_num*	Настраивает профиль SVGL
	ip igmp snooping svgl vlan	Указывает SVGL Shared VLAN
	ip igmp snooping svgl subvlan	Указывает SVGL sub VLAN
Настройка обработки пакетов	(Опционально) Он используется для настройки соответствующих конфигураций обработки пакетов протокола	
	ip igmp snooping vlan *vlan-id* **mrouter interface** *interface-id*	Настраивает статический порт маршрутизатора
	ip igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*	Настраивает статический порт-участник
	ip igmp snooping vlan *vlan-id* **mrouter learn pim-dvmrp**	Включает динамическое изучение портов маршрутизатора
	ip igmp snooping dyn-mr-aging-time *time*	Настраивает время устаревания порта динамического маршрутизатора
	ip igmp snooping host-aging-time *time*	Настраивает время устаревания динамического порта-участника

Конфигурация	Описание и команда	
Настройка обработки пакетов	**ip igmp snooping fast-leave enable**	Включает функцию immediate-leave для динамического порта-участника
	ip igmp snooping query-max-response-time *time*	Настраивает максимальное время ответа пакета Query IGMP
	ip igmp snooping suppression enable	Включает подавление пакетов Report IGMP
Настройка управления безопасностью IGMP	(Опционально) Гарантируется безопасность, когда пользователь запрашивает профиль multicast	
	ip igmp snooping filter *profile-number*	Настраивает фильтрацию профилей для доступа пользователей
	ip igmp snooping vlan *num* **filter** *profile-number*	Настраивает фильтрацию профилей для каждой VLAN для доступа пользователей
	ip igmp snooping l2-entry-limit *number*	Настраивает максимальное количество профилей глобально для доступа пользователей
	ip igmp snooping max-groups *number*	Настраивает максимальное количество динамических профилей для доступа пользователей
	ip igmp snooping source-check port	Включает проверку IP-адреса источника, что гарантирует легальность multicast-трафика из порта маршрутизатора

Конфигурация	Описание и команда	
Настройка управления безопасностью IGMP	**ip igmp snooping source-check default-server** *address*	Включает проверку IP-адреса источника. Multicast-трафик, IP-адрес источника которого соответствует указанному IP-адресу источника, считается легальным трафиком
	ip igmp snooping limit-ipmc vlan *vid* **address** *group-address* **server** *source-address*	Указывает VLAN. В multicast-трафике multicast-адресов легальным трафиком считается тот, чей IP-адрес источника соответствует указанному IP-адресу источника
	ip igmp snooping preview *profile-number*	Включает функцию предварительного просмотра для указанного профиля
	ip igmp snooping preview interval *num*	Настраивает продолжительность предварительного просмотра
Настройка профиля IGMP	(Опционально) Он используется для определения диапазона адресов multicast, которые разрешают или запрещают доступ пользовательского хоста	
	ip igmp profile *profile-number*	Создает профиль
	range *low-address high_address*	Настраивает диапазон профиля
	permit	Разрешает доступ пользовательского хоста
	deny	Запрещает доступ пользовательского хоста
Настройка IGMP QinQ	(Опционально) Используется для настройки интерфейса QinQ для пересылки multicast-пакетов с использованием идентификатора VLAN (VID), переносимого пакетами	

Конфигурация	Описание и команда	
Настройка IGMP QinQ	**ip igmp snooping tunnel**	Настраивает QinQ для прозрачной передачи пакетов IGMP
Настройка IGMP Querier	(Опционально) Используется для включения функции querier IGMP в сети без устройства multicast уровня 3	
	ip igmp snooping querier	Включает функцию глобального querier
	ip igmp snooping vlan *num* **querier**	Включает querier для VLAN
	ip igmp snooping querier version *num*	Указывает версию IGMP для querier-ов глобально
	ip igmp snooping vlan *num* **querier version** *num*	Указывает версию IGMP для querier-а VLAN
	ip igmp snooping querier address *a.b.c.d*	Настраивает IP-адрес источника querier-ов глобально
	ip igmp snooping vlan *num* **querier address** *a.b.c.d*	Настраивает IP-адрес источника для querier-а VLAN
	ip igmp snooping querier query-interval *num*	Настраивает интервал Query для querier-ов глобально
	ip igmp snooping vlan *num* **querier query-interval** *num*	Настраивает интервал Query для querier-а VLAN
	ip igmp snooping querier max-response-time *num*	Настраивает максимальное время ответа для пакетов Query глобально
	ip igmp snooping vlan *num* **querier max-response-time** *num*	Настраивает максимальное время ответа пакетов Query для VLAN
	ip igmp snooping querier timer expiry *num*	Настраивает таймер устаревания для querier-ов глобально

Конфигурация	Описание и команда	
Настройка IGMP Querier	**ip igmp snooping vlan** *num* **querier timer expiry** *num*	Настраивает таймер устаревания для querier-a VLAN

9.4.1. Настройка основных функций IGMP snooping (режим IVGL)

9.4.1.1. Эффект конфигурации

- Включите IGMP snooping для реализации multicast уровня 2.
- Предоставьте независимые сервисы multicast для каждой VLAN.

9.4.1.2. Примечания

Multicast IP-адресация не может быть реализована в режиме SVGL. Если необходимо использовать multicast IP-адресацию, выберите режим IVGL.

9.4.1.3. Шаги настройки

Включение глобального IGMP snooping в режиме IVGL

Обязательный.

После того, как IGMP snooping включено глобально, эта функция будет включена для всех VLAN.

Если не указано иное, рекомендуется запустить глобальное IGMP snooping на всех устройствах, подключенных к хостам пользователей.

Отключение IGMP Snooping для VLAN

(Опционально) Вы можете использовать эту функцию, если хотите отключить IGMP snooping в определенных VLAN.

Только если глобальное IGMP snooping включено, его можно отключить в определенных VLAN.

В режиме IVGL каждая VLAN может пользоваться независимыми сервисами multicast. Отключение каких-либо сервисов multicast VLAN не повлияет на сервисы, предоставляемые другими.

9.4.1.4. Проверка

- Запустите команду **show ip igmp snooping gda-table**, чтобы отобразить таблицу пересылки IGMP snooping, и убедитесь, что порты-участники включают только те, которые подключаются к хостам-участникам.
- Запустите команду **show ip igmp snooping**, чтобы отобразить базовую информацию об IGMP snooping и убедиться, что IGMP snooping работает в режиме IVGL.

9.4.1.5. Связанные команды

Включение глобального IGMP snooping в режиме IVGL

Команда	**ip igmp snooping ivgl**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После выполнения этой команды IGMP snooping будет запущено во всех VLAN. По умолчанию IGMP snooping отключено

Отключение IGMP Snooping для VLAN

Команда	**show ip igmp snooping gda-table**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Только если глобальное IGMP snooping включено, его можно отключить в определенных VLAN. В режиме IVGL вы можете отключить IGMP snooping в любой VLAN

Отображение записи IGMP snooping

Команда	**show ip igmp snooping gda-table**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Эта команда используется для проверки того, что порты включают только те, которые подключаются к хостам-участникам

Отображение рабочего режима IGMP Snooping

Команда	**show ip igmp snooping**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если устройство работает в режиме IVGL, отображается следующая информация: IGMP Snooping running mode: IVGL

9.4.1.6. Пример конфигурации

Предоставление сервисов multicast уровня 2 для хостов подсети (Subnet)

Сценарий:

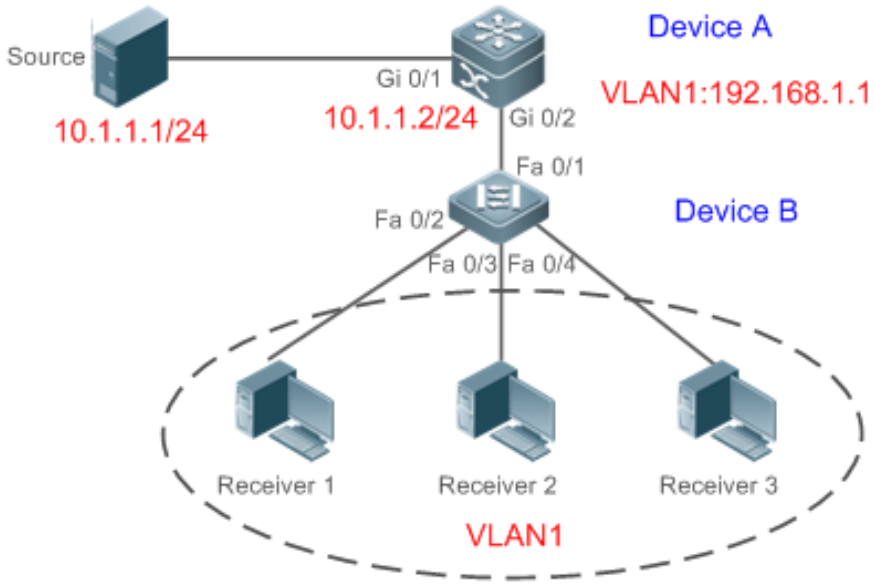

Рисунок 9-5.

	A — это маршрутизатор multicast, подключенный непосредственно к источнику multicast. B — устройство уровня 2, подключенное непосредственно к пользовательскому хосту. Приемник 1, Приемник 2 и Приемник 3 принадлежат VLAN 1
Шаги настройки	• Настройте IP-адрес и VLAN. • Включите multicast-маршрутизацию на A и включите протокол multicast-маршрутизации на интерфейсе уровня 3 (Gi0/1 и VLAN 1). • Включите IGMP snooping на B и выберите режим IVGL
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal

	B(config)# ip igmp snooping ivg
Проверка	Отправьте пакеты из источника (10.1.1.1) в G (229.1.1.1), чтобы добавить Приемник 1 в G. • Убедитесь, что пакеты (10.1.1.1 и 229.1.1.1) получены Приемником 1. • Отобразите запись переадресации IGMP snooping на B и убедитесь, что порт (10.1.1.1, 229.1.1.1, 1) включает только Fa0/2. • Проверьте, установлен ли рабочий режим IGMP snooping на IVGL
B	B# show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*,224.1.1.1, 1): VLAN(1) 2 OPORTS: FastEthernet 0/1(M) FastEthernet 0/2(D) B# show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65 536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Global Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds) vlan 1 ---------- IGMP Snooping state: Enable Multicast router learning mode: pim-dvmrp

	IGMP Fast-Leave: Disabled IGMP VLAN querier: Disable IGMP VLAN Mode: STATIC

9.4.1.7. Распространенные ошибки

Неправильный рабочий режим IGMP snooping.

9.4.2. Настройка основных функций IGMP snooping (режим SVGL)

9.4.2.1. Эффект конфигурации

- Включите IGMP snooping и выберите режим SVGL для реализации multicast уровня 2.
- Поделитесь сервисами multicast VLAN.

9.4.2.2. Шаги настройки

Включение глобального IGMP snooping в режиме SVGL

Обязательный.

Включите глобальное IGMP snooping в режиме SVGL.

Настройте диапазон связанных профилей SVGL.

Указание SVGL Shared VLAN

(Опционально) По умолчанию VLAN 1 используется как Shared VLAN. Вы можете настроить эту конфигурацию для других параметров.

Указание SVGL sub VLAN

(Опционально) По умолчанию все сети VLAN используются в качестве sub VLAN SVGL и могут совместно использовать сервисы multicast Shared VLAN. Вы можете настроить эту конфигурацию для других параметров.

9.4.2.3. Проверка

- Запустите команду **show ip igmp snooping**, чтобы отобразить базовую информацию о IGMP snooping и убедиться, что IGMP snooping работает в режиме SVGL.
- Запустите команду **show ip igmp snooping gda-table**, чтобы проверить правильность формирования записей multicast между VLAN.

