

Руководство по настройке
Конфигурация IP-маршрутизации
Ethernet-коммутаторы ЦОД
серия QSW-7600

Оглавление

1. НАСТРОЙКА ПОЛИТИК МАРШРУТИЗАЦИИ 35
1.1. Обзор 35
1.2. Приложения 35
1.2.1. Фильтрация маршрутов 35
1.2.1.1. Сценарий 36
1.2.1.2. Развертывание 36
1.2.2. Перераспределение маршрутов 36
1.2.2.1. Сценарий 37
1.2.2.2. Развертывание 37
1.2.3. PBR 37
1.2.3.1. Сценарий 38
1.2.3.2. Развертывание 38
1.3. Функции 39
1.3.1. Обзор 39
1.3.2. Список фильтрации 39
1.3.2.1. Принцип работы 39
1.3.2.2. Сопутствующая конфигурация 40
1.3.3. Карта маршрута 41
1.3.3.1. Принцип работы 41
1.3.3.2. Сопутствующая конфигурация 41
1.4. Конфигурация 45
1.4.1. Настройка карты маршрутов 46
1.4.1.1. Эффект конфигурации 46
1.4.1.2. Примечания 46
1.4.1.3. Шаги настройки 47
1.4.1.4. Проверка 48
1.4.1.5. Связанные команды 48
1.4.1.6. Пример конфигурации 66
1.4.1.7. Распространенные ошибки 70
1.4.2. Настройка списка фильтрации 71
1.4.2.1. Эффект конфигурации 71
1.4.2.2. Примечания 71
1.4.2.3. Шаги настройки 71
1.4.2.4. Проверка 71
1.4.2.5. Связанные команды 71
1.4.2.6. Пример конфигурации 75

1.4.2.7. Распространенные ошибки 86
1.5. Мониторинг 86
1.5.1. Отображение 86
2. НАСТРОЙКА КЛЮЧЕЙ 88
2.1. Обзор 88
2.2. Приложения 88
2.2.1. RIP-аутентификация 88
2.2.1.1. Сценарий 88
2.2.1.2. Развертывание 88
2.3. Функции 89
2.3.1. Обзор 89
2.3.2. Цепочка ключей 89
2.3.2.1. Принцип работы 89
2.3.2.2. Сопутствующая конфигурация 89
2.4. Конфигурация 90
2.4.1. Настройка цепочки ключей 90
2.4.1.1. Эффект конфигурации 90
2.4.1.2. Примечания 90
2.4.1.3. Шаги настройки 90
2.4.1.4. Проверка 91
2.4.1.5. Связанные команды 91
2.4.1.6. Пример конфигурации 93
2.4.1.7. Распространенные ошибки 94
2.5. Мониторинг 95
2.5.1. Отображение 95
3. НАСТРОЙКА RIP 96
3.1. Обзор 96
3.1.1.1. Протоколы и стандарты 96
3.2. Приложения 96
3.2.1. Базовое приложение RIP 96
3.2.1.1. Сценарий 96
3.2.1.2. Развертывание 97
3.2.2. Взаимодействие между RIP и BGP 97
3.2.2.1. Сценарий 97
3.2.2.2. Развертывание 98
3.3. Функции 98
3.3.1. Базовые определения 98

3.3.1.1. Обзор 98
3.3.2. RIPv1 и RIPv2 99
3.3.2.1. Принцип работы 99
3.3.2.2. Сопутствующая конфигурация 99
3.3.3. Обмен информацией о маршрутизации 100
3.3.3.1. Принцип работы 101
3.3.3.2. Сопутствующая конфигурация 102
3.3.4. Алгоритм маршрутизации 103
3.3.4.1. Принцип работы 103
3.3.4.2. Сопутствующая конфигурация 105
3.3.5. Как избежать петель маршрута 105
3.3.5.1. Принцип работы 105
3.3.5.2. Сопутствующая конфигурация 107
3.3.6. Меры безопасности 107
3.3.6.1. Принцип работы 107
3.3.6.2. Сопутствующая конфигурация 108
3.3.7. Меры надежности 108
3.3.7.1. Принцип работы 108
3.3.7.2. Сопутствующая конфигурация 109
3.3.8. Несколько экземпляров 109
3.3.8.1. Принцип работы 109
3.3.8.2. Сопутствующая конфигурация 109
3.4. Конфигурация 110
3.4.1. Настройка основных функций RIP 114
3.4.1.1. Эффект конфигурации 114
3.4.1.2. Примечания 114
3.4.1.3. Шаги настройки 114
3.4.1.4. Проверка 115
3.4.1.5. Связанные команды 115
3.4.1.6. Пример конфигурации 117
3.4.1.7. Распространенные ошибки 120
3.4.2. Управление взаимодействием пакетов RIP 120
3.4.2.1. Эффект конфигурации 120
3.4.2.2. Примечания 121
3.4.2.3. Шаги настройки 121
3.4.2.4. Проверка 122
3.4.2.5. Связанные команды 122
3.4.2.6. Пример конфигурации 124

3.4.2.7. Распространенные ошибки 125
3.4.3. Включение триггерных обновлений 125
3.4.3.1. Эффект конфигурации 125
3.4.3.2. Примечания 125
3.4.3.3. Шаги настройки 125
3.4.3.4. Проверка 126
3.4.3.5. Связанные команды 126
3.4.3.6. Пример конфигурации 127
3.4.3.7. Распространенные ошибки 128
3.4.4. Включение проверки адреса источника 128
3.4.4.1. Эффект конфигурации 128
3.4.4.2. Примечания 128
3.4.4.3. Шаги настройки 128
3.4.4.4. Проверка 129
3.4.4.5. Связанные команды 129
3.4.4.6. Пример конфигурации 129
3.4.5. Включение аутентификации 130
3.4.5.1. Эффект конфигурации 130
3.4.5.2. Примечания 130
3.4.5.3. Шаги настройки 130
3.4.5.4. Проверка 131
3.4.5.5. Связанные команды 131
3.4.5.6. Пример конфигурации 133
3.4.5.7. Распространенные ошибки 134
3.4.6. Включение суммирования маршрутов 134
3.4.6.1. Эффект конфигурации 134
3.4.6.2. Примечания 134
3.4.6.3. Шаги настройки 135
3.4.6.4. Проверка 135
3.4.6.5. Связанные команды 135
3.4.6.6. Пример конфигурации 136
3.4.6.7. Распространенные ошибки 137
3.4.7. Включение маршрутов Supernetting 137
3.4.7.1. Эффект конфигурации 137
3.4.7.2. Примечания 137
3.4.7.3. Шаги настройки 137
3.4.7.4. Проверка 137
3.4.7.5. Связанные команды 137

3.4.7.6. Пример конфигурации 138
3.4.8. Объявление маршрута по умолчанию или внешних маршрутов 139
3.4.8.1. Эффект конфигурации 139
3.4.8.2. Примечания 139
3.4.8.3. Шаги настройки 139
3.4.8.4. Проверка 140
3.4.8.5. Связанные команды 140
3.4.8.6. Пример конфигурации 143
3.4.9. Настройка правил фильтрации маршрутов 143
3.4.9.1. Эффект конфигурации 143
3.4.9.2. Примечания 143
3.4.9.3. Шаги настройки 144
3.4.9.4. Проверка 144
3.4.9.5. Связанные команды 144
3.4.9.6. Пример конфигурации 146
3.4.9.7. Распространенные ошибки 147
3.4.10. Изменение параметров выбора маршрута 147
3.4.10.1. Эффект конфигурации 147
3.4.10.2. Примечания 148
3.4.10.3. Шаги настройки 148
3.4.10.4. Проверка 148
3.4.10.5. Связанные команды 148
3.4.10.6. Пример конфигурации 150
3.4.11. Изменение таймеров 151
3.4.11.1. Эффект конфигурации 151
3.4.11.2. Примечания 151
3.4.11.3. Шаги настройки 151
3.4.11.4. Проверка 151
3.4.11.5. Связанные команды 152
3.4.11.6. Пример конфигурации 153
3.4.11.7. Распространенные ошибки 154
3.4.12. Включение корреляции BFD 154
3.4.12.1. Эффект конфигурации 154
3.4.12.2. Примечания 154
3.4.12.3. Шаги настройки 154
3.4.12.4. Проверка 154
3.4.12.5. Связанные команды 155
3.4.12.6. Пример конфигурации 155

3.4.12.7. Распространенные ошибки 156
3.4.13. Включение быстрого перенаправления 157
3.4.13.1. Эффект конфигурации 157
3.4.13.2. Примечания 157
3.4.13.3. Шаги настройки 157
3.4.13.4. Проверка 157
3.4.13.5. Связанные команды 157
3.4.13.6. Пример конфигурации 158
3.4.13.7. Распространенные ошибки 159
3.4.14. Включение GR 159
3.4.14.1. Эффект конфигурации 159
3.4.14.2. Примечания 159
3.4.14.3. Шаги настройки 159
3.4.14.4. Проверка 160
3.4.14.5. Связанные команды 160
3.4.14.6. Пример конфигурации 161
3.4.15. Включение нескольких экземпляров 162
3.4.15.1. Эффект конфигурации 162
3.4.15.2. Примечания 162
3.4.15.3. Шаги настройки 162
3.4.15.4. Проверка 162
3.4.15.5. Связанные команды 162
3.4.15.6. Пример конфигурации 164
3.5. Мониторинг 165
3.5.1. Отображение 165
3.5.1.1. Отладка 165
4. НАСТРОЙКА OSPFV2 167
4.1. Обзор 167
4.1.1. Протоколы и стандарты 167
4.2. Приложения 168
4.2.1. Внутридоменное взаимодействие 169
4.2.1.1. Сценарий 169
4.2.1.2. Развертывание 170
4.2.2. Междоменное взаимодействие 170
4.2.2.1. Сценарий 170
4.2.2.2. Развертывание 170
4.3. Функции 170

4.3.1. Базовые определения 170
4.3.2. Обзор 175
4.3.3. Протоколы маршрутизации по состоянию канала 175
4.3.3.1. Принцип работы 175
4.3.3.2. Сопутствующая конфигурация 179
4.3.4. Управление маршрутами OSPF 180
4.3.4.1. Принцип работы 180
4.3.4.2. Сопутствующая конфигурация 184
4.3.5. Повышенная безопасность и надежность 186
4.3.5.1. Принцип работы 186
4.3.5.2. Сопутствующая конфигурация 189
4.3.6. Управление сетью 191
4.3.6.1. Принцип работы 191
4.3.6.2. Сопутствующая конфигурация 192
4.4. Конфигурация 192
4.4.1. Настройка основных функций OSPF 200
4.4.1.1. Эффект конфигурации 200
4.4.1.2. Примечания 200
4.4.1.3. Шаги настройки 200
4.4.1.4. Проверка 201
4.4.1.5. Связанные команды 201
4.4.1.6. Пример конфигурации 204
4.4.1.7. Распространенные ошибки 207
4.4.2. Установка типа сети 207
4.4.2.1. Эффект конфигурации 207
4.4.2.2. Примечания 208
4.4.2.3. Шаги настройки 208
4.4.2.4. Проверка 208
4.4.2.5. Связанные команды 208
4.4.2.6. Пример конфигурации 210
4.4.2.7. Распространенные ошибки 212
4.4.3. Настройка перераспределения маршрутов и маршрута по умолчанию 212
4.4.3.1. Эффект конфигурации 212
4.4.3.2. Примечания 212
4.4.3.3. Шаги настройки 212
4.4.3.4. Проверка 212
4.4.3.5. Связанные команды 213
4.4.3.6. Пример конфигурации 215

4.4.3.7. Распространенные ошибки 218
4.4.4. Настройка тупиковой области и области NSSA 218
4.4.4.1. Эффект конфигурации 218
4.4.4.2. Примечания 218
4.4.4.3. Шаги настройки 218
4.4.4.4. Проверка 219
4.4.4.5. Связанные команды 219
4.4.4.6. Пример конфигурации 221
4.4.4.7. Распространенные ошибки 225
4.4.5. Настройка суммирования маршрутов 226
4.4.5.1. Эффект конфигурации 226
4.4.5.2. Примечания 226
4.4.5.3. Шаги настройки 226
4.4.5.4. Проверка 226
4.4.5.5. Связанные команды 226
4.4.5.6. Пример конфигурации 228
4.4.5.7. Распространенные ошибки 229
4.4.6. Настройка фильтрации маршрутов 230
4.4.6.1. Эффект конфигурации 230
4.4.6.2. Примечания 230
4.4.6.3. Шаги настройки 230
4.4.6.4. Проверка 230
4.4.6.5. Связанные команды 231
4.4.6.6. Пример конфигурации 233
4.4.6.7. Распространенные ошибки 234
4.4.7. Изменение стоимости маршрута и AD 234
4.4.7.1. Эффект конфигурации 234
4.4.7.2. Примечания 234
4.4.7.3. Шаги настройки 234
4.4.7.4. Проверка 235
4.4.7.5. Связанные команды 235
4.4.7.6. Пример конфигурации 240
4.4.7.7. Распространенные ошибки 241
4.4.8. Включение аутентификации 241
4.4.8.1. Эффект конфигурации 241
4.4.8.2. Примечания 241
4.4.8.3. Шаги настройки 241
4.4.8.4. Проверка 242

4.4.8.5. Связанные команды 242
4.4.8.6. Пример конфигурации 245
4.4.8.7. Распространенные ошибки 246
4.4.9. Включение переполнения 246
4.4.9.1. Эффект конфигурации 246
4.4.9.2. Примечания 246
4.4.9.3. Шаги настройки 246
4.4.9.4. Проверка 247
4.4.9.5. Связанные команды 247
4.4.9.6. Пример конфигурации 249
4.4.9.7. Распространенные ошибки 250
4.4.10. Изменение максимального количества одновременных соседей 250
4.4.10.1. Эффект конфигурации 250
4.4.10.2. Примечания 250
4.4.10.3. Шаги настройки 250
4.4.10.4. Проверка 250
4.4.10.5. Связанные команды 251
4.4.10.6. Пример конфигурации 251
4.4.11. Отключение проверки адреса источника 252
4.4.11.1. Эффект конфигурации 252
4.4.11.2. Примечания 253
4.4.11.3. Шаги настройки 253
4.4.11.4. Проверка 253
4.4.11.5. Связанные команды 253
4.4.11.6. Пример конфигурации 253
4.4.12. Отключение проверки MTU 254
4.4.12.1. Эффект конфигурации 254
4.4.12.2. Примечания 255
4.4.12.3. Шаги настройки 255
4.4.12.4. Проверка 255
4.4.12.5. Связанные команды 255
4.4.12.6. Пример конфигурации 255
4.4.13. Включение двустороннего обслуживания 256
4.4.13.1. Эффект конфигурации 256
4.4.13.2. Примечания 256
4.4.13.3. Шаги настройки 256
4.4.13.4. Проверка 256
4.4.13.5. Связанные команды 257

4.4.13.6. Пример конфигурации 257
4.4.14. Включение GR 258
4.4.14.1. Эффект конфигурации 258
4.4.14.2. Примечания 258
4.4.14.3. Шаги настройки 258
4.4.14.4. Проверка 258
4.4.14.5. Связанные команды 259
4.4.14.6. Пример конфигурации 261
4.4.14.7. Распространенные ошибки 262
4.4.15. Включение NSR 262
4.4.15.1. Эффект конфигурации 262
4.4.15.2. Примечания 262
4.4.15.3. Шаги настройки 262
4.4.15.4. Проверка 262
4.4.15.5. Связанные команды 262
4.4.15.6. Пример конфигурации 263
4.4.15.7. Распространенные ошибки 264
4.4.16. Корреляция OSPF с BFD 264
4.4.16.1. Эффект конфигурации 264
4.4.16.2. Примечания 264
4.4.16.3. Шаги настройки 264
4.4.16.4. Проверка 264
4.4.16.5. Связанные команды 265
4.4.16.6. Пример конфигурации 265
4.4.17. Включение быстрого перенаправления 267
4.4.17.1. Эффект конфигурации 267
4.4.17.2. Примечания 267
4.4.17.3. Шаги настройки 267
4.4.17.4. Проверка 267
4.4.17.5. Связанные команды 268
4.4.17.6. Пример конфигурации 269
4.4.18. Включение iSPF 271
4.4.18.1. Эффект конфигурации 271
4.4.18.2. Примечания 271
4.4.18.3. Шаги настройки 271
4.4.18.4. Проверка 271
4.4.18.5. Связанные команды 271
4.4.18.6. Пример конфигурации 271

4.4.19. Настройка функции управления сетью 274
4.4.19.1. Эффект конфигурации 274
4.4.19.2. Примечания 274
4.4.19.3. Шаги настройки 274
4.4.19.4. Проверка 275
4.4.19.5. Связанные команды 275
4.4.19.6. Пример конфигурации 277
4.4.19.7. Распространенные ошибки 278
4.4.20. Изменение параметров управления протоколом 278
4.4.20.1. Эффект конфигурации 278
4.4.20.2. Примечания 278
4.4.20.3. Шаги настройки 278
4.4.20.4. Проверка 279
4.4.20.5. Связанные команды 279
4.4.20.6. Пример конфигурации 284
4.4.20.7. Распространенные ошибки 285
4.5. Мониторинг 286
4.5.1.1. Очистка 286
4.5.1.2. Отображение 286
4.5.1.3. Отладка 287
5. НАСТРОЙКА OSPFV3 288
5.1. Обзор 288
5.1.1.1. Протоколы и стандарты 288
5.2. Приложения 289
5.2.1. Внутридоменное взаимодействие 289
5.2.1.1. Сценарий 289
5.2.1.2. Развертывание 290
5.2.2. Междоменное взаимодействие 290
5.2.2.1. Сценарий 290
5.2.2.2. Развертывание 291
5.3. Функции 291
5.3.1. Базовые определения 291
5.3.2. Обзор 296
5.3.3. Протоколы маршрутизации по состоянию канала 296
5.3.3.1. Принцип работы 297
5.3.3.2. Сопутствующая конфигурация 300
5.3.4. Управление маршрутами OSPF 302