9.4.2.4. Связанные команды

Включение глобального IGMP snooping в режиме SVGL

Команда	**ip igmp snooping svgl**
Командный режим	Режим глобальной конфигурации

Руководство по использованию	По умолчанию IGMP snooping отключено. После выбора режима SVGL необходимо связать диапазон профилей внутри адресов multicast SVGL

Настройка профиля SVGL

Команда	**ip igmp snooping svgl profile** *profile_num*
Описание параметра	*profile_num*: настраивает SVGL для связывания профиля
Командный режим	Режим глобальной конфигурации
Руководство по использованию	По умолчанию с SVGL не связан ни один профиль

Указание SVGL Shared VLAN

Команда	**ip igmp snooping svgl vlan** *vid*
Описание параметра	*vid*: указывает на VLAN
Командный режим	Режим настройки интерфейса
Руководство по использованию	По умолчанию VLAN 1 используется как Shared VLAN

Указание SVGL sub VLAN

Команда	**ip igmp snooping svgl subvlan** *vid-range*
Описание параметра	*vid-range*: указывает идентификатор VLAN или диапазон идентификаторов VLAN
Командный режим	Режим настройки интерфейса
Руководство по использованию	По умолчанию все сети VLAN, кроме Shared VLAN, используются как sub VLAN-ы

Отображение рабочего режима IGMP Snooping

Команда	**show ip igmp snooping**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если устройство работает в режиме SVGL, отображается следующая информация: IGMP Snooping running mode: SVGL

9.4.2.5. Пример конфигурации

Включение SVGL на устройстве доступа

Сценарий:

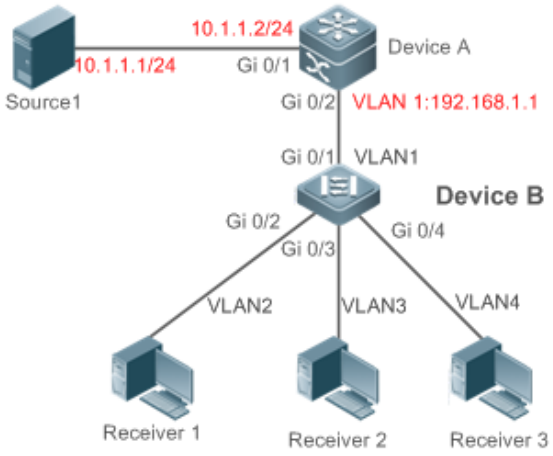

Рисунок 9-6.

	A — это маршрутизатор multicast, подключенный непосредственно к источнику multicast. B — устройство уровня 2, подключенное непосредственно к пользовательскому хосту. Приемник 1 подключен к VLAN 2, Приемник 2 подключен к VLAN 3, а Приемник 3 подключен к VLAN 4
Шаги настройки	• Настройте IP-адрес и VLAN. (пропущено) • Включите multicast-маршрутизацию на A и включите протокол multicast-маршрутизации на интерфейсе уровня 3 (Gi0/1 и VLAN 1). • Включите IGMP snooping на B и выберите режим SVGL. • Настройте диапазон связанных адресов multicast SVGL на B
A	A# configure terminal A(config)# ip multicast-routing

	A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#range 224.1.1.1 238.1.1.1 B(config-profile)#exit B(config)#ip igmp snooping svgl B(config)#ip igmp snooping svgl profile 1
Проверка	Отправьте пакеты из источника (10.1.1.1) в G (229.1.1.1) и добавьте Приемник 1, Приемник 2 и Приемник 3 в G. • Убедитесь, что пакеты (10.1.1.1 и 224.1.1.1) получены Приемником 1, Приемником 2 и Приемником 3. • Отобразите запись пересылки IGMP snooping на B и убедитесь, что порты (*, 224.1.1.1, 1) включают Gi0/2, Gi0/3 и Gi0/4. • Проверьте, является ли рабочим режимом IGMP snooping SVGL
B	B# show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*,224.1.1.1, 1): VLAN(2) 1 OPORTS: GigabitEthernet 0/2(D) VLAN(3) 1 OPORTS: GigabitEthernet 0/3(D) VLAN(4) 1 OPORTS: GigabitEthernet 0/4(D) B# show ip igmp snooping IGMP Snooping running mode: SVGL

	IGMP Snooping L2-entry-limit: 65 536 SVGL vlan: 1 SVGL profile number: 1 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

9.4.2.6. Распространенные ошибки

- Профиль SVGL не настроен.
- Отправленный multicast-трафик не входит в профиль SVGL.

9.4.3. Настройка основных функций IGMP snooping (режим IVGL-SVGL)

9.4.3.1. Эффект конфигурации

- Включите IGMP snooping и выберите режим IVGL-SVGL для реализации multicast уровня 2.
- Профили SVGL могут совместно использовать сервисы multicast.
- Профили, отличные от SVGL (non-SVGL), работают в режиме IVGL.

9.4.3.2. Шаги настройки

Включение глобального IGMP snooping в режиме IVGL-SVGL

Обязательный.

Включите глобальное IGMP snooping в режиме IVGL-SVGL.

Настройте диапазон связанных профилей SVGL.

Указание SVGL Shared VLAN

(Необязательно) По умолчанию VLAN 1 используется как Shared VLAN. Вы можете настроить эту конфигурацию для других параметров.

Указание SVGL sub VLAN

(Необязательно) По умолчанию все сети VLAN используются в качестве Sub VLAN SVGL и могут совместно использовать сервисы multicast Shared VLAN. Вы можете настроить эту конфигурацию для других параметров.

9.4.3.3. Проверка

- Запустите команду **show ip igmp snooping**, чтобы отобразить базовую информацию о IGMP snooping и убедиться, что IGMP snooping работает в режиме IVGL-SVGL.
- Запустите команду **show ip igmp snooping gda-table**, чтобы проверить, правильно ли сформированы записи multicast между VLAN (inter-VLAN) для профилей SVGL.
- Запустите команду **show ip igmp snooping gda-table**, чтобы проверить, правильно ли сформированы записи multicast внутри VLAN (intra-VLAN) для профилей SVGL.

9.4.3.4. Связанные команды

Включение глобального IGMP snooping в режиме IVGL-SVGL

Команда	**ip igmp snooping ivgl-svgl**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	По умолчанию IGMP snooping отключено. После выбора режима IVGL-SVGL необходимо связать профили SVGL

Настройка профиля SVGL

Команда	**ip igmp snooping svgl profile** *profile_num*
Описание параметра	*profile_num*: настраивает SVGL для связывания профиля
Командный режим	Режим глобальной конфигурации
Руководство по использованию	По умолчанию с SVGL не связан ни один профиль

Указание SVGL Shared VLAN

Команда	**ip igmp snooping svgl vlan** *vid*
Описание параметра	*vid*: указывает на VLAN
Командный режим	Режим настройки интерфейса
Руководство по использованию	По умолчанию VLAN 1 используется как Shared VLAN

Указание SVGL sub VLAN

Команда	**ip igmp snooping svgl subvlan** *vid-range*
Описание параметра	*vid-range*: указывает идентификатор VLAN или диапазон идентификаторов VLAN
Командный режим	Режим настройки интерфейса
Руководство по использованию	По умолчанию все сети VLAN, кроме Shared VLAN, используются как Sub VLAN

Отображение рабочего режима IGMP Snooping

Команда	**show ip igmp snooping**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если устройство работает в режиме SVGL, отображается следующая информация: IGMP Snooping running mode: SVGL

Отображение рабочего режима IGMP Snooping

Команда	**show ip igmp snooping**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если устройство работает в режиме IVGL-SVGL, отображается следующая информация: IGMP Snooping running mode: IVGL-SVGL

9.4.3.5. Пример конфигурации

Включение IVGL-SVGL на устройстве доступа

Сценарий:

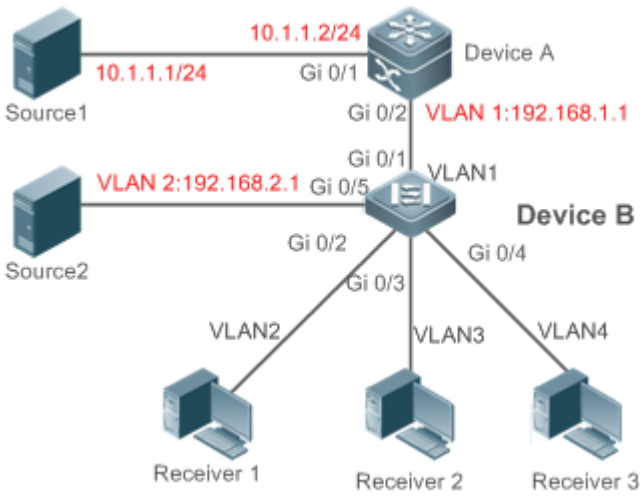

Рисунок 9-7.

	A является маршрутизатором multicast и подключен непосредственно к источнику multicast 1. B является устройством уровня 2 и подключено непосредственно к пользовательскому хосту и источнику multicast 2. Приемник 1 подключен к VLAN 2, Приемник 2 подключен к VLAN 3, а Приемник 3 подключен к VLAN 4
Шаги настройки	• Настройте IP-адрес и VLAN. • Включите multicast-маршрутизацию на A и включите протокол multicast-маршрутизации на интерфейсе уровня 3 (Gi0/1 и VLAN 1). • Включите IGMP snooping на B и выберите режим IVGL-SVGL. • Настройте диапазон связанных адресов multicast SVGL на B
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal

	B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#range 224.1.1.1 238.1.1.1 B(config-profile)#exit B(config)#ip igmp snooping ivgl-svgl B(config)#ip igmp snooping svgl profile 1
Проверка	Отправьте пакеты из источника 1 (10.1.1.1) в G (224.1.1.1) и добавьте приемник 1, приемник 2 и приемник 3 в G. Отправьте пакеты из источника 2 (192.168.2.1) в пункт назначения (239.1.1.1) и добавьте приемник 1 239.1.1.1. • Убедитесь, что пакеты (10.1.1.1 и 224.1.1.1) получены Приемником 1, Приемником 2 и Приемником 3. • Убедитесь, что пакеты (192.168.2.1 и 239.1.1.1) могут быть получены Приемником 1. • Отобразите запись переадресации IGMP snooping на B и убедитесь, что порты (*, 224.1.1.1, 1) включают Gi0/2, Gi0/3 и Gi0/4, а порт (*, 239.1.1.1, 1) — Gi0. /2. • Проверьте, является ли рабочий режим IGMP snooping IVGL-SVGL
B	B# show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*,224.1.1.1, 1): VLAN(2) 1 OPORTS: GigabitEthernet 0/2(D) VLAN(3) 1 OPORTS: GigabitEthernet 0/3(D) VLAN(4) 1 OPORTS: GigabitEthernet 0/4(D) (*,239.1.1.1, 2): VLAN(2) 1 OPORTS: GigabitEthernet 0/2(D) B# show ip igmp snooping IGMP Snooping running mode: IVGL-SVGL IGMP Snooping L2-entry-limit: 65 536

	SVGL vlan: 1 SVGL profile number: 0 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

9.4.3.6. Распространенные ошибки

- Профиль SVGL не настроен.
- Отправленный multicast-трафик не входит в профиль SVGL.
- Multicast-трафик IVGL не может пересылаться в профиле SVGL.

9.4.4. Настройка обработки пакетов

9.4.4.1. Эффект конфигурации

- Настройте указанные порты в качестве статических портов маршрутизатора для получения multicast-трафика из всех профилей.
- Настройте указанные порты в качестве статических портов-участников для получения multicast-трафика из указанных профилей.
- Включите подавление пакетов Report, чтобы пересылать только первый пакет Report из указанной VLAN или профиля на порт маршрутизатора в течение интервала Query, а следующие пакеты Report не будут пересылаться на порт маршрутизатора, тем самым уменьшая количество пакетов в сети.
- Настройте функцию Immediate-Leave для удаления порта из записи портов-участников, когда порт получает пакет Leave.
- Отключите динамическое изучение портов маршрутизатора, чтобы отключить изучение любого порта маршрутизатора.
- В зависимости от сетевой нагрузки и конфигурации multicast-устройства вы можете настроить время устаревания порта маршрутизатора и порта-участника, а также максимальное время ответа пакета Query.

9.4.4.2. Примечания

Только после настройки basic IGMP snooping соответствующие конфигурации вступят в силу.

9.4.4.3. Шаги настройки

Настройка статического порта маршрутизатора

- Опционально.
- Вы можете выполнить эту настройку, если хотите указать статический порт для приема всего multicast-трафика внутри VLAN.

Настройка статического порта-участника

- Опционально.
- Вы можете выполнить эту настройку, если хотите указать статический порт для приема определенного multicast-трафика в VLAN.

Включение подавления пакетов Report

- Опционально.
- Если имеется несколько получателей для получения пакетов из одного и того же профиля multicast, вы можете включить подавление пакетов Report, чтобы подавить количество отправляемых пакетов Report.

Включение функции Immediate-Leave

- Опционально.
- Если на порту имеется только один приемник, вы можете включить Leave, чтобы ускорить конвергенцию протокола после выхода.