5.3.4.1. Принцип работы 302
5.3.4.2. Сопутствующая конфигурация 305
5.3.5. Повышенная безопасность и надежность 307
5.3.5.1. Принцип работы 307
5.3.5.2. Сопутствующая конфигурация 309
5.3.6. Функции управления сетью 310
5.3.6.1. Принцип работы 310
5.3.6.2. Сопутствующая конфигурация 311
5.4. Конфигурация 311
5.4.1. Настройка основных функций OSPF 316
5.4.1.1. Эффект конфигурации 316
5.4.1.2. Примечания 316
5.4.1.3. Шаги настройки 316
5.4.1.4. Проверка 317
5.4.1.5. Связанные команды 317
5.4.1.6. Пример конфигурации 320
5.4.1.7. Распространенные ошибки 324
5.4.2. Установка типа сети 324
5.4.2.1. Эффект конфигурации 324
5.4.2.2. Примечания 324
5.4.2.3. Шаги настройки 325
5.4.2.4. Проверка 325
5.4.2.5. Связанные команды 325
5.4.2.6. Пример конфигурации 327
5.4.2.7. Распространенные ошибки 328
5.4.3. Настройка перераспределения маршрутов и маршрута по умолчанию 328
5.4.3.1. Эффект конфигурации 328
5.4.3.2. Примечания 328
5.4.3.3. Шаги настройки 329
5.4.3.4. Проверка 329
5.4.3.5. Связанные команды 329
5.4.3.6. Пример конфигурации 332
5.4.3.7. Распространенные ошибки 335
5.4.4. Настройка тупиковой области и области NSSA 335
5.4.4.1. Эффект конфигурации 335
5.4.4.2. Примечания 335
5.4.4.3. Шаги настройки 336
5.4.4.4. Проверка 336

5.4.4.5. Связанные команды 336
5.4.4.6. Пример конфигурации 339
5.4.4.7. Распространенные ошибки 342
5.4.5. Настройка суммирования маршрутов 342
5.4.5.1. Эффект конфигурации 342
5.4.5.2. Примечания 342
5.4.5.3. Шаги конфигурации 342
5.4.5.4. Проверка 342
5.4.5.5. Связанные команды 343
5.4.5.6. Пример конфигурации 344
5.4.5.7. Распространенные ошибки 345
5.4.6. Настройка фильтрации маршрутов 345
5.4.6.1. Эффект конфигурации 345
5.4.6.2. Примечания 345
5.4.6.3. Шаги настройки 346
5.4.6.4. Проверка 346
5.4.6.5. Связанные команды 346
5.4.6.6. Пример конфигурации 348
5.4.6.7. Распространенные ошибки 349
5.4.7. Изменение стоимости маршрута и AD 349
5.4.7.1. Эффект конфигурации 349
5.4.7.2. Примечания 349
5.4.7.3. Шаги настройки 349
5.4.7.4. Проверка 350
5.4.7.5. Связанные команды 350
5.4.7.6. Пример конфигурации 353
5.4.7.7. Распространенные ошибки 354
5.4.8. Включение аутентификации 354
5.4.8.1. Эффект конфигурации 354
5.4.8.2. Примечания 354
5.4.8.3. Шаги настройки 354
5.4.8.4. Проверка 354
5.4.8.5. Связанные команды 355
5.4.8.6. Пример конфигурации 358
5.4.8.7. Распространенные ошибки 359
5.4.9. Изменение максимального количества одновременных соседей 359
5.4.9.1. Эффект конфигурации 359
5.4.9.2. Примечания 359

5.4.9.3. Шаги настройки 359
5.4.9.4. Проверка 359
5.4.9.5. Связанные команды 359
5.4.9.6. Пример конфигурации 360
5.4.10. Отключение проверки MTU 361
5.4.10.1. Эффект конфигурации 361
5.4.10.2. Примечания 361
5.4.10.3. Шаги настройки 361
5.4.10.4. Проверка 361
5.4.10.5. Связанные команды 361
5.4.10.6. Пример конфигурации 362
5.4.11. Включение двустороннего обслуживания 362
5.4.11.1. Эффект конфигурации 362
5.4.11.2. Примечания 363
5.4.11.3. Шаги настройки 363
5.4.11.4. Проверка 363
5.4.11.5. Связанные команды 363
5.4.11.6. Пример конфигурации 363
5.4.12. Корреляция OSPF с BFD 364
5.4.12.1. Эффект конфигурации 364
5.4.12.2. Примечания 364
5.4.12.3. Шаги настройки 364
5.4.12.4. Проверка 364
5.4.12.5. Связанные команды 365
5.4.12.6. Пример конфигурации 366
5.4.13. Включение GR 367
5.4.13.1. Эффект конфигурации 367
5.4.13.2. Примечания 367
5.4.13.3. Шаги настройки 367
5.4.13.4. Проверка 367
5.4.13.5. Связанные команды 368
5.4.13.6. Пример конфигурации 370
5.4.13.7. Распространенные ошибки 370
5.4.14. Настройка функций управления сетью 371
5.4.14.1. Эффект конфигурации 371
5.4.14.2. Примечания 371
5.4.14.3. Шаги настройки 371
5.4.14.4. Проверка 371

5.4.14.5. Связанные команды 372
5.4.14.6. Пример конфигурации 373
5.4.15. Изменение параметров управления протоколом 374
5.4.15.1. Эффект конфигурации 374
5.4.15.2. Примечания 374
5.4.15.3. Шаги настройки 374
5.4.15.4. Проверка 375
5.4.15.5. Связанные команды 375
5.4.15.6. Пример конфигурации 380
5.4.15.7. Распространенные ошибки 382
5.5. Мониторинг 382
5.5.1. Очистка 382
5.5.2. Отображение 382
5.5.3. Отладка 383
6. НАСТРОЙКА IS-IS 384
6.1. Обзор 384
6.1.1. Протоколы и стандарты 384
6.2. Приложения 384
6.2.1. Планарная топология 385
6.2.1.1. Сценарий 385
6.2.1.2. Развертывание 385
6.2.2. Иерархическая топология 385
6.2.2.1. Сценарий 385
6.2.2.2. Развертывание 386
6.3. Функции 386
6.3.1. Базовые определения 386
6.4. Обзор 388
6.4.1. Иерархия сети IS-IS 389
6.4.1.1. Принцип работы 389
6.4.1.2. Сопутствующая конфигурация 390
6.4.2. Режим кодирования адреса IS-IS 390
6.4.2.1. Принцип работы 391
6.4.2.2. Сопутствующая конфигурация 391
6.4.3. Типы пакетов IS-IS 391
6.4.3.1. Принцип работы 391
6.4.3.2. Сопутствующая конфигурация 392
6.4.4. Выборы DIS 393

6.4.4.1. Принцип работы 393
6.4.4.2. Сопутствующая конфигурация 393
6.4.5. Поддерживаемые IS-IS типы TLV 394
6.4.5.1. Принцип работы 394
6.4.5.2. Сопутствующая конфигурация 395
6.4.6. Расширение фрагмента LSP 395
6.4.6.1. Принцип работы 395
6.4.6.2. Сопутствующая конфигурация 396
6.4.7. IS-IS VRF 397
6.4.7.1. Принцип работы 397
6.4.7.2. Сопутствующая конфигурация 398
6.4.8. IS-IS MTR 398
6.4.8.1. Принцип работы 398
6.4.8.2. Сопутствующая конфигурация 400
6.4.9. Сосед IS-IS 401
6.5. Конфигурация 401
6.5.1. Включение IS-IS 413
6.5.1.1. Эффект конфигурации 413
6.5.1.2. Примечания 414
6.5.1.3. Шаги настройки 414
6.5.1.4. Проверка 414
6.5.1.5. Связанные команды 415
6.5.1.6. Пример конфигурации 416
6.5.1.7. Распространенные ошибки 420
6.5.2. Настройка пакетов Hello IS-IS 420
6.5.2.1. Эффект конфигурации 420
6.5.2.2. Примечания 420
6.5.2.3. Шаги настройки 420
6.5.2.4. Проверка 421
6.5.2.5. Связанные команды 421
6.5.2.6. Пример конфигурации 422
6.5.3. Настройка IS-IS LSP 422
6.5.3.1. Эффект конфигурации 422
6.5.3.2. Примечания 423
6.5.3.3. Шаги настройки 424
6.5.3.4. Проверка 425
6.5.3.5. Связанные команды 425
6.5.3.6. Пример конфигурации 430