Отключение динамического изучения порта маршрутизатора

- Опционально.
- Эта функция используется, когда multicast-трафик необходимо пересылать только в пределах топологии уровня 2, но не на маршрутизатор уровня 3.

Настройка времени устаревания порта динамического маршрутизатора

- Опционально.
- Эта функция используется, когда multicast-трафик необходимо пересылать только в пределах топологии уровня 2, но не на маршрутизатор уровня 3.

Настройка времени устаревания динамического порта-участника

- Опционально.
- Вы можете настроить время устаревания в зависимости от нагрузки на сеть.

Настройка максимального времени ответа пакета Query

- Опционально.
- Вы можете настроить время устаревания на основе интервала отправки пакетов Query IGMP подключенным multicast-маршрутизатором. Обычно время устаревания рассчитывается следующим образом: Интервал отправки пакетов Query IGMP x 2 + Максимальное время ответа пакетов IGMP.

9.4.4.4. Проверка

- Запустите команду **show ip igmp snooping mrouter**, чтобы проверить, имеет ли настроенный статический порт маршрутизатора букву «S» в отображаемой информации о конфигурации.
- Запустите команду **show ip igmp snooping gda**, чтобы проверить, помечен ли настроенный статический порт-участник буквой «S».
- Запустите команду **show ip igmp snooping**, чтобы проверить, действуют ли подавление пакетов Report, немедленный выход (immediate leave), изучение порта

маршрутизатора, время устаревания порта маршрутизатора, время устаревания порта-участника и максимальное время ответа пакета Query.

9.4.4.5. Связанные команды

Настройка статический порта маршрутизатора

Команда	**ip igmp snooping vlan** *vid* **mrouter interface** *interface-type interface-number*
Описание параметра	*vid*: указывает на VLAN. Значение варьируется от 1 до 4094. *interface-type interface-number*: указывает имя интерфейса
Командный режим	Режим глобальной конфигурации
Руководство по использованию	В режиме SVGL, если Sub VLAN не настроена, могут вступить в силу только конфигурации статического порта маршрутизатора в Shared VLAN, а остальные можно настроить, но они не вступят в силу. Если настроена Sub VLAN, могут вступить в силу только конфигурации статический порта маршрутизатора в Shared VLAN или non-sub VLAN, а остальные можно настроить, но они не вступят в силу. В режиме IVGL-SVGL, если Sub VLAN не настроена, конфигурации статических портов маршрутизатора во всех VLAN могут вступить в силу; если настроена Sub VLAN, могут вступить в силу только конфигурации статического порта маршрутизатора в Shared VLAN или non-sub VLAN, а остальные можно настроить, но они не вступят в силу. В режиме IVGL могут вступить в силу настройки статических портов маршрутизатора во всех сетях VLAN

Настройка статического порта-участника

Команда	**ip igmp snooping vlan** *vid* **static** *group-address* **interface** *interface-type interface-number*
Описание параметра	*vid*: указывает на VLAN. Значение варьируется от 1 до 4094. *group-address*: указывает адрес профиля. *interface-type interface-number*: указывает имя интерфейса
Командный режим	Режим глобальной конфигурации
Руководство по использованию	По умолчанию статический порт-участник не настроен

Включение подавления пакетов Report

Команда	**ip igmp snooping suppression enable**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если подавление пакетов Report включено, только первый пакет Report из указанной VLAN или профиля пересылается на порт маршрутизатора в течение интервала Query, а последующие пакеты Report не будут пересылаться на порт маршрутизатора, тем самым уменьшая количество пакетов на сеть. Подавить можно только пакеты Report IGMPv1 и IGMPv2, а пакеты Report IGMPv3 подавить невозможно

Включение функции Immediate-Leave

Команда	**ip igmp snooping fast-leave enable**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если эта функция включена, порт будет удален из записи порта-участника, когда порт получит пакет Leave. После этого пакеты больше не будут пересылаться на этот порт при получении пакетов Query указанных профилей. Пакеты Leave включают пакеты Leave IGMPv2, а также пакеты Report IGMPv3, которые включают типы, но не содержат адреса источника. Функция Immediate-Leave применяется только в том случае, когда к порту устройства подключен только один хост. Он используется для экономии полосы пропускания и ресурсов

Включение динамического изучения порта маршрутизатора

Команда	**ip igmp snooping** [**vlan** *vid*] **mrouter learn pim-dvmrp**
Описание параметра	**vlan** *vid*: указывает VLAN. Эта конфигурация по умолчанию применяется ко всем VLAN
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Порт маршрутизатора — это порт, который напрямую подключен к устройству multicast, использующему IGMP snooping, и соседнему устройству multicast, использующему протокол multicast-маршрутизации. По умолчанию включено динамическое изучение портов маршрутизатора, и устройство автоматически прослушивает пакеты Query IGMP, пакеты DVMRP и пакеты PIM Hello

Настройка времени устаревания порта динамического маршрутизатора

Команда	**ip igmp snooping dyn-mr-aging-time** *seconds*
Описание параметра	*seconds*: указывает время устаревания порта динамического маршрутизатора в секундах. Значение варьируется от 1 до 3600
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если порт динамического маршрутизатора не получит пакет general Query IGMP или пакет Hello PIM до истечения таймера устаревания, устройство удалит этот порт из записи порта маршрутизатора. Если включено динамическое изучение порта маршрутизатора, вы можете запустить эту команду, чтобы настроить время устаревания порта динамического маршрутизатора. Если время устаревания слишком короткое, multicast-устройство может часто добавлять или удалять порт маршрутизатора

Настройка времени устаревания динамического порта-участника

Команда	**ip igmp snooping host-aging-time** *seconds*
Описание параметра	*seconds*: указывает время устаревания
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Время устаревания динамического порта-участника указывает время, когда порт устройства получает пакет Join IGMP, отправленный с хоста для подписки на профиль IP multicast-маршрутизации. При получении пакета Join IGMP время устаревания динамического порта-участника будет сброшено. Значение времени таймера — это время устаревания хоста. По истечении времени таймера multicast-устройство считает, что для данного порта не существует пользовательского хоста для приема multicast-пакета, и удаляет этот порт из записи порта-участника IGMP snooping. После того, как время устаревания настроено, время устаревания следующих полученных пакетов Join IGMP будет равно времени устаревания хоста. Эта конфигурация вступит в силу после получения следующего пакета Join IGMP, и таймер используемого порта не будет обновляться

Настройка максимального времени ответа пакета Query

Команда	**ip igmp snooping query-max-response-time** *seconds*
Описание параметра	*seconds*: указывает максимальное время отклика

Командный режим	Режим глобальной конфигурации
Руководство по использованию	Когда получен пакет general Query IGMP, multicast-устройство сбрасывает время устаревания всех динамических портов-участников, которое равно максимальному времени ответа на Query (query-max-response-time). По истечении времени таймера multicast-устройство считает, что для данного порта не существует пользовательского хоста для приема multicast-пакета, и удаляет этот порт из записи порта-участника IGMP snooping. При получении пакета Query, специфичного для профиля IGMP, multicast-устройство сбрасывает время устаревания всех динамических портов-участников определенного профиля, то есть query-max-response-time. По истечении времени таймера multicast-устройство считает, что для данного порта не существует пользовательского хоста для приема multicast-пакета, и удаляет этот порт из записи порта-участника IGMP snooping. Эта конфигурация вступит в силу после получения следующего пакета Query, и используемый таймер не будет обновлен. Таймер пакета Query, специфичного для профиля IGMPv3, не обновляется

Отображение портов маршрутизатора

Команда	**show ip igmp snooping mroute**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если порт маршрутизатора успешно настроен, в информации о порте будет отображаться буква «S». QTECH(config)#show ip igmp snooping mrouter Multicast Switching Mroute Portwww.qtech.ru D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/1(S)

Отображение информации о динамическом изучении портов маршрутизатора

Команда	**show ip igmp snooping**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса

Руководство по использованию	Запустите команду **show ip igmp snooping**, чтобы отобразить время устаревания и состояние изучения порта динамического маршрутизатора. Dynamic Mroute Aging Time : 300(Seconds) Multicast router learning mode: pim-dvmrp

Отображение информации о порте-участнике

Команда	**show ip igmp snooping gda-table**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если порт-участник успешно настроен, в информации о порте будет отображаться буква «S». QTECH(config)#show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*, 224.1.1.1, 1): VLAN(1) 1 OPORTS: GigabitEthernet 0/1(S

Отображение других параметров

Команда	**show ip igmp snooping**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Запустите команду **show ip igmp snooping**, чтобы отобразить время устаревания порта маршрутизатора, время устаревания динамического порта-участника, время ответа пакета Query, подавление пакетов Report и Immediate Leave. IGMP Fast-Leave: Enable IGMP Report suppress: Enable Query Max Response Time: 20(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

9.4.4.6. Пример конфигурации

Настройка статического порта маршрутизатора и статического порта-участника

Шаги настройки	Настройте базовые (basic) функции IGMP snooping. Настройте статический порт маршрутизатора и статический порт-участник
	QTECH# configure terminal QTECH(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet 0/0 QTECH(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/0 QTECH(config)# end
Проверка	Запустите команды **show ip igmp snooping mrouter** и **show ip igmp snooping gda-table**, чтобы проверить, вступила ли конфигурация в силу
	QTECH#show ip igmp snooping mrouter Multicast Switching Mroute Port D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/0(S) QTECH#show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*, 224.1.1.1, 1): VLAN(1) 1 OPORTS: GigabitEthernet 0/0(SM)

Включение подавления пакетов Report

Сценарий:

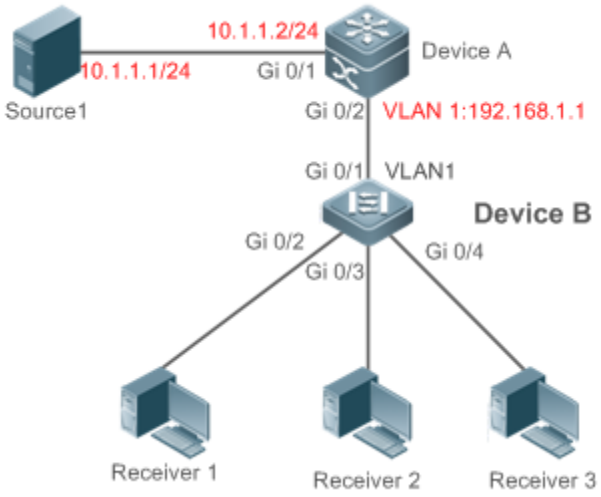

Рисунок 9-8.

	A является маршрутизатором multicast и подключен непосредственно к источнику multicast 1. B является устройством уровня 2 и подключено непосредственно к пользовательскому хосту и источнику multicast 2. Приемник 1, Приемник 2 и Приемник 3 подключены к VLAN 1
Шаги настройки	• Настройте IP-адрес и VLAN. (пропущено) • Включите multicast-маршрутизацию на A и включите протокол multicast-маршрутизации на интерфейсе уровня 3 (Gi0/1 и VLAN 1). • Включите IGMP snooping на B и выберите режим IVGL. • Включите подавление пакетов Report на B
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)#ip igmp snooping ivgl B(config)# ip igmp snooping suppression enable

Проверка	Проверьте, добавлены ли Приемник 1 и Приемник 2 в профиль 239.1.1.1, и с интерфейса Gi0/1 в B пересылаются только пакеты Report IGMP профиля 239.1.1.1
B	B# show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65 536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Snooping version: 2IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

Настройка других параметров

Шаги настройки	• Настройте базовые функции IGMP snooping. • Включите функцию Immediate-Leave. • Отключите изучение портов маршрутизатора. • Настройте время устаревания порта маршрутизатора. • Настройка времени устаревания порта-участника. • Настройте время ответа пакета Query
	QTECH# configure terminal QTECH(config)# ip igmp snooping fast-leave enable QTECH(config)# no ip igmp snooping mrouter learn pim-dvmrp QTECH(config)#ip igmp snooping dyn-mr-aging-time 200 QTECH(config)#ip igmp snooping host-aging-time 100 QTECH(config)#ip igmp snooping query-max-response-time 60 QTECH(config)# end
Проверка	Запустите команду **show ip igmp snooping**, чтобы проверить успешность настройки
	QTECH#show ip igmp snooping IGMP Snooping running mode: IVGL

	IGMP Snooping L2-entry-limit: 65 536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Enable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Snooping version: 2Query Max Response Time: 60(Seconds) IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 200(Seconds) Dynamic Host Aging Time : 100(Seconds)

9.4.4.7. Распространенные ошибки

Основные функции IGMP snooping не настроены или настройка не выполнена.