6.5.4. Настройка SNP IS-IS 432
6.5.4.1. Эффект конфигурации 432
6.5.4.2. Шаги настройки 433
6.5.4.3. Проверка 433
6.5.4.4. Связанные команды 433
6.5.4.5. Пример конфигурации 433
6.5.5. Настройка типа уровня IS-IS 434
6.5.5.1. Эффект конфигурации 434
6.5.5.2. Примечания 434
6.5.5.3. Шаги настройки 434
6.5.5.4. Проверка 434
6.5.5.5. Связанные команды 434
6.5.5.6. Пример конфигурации 435
6.5.6. Настройка аутентификации IS-IS 439
6.5.6.1. Эффект конфигурации 439
6.5.6.2. Примечания 439
6.5.6.3. Шаги настройки 439
6.5.6.4. Проверка 440
6.5.6.5. Связанные команды 440
6.5.6.6. Пример конфигурации 446
6.5.6.7. Распространенные ошибки 449
6.5.7. Настройка IS-IS GR 449
6.5.7.1. Эффект конфигурации 449
6.5.7.2. Примечания 453
6.5.7.3. Шаги настройки 453
6.5.7.4. Проверка 454
6.5.7.5. Связанные команды 454
6.5.8. Настройка IS-IS NSR 454
6.5.8.1. Эффект конфигурации 454
6.5.8.2. Примечания 455
6.5.8.3. Шаги настройки 455
6.5.8.4. Проверка 455
6.5.8.5. Связанные команды 455
6.5.9. Настройка поддержки BFD для IS-IS 456
6.5.9.1. Эффект конфигурации 456
6.5.9.2. Примечания 456
6.5.9.3. Шаги настройки 457
6.5.9.4. Проверка 457

6.5.9.5. Связанные команды 457
6.5.9.6. Пример конфигурации 459
6.5.9.7. Распространенные ошибки 459
6.5.10. Установка бита перегрузки IS-IS 459
6.5.10.1. Эффект конфигурации 459
6.5.10.2. Примечания 460
6.5.10.3. Шаги настройки 460
6.5.10.4. Проверка 460
6.5.10.5. Связанные команды 461
6.5.10.6. Пример конфигурации 461
6.5.11. Настройка IS-IS VRF 462
6.5.11.1. Эффект конфигурации 462
6.5.11.2. Примечания 463
6.5.11.3. Шаги настройки 463
6.5.11.4. Проверка 463
6.5.11.5. Связанные команды 463
6.5.11.6. Пример конфигурации 464
6.5.11.7. Распространенные ошибки 464
6.5.12. Настройка IS-IS MTR 465
6.5.12.1. Эффект конфигурации 465
6.5.12.2. Примечания 465
6.5.12.3. Шаги настройки 465
6.5.12.4. Проверка 465
6.5.12.5. Связанные команды 465
6.5.12.6. Пример конфигурации 466
6.5.12.7. Распространенные ошибки 471
6.5.13. Настройка SNMP для IS-IS 471
6.5.13.1. Эффект конфигурации 471
6.5.13.2. Примечания 471
6.5.13.3. Шаги настройки 471
6.5.13.4. Проверка 472
6.5.13.5. Связанные команды 472
6.5.13.6. Пример конфигурации 474
6.5.14. Настройка двустороннего обслуживания IS-IS 474
6.5.14.1. Эффект конфигурации 474
6.5.14.2. Примечания 474
6.5.14.3. Шаги настройки 474
6.5.14.4. Проверка 474

6.5.14.5. Связанные команды 475
6.5.14.6. Пример конфигурации 475
6.5.15. Настройка других параметров IS-IS 476
6.5.15.1. Эффект конфигурации 476
6.5.15.2. Шаги настройки 476
6.5.15.3. Проверка 478
6.5.15.4. Связанные команды 479
6.5.15.5. Пример конфигурации 489
6.6. Мониторинг 495
6.6.1. Очистка 495
6.6.2. Отображение 496
6.6.3. Отладка 497
7. НАСТРОЙКА BGP 498
7.1. Обзор 498
7.1.1.1. Протоколы и стандарты 499
7.2. Приложения 499
7.2.1. Объявление маршрута между AS 499
7.2.1.1. Сценарий 499
7.2.1.2. Развертывание 500
7.2.2. Reflection маршрута внутри AS 500
7.2.2.1. Сценарий 500
7.2.2.2. Развертывание 500
7.3. Функции 501
7.3.1. Основная концепция 501
7.3.2. Обзор 501
7.3.3. Создание соседа BGP 504
7.3.3.1. Принцип работы 504
7.3.3.2. Сопутствующая конфигурация 505
7.3.4. Настройка reflector-а маршрута BGP 506
7.3.4.1. Принцип работы 506
7.3.4.2. Сопутствующая конфигурация 507
7.3.5. Настройка объединения BGP 507
7.3.5.1. Принцип работы 507
7.3.5.2. Сопутствующая конфигурация 507
7.3.6. Перераспределение информации о локальной сети AS в BGP 508
7.3.6.1. Принцип работы 508
7.3.6.2. Сопутствующая конфигурация 508

7.3.7. Управление обменом маршрутами между peer-ами BGP 509
7.3.7.1. Принцип работы 509
7.3.7.2. Сопутствующая конфигурация 509
7.3.8. Получение доступных сетей других AS из BGP 510
7.3.8.1. Принцип работы 510
7.3.8.2. Сопутствующая конфигурация 511
7.3.9. Настройка синхронизации между BGP и IGP 511
7.3.9.1. Принцип работы 511
7.3.9.2. Сопутствующая конфигурация 512
7.3.10. Настройка программного сброса BGP 512
7.3.10.1. Принцип работы 512
7.3.10.2. Сопутствующая конфигурация 513
7.3.11. Настройка атрибутов маршрута BGP 513
7.3.11.1. Принцип работы 513
7.3.11.2. Сопутствующая конфигурация 514
7.3.12. Настройка агрегации маршрутов BGP 516
7.3.12.1. Принцип работы 516
7.3.12.2. Сопутствующая конфигурация 516
7.3.13. Настройка подавления маршрутов BGP 517
7.3.13.1. Принцип работы 517
7.3.13.2. Сопутствующая конфигурация 517
7.3.14. Настройка расстояния управления BGP 518
7.3.14.1. Принцип работы 518
7.3.14.2. Сопутствующая конфигурация 519
7.3.15. Настройка multipath-балансировки нагрузки BGP 519
7.3.15.1. Принцип работы 519
7.3.15.2. Сопутствующая конфигурация 520
7.3.16. Настройка BGP FRR 520
7.3.16.1. Принцип работы 520
7.3.16.2. Сопутствующая конфигурация 521
7.3.17. Настройка быстрого изымания (Fast Withdrawal) указанных маршрутов BGP 521
7.3.17.1. Принцип работы 521
7.3.17.2. Сопутствующая конфигурация 521
7.3.18. Настройка BGP Multi-path Bypass Protection 522
7.3.18.1. Принцип работы 522
7.3.18.2. Сопутствующая конфигурация 522

7.3.19. Разрешение reflector-a маршрута BGP для изменения атрибутов маршрута 522
7.3.19.1. Принцип работы 523
7.3.19.2. Сопутствующая конфигурация 523
7.3.20. Настройка устройства BGP для объявления маршрута с самым низким приоритетом при перезапуске 523
7.3.20.1. Принцип работы 523
7.3.20.2. Сопутствующая конфигурация 524
7.3.21. Настройка таймеров BGP 524
7.3.21.1. Принцип работы 524
7.3.21.2. Сопутствующая конфигурация 524
7.3.22. Настройка механизмов обновления маршрутов BGP 525
7.3.22.1. Принцип работы 525
7.3.22.2. Сопутствующая конфигурация 526
7.3.23. Настройка функции обновления, запускаемого по событию следующего hop-a BGP 526
7.3.23.1. Принцип работы 526
7.3.23.2. Сопутствующая конфигурация 527
7.3.24. Настройка LOCAL AS BGP 527
7.3.24.1. Принцип работы 527
7.3.24.2. Сопутствующая конфигурация 527
7.3.25. Настройка защиты емкости BGP 528
7.3.25.1. Принцип работы 528
7.3.25.2. Сопутствующая конфигурация 528
7.3.26. Настройка BGP GR 529
7.3.26.1. Принцип работы 529
7.3.26.2. Сопутствующая конфигурация 531
7.3.27. Настройка 4-байтовых номеров AS BGP 532
7.3.27.1. Принцип работы 532
7.3.27.2. Сопутствующая конфигурация 533
7.3.28. Настройка регулярного выражения 533
7.3.28.1. Принцип работы 533
7.3.28.2. Сопутствующая конфигурация 534
7.3.29. Настройка сохранения сеанса BGP 534
7.3.29.1. Принцип работы 534
7.3.29.2. Сопутствующая конфигурация 534
7.3.30. Настройка отложенного объявления BGP при перезапуске системы 535
7.3.30.1. Принцип работы 535

7.3.30.2. Сопутствующая конфигурация 535
7.3.31. Настройка отложенного объявления BGP для первых маршрутов 535
7.3.31.1. Принцип работы 535
7.3.31.2. Сопутствующая конфигурация 536
7.3.32. Настройка BGP NSR 536
7.3.32.1. Принцип работы 536
7.3.32.2. Сопутствующая конфигурация 537
7.3.33. Настройка маршрутов BGP как рекурсивные только для маршрутов хоста 537
7.3.33.1. Принцип работы 538
7.3.33.2. Сопутствующая конфигурация 538
7.3.34. Настройка обнаружения исходящей петли для соседа BGP 538
7.3.34.1. Принцип работы 538
7.3.34.2. Сопутствующая конфигурация 538
7.3.35. Плавное закрытие соединения BGP 539
7.3.35.1. Принцип работы 539
7.3.35.2. Сопутствующая конфигурация 539
7.3.36. Настройка расширенного импорта маршрутов VPN 540
7.3.36.1. Принцип работы 540
7.3.36.2. Сопутствующая конфигурация 540
7.3.37. Группа обновления маршрутов BGP 540
7.3.37.1. Принцип работы 540
7.3.38. Настройка BGP EVPN 540
7.3.38.1. Принцип работы 540
7.3.38.2. Сопутствующая конфигурация 541
7.3.39. Другие связанные конфигурации 542
7.4. Конфигурация 542
7.4.1. Настройка peer-a BGP (группы) 544
7.4.1.1. Эффект конфигурации 544
7.4.1.2. Примечания 544
7.4.1.3. Шаги настройки 544
7.4.1.4. Проверка 545
7.4.1.5. Связанные команды 545
7.4.1.6. Пример конфигурации 546
7.4.1.7. Распространенные ошибки 554
7.4.2. Настройка аутентификации MD5 554
7.4.2.1. Эффект конфигурации 554
7.4.2.2. Примечания 554

7.4.2.3. Шаги настройки 554
7.4.2.4. Проверка 554
7.4.2.5. Связанные команды 554
7.4.2.6. Пример конфигурации 556
7.4.2.7. Распространенные ошибки 561
7.4.3. Настройка reflector-а маршрута 561
7.4.3.1. Эффект конфигурации 561
7.4.3.2. Примечания 561
7.4.3.3. Шаги настройки 561
7.4.3.4. Проверка 561
7.4.3.5. Связанные команды 562
7.4.3.6. Пример конфигурации 563
7.4.4. Настройка объединения AS 567
7.4.4.1. Эффект конфигурации 567
7.4.4.2. Примечания 567
7.4.4.3. Шаги настройки 567
7.4.4.4. Проверка 568
7.4.4.5. Связанные команды 568
7.4.4.6. Пример конфигурации 570
7.4.4.7. Распространенные ошибки 576
7.4.5. Настройка multipath-балансировки нагрузки BGP 576
7.4.5.1. Эффект конфигурации 576
7.4.5.2. Примечания 576
7.4.5.3. Шаги настройки 576
7.4.5.4. Проверка 576
7.4.5.5. Связанные команды 577
7.4.5.6. Пример конфигурации 578
7.4.5.7. Распространенные ошибки 582
7.4.6. Настройка EBGP FRR 582
7.4.6.1. Эффект конфигурации 582
7.4.6.2. Примечания 582
7.4.6.3. Шаги настройки 582
7.4.6.4. Проверка 582
7.4.6.5. Связанные команды 583
7.4.6.6. Пример конфигурации 584
7.4.6.7. Распространенные ошибки 587
7.4.7. Настройка быстрого изымания указанных маршрутов BGP 587
7.4.7.1. Эффект конфигурации 587

7.4.7.2. Примечания 587
7.4.7.3. Шаги настройки 587
7.4.7.4. Проверка 587
7.4.7.5. Связанные команды 588
7.4.7.6. Пример конфигурации 589
7.4.8. Настройка локальных AS 589
7.4.8.1. Эффект конфигурации 589
7.4.8.2. Шаги настройки 589
7.4.8.3. Проверка 589
7.4.8.4. Связанные команды 590
7.4.8.5. Пример конфигурации 591
7.4.9. Настройка BGP GR 592
7.4.9.1. Эффект конфигурации 592
7.4.9.2. Примечания 592
7.4.9.3. Шаги настройки 592
7.4.9.4. Проверка 593
7.4.9.5. Связанные команды 593
7.4.9.6. Пример конфигурации 594
7.4.9.7. Распространенные ошибки 597
7.4.10. Настройка семейства адресов BGP IPv6 597
7.4.10.1. Эффект конфигурации 597
7.4.10.2. Примечания 597
7.4.10.3. Шаги настройки 597
7.4.10.4. Проверка 597
7.4.10.5. Связанные команды 597
7.4.10.6. Пример конфигурации 599
7.4.10.7. Распространенные ошибки 601
7.4.11. Настройка BGP EVPN 601
7.4.11.1. Примечания 601
7.4.11.2. Шаги настройки 601
7.4.11.3. Проверка 602
7.4.11.4. Связанные команды 602
7.4.11.5. Пример конфигурации 607
7.4.11.6. Распространенные ошибки 611
7.4.12. Настройка соединения с устройствами, поддерживающими только 2-байтовые номера AS 611
7.4.12.1. Эффект конфигурации 611
7.4.12.2. Шаги настройки 611

7.4.12.3. Проверка 611
7.4.12.4. Связанные команды 611
7.4.12.5. Пример конфигурации 612
7.4.13. Использование локальных адресов каналов IPv6 для установления соседства BGP 614
7.4.13.1. Эффект конфигурации 614
7.4.13.2. Примечания 614
7.4.13.3. Шаги настройки 614
7.4.13.4. Проверка 615
7.4.13.5. Связанные команды 615
7.4.13.6. Пример конфигурации 617
7.4.13.7. Распространенные ошибки 619
7.4.14. Настройка BGP NSR 619
7.4.14.1. Эффект конфигурации 619
7.4.14.2. Примечания 619
7.4.14.3. Шаги настройки 619
7.4.14.4. Проверка 620
7.4.14.5. Связанные команды 620
7.4.14.6. Пример конфигурации 621
7.4.14.7. Распространенные ошибки 622
7.4.15. Настройка маршрутов BGP, чтобы быть рекурсивными только для маршрутов хоста 622
7.4.15.1. Эффект конфигурации 622
7.4.15.2. Примечания 622
7.4.15.3. Шаги настройки 622
7.4.15.4. Проверка 623
7.4.15.5. Связанные команды 623
7.4.15.6. Пример конфигурации 623
7.4.15.7. Распространенные ошибки 624
7.4.16. Настройка обнаружения исходящей петли для соседа BGP 624
7.4.16.1. Эффект конфигурации 624
7.4.16.2. Примечания 624
7.4.16.3. Шаги настройки 624
7.4.16.4. Проверка 624
7.4.16.5. Связанные команды 624
7.4.16.6. Пример конфигурации 625
7.4.17. Плавное закрытие соединений BGP 627
7.4.17.1. Эффект конфигурации 627

7.4.17.2. Шаги настройки 627
7.4.17.3. Проверка 627
7.4.17.4. Связанные команды 628
7.4.17.5. Пример конфигурации 629
7.4.18. Настройка EBGP Multi-path Bypass Protection 631
7.4.18.1. Эффект конфигурации 631
7.4.18.2. Примечания 631
7.4.18.3. Шаги настройки 631
7.4.18.4. Проверка 631
7.4.18.5. Связанные команды 632
7.4.18.6. Пример конфигурации 633
7.4.19. Настройка Inter-VRF Multi-Path Route Import 637
7.4.19.1. Эффект конфигурации 637
7.4.19.2. Шаги настройки 637
7.4.19.3. Проверка 637
7.4.19.4. Связанные команды 638
7.4.19.5. Пример конфигурации 640
7.5. Мониторинг 643
7.5.1. Очистка 643
7.5.2. Отображение 643
7.5.3. Отладка 644
8. НАСТРОЙКА RIPNG 645
8.1. Обзор 645
8.1.1. Протоколы и стандарты 645
8.2. Приложение 645
8.3. Функции 646
8.3.1. Базовые определения 646
8.3.2. Особенность 646
8.3.3. RIPng и RIP 646
8.3.3.1. Принцип работы 646
8.3.3.2. Сопутствующая конфигурация 646
8.3.4. Обмен информацией о маршрутизации 647
8.3.4.1. Принцип работы 647
8.3.4.2. Сопутствующая конфигурация 648
8.3.5. Алгоритм маршрутизации 648
8.3.5.1. Принцип работы 648
8.3.5.2. Сопутствующая конфигурация 650