9.4.5. Настройка управления безопасностью IGMP

9.4.5.1. Эффект конфигурации

- Настройте диапазон адресов multicast, к которым может получить доступ пользователь.
- Настройте, чтобы разрешить пользователю из неавторизованного профиля просматривать канал multicast.
- Настройте количество адресов multicast, к которым может получить доступ пользователь.
- Настройте ограничение на получение пользователем только multicast-трафика из порта маршрутизатора, чтобы предотвратить нелегальный multicast-трафик, отправляемый конечным пользователем.
- Настройте ограничение на получение пользователем только multicast-трафика с назначенных исходных IP-адресов, чтобы предотвратить нелегальный multicast-трафик.

9.4.5.2. Примечания

Необходимо настроить основные функции IGMP snooping.

9.4.5.3. Шаги настройки

Настройка фильтрации профилей

- Опционально.
- Если вы хотите ограничить количество пакетов профиля, принимаемых портом, вы можете настроить фильтрацию профиля на порту.
- Если вы хотите ограничить количество multicast-пакетов, принимаемых VLAN, вы можете настроить фильтрацию профиля для каждой VLAN.

Включение предварительного просмотра multicast

- Опционально.
- Вы можете включить предварительный просмотр multicast для пользователя из неавторизованного профиля.

Настройка максимального количества профилей

- Опционально.
- Если вы хотите ограничить количество профилей multicast, которые порт может получать, вы можете настроить максимальное количество профилей multicast, разрешенных для этого порта.
- Если вы хотите ограничить количество профилей multicast, которые разрешено получать глобальным портам, вы можете настроить максимальное количество профилей multicast, разрешенных для этих портов.

Настройка проверки порта источника

- Опционально.
- Вы можете выполнить эту настройку, если хотите разрешить порту получать только multicast-трафик от порта маршрутизатора.

Настройка проверки IP-адреса источника

- Опционально.
- Вы можете выполнить эту настройку, чтобы указать IP-адрес источника для всех профилей multicast всех VLAN. Легальным считается только multicast-трафик, IP-адрес источника которого совпадает с заданным.
- Вы также можете указать исходные IP-адреса для определенных профилей multicast в определенных VLAN. Среди multicast-трафика, полученного от конкретных профилей multicast внутри VLAN, только тот, у которого IP-адрес источника совпадает с заданным, считается легальным и будет пересылаться устройством multicast; другой трафик будет отброшен.

9.4.5.4. Проверка

- Запустите команду **show ip igmp snooping interfaces**, чтобы отобразить фильтрацию профилей и максимальное количество профилей multicast для порта.
- Запустите команду **show ip igmp snooping vlan**, чтобы отобразить фильтрацию профиля для каждой VLAN.
- Запустите команду **show ip igmp snooping**, чтобы проверить, вступило ли в силу максимальное количество глобальных профилей multicast, функция предварительного просмотра, проверка порта источника и проверка IP-адреса источника.

9.4.5.5. Связанные команды

Настройка фильтрации профилей

Команда	**ip igmp snooping filter** *profile-number*
Описание параметра	*profile-number*: указывает номер профиля

Командный режим	Режим настройки интерфейса

Настройка фильтрации профиля для каждой VLAN

Команда	**ip igmp snooping vlan** *vid* **filter** *profile-number*
Описание параметра	*vid*: указывает на VLAN. Значение варьируется от 1 до 4094. *profile-number*: указывает номер профиля
Командный режим	Режим глобальной конфигурации

Настройка максимального количества профилей на порту

Команда	**ip igmp snooping max-groups** *number*
Описание параметра	*number*: указывает максимальное количество профилей multicast
Командный режим	Режим настройки интерфейса
Руководство по использованию	Это значение указывает только количество динамических профилей multicast, количество статических профилей не учитывается. Счетчик multicast-профилей зависит от VLAN, к которой принадлежит порт. Например, если порт принадлежит трем VLAN, и все три из них одновременно получают пакет Query от профиля multicast 224.1.1.1, то счетчик профилей multicast будет равен 3, а не 1

Настройка максимального количества глобальных профилей

Команда	**ip igmp snooping l2-entry-limit** *number*
Описание параметра	*number*: указывает максимальное количество профилей multicast
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Это значение включает в себя количество как динамических, так и статических профилей

Настройка проверки порта источника

Команда	**ip igmp snooping source-check port**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После включения проверки порта источника multicast-трафик, полученный устройством, будет отброшен, если в сетевой среде не обнаружен порт маршрутизатора

Настройка проверки IP-адреса источника

Команда	**ip igmp snooping source-check default-server** *source-address*
Описание параметра	*source-address*: указывает IP-адрес источника
Командный режим	Режим глобальной конфигурации

Включение проверки IP-адреса источника для определенного профиля

Команда	**ip igmp snooping limit-ipmc vlan** *vid* **address** *group-address* **server** *source-address*
Описание параметра	*vid*: идентификатор VLAN *group-address*: указывает адрес профиля. *source-address*: указывает IP-адрес источника
Командный режим	Режим глобальной конфигурации

Включение предварительного просмотра

Команда	**ip igmp snooping preview** *profile-number*
Описание параметра	*profile-number*: указывает диапазон адресов multicast, разрешенных для предварительного просмотра. Значение варьируется от 1 до 1024
Командный режим	Режим глобальной конфигурации

Настройка продолжительности предварительного просмотра

Команда	**ip igmp snooping preview interval** *num*
Описание параметра	*num*: указывает продолжительность предварительного просмотра в диапазоне от 1 до 300 с (по умолчанию 60 с)
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта конфигурация позволяет неавторизованным пользователям получать multicast-трафик в течение периода предварительного просмотра. По истечении заданного времени предварительный просмотр будет остановлен; предварительный просмотр можно возобновить через 300 с

Отображение фильтрации профиля по портам

Команда	**show ip igmp snooping interface**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если функция настроена, профиль будет отображаться, например: QTECH#show ip igmp snooping interfaces gigabitEthernet 0/1 Interface Filter profile number max-group ---------- ---------- --------- GigabitEthernet 0/1 1

Отображение фильтрации профиля для каждой VLAN

Команда	**show ip igmp snooping vlan**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если функция настроена, профиль будет отображаться, например: IGMP VLAN filter: 1

Отображение максимального количества профилей интерфейса

Команда	**show ip igmp snooping interface**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса

Руководство по использованию	Если настроено максимальное количество multicast-адресов для порта, будет отображаться значение, например: QTECH#show ip igmp snooping interfaces gigabitEthernet 0/1 Interface Filter profile number max-group ---------- ---------- --------- GigabitEthernet 0/1 1 200

Отображение максимального количества глобальных профилей

Команда	**show ip igmp snooping vlan**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если функция настроена, профиль будет отображаться, например: IGMP Snooping L2-entry-limit: 65 536

Отображение информации о проверке порта источника

Команда	**show ip igmp snooping vlan**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если проверка порта источника включена, будет отображена следующая информация: Source port check: Enable

Отображение информации о проверке IP источника

Команда	**show ip igmp snooping vlan**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если проверка IP-адреса источника включена, будет отображена следующая информация: Source ip check: Enable

Отображение информации о функции предварительного просмотра

Команда	**show ip igmp snooping**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса

Руководство по использованию	Если для порта настроен диапазон адресов multicast, предварительный просмотр будет включен, например: IGMP Preview: Enable IGMP Preview group aging time : 60(Seconds)

9.4.5.6. Пример конфигурации

Настройка фильтрации профилей и максимального количества требуемых профилей

Сценарий:

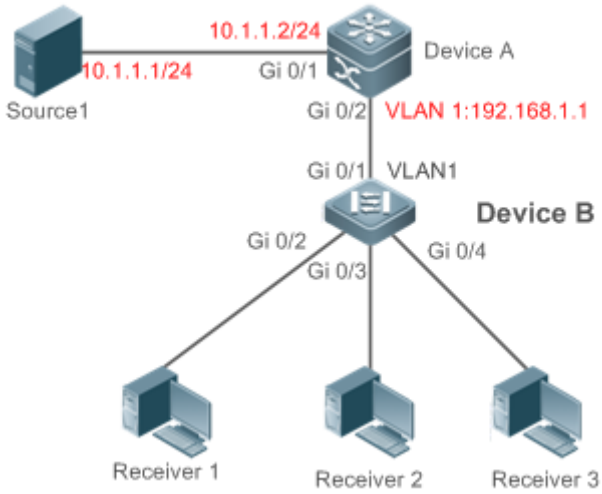

Рисунок 9-9.

	A является маршрутизатором multicast и подключен непосредственно к источнику multicast 1. B является устройством уровня 2 и подключено непосредственно к пользовательскому хосту и источнику multicast 2. Приемник 1, Приемник 2 и Приемник 3 подключены к VLAN 1. Настроив VLAN 1, вы можете разрешить пользователям во VLAN 1 получать только те профили, адреса которых находятся в диапазоне от 225.1.1.1 до 225.1.255.255. Вы можете настроить Приемник 1 на получение только профилей с адресами от 225.1.1.1 до 225.1.1.255, Приемник 2 на получение только профилей с адресами от 225.1.2.1 до 255.1.2.255, а Приемник 3 на получение только тех профилей, чьи адреса варьируются от 225.1.3.1 до 225.1.3.255. К порту можно добавить не более 10 профилей, а глобально — не более 100 профилей
Шаги настройки	• Настройте IP-адрес и VLAN. (пропущено)

	• Включите multicast-маршрутизацию на A и включите протокол multicast-маршрутизации на интерфейсе уровня 3 (Gi0/1 и VLAN 1). • Включите IGMP snooping на B и выберите режим IVGL. • Настройте диапазон и максимальное количество адресов multicast на B
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)#ip igmp snooping ivgl B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#rang B(config-profile)#range 225.1.1.1 225.1.255.255 B(config-profile)#exit B(config)#ip igmp profile 2 B(config-profile)#permit B(config-profile)#range 225.1.1.1 225.1.1.255 B(config-profile)#exit B(config)#ip igmp profile 3 B(config-profile)#permit B(config-profile)#range 225.1.2.1 225.1.2.255 B(config-profile)#exit B(config)#ip igmp profile 4 B(config-profile)#permit B(config-profile)#range B(config-profile)#range 225.1.3.1 225.1.3.255 B(config-profile)#exit B(config)#ip igmp snooping l2-entry-limit 100 B(config)#ip igmp snooping vlan 1 filter 1 B(config)#int gigabitEthernet 0/2

	QTECH(config-if-GigabitEthernet 0/0)#ip igmp snooping filter 2 QTECH(config-if-GigabitEthernet 0/0)#ip igmp snooping max-groups 10 B(config)#int gigabitEthernet 0/3 QTECH(config-if-GigabitEthernet 0/0)#ip igmp snooping filter 3 QTECH(config-if-GigabitEthernet 0/0)#ip igmp snooping max-groups 10 B(config)#int gigabitEthernet 0/4 QTECH(config-if-GigabitEthernet 0/0)#ip igmp snooping filter 4 QTECH(config-if-GigabitEthernet 0/0)#ip igmp snooping max-groups 10
Проверка	• Запустите команду **show ip igmp snooping interfaces**, чтобы отобразить фильтрацию профилей и максимальное количество профилей multicast для порта. • Запустите команду **show ip igmp snooping**, чтобы отобразить максимальное количество глобальных групп multicast
B	B#show ip igmp snooping interfaces Interface Filter profile number max-group ---------- ---------- --------- GigabitEthernet 0/2 2 10 GigabitEthernet 0/3 3 10 GigabitEthernet 0/4 4 10 B#show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 100 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

Настройка проверки порта источника

Сценарий:

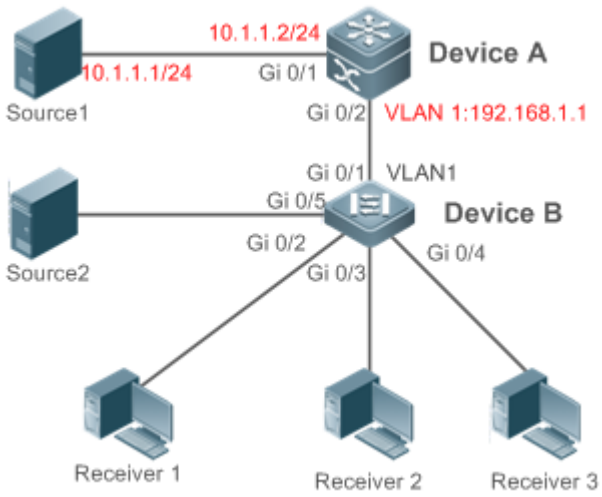

Рисунок 9-10.