8.3.6. Как избежать петель маршрута 650
8.3.6.1. Принцип работы 650
8.3.6.2. Сопутствующая конфигурация 652
8.4. Конфигурация 652
8.4.1. Настройка основных функций RIPng 653
8.4.1.1. Эффект конфигурации 653
8.4.1.2. Примечания 653
8.4.1.3. Шаги настройки 654
8.4.1.4. Проверка 654
8.4.1.5. Связанные команды 654
8.4.1.6. Пример конфигурации 656
8.4.1.7. Распространенные ошибки 659
8.4.2. Объявление маршрута по умолчанию или внешних маршрутов 659
8.4.2.1. Эффект конфигурации 659
8.4.2.2. Примечания 659
8.4.2.3. Шаги настройки 659
8.4.2.4. Проверка 659
8.4.2.5. Связанные команды 660
8.4.2.6. Пример конфигурации 661
8.4.3. Настройка правил фильтрации маршрутов 662
8.4.3.1. Эффект конфигурации 662
8.4.3.2. Примечания 662
8.4.3.3. Шаги настройки 662
8.4.3.4. Проверка 663
8.4.3.5. Связанные команды 663
8.4.3.6. Пример конфигурации 663
8.4.4. Изменение параметров выбора маршрута 664
8.4.4.1. Эффект конфигурации 664
8.4.4.2. Примечания 664
8.4.4.3. Шаги настройки 664
8.4.4.4. Проверка 665
8.4.4.5. Связанные команды 665
8.4.4.6. Пример конфигурации 666
8.4.5. Изменение таймеров 667
8.4.5.1. Эффект конфигурации 667
8.4.5.2. Примечания 667
8.4.5.3. Шаги настройки 667
8.4.5.4. Проверка 667

8.4.5.5. Связанные команды 667
8.4.5.6. Пример конфигурации 668
8.4.5.7. Распространенные ошибки 669
8.5. Мониторинг 669
8.5.1. Отображение 669
8.5.2. Отладка 669
9. НАСТРОЙКА PBR 670
9.1. Обзор 670
9.2. Приложениес 670
9.2.1. Выбор интернет-провайдера с помощью PBR 670
9.2.1.1. Сценарий 671
9.2.1.2. Развертывание 671
9.2.2. Реализация классификации трафика с помощью PBR 672
9.2.2.1. Сценарий 672
9.2.2.2. Развертывание 673
9.3. Функции 673
9.3.1. Настройка политики 673
9.3.1.1. Выполнение политик 673
9.3.1.2. Условия соответствия политик 674
9.3.1.3. Действие обработки для политики 675
9.3.2. Настройка PBR 677
9.3.2.1. PBR 677
9.3.2.2. Резервное копирование или балансировка нагрузки 678
9.3.2.3. Корреляция с BFD 678
9.3.2.4. Корреляция с Track 678
9.3.2.5. PBR на основе адреса источника 679
9.4. Ограничения 679
9.5. Конфигурация 679
9.5.1. Настройка основных функций PBR 681
9.5.1.1. Эффект конфигурации 681
9.5.1.2. Примечания 681
9.5.1.3. Шаги настройки 681
9.5.1.4. Проверка 683
9.5.1.5. Пример конфигурации 690
9.5.1.6. Распространенные ошибки 699
9.5.2. Настройка резервного копирования или балансировки нагрузки 700
9.5.2.1. Эффект конфигурации 700

9.5.2.2. Примечания 700
9.5.2.3. Шаги настройки 701
9.5.2.4. Проверка 702
9.5.2.5. Пример конфигурации 703
9.5.3. Настройка PBR на основе адреса источника 706
9.5.3.1. Эффект конфигурации 706
9.5.3.2. Примечания 706
9.5.3.3. Шаги настройки 706
9.5.3.4. Проверка 709
9.5.3.5. Пример конфигурации 711
9.6. Мониторинг 716
9.6.1. Очистка 716
9.6.2. Отображение 716
9.6.3. Отладка 717
10. УПРАВЛЕНИЕ МАРШРУТАМИ 719
10.1. Обзор 719
10.2. Приложения 719
10.2.1. Основные функции статического маршрута 720
10.2.1.1. Сценарий 720
10.2.1.2. Развертывание 720
10.2.2. Плавающий статический маршрут 721
10.2.2.1. Сценарий 721
10.2.2.2. Развертывание 721
10.2.3. Статический маршрут балансировки нагрузки 722
10.2.3.1. Сценарий 722
10.2.3.2. Развертывание 722
10.2.4. Корреляция статических маршрутов с Track, BFD или ARP 722
10.2.4.1. Сценарий 722
10.2.4.2. Развертывание 724
10.2.5. Быстрое перенаправление статических маршрутов 724
10.2.5.1. Сценарий 724
10.2.5.2. Развертывание 725
10.2.6. Преобразование ARP-to-host 725
10.2.6.1. Сценарий 725
10.2.6.2. Развертывание 726
10.3. Функции 726
10.3.1. Расчет маршрута 726

10.3.1.1. Функция маршрутизации 726
10.3.1.2. Динамический маршрут 726
10.3.1.3. Статический маршрут 726
10.3.1.4. Преобразование ARP-to-host 727
10.3.2. Оптимальный выбор маршрута 727
10.3.2.1. Административное расстояние 727
10.3.2.2. Маршрут равной стоимости 727
10.3.2.3. Плавающий маршрут 727
10.3.3. Маршрут по умолчанию 727
10.3.3.1. Статический маршрут по умолчанию 728
10.3.3.2. Сеть по умолчанию 728
10.3.4. Надежность маршрута 728
10.3.4.1. Корреляция с Track 728
10.3.4.2. Корреляция с BFD 728
10.3.4.3. Корреляция с ARP 728
10.3.4.4. Быстрое перенаправление 728
10.4. Конфигурация 729
10.4.1. Настройка статического маршрута 730
10.4.1.1. Эффект конфигурации 730
10.4.1.2. Примечания 731
10.4.1.3. Шаги настройки 731
10.4.1.4. Проверка 733
10.4.1.5. Пример конфигурации 734
10.4.1.6. Распространенные ошибки 740
10.4.2. Настройка маршрута по умолчанию 740
10.4.2.1. Эффект конфигурации 740
10.4.2.2. Примечания 741
10.4.2.3. Шаги настройки 741
10.4.2.4. Проверка 744
10.4.2.5. Пример конфигурации 744
10.4.3. Настройка ограничений маршрута 745
10.4.3.1. Эффект конфигурации 745
10.4.3.2. Примечания 746
10.4.3.3. Шаги настройки 746
10.4.3.4. Проверка 748
10.4.3.5. Пример конфигурации 749
10.4.4. Сопоставление статического маршрута с BFD 750
10.4.4.1. Эффект конфигурации 750

10.4.4.2. Примечания 750
10.4.4.3. Шаги настройки 751
10.4.4.4. Проверка 752
10.4.4.5. Пример конфигурации 752
10.4.4.6. Распространенные ошибки 753
10.4.5. Настройка статического быстрого перенаправления 753
10.4.5.1. Эффект конфигурации 753
10.4.5.2. Примечания 753
10.4.5.3. Шаги настройки 754
10.4.5.4. Проверка 754
10.4.5.5. Пример конфигурации 755
10.4.5.6. Распространенные ошибки 756
10.4.6. Настройка преобразования ARP-to-host 756
10.4.6.1. Эффект конфигурации 756
10.4.6.2. Примечания 756
10.4.6.3. Шаги настройки 757
10.4.6.4. Проверка 757
10.4.6.5. Пример конфигурации 758
10.4.6.6. Распространенные ошибки 760
10.5. Мониторинг 760
10.5.1. Отображение 760
10.5.2. Отладка 760
11. НАСТРОЙКА VRF 762
11.1. Обзор 762
11.2. Приложения 762
11.2.1. Локальный доступ Inter-VPN 762
11.2.1.1. Сценарий 762
11.2.1.2. Сопутствующая конфигурация 763
11.2.2. VRF только на границах провайдера (PE) 763
11.2.2.1. Сценарий 763
11.2.2.2. Развертывание 764
11.2.3. VRF на CE и PE (приложение MCE) 764
11.2.3.1. Сценарий 764
11.2.3.2. Развертывание 765
11.3. Функции 765
11.3.1. Обзор 765
11.3.2. VPN-экземпляр 766

11.3.2.1. Принцип работы 766
11.3.2.2. Сопутствующая конфигурация 766
11.3.3. VPN-маршрут 766
11.3.4. Атрибут VPN-маршрута 767
11.3.4.1. Принцип работы 767
11.3.4.2. Сопутствующая конфигурация 767
11.4. Конфигурация 768
11.4.1. Настройка таблицы VRF для одного протокола 769
11.4.1.1. Эффект конфигурации 769
11.4.1.2. Примечания 769
11.4.1.3. Шаги настройки 769
11.4.1.4. Проверка 770
11.4.1.5. Связанные команды 771
11.4.1.6. Пример конфигурации 774
11.4.1.7. Распространенные ошибки 778
11.4.2. Настройка многопротокольной таблицы VRF 778
11.4.2.1. Эффект конфигурации 778
11.4.2.2. Примечания 778
11.4.2.3. Шаги настройки 778
11.4.2.4. Проверка 779
11.4.2.5. Связанные команды 779
11.4.2.6. Пример конфигурации 783
11.4.2.7. Распространенные ошибки 789
11.5. Мониторинг 789
11.5.1. Очистка 789
11.5.2. Отображение 789
11.5.3. Отладка 790
12. НАСТРОЙКА L3MAC 791
12.1. Обзор 791
12.2. Приложения 791
12.2.1. Сценарий центра обработки данных 791
12.2.1.1. Сценарий 791
12.2.1.2. Развертывание 791
12.3. Конфигурация 792
12.3.1. Добавление MAC-адреса уровня 3 792
12.3.1.1. Эффект конфигурации 792
12.3.1.2. Примечания 792

12.3.1.3. Шаги настройки 792
12.3.1.4. Проверка 792
12.3.1.5. Пример конфигурации 793
12.4. Мониторинг 794
12.4.1. Отображение 794
13. НАСТРОЙКА ЗАПРОСА МОЩНОСТИ ОБОРУДОВАНИЯ 795
13.1. Обзор 795
13.2. Функции 795
13.2.1. Базовые определения 795
13.3. Мониторинг 795
13.3.1. Отображение 795
14. ОБЩАЯ ИНФОРМАЦИЯ 796
14.1. Гарантия и сервис 796
14.2. Техническая поддержка 796
14.3. Электронная версия документа 796

1. НАСТРОЙКА ПОЛИТИК МАРШРУТИЗАЦИИ

1.1. Обзор

Политики маршрутизации — это набор политик для изменения пути пересылки пакетов или информации о маршрутизации, который часто реализуется с помощью списка фильтрации и карты маршрутов. Политики маршрутизации гибко и широко применяются следующими методами:

- Используйте список фильтрации в протоколе маршрутизации для фильтрации или изменения информации о маршрутизации.
- Используйте карту маршрутов в протоколе маршрутизации для фильтрации или изменения информации о маршрутизации. Где карта маршрута может дополнительно использовать список фильтрации.
- Используйте карту маршрутов в маршрутизации на основе политик (PBR) для управления пересылкой пакетов или изменения полей пакетов.

1.2. Приложения

Приложение	Описание
Фильтрация маршрутов	Используйте список фильтрации в протоколе маршрутизации для фильтрации информации о маршрутизации, отправляемой или получаемой протоколом
Перераспределение маршрутов	Используйте карту маршрутов в протоколе маршрутизации для фильтрации или изменения информации о маршрутизации и перераспределения маршрутов RIP в OSPF. Перераспределять можно только маршруты RIP с 4 hop-ами
PBR	Используйте карту маршрутов в PBR для управления пересылкой пакетов или изменения полей пакетов и указания оптимальных выходных интерфейсов для пакетов из разных подсетей

1.2.1. Фильтрация маршрутов

По умолчанию протокол маршрутизации объявляет и изучает всю информацию о маршрутизации. При использовании списка фильтрации протокол маршрутизации объявляет только необходимые маршруты или получает только необходимую информацию о маршрутизации.

1.2.1.1. Сценарий

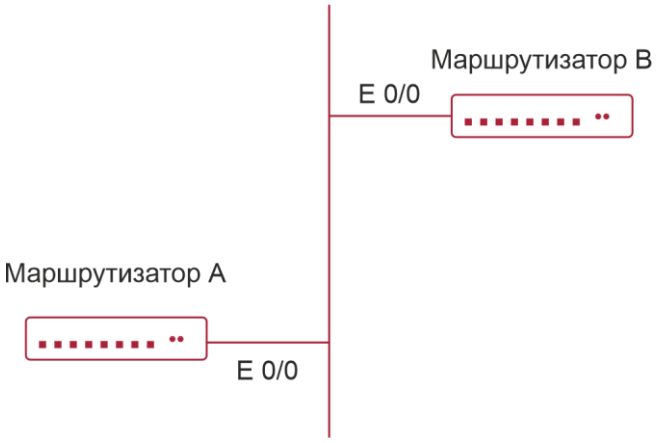


Рисунок 1-1.

Как показано на Рисунке 1-1, маршрутизатор A имеет маршруты к 3 сетям: 10.0.0.0, 20.0.0.0 и 30.0.0.0.

Настройте список фильтрации на маршрутизаторах для достижения следующих целей:

- Отфильтруйте отправленную информацию о маршрутизации на маршрутизаторе A, чтобы отфильтровать маршруты, которые маршрутизатору A не нужно отправлять.
- Отфильтруйте полученную информацию о маршрутизации на маршрутизаторе B, чтобы отфильтровать маршруты, которые маршрутизатору B не нужно изучать.

1.2.1.2. Развертывание

- Отфильтруйте отправленную информацию о маршрутизации 30.0.0.0 на маршрутизаторе A.
- Отфильтруйте полученную информацию о маршрутизации 20.0.0.0 на маршрутизаторе B, чтобы гарантировать, что маршрутизатор B изучит только информацию о маршрутизации 10.0.0.0.

1.2.2. Перераспределение маршрутов

По умолчанию перераспределение маршрутов перераспределяет всю информацию о маршрутизации из одного протокола маршрутизации в другой протокол маршрутизации. Все атрибуты маршрутизации также будут унаследованы. Вы можете использовать карту маршрутов для выполнения условного управления перераспределением между двумя протоколами маршрутизации, включая:

- Укажите диапазон перераспределения маршрутов и перераспределяйте только маршрутную информацию, соответствующую определенным правилам.
- Установите атрибуты маршрутов, созданных при перераспределении.

1.2.2.1. Сценарий



Рисунок 1-2.

Как показано Рисунке 1-2, настройте перераспределение маршрутов на устройствах для достижения следующих целей:

- Перераспределите в OSPF только маршруты RIP с 4 hop-ами.
- В домене маршрутизации OSPF исходная метрика этого маршрута равна 40, тип маршрута — внешний маршрут тип-1 (type-1), а значение тега маршрута установлено на 40.

1.2.2.2. Развертывание

- Настройте маршрут с 4 hop-ами в карте маршрутов rip_to_ospf:match и установите начальную метрику этого маршрута на 40, тип маршрута на внешний маршрут тип-1 и значение тега маршрута на 40.
- Настройте перераспределение маршрутов, чтобы перераспределить маршруты RIP в OSPF, и используйте карту маршрутов rip_to_ospf.

1.2.3. PBR

PBR реализуется путем применения карты маршрутов, включая политики, к интерфейсам и устройствам.

Подобно статической маршрутизации, PBR также настраивается вручную, при этом рекурсивная маршрутизация поддерживает автоматическое обновление при изменениях в сети. По сравнению со статической и динамической маршрутизацией PBR более гибкая. Статическая и динамическая маршрутизация может пересылать пакеты только на основе адресов назначения. PBR может пересылать пакеты на основе адресов источника и назначения, длины пакета и входного интерфейса.

1.2.3.1. Сценарий

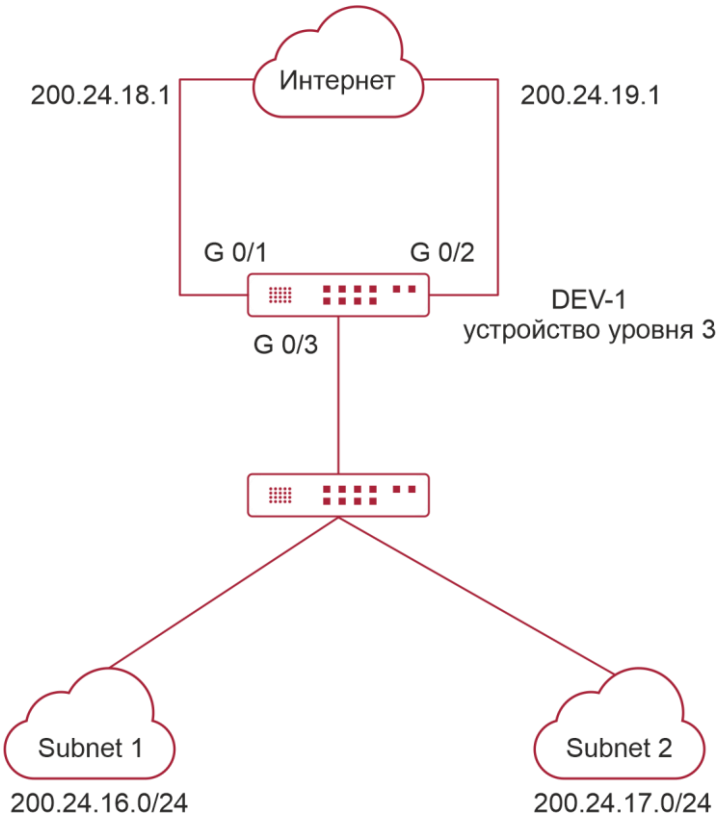


Рисунок 1-3.

Настройте PBR на устройстве DEV1 уровня 3 для достижения следующих целей:

- Пакеты из подсети 1 (200.24.16.0/24) сначала отправляются из GE0/1.
- Пакеты из подсети 2 (200.24.17.0/24) сначала отправляются из GE0/2.

1.2.3.2. Развертывание

- Настройте два разных списка ACL для сопоставления пакетов из подсетей 1 и 2 соответственно.
- Настройте карту маршрутов RM_FOR_PBR: политика 10 используется для обеспечения того, чтобы «пакеты из подсети 1 отправлялись сначала из GE0/1»; политика 20 используется для обеспечения того, чтобы «пакеты из подсети 2 сначала отправлялись из GE0/2».
- Выполните PBR для пакетов, полученных от GE0/3, и используйте карту маршрутов RM_FOR_PBR.