	A является маршрутизатором multicast и подключен непосредственно к источнику multicast 1. B является устройством уровня 2 и подключено непосредственно к пользовательскому хосту и источнику multicast 2. Приемник 1, Приемник 2 и Приемник 3 подключены к VLAN 1. Источник 1 отправляет трафик multicast-адреса из профиля 224.1.1.1, а источник 2 отправляет трафик multicast-адреса из профиля 225.1.1.1. Приемник 1 может запросить профили 224.1.1.1 и 225.1.1.1 соответственно. Проверка порта источника включена
Шаги настройки	• Настройте IP-адрес и VLAN. • Включите multicast-маршрутизацию на A и включите протокол multicast-маршрутизации на интерфейсе уровня 3 (Gi0/1 и VLAN 1). • Включите IGMP snooping на B и выберите режим IVGL. • Включите проверку порта источника на B
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit

B	B# configure terminal B(config)#ip igmp snooping ivgl B(config)#ip igmp snooping source-check port
Проверка	• Запустите команду **show ip igmp snooping mroute**, чтобы проверить, изучен ли Gi0/1 как порт маршрутизатора. • Проверьте, может ли Приемник 1 запрашивать multicast-трафик профиля 224.1.1 и не может ли запросить трафик профиля 225.1.1.1
B	Multicast Switching Mroute Port D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/1(S) B#show ip igmp snooping IGMP Snooping L2-entry-limit: 100 Source port check: Enable Source ip check: Disable

Настройка проверки IP-адреса источника

Сценарий:

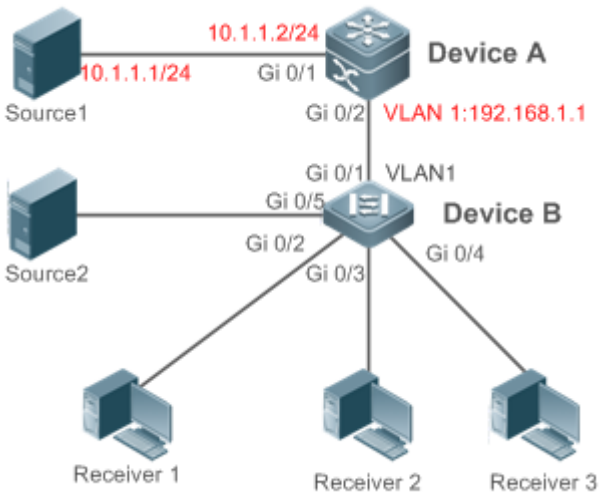

Рисунок 9-11.

	A является маршрутизатором multicast и подключен непосредственно к источнику multicast 1. B является устройством уровня 2 и подключено непосредственно к пользовательскому хосту и источнику multicast 2. Приемник 1, Приемник 2 и Приемник 3 подключены к VLAN 1. Источник 1 отправляет трафик multicast-адреса из профилей 10.1.1.1 и 224.1.1.1, Источник 2 отправляет трафик multicast-адреса из профилей 192.168.1.3 и 225.1.1.1, а Источник 3 отправляет трафик multicast-адреса из профилей 192.168.1.3 и 226.1. 1.1. Приемник 1 может запросить профили 224.1.1.1, 225.1.1.1 и 226.1.1.1 соответственно. IP-адрес по умолчанию для проверки IP-адреса источника — 10.1.1.1. Настройте limit-ipmc и multicast-трафик профиля 225.1.1.1 и установите легальный адрес источника 192.168.1.3
Шаги настройки	• Настройте IP-адрес и VLAN. • Включите multicast-маршрутизацию на A и включите протокол multicast-маршрутизации на интерфейсе уровня 3 (Gi0/1 и VLAN 1). • Включите IGMP snooping на B и выберите режим IVGL. • Включите проверку порта источника на B
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)#ip igmp snooping ivgl B(config)# ip igmp snooping source-check default-server 10.1.1.1 B(config)# ip igmp snooping limit-ipmc vlan 1 address 225.1.1.1 server 192.168.1.3
Проверка	• Запустите команду **show ip igmp snooping**, чтобы проверить, включена ли проверка IP-адреса источника. • Проверьте, может ли Приемник 1 запрашивать multicast-трафик профилей 224.1.1 и 225.1.1.1 и не может ли запросить трафик профиля 226.1.1.1
B	B#show ip igmp snooping

	IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65 536 Source port check: Disable Source ip check: Enable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

9.4.5.7. Распространенные ошибки

- Основные функции IGMP snooping не настроены или настройка не выполнена.
- Порт multicast-маршрутизатора не изучен, что приводит к невозможности получения multicast-трафика.
- IP-адрес для проверки IP-адреса источника не соответствует IP-адресу multicast, что приводит к невозможности получения multicast-трафика.

9.4.6. Настройка профиля IGMP

9.4.6.1. Эффект конфигурации

Создайте профиль фильтрации IGMP.

9.4.6.2. Шаги настройки

Создать профиль

- (Опционально) Создайте профиль фильтрации IGMP.

Настройка диапазона профиля

- (Опционально) Настройте диапазон адресов профиля multicast.

Настройка фильтрации профилей

- (Опционально) Настройте режим фильтрации профиля, чтобы **permit** или **deny** (разрешить или запретить).

9.4.6.3. Проверка

Запустите команду **show running-config**, чтобы проверить, вступили ли в силу предыдущие конфигурации.

9.4.6.4. Связанные команды

Создать профиль

Команда	**ip igmp profile** *profile-number*
Описание параметра	*profile-number*: указывает номер профиля
Командный режим	Режим глобальной конфигурации

Настройка диапазона профиля

Команда	**range** *low-ip-address* [*high-ip-address*]
Описание параметра	*low-ip-address*: указывает начальный адрес. *high-ip-address*: указывает конечный адрес. По умолчанию настроен только один адрес
Командный режим	Режим настройки профиля
Руководство по использованию	Вы можете настроить несколько адресов. Если IP-адреса разных диапазонов идут последовательно, адреса будут объединены

Настройка фильтрации профилей

Команда	**deny**
Командный режим	Режим настройки профиля
Руководство по использованию	Если для режима фильтрации профиля установлено значение «deny», а диапазон профилей multicast не указан, ни один профиль не может быть запрещен, что означает разрешение для всех профилей

Настройка фильтрации профилей

Команда	**permit**
Командный режим	Режим настройки профиля
Руководство по использованию	Если режим фильтрации профиля настроен на «permit», а диапазон профилей multicast не указан, ни один профиль не будет разрешен, что означает запрет для всех профилей

9.4.6.5. Пример конфигурации

Создание профиля фильтрации

Шаги настройки	Создайте профиль фильтрации
	B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#range B(config-profile)#range 224.1.1.1 235.1.1.1 B(config-profile)#
Проверка	Запустите команду **show running-config**, чтобы проверить успешность настройки
	ip igmp profile 1 permit range 224.1.1.1 235.1.1.1 !

9.4.6.6. Распространенные ошибки

- Основные функции IGMP snooping не настроены или настройка не выполнена.
- Режим профиля настроен на **permit**, но диапазон multicast-профилей не указан, что приводит к запрету всех профилей.

9.4.7. Настройка IGMP QinQ

9.4.7.1. Эффект конфигурации

Создайте запись multicast во VLAN, где расположены пакеты IGMP. Пересылайте пакеты IGMP во VLAN, где эти пакеты расположены, реализуя прозрачную передачу.

9.4.7.2. Примечания

Необходимо настроить основные функции IGMP snooping.

9.4.7.3. Шаги настройки

Настройка прозрачной передачи QinQ

Если интерфейсу QinQ необходимо пересылать multicast-пакеты в сети VLAN, где указаны VID-ы пакетов, включите QinQ для реализации прозрачной передачи.

9.4.7.4. Проверка

Запустите команду **show ip igmp snooping**, чтобы проверить, вступила ли конфигурация в силу.

9.4.7.5. Связанные команды

Настройка прозрачной передачи QinQ

Команда	**ip igmp snooping tunnel**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Включите QinQ для реализации прозрачной передачи пакетов IGMP

Отображение конфигурации QinQ

Команда	**show ip igmp snooping**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса
Руководство по использованию	Если QinQ включен, отображается следующее содержимое. IGMP Tunnel: Enable

9.4.7.6. Пример конфигурации

Настройка прозрачной передачи QinQ

Шаги настройки	• Настройте базовые функции IGMP snooping. • Настройте прозрачную передачу QinQ
	QTECH# configure terminal QTECH(config)# ip igmp snooping tunnel QTECH(config)# QTECH(config)# end
Проверка	Запустите команду **show ip igmp snooping**, чтобы проверить успешность настройки
	IGMP Tunnel: Enable

9.4.7.7. Распространенные ошибки

Основные функции IGMP snooping не настроены или настройка не выполнена.

9.4.8. Настройка IGMP Querier

9.4.8.1. Эффект конфигурации

Настройте устройство как IGMP querier, который будет периодически отправлять пакеты Query IGMP и собирать необходимую пользователю информацию.

9.4.8.2. Примечания

Необходимо настроить основные функции IGMP snooping.

9.4.8.3. Шаги настройки

Включение функции Querier

- (Опционально) Включите функцию Querier IGMP глобально или для указанной VLAN.
- (Опционально) Отключите функцию Querier IGMP для указанной VLAN.

Настройка IP-адреса источника Querier

- (Опционально) Вы можете настроить IP-адрес источника пакета Query, отправляемого Querier, на основе VLAN.
- После включения Querier необходимо указать IP-адрес источника для Querier; в противном случае конфигурация не вступит в силу.

Настройка максимального времени ответа пакета Query

(Опционально) Отрегулируйте максимальное время ответа, передаваемое пакетом Query IGMP. Поскольку IGMPv1 не поддерживает передачу максимального времени ответа пакетом Query, эта конфигурация не вступает в силу, когда Querier использует IGMPv1.

Настройка Query-интервала Querier

(Опционально) Настройте интервал Query IGMP для отправки пакетов Query.

Настройка таймера устаревания Querier

(Опционально) Настройте таймер устаревания других querier-ов IGMP в сети.

Указание версии IGMP для Querier

(Опционально) Укажите версию IGMP для Querier (по умолчанию IGMPv2).

9.4.8.4. Проверка

Запустите команду **show ip igmp snooping querier detail**, чтобы проверить, вступила ли конфигурация в силу.

9.4.8.5. Связанные команды

Включение функции IGMP Querier

Команда	**ip igmp snooping** [**vlan** *vid*] **querier**
Описание параметра	**vlan** *vid*: указывает VLAN. Эта конфигурация по умолчанию применяется ко всем VLAN
Командный режим	Режим глобальной конфигурации
Руководство по использованию	IGMP querier для указанной VLAN вступит в силу только после включения глобального querier-а IGMP. Если глобальный IGMP querier отключен, IGMP querier для всех VLAN будет отключен

Настройка IP-адреса источника Querier

Команда	**ip igmp snooping** [**vlan** *vid*] **querier address** *a.b.c.d*
Описание параметра	**vlan** *vid*: указывает VLAN. Эта конфигурация по умолчанию применяется ко всем VLAN. *a.b.c.d*: указывает IP-адрес источника
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После включения querier необходимо указать IP-адрес источника для querier-a; в противном случае конфигурация не вступит в силу. Если IP-адрес источника указан VLAN-ом, этот адрес будет использоваться преимущественно

Настройка максимального времени ответа Querier

Команда	**ip igmp snooping** [**vlan** *vid*] **querier max-response-time** *seconds*
Описание параметра	**vlan** *vid*: указывает VLAN. Эта конфигурация по умолчанию применяется ко всем VLAN. *seconds*: указывает максимальное время отклика. В единицах секунды. Значение варьируется от 1 до 25
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если интервал Query указан VLAN-ом, это значение будет использоваться преимущественно

Настройка Query-интервала Querier

Команда	**ip igmp snooping** [**vlan** *vid*] **querier query-interval** *seconds*
Описание параметра	**vlan** *vid*: указывает VLAN. Эта конфигурация по умолчанию применяется ко всем VLAN. *seconds*: указывает интервал Query в секундах. Значение варьируется от 1 до 18 000
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если интервал Query указан VLAN-ом, это значение будет использоваться преимущественно

Настройка таймера устаревания Querier

Команда	**ip igmp snooping** [**vlan** *vid*] **querier timer expiry**
Описание параметра	**vlan** *vid*: указывает VLAN. Эта конфигурация по умолчанию применяется ко всем VLAN. *seconds*: указывает время ожидания в секундах. Значение варьируется от 60 до 300
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Устройство может не быть выбрано в качестве querier-а, даже если его функция querier-а включена. Если устройство, которое не удалось выбрать, не получает пакет Query, отправленный querier-ом в течение времени устаревания, используемый Querier считается устаревшим, и будет инициирован новый цикл выбора. Если время устаревания указано во VLAN, это значение будет использоваться преимущественно

Указание версии IGMP для Querier-а

Команда	**ip igmp snooping** [**vlan** *vid*] **querier version 1**
Описание параметра	**vlan** *vid*: указывает VLAN. Эта конфигурация по умолчанию применяется ко всем VLAN
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Querier может быть запущен в IGMPv1 и IGMPv2 (по умолчанию IGMPv2). Вы также можете запустить команду для настройки версии IGMPv1. Если версия IGMP для querier-а указана VLAN-ом, эта версия будет использоваться преимущественно

Отображение конфигурации IGMP Querier

Команда	**show ip igmp snooping querier detail**
Командный режим	Режим привилегированного EXEC, режим глобальной конфигурации или режим конфигурации интерфейса

Руководство по использованию	Если QinQ включен, отображается следующее содержимое.
	`QTECH(config)#show ip igmp snooping querier detail`
	`Vlan IP Address IGMP Version Port`
	`----------`

	Global IGMP switch querier status ---------- admin state: Enable admin version: 2 source IP address: 1.1.1.1 query-interval (sec): 60 max-response-time (sec): 10 querier-timeout (sec): 125 Vlan 1: IGMP switch querier status ---------- admin state: Disable admin version: 2 source IP address: 1.1.1.1 query-interval (sec): 60 max-response-time (sec): 10 querier-timeout (sec): 125 operational state: Disable operational version: 2

9.4.8.6. Пример конфигурации

Включение функции IGMP Querier

Сценарий:

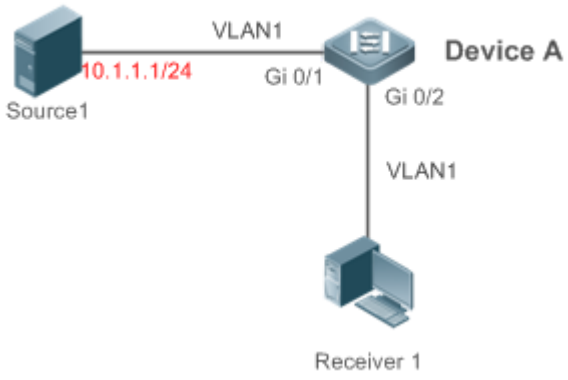

Рисунок 9-12.

	В сценарии без оборудования multicast уровня 3 multicast-трафик может перенаправляться только в сеть уровня 2. A действует как устройство уровня 2 для подключения к источнику и приемнику multicast
Шаги настройки	• Включите глобальное IGMP snooping на A в режиме IVGL. • Включите IGMP Querier для VLAN 1 на A
A	A(config)#ip igmp snooping ivgl A(config)#ip igmp snooping querier A(config)#ip igmp snooping querier address 10.1.1.1 A(config)#ip igmp snooping vlan 1 querier
Проверка	Запустите команду **show ip igmp snooping querier**, чтобы проверить, вступил ли в силу querier VLAN 1
A	A(config)#show ip igmp snooping querier Vlan IP Address IGMP Version Port --- 1 10.1.1.1 2 switch A(config)#show ip igmp snooping querier vlan 1 Vlan 1: IGMP switch querier statuswww.qtech.ru --- elected querier is 10.1.1.1 (this switch querier) --- admin state : Enable admin version : 2 source IP address : 10.1.1.1 query-interval (sec) : 60 max-response-time (sec) : 10 querier-timeout (sec) : 125 operational state : Querier operational version : 2

9.4.8.7. Распространенные ошибки

IP-адрес источника не настроен для querier-a, и querier не вступает в силу.

9.5. Мониторинг

9.5.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере важной информации и, таким образом, к прерыванию работы служб.

Описание	Команда
Очищает статистику IGMP snooping	**clear ip igmp snooping statistics**
Очищает порты динамического маршрутизатора и порты-участники	**clear ip igmp snooping gda-table**

9.5.2. Отображение

Описание	Команда
Отображает базовые конфигурации IGMP snooping	**show ip igmp snooping** [**vlan** *vlan-id*]
Отображает статистику IGMP snooping	**show ip igmp snooping statistics** [**vlan** *vlan-id*]
Отображает порты маршрутизатора	**show ip igmp snooping mrouter**
Отображает записи IGMP snooping	**show ip igmp snooping gda-table**
Отображает профиль	**show ip igmp profile** [*profile-number*]
Отображает конфигурации IGMP snooping на интерфейсе	**show ip igmp snooping interface** *interface-name*
Отображает IGMP Querier	**show ip igmp snooping querier** [**detail**]
Отображает информацию о пользователе	**show ip igmp snooping user-info**

9.5.3. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Поэтому отключайте отладку сразу после использования.

Описание	Команда
Отладка всех функций IGMP Snooping	**debug igmp-snp**
Отладка событий IGMP snooping	**debug igmp-snp event**
Отладка пакетов IGMP snooping	**debug igmp-snp packet**
Отладка связи между IGMP snooping и MSF	**debug igmp-snp msf**
Отладка сигналов IGMP snooping	**debug igmp-snp warning**

10. НАСТРОЙКА MLD SNOOPING

10.1. Обзор

Multicast Listener Discovery (MLD) Snooping используется для контроля и управления поведением пересылки multicast-пакетов IPv6 на уровне 2.

Устройство, на котором выполняется MLD Snooping, анализирует пакеты MLD, полученные портом, для создания сопоставления между портом и MAC-адресом multicast и пересылает данные multicast IPv6 на уровне 2 на основе сопоставления. Когда MLD Snooping отключено, multicast-пакеты IPv6 передаются на уровне 2. Когда MLD Snooping включено, пакеты multicast-данных известной группы multicast IPv6 пересылаются указанному приемнику на уровне 2 вместо broadcast-рассылки на уровне 2.

10.1.1. Протоколы и стандарты

RFC4541: Рекомендации для Internet Group Management Protocol (IGMP) и Multicast Listener Discovery (MLD) Snooping коммутаторов.

10.1.2. Два типа портов MLD Snooping

Как показано на Рисунке 10-1, устройство multicast уровня 3 подключено к источнику multicast. На устройстве доступа включен MLD Snooping. Хост A и Хост B являются приемниками (то есть участниками группы multicast IPv6).

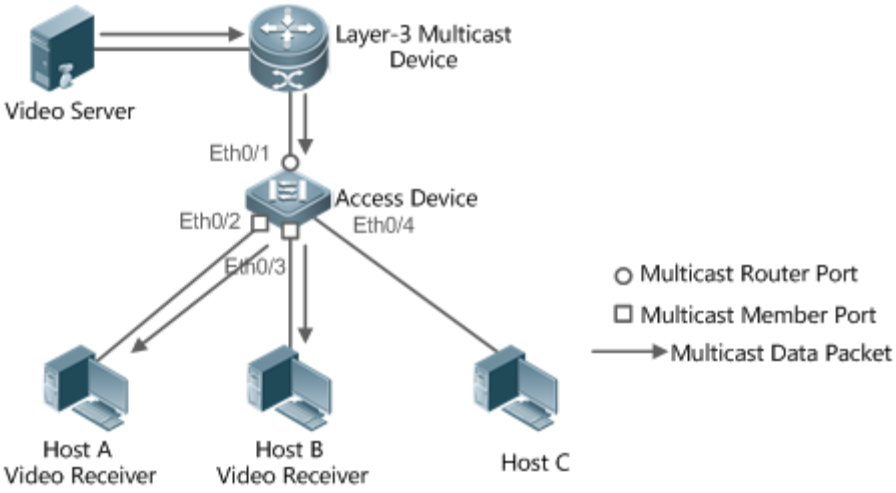

Рисунок 10-1. Два типа портов MLD Snooping

- Порт multicast-маршрутизатора: указывает порт на устройстве доступа для подключения к устройству multicast уровня 3, например, порт Eth0/1 устройства доступа.
- Порт участника: сокращение от порта участника группы multicast IPv6, также называемого Listener-портом, и указывает порт на устройстве доступа для подключения к участнику группы multicast IPv6, например, порт Eth0/2 и порт Eth0/3 на устройстве доступа.

10.1.3. Режим работы MLD Snooping

- Режим DISABLE: в этом режиме MLD Snooping не действует. То есть устройство multicast уровня 2 не делает «snoop» пакетов MLD между хостом и маршрутизатором, а потоки multicast транслируются внутри VLAN.

- Режим Independent VLAN Group Learn (IVGL). В этом режиме multicast-потоки между VLAN взаимно независимы. Хост может запрашивать только порт multicast-маршрутизатора в той же VLAN, что и хост, для получения multicast-пакетов и может пересылать полученные пакеты multicast-данных любой VLAN только на порт-участник и порт multicast-маршрутизатора в той же VLAN, что и хост.
- Режим Shared VLAN Group Learn (SVGL). В этом режиме хосты VLAN совместно используют один и тот же поток multicast. Хост в одной VLAN может запрашивать multicast-потоки из другой VLAN. Если указана Shared VLAN, только потоки multicast-данных этой VLAN могут пересылаться на хосты других VLAN. Потоки multicast-данных Shared VLAN могут пересылаться на порты-участники этого multicast-адреса, даже если некоторые порты-участники не принадлежат к Shared VLAN. В режиме SVGL профили MLD должны использоваться для выделения пакета диапазонов адресов multicast для SVGL. В пределах диапазонов multicast-адресов порты-участники в записях multicast-пересылки поддерживают пересылку пакетов через VLAN. По умолчанию все диапазоны групп не входят в диапазоны приложений SVGL, и все multicast-пакеты отбрасываются.
- Режим IVGL-SVGL: в этом режиме сосуществуют IVGL и SVGL. Вы можете использовать профили MLD для выделения пакета диапазонов адресов multicast для SVGL. В пределах диапазонов multicast-адресов порты-участники в записях multicast-пересылки поддерживают пересылку пакетов через VLAN. Порты-участники в записях переадресации multicast, соответствующие другим диапазонам адресов multicast, должны принадлежать одной и той же VLAN.

10.1.4. Принцип работы MLD Snooping

Устройство, на котором работает MLD Snooping, обрабатывает различные пакеты MLD следующим образом:

MLD QUERY

Устройство multicast уровня 3 регулярно отправляет пакет General Query MLD всем хостам и маршрутизаторам (с адресом FF02::1) в сегменте локальной сети для запроса (query) участников группы multicast IPv6 в этом сегменте сети. При получении пакета General Query MLD устройство, на котором выполняется MLD Snooping, пересылает пакет на все порты во VLAN, кроме порта, принимающего пакет, и обрабатывает порт, принимающий пакет, следующим образом:

- Если порт уже находится в списке портов multicast-маршрутизатора, его таймер устаревания сбрасывается.
- Если порт отсутствует в списке портов multicast-маршрутизатора, порт добавляется в список портов multicast-маршрутизатора и запускается его таймер устаревания.
- Каждый раз, когда multicast-устройство уровня 2 получает пакет General Query MLD, оно запускает таймер устаревания для каждого порта-участника и обновляет время таймера до настроенного максимального времени ответа пакета Query MLD. Когда время таймера устаревания порта уменьшается до 0, считается, что ни один участник не получает потоки multicast через этот порт, и поэтому устройство multicast уровня 2 удаляет порт из таблицы пересылки MLD Snooping.
- Каждый раз, когда multicast-устройство уровня 2 получает пакет Query MLD для группы, оно запускает таймер устаревания для каждого порта-участника в конкретной группе и обновляет время таймера до настроенного максимального времени ответа пакета Query MLD. Когда время таймера устаревания порта уменьшается до 0, считается, что ни один из участников не получает потоки

multicast через этот порт, и поэтому устройство multicast уровня 2 удаляет порт из таблицы пересылки MLD Snooping.

- Когда устройство multicast уровня 2 получает пакет Query MLD Group-Specific, оно больше не обновляет два предыдущих типа таймеров.

MLD REPORT

В любом из следующих случаев хост отправляет пакет Membership Report MLD в querier MLD.

- После получения пакета Query MLD (General Query или Group-Specific Query) хост-участник группы multicast IPv6 отвечает пакетом Membership Report MLD.
- Если хосту необходимо присоединиться к группе multicast IPv6, он активно отправляет пакет Membership ReportMLD querier-у MLD с запросом на присоединение к этой группе multicast IPv6.

При получении пакета Membership Report MLD устройство, на котором выполняется MLD Snooping, пересылает его на все порты multicast-маршрутизатора во VLAN, извлекает из пакета адрес группы multicast IPv6, к которой должен присоединиться хост, и обрабатывает порт, получающий пакет, следующим образом:

- Если нет записи переадресации, соответствующей группе multicast IPv6, создается запись переадресации, порт добавляется в список выходных портов как динамический порт-участник и запускается его таймер устаревания.
- Если существует запись пересылки, соответствующая группе multicast IPv6, но порт не содержится в списке выходных портов, порт добавляется в список выходных портов как динамический порт-участник, и запускается его таймер устаревания.
- Если существует запись пересылки, соответствующая группе multicast IPv6, и динамический порт-участник содержится в списке выходных портов, его таймер устаревания сбрасывается.

MLD LEAVE

Когда хост покидает группу multicast IPv6, он отправляет пакет MLD Leave (с адресом FF02::2), чтобы уведомить маршрутизатор multicast о том, что он покинул группу multicast IPv6. При получении пакета MLD Leave от порта-участника устройство, на котором выполняется MLD Snooping, напрямую пересылает его на порт multicast-маршрутизатора. Если функция быстрого выхода включена, устройство напрямую удаляет порт из списка портов переадресации соответствующей группы multicast.

10.1.5. Проверка порта источника

Функция проверки порта источника MLD Snooping повышает безопасность сети.

Эта функция строго ограничивает входные порты multicast-потоков MLD. Когда эта функция отключена, multicast-потоки с любого порта действительны, и устройство multicast уровня 2 пересылает их на зарегистрированные порты-участники в соответствии со списком пересылки MLD Snooping. Когда эта функция включена, действительны multicast-потоки только с портов multicast-маршрутизатора, и multicast-устройство уровня 2 перенаправляет их на зарегистрированные порты. Потоки multicast-данных из портов маршрутизатора, не поддерживающих multicast, являются недействительными и отбрасываются.

10.2. Приложения

Приложение	Описание
MLD Snooping SVGL Trans-VLAN Multicast по требованию	MLD Snooping работает в режиме SVGL
Фильтрация порта источника	Multicast-потоки принимаются только с портов multicast-маршрутизатора

10.2.1. MLD Snooping SVGL Trans-VLAN Multicast по требованию

10.2.1.1. Сценарий

Как показано на Рисунке 10-2, Хост A VLAN 3 и Хост B VLAN 4 заказывают видео. Видеопотоки находятся во VLAN 2.

Включите режим SVGL на устройстве доступа и настройте Shared VLAN 2.

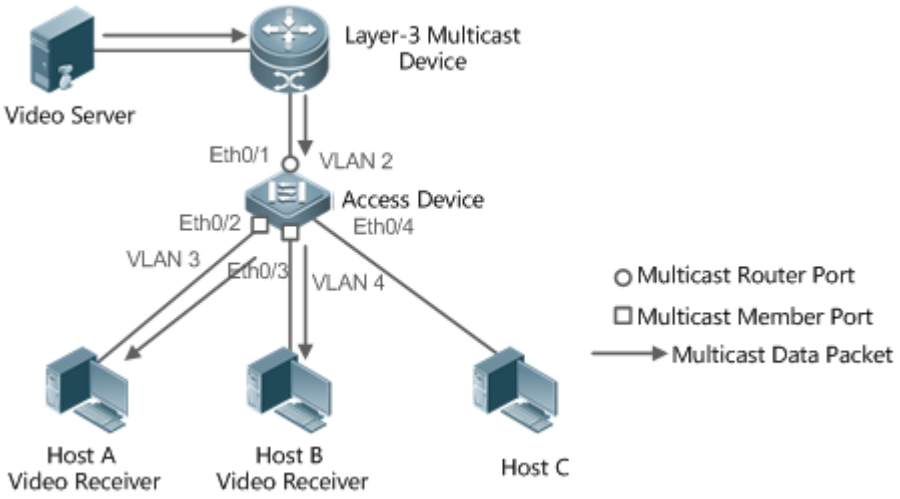

Рисунок 10-2.

VLAN 2 — это Shared VLAN.

VLAN 3 и VLAN 4 — это сети VLAN, через которые выводится сервис видео по запросу.

10.2.1.2. Развертывание

- Включите протокол multicast уровня 3 на устройстве multicast уровня 3.
- Включите режим SVGL на устройстве уровня 2.

10.2.2. Фильтрация порта источника

10.2.2.1. Сценарий

Как показано на Рисунке 10-3, когда настроена функция проверки порта источника, видеопотоки можно принимать только с порта исходного multicast-маршрутизатора. Multicast-видеопотоки с других портов недействительны и отбрасываются. Обратите

внимание, что, если настроена функция проверки порта источника, должен быть хотя бы один порт multicast-маршрутизатора. В противном случае фильтрация пакетов не выполняется на порту multicast-маршрутизатора, даже если фильтрация порта источника включена. Если функция проверки порта источника не настроена, по умолчанию принимаются multicast-видеопотоки со всех портов.

- Включите режим IVGL на устройстве доступа.

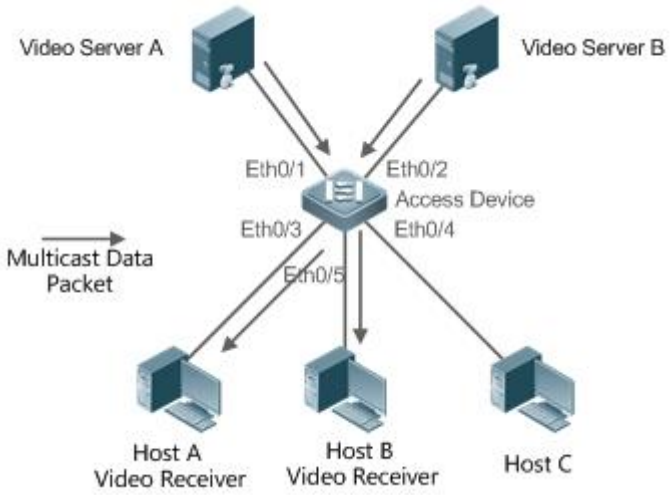

Рисунок 10-3.

Порт Eth0/1 — это порт multicast-маршрутизатора, а порт Eth0/2 — порт маршрутизатора без multicast.

Видеосерверы отправляют одни и те же multicast-видеопотоки.

Хосты A и B могут получать multicast-потоки только с Видеосервера A.

10.2.2.2. Развертывание

- Включите функцию проверки порта источника и настройте статический порт multicast-маршрутизатора.
- Включите режим IVGL на устройстве уровня 2.

10.3. Функции

10.3.1. Базовые определения

Порт multicast-маршрутизатора и порт-участник

Порты multicast-маршрутизатора подразделяются на динамические порты multicast-маршрутизатора и статические порты multicast-маршрутизатора. Если MLD Snooping включено, когда на порту включена функция изучения порта динамического multicast-маршрутизатора, после получения Query MLD или пакета PIMv6-Hello порт изучает порт динамического multicast-маршрутизатора и запускает таймер устаревания порта динамического multicast-маршрутизатора. Статический порт multicast-маршрутизатора можно добавить, настроив команду **ipv6 mld snooping vlan mrouter**.

Порты-участники подразделяются на динамические порты-участники и статические порты-участники. Если MLD Snooping включено, после получения пакета Report MLD порт изучает динамический порт-участник маршрутизатора и запускает таймер устаревания динамического порта-участника. Статический порт-участник можно добавить, настроив команду **ipv6 mld snooping vlan static interface**.

Fast Leave (быстрый выход) и подавление пакетов

Если функция Fast Leave включена, порт удаляется напрямую после получения пакета MLD Leave. Функция Fast Leave применима только в сценариях, в которых к порту подключен только один пользователь, и помогает экономить полосу пропускания. Когда к порту подключено несколько пользователей, если включена функция Fast Leave, другие пользователи, желающие получать пакеты, не смогут получить какие-либо пакеты.

Если функция подавления пакетов включена, в течение одного периода Query пересылается только первый пакет Report MLD.

10.3.2. Обзор

Особенность	Описание
Глобальное включение MLD Snooping	Глобально включает MLD Snooping и настраивает режим работы
MLD Snooping на основе VLAN	Включает или отключает MLD Snooping для одной VLAN, когда MLD Snooping включено глобально
Время устаревания портов multicast-маршрутизатора	Регулирует время устаревания динамических портов multicast-маршрутизатора. Время устаревания по умолчанию составляет 300 с
Изучение динамического порта multicast-маршрутизатора	После получения пакета Query MLD или пакета Hello PIMv6 порт изучается как динамический порт multicast-маршрутизатора
Fast Leave портов-участников группы multicast	Порт-участник можно быстро удалить вместо устаревания и удаления после истечения интервала Group-Specific Query
Подавление пакетов Report MLD	В течение одного периода Query обрабатывается только первый пакет Report, что снижает рабочую нагрузку на модуль
Проверка порта источника	Потоки multicast, полученные только от порта маршрутизатора multicast, могут пересылаться. Пакеты, полученные от портов маршрутизатора, не поддерживающих multicast, не могут пересылаться
Фильтрация групп multicast на основе портов	Могут быть получены только групповые multicast-пакеты, соответствующие условиям фильтра
Максимальное количество групп multicast, поддерживаемых портом	Ограничивает максимальное количество групп multicast, к которым может присоединиться порт

10.3.3. Глобальное включение MLD Snooping

Глобально включите MLD Snooping и настройте режим работы. Можно изучить записи multicast-пересылки, и потоки multicast перенаправляются на указанный порт.

10.3.3.1. Принцип работы

Включите MLD Snooping. Когда получен пакет Report MLD со временем time to live (TTL), равным 1, создается запись multicast-пересылки, и исходящим пунктом (выходом) пересылки является этот порт.

Изучение динамического порта-участника

После получения действительного пакета Report MLD изучается динамический порт-участник и создается запись пересылки. Выходом пересылки этой записи является порт-участник.

Координационные параметры

Настройте функцию подавления пакетов Report MLD.

10.3.3.2. Сопутствующая конфигурация

Настройте функцию подавления пакетов Report MLD так, чтобы в течение одного периода Query обрабатывался только первый Report, тем самым уменьшая количество пакетов в сети.

10.3.4. MLD Snooping на основе VLAN

Включите или отключите MLD Snooping для одной VLAN. По умолчанию, если MLD Snooping включено глобально, функция MLD Snooping включена для каждой VLAN.

10.3.4.1. Сопутствующая конфигурация

Глобально настройте MLD Snooping. Затем настройте MLD Snooping для одной VLAN.

10.3.5. Время устаревания портов multicast-маршрутизатора

Порты multicast-маршрутизатора подразделяются на динамические порты multicast-маршрутизатора и статические порты multicast-маршрутизатора. По умолчанию время устаревания динамического порта multicast-маршрутизатора составляет 300 с. Статические порты multicast-маршрутизатора не устаревают.

10.3.5.1. Сопутствующая конфигурация

Возможность изучения с помощью функции изучения динамического порта multicast-маршрутизатора.

10.3.6. Изучение динамического порта multicast-маршрутизатора

По умолчанию все порты поддерживают функцию изучения динамических портов multicast-маршрутизатора.

10.3.6.1. Принцип работы

Если порт поддерживает функцию изучения динамического порта multicast-маршрутизатора, после получения пакета Query MLD или пакета Hello PIMv6 порт изучается как динамический порт multicast-маршрутизатора.

10.3.6.2. Сопутствующая конфигурация

Настройте порт как статический порт multicast-маршрутизатора.

10.3.7. Время устаревания динамических портов-участников

Порты-участники подразделяются на динамические порты-участники и статические порты-участники. По умолчанию время устаревания динамического порта-участника составляет 260 с. Статические порты-участники не устаревают.

10.3.8. Fast Leave портов-участников группы multicast

По умолчанию функция Fast Leave портов-участников группы multicast отключена. Если функция Fast Leave включена, порт удаляется напрямую после получения готового пакета.

10.3.9. Подавление пакетов Report MLD

По умолчанию функция подавления пакетов Report MLD отключена. Если функция включена, в течение одного интервала Query обрабатывается только первый пакет Report, тем самым уменьшая количество пакетов в сети.

10.3.10. Проверка порта источника

По умолчанию функция проверки порта источника отключена.

10.3.10.1. Принцип работы

Если функция проверки порта источника включена, действительными являются только пакеты от портов multicast-маршрутизатора, а пакеты от портов не multicast-маршрутизатора — недействительными.

10.3.10.2. Сопутствующая конфигурация

Настройте порт как статический порт multicast-маршрутизатора.

10.3.11. Фильтрация групп multicast на основе портов

При определенных обстоятельствах вы можете использовать функцию фильтрации портов, чтобы контролировать порт для пересылки multicast-пакетов только определенного диапазона.

10.3.12. Максимальное количество групп multicast, поддерживаемых портом

Максимальное количество групп multicast, которым разрешено присоединиться порту, может контролировать максимальное количество групп multicast, поддерживаемых портом.

10.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций MLD Snooping	**ipv6 mld snooping**	Включает MLD Snooping и определяет режим работы
	ipv6 mld snooping vlan *vlan-id* **mrouter interface** *interface-id*	Настраивает статический порт multicast-маршрутизатора

Конфигурация	Описание и команда	
Настройка основных функций MLD Snooping	**ipv6 mld snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id*	Настраивает статический порт-участник
	ipv6 mld profile *profile-num*	Настраивает профиль
	ipv6 mld snooping source-check port	Настраивает проверку порта источника
	ipv6 mld snooping filter *profile-num*	Настраивает фильтрацию multicast групп для порта
	ipv6 mld snooping max-groups *num*	Настраивает максимальное количество групп multicast, к которым может присоединиться порт

10.4.1. Настройка основных функций MLD Snooping

10.4.1.1. Эффект конфигурации

Включите MLD Snooping и настройте режим работы.

10.4.1.2. Примечания

- Включите MLD Snooping и установите рабочий узел на SVGL. Режим MLD Snooping SVGL не может сосуществовать с multicast-рассылкой уровня 3 IPv4 или IPv6.
- Если рабочим режимом является SVGL или IVGL-SVGL, необходимо связать профиль, чтобы указать диапазон групп multicast, в котором применяется режим SVGL.

10.4.1.3. Шаги настройки

Включение IPv6 MLD Snooping

Обязательный.

10.4.1.4. Проверка

Запустите команду **show ipv6 mld snooping**, чтобы проверить, включено ли MLD Snooping.

- Проверьте, может ли устройство создавать правильные записи multicast.

10.4.1.5. Связанные команды

Включение IPv6 MLD Snooping

Команда	**ipv6 mld snooping** *mode*
Описание параметра	*mode*: определяет режим работы
Командный режим	Режим глобальной конфигурации

Настройка профиля

Команда	**ipv6 mld profile** *profile-num*
Описание параметра	*profile-num*: указывает номер профиля
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы настроить профиль и войти в режим настройки профиля

Настройка статический порта multicast-маршрутизатора

Команда	**ipv6 mld snooping vlan** *vlan-id* **mrouter interface** *interface-id*
Описание параметра	*vlan-id*: указывает идентификатор VLAN. *interface-id*: указывает на изменения интерфейса
Командный режим	Режим глобальной конфигурации

Настройка статического порта-участника

Команда	**ipv6 mld snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id*
Описание параметра	*vlan-id*: указывает идентификатор VLAN. *ip-addr*: указывает адрес группы. *interface-id*: указывает на изменения интерфейса
Командный режим	Режим глобальной конфигурации

Настройка проверки порта источника

Команда	**ipv6 mld snooping source-check port**
Командный режим	Режим глобальной конфигурации

Настройка фильтрации multicast групп на основе порта

Команда	**ipv6 mld snooping filter** *profile-num*
Описание параметра	*profile-num*: указывает номер профиля
Командный режим	Порт конфигурации интерфейса

Настройка максимального количества групп multicast, поддерживаемых портом

Команда	**ipv6 mld snooping max-groups** *num*
Описание параметра	*num*: указывает количество групп
Командный режим	Порт конфигурации интерфейса

Настройка подавления пакетов Report

Команда	**ipv6 mld snooping suppression enable**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если функция подавления пакетов Report включена, только первый пакет Report конкретной VLAN и группы пересылается на порт multicast-маршрутизатора в течение одного интервала Query. Последующие пакеты Report пересылаются на порт multicast-маршрутизатора, чтобы уменьшить количество пакетов в сети. Эта функция может подавлять только пакеты Report MLDv1. Он недействителен для пакетов Report MLDv2

Настройка Fast Leave порта

Команда	**ipv6 mld snooping fast-leave enable**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если функция Fast Leave порта включена, после получения пакета Leave порт напрямую удаляется из портов-участников в соответствующих записях пересылки. Позже, при получении соответствующего пакета Group-Specific Query, устройство не пересылает пакет на этот порт. Пакет Leaver включает пакет Leave для MLDv1, включает тип MLDv2 и пакет Report, не содержащий адреса источника. Эта функция применима только к сценариям, в которых к порту подключен только один пользователь, и помогает экономить полосу пропускания и ресурсы

Настройка изучения динамических портов multicast-маршрутизатора

Команда	**ipv6 mld snooping** [**vlan** *vid*] **mrouter learn**
Описание параметра	**vlan** *id*: указывает идентификатор VLAN. По умолчанию эта функция применима ко всем VLAN
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Порт multicast-маршрутизатора — это порт, который напрямую соединяет устройство multicast с поддержкой MLD Snooping к соседнему устройству multicast, в котором включен протокол multicast-маршрутизации. По умолчанию, когда функция изучения динамического порта multicast-маршрутизатора включена, устройство автоматически прослушивает пакет MLD Query/PIM Hello и динамически определяет порт multicast-маршрутизатора

Настройка времени устаревания динамических портов multicast-маршрутизатора

Команда	**ipv6 mld snooping dyn-mr-aging-time** *seconds*
Описание параметра	*seconds*: указывает срок устаревания динамических портов multicast-маршрутизатора. Единица измерения — секунда, значение варьируется от 1 до 3600
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Если динамический порт multicast-маршрутизатора не получает пакет General Query MLD или пакет Hello PIM до истечения срока его устаревания, устройство удаляет порт из списка портов multicast-маршрутизатора. Когда функция изучения динамического multicast-маршрутизатора включена, вы можете использовать эту команду для настройки времени устаревания динамических портов multicast-маршрутизатора. Если время устаревания слишком короткое, порт multicast-маршрутизатора может часто добавляться и удаляться

Настройка времени устаревания динамических портов-участников

Команда	**ipv6 mld snooping host-aging-time** *seconds*
Описание параметра	*seconds*: указывает время устаревания
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Время устаревания динамического порта-участника относится к времени устаревания, установленному, когда динамический порт-участник устройства получает от хоста пакет MLD о присоединении к определенной группе multicast IPv6. После получения пакета Join MLD от динамического порта-участника устройство сбрасывает таймер устаревания динамического порта-участника и устанавливает время таймера на время устаревания хоста. Если время таймера истекает, считается, что ни один пользовательский хост не получает multicast-пакеты через этот порт, а затем устройство multicast удаляет порт из списка портов-участников MLD Snooping. После настройки этой команды значение таймера устаревания динамических портов-участников при последующем получении пакетов MLD Join равно времени устаревания хоста. Время устаревания вступает в силу сразу после настройки, и таймеры запущенных портов-участников обновляются

Настройка времени ответа пакетов Query

Команда	**ipv6 mld snooping query-max-response-time** *seconds*
Описание параметра	*seconds*: указывает время отклика
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После получения пакета General Query MLD от порта multicast-устройство сбрасывает таймеры устаревания всех динамических портов-участников и устанавливает время таймера на

	максимальное время ответа на Query (query-max-response-time). Если время таймера истекает, считается, что ни один пользовательский хост не получает multicast-пакеты через порт, а затем устройство multicast удаляет порт из списка портов-участников MLD Snooping. После получения пакета Group-Specific Query MLD из порта multicast-устройство сбрасывает таймеры устаревания всех динамических портов-участников в конкретной группе и устанавливает время таймера на максимальное время ответа на Query. Если время таймера истекает, считается, что ни один пользовательский хост не получает multicast-пакеты через порт, а затем устройство multicast удаляет порт из списка портов-участников MLD Snooping. Конфигурация вступит в силу, когда пакет Query будет получен в следующий раз, и конфигурация запущенных в данный момент таймеров не будет обновлена. Для пакетов Group-Specific Query MLDv2 таймеры не обновляются

Проверка портов multicast-маршрутизатора

Команда	**show ipv6 mld snooping mroute**
Командный режим	Привилегированный режим EXEC, режим глобальной конфигурации, режим конфигурации интерфейса
Руководство по использованию	Если порт multicast-маршрутизатора успешно настроен, в отображаемой информации об интерфейсе отображается знак «S». Например: QTECH(config)#show ipv6 mld snooping mrouter Multicast Switching Mroute Port D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/1(S)

Проверка изучения динамических портов multicast-маршрутизатора

Команда	**show ipv6 mld snooping**
Командный режим	Привилегированный режим EXEC, режим глобальной конфигурации, режим настройки интерфейса
Руководство по использованию	Запустите команду **show ip igmp snooping**, чтобы проверить время устаревания и состояние изучения динамических портов multicast-маршрутизатора. Dynamic Mroute Aging Time : 300(Seconds)

	Multicast router learning mode: Enable

Проверка портов-участников

Команда	**show ipv6 mld snooping gda-table**
Командный режим	Привилегированный режим EXEC, режим глобальной конфигурации, режим конфигурации интерфейса
Руководство по использованию	Если порт-участник успешно настроен, в отображаемой информации об интерфейсе отображается знак «S». Например: QTECH(config)#show ipv6 mld snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*, FF15::100, 1): VLAN(1) 2 OPORTS: GigabitEthernet 3/7(S)

Проверка других параметров

Команда	**show ipv6 mld snooping**
Командный режим	Привилегированный режим EXEC, режим глобальной конфигурации, режим конфигурации интерфейса
Руководство по использованию	Запустите команду **show ipv6 mld snooping**, чтобы проверить время устаревания портов multicast-маршрутизатора, время устаревания динамических портов-участников, время ответа пакета Query, подавление пакетов Report и параметры Fast Leave. MLD-snooping mode: IVGL Source port check: Disable MLD Fast-Leave: Disable MLD Report suppress: Disable Query Max Response Time: 10 (Seconds) Dynamic Mroute Aging Time: 300(Seconds) Dynamic Host Aging Time: 260(Seconds)

10.5. Мониторинг

10.5.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере важной информации и, таким образом, к прерыванию работы служб.

Описание	Команда
Очищает записи MLD Snooping multicast-пересылки	**clear ipv6 mld snooping gda-table**
Очищает статистику MLD Snooping	**clear ipv6 mld snooping statistics**

10.5.2. Отображение

Описание	Команда
Отображает текущий режим MLD Snooping	**show ipv6 mld snooping**
Отображает записи пересылки MLD Snooping	**show ipv6 mld snooping gda-table**
Отображает статистику MLD Snooping	**show ipv6 mld snooping statistics**
Отображает порты multicast-маршрутизатора MLD Snooping	**show ipv6 mld snooping mrouter**
Отображает информацию об интерфейсе MLD Snooping, профили фильтрации интерфейса и максимальное количество групп, к которым может присоединиться порт	**show ipv6 mld snooping interfaces** *interface-type interface-name*
Отображает информацию multicast-рассылки об одной VLAN, в которой настроено MLD Snooping	**show ipv6 mld snooping vlan** *vid*
Отображает профиль MLD	**show ipv6 mld profile** *profile-number*

11. ОБЩАЯ ИНФОРМАЦИЯ

11.1. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» −> «Гарантийное обслуживание».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» −> «Взять оборудование на тест».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

11.2. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться нашей автоматизированной системой запросов технического сервис-центра helpdesk.qtech.ru.

Телефон Технической поддержки +7 (495) 269-08-81

Центральный офис +7 (495) 477-81-18

11.3. Электронная версия документа

Дата публикации 26.12.2024

https://files.qtech.ru/upload/switchers/QSW-6910/QSW-6910_multicast_config_guide.pdf