1.3. Функции

1.3.1. Обзор

Особенность	Описание
Список фильтрации	Определите группу списков на основе атрибута маршрута, который может использоваться протоколом маршрутизации для фильтрации маршрутов
Карта маршрута	Политика определяет: «Если соблюдаются определенные условия, вы можете выполнять определенные действия по обработке»

1.3.2. Список фильтрации

Списки фильтрации — это группа списков, определенные на основе атрибута маршрутизации, и являются инструментом фильтрации политик маршрутизации. Независимые списки фильтрации бессмысленны и могут использоваться для фильтрации маршрутов только тогда, когда они применяются в протоколе маршрутизации.

1.3.2.1. Принцип работы

В зависимости от различных атрибутов маршрутизации списки фильтрации подразделяются на следующие типы:

Список управления доступом (Access Control List (ACL))

Списки ACL включают списки ACL IPv4 и IPv6. При определении списков ACL вы можете указать адреса и маски IPv4/IPv6, соответствующие сегменту сети назначения или адресам следующего hop-a (next-hop) информации о маршрутизации.

Описание списков ACL см. в Руководстве ACL&QoS Configuration/Настройка ACL.

Список префиксов адресов (список префиксов (prefix-list))

Подобно спискам ACL, списки префиксов, включая списки префиксов IPv4 и списки префиксов IPv6, используются для сопоставления сегментов сети назначения с информацией о маршрутизации во время фильтрации маршрутов.

Список AS-путей

Списки AS-путей используются только для BGP. Они используются для сопоставления путей AS во время фильтрации маршрутов BGP.

Список фильтрации атрибутов сообщества (Список сообщества (Community-List))

Списки сообществ используются только для BGP. Они используются для сопоставления атрибутов сообщества во время фильтрации маршрутов BGP.

Расширенный список фильтрации атрибутов сообщества (Extcommunity-List)

Списки Extcommunity используются только для BGP. Они используются для сопоставления расширенных атрибутов сообщества во время фильтрации маршрутов BGP.

1.3.2.2. Сопутствующая конфигурация

Создание списка управления доступом (ACL)

По умолчанию ACL не настроен и политика не установлена.

В режиме глобальной конфигурации запустите команду **ip access-list** { **extended** | **standard** } { *id* | *name* } для создания списка управления доступом IPv4.

В ACL можно установить несколько политик, отсортированных по их порядковым номерам. Политики имеют два режима работы: разрешить (permit) и запретить (deny).

Создание списка префиксов

По умолчанию список префиксов не настроен и запись не задана.

В режиме глобальной конфигурации запустите команду **ip prefix-list** *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*] для создания списка префиксов IPv4 и добавления записи префикса в список.

Вы можете установить несколько записей в списке префиксов, отсортированных по их порядковым номерам. Записи имеют два режима работы: разрешить (permit) и запретить (deny).

Запустите команду **ip prefix-list** *prefix-list-name* **description** *descripton-text*, чтобы добавить описание в список префиксов.

Запустите команду **ip prefix-list sequence-number**, чтобы включить функцию сортировки для списка префиксов.

Создание списка AS-путей

По умолчанию список путей AS не настроен и запись не задана.

В режиме глобальной конфигурации запустите команду **ip as-path access-list** *path-list-num* { **permit** | **deny** } *regular-expression* для создания списка AS-путей и добавления записи в список.

Вы можете установить несколько записей в списке AS-путей. Записи имеют два режима работы: разрешить (permit) и запретить (deny).

Создание списка сообщества

По умолчанию список сообществ не настроен и запись не задана.

В режиме глобальной конфигурации запустите команду **ip community-list** { { **standard** | **expanded** } *community-list-name* | *community-list-number* } { **permit** | **deny** } [*community-number..*] для создания списка сообщества и добавления записи в список.

Вы можете установить несколько записей в списке сообщества. Записи имеют два режима работы: разрешить (permit) и запретить (deny).

Создание списка Extcommunity

По умолчанию список excommunity не настроен и запись не задана.

В режиме глобальной конфигурации запустите команду **ip extcommunity-list** {*standard-list* **| standard** *list-name* } { **permit | deny** } [**rt** *value*] [**soo** *value*] для создания стандартного списка extcommunity и добавления записи в список.

Запустите команду **ip extcommunity-list** {*expanded-list* | **expanded** *list-name* } { **permit | deny** } [*regular-expression*] для создания списка extcommunity и добавления записи в список.

Вы также можете запустить команду **ip extcommunity-list** {*expanded-list* | **expanded** *list-name*| *standard-list* | **standard** *list-name* } для создания списка extcommunity и входа в режим конфигурации **ip extcommunity-list** для добавления записей.

Вы можете установить несколько записей в списке extcommunity. Записи имеют два режима работы: разрешить (permit) и запретить (deny).

1.3.3. Карта маршрута

Политика — это оператор «match…, set…», который указывает, что «если определенные условия совпадают, вы можете выполнить некоторые действия по обработке».

1.3.3.1. Принцип работы

Выполнение политик

Карта маршрутов может содержать несколько политик. Каждая политика имеет соответствующий порядковый номер. Меньший порядковый номер означает более высокий приоритет. Политики выполняются на основе их порядковых номеров. Как только условие соответствия политики выполнено, необходимо выполнить действие обработки для этой политики и завершить работу карты маршрутов. Если ни одно из условий соответствия какой-либо политики не выполнено, никакие действия по обработке выполняться не будут.

Режимы работы политик

Политики имеют два режима работы:

- Разрешение (permit): когда условие соответствия политики выполнено, действие обработки для этой политики будет выполнено, и карта маршрутов завершится.
- Запрет (deny): если условие соответствия политики выполнено, действие обработки для этой политики не будет выполняться и карта маршрутов закроется.

Соответствующие условия политик

Условие соответствия политики может содержать 0, 1 или несколько правил соответствия.

- Если условие сопоставления содержит 0 правил сопоставления, ни один пакет не будет сопоставлен.
- Если условие сопоставления содержит одно или несколько правил сопоставления, все правила должны быть сопоставлены.

Обработка действия для политики

Действие обработки политики может содержать 0, 1 или несколько установленных правил.

- Если действие обработки содержит 0 установленных правил, действие обработки выполняться не будет, и карта маршрута будет немедленно закрыта.
- Если действие обработки содержит одно или несколько установленных правил, все действия обработки будут выполнены, а затем карта маршрута завершится.

ПРИМЕЧАНИЕ: если заданные правила имеют разные приоритеты, вступит в силу установленное правило с наивысшим приоритетом.

1.3.3.2. Сопутствующая конфигурация

Создание карты маршрутов (политики)

По умолчанию карта маршрутов не настроена и политика не задана.

В режиме глобальной конфигурации вы можете запустить команду **route-map** *route-map-name* [**permit** | **deny**] [*sequence-number*] для создания карты маршрутов и добавления политики в карту маршрутов.

В карте маршрутов можно установить несколько политик. Каждая политика использует разные порядковые номера.

Установка условий соответствия политики

По умолчанию правило соответствия не установлено (то есть условие соответствия политики содержит 0 правил соответствия).

В режиме карты маршрутов запустите команду **match**, чтобы установить правила соответствия. Одна команда **match** сопоставлена с одним правилом соответствия.

ПО предоставляет множество команд **match** для установки гибких условий соответствия.

Команда	Описание
match as-path	Использует атрибут AS_PATH маршрута BGP в качестве условия соответствия
match community	В качестве условия соответствия используется атрибут сообщества маршрута BGP
match extcommunity	В качестве условия соответствия используется атрибут расширенного сообщества маршрута BGP
match interface	Использует выходной интерфейс маршрута в качестве условия соответствия
match ip address	В качестве условия соответствия используется IPv4-адрес назначения маршрута
match ip next-hop	В качестве условия соответствия используется IPv4-адрес следующего hop-а маршрута
match ip route-source	Использует исходный IPv4-адрес маршрута в качестве условия соответствия
match ipv6 address	В качестве условия соответствия используется IPv6-адрес назначения маршрута
match ipv6 next-hop	В качестве условия соответствия используется IPv6-адрес следующего hop-а маршрута
match ipv6 route-source	Использует исходный IPv6-адрес маршрута в качестве условия соответствия
match metric	Использует метрику маршрута в качестве условия соответствия
match origin	Использует источник маршрута в качестве условия соответствия

Команда	Описание
match route-type	Использует тип маршрута в качестве условия соответствия
match tag	Использует значение тега маршрута в качестве условия соответствия

Настройка действий обработки политики

По умолчанию заданное правило не настроено (то есть действие обработки политики содержит 0 заданных правил).

В режиме карты маршрутов выполните команду **set**, чтобы настроить установленные правила. Одна команда **set** сопоставляется с одним правилом набора.

ПО предоставляет множество команд **set** для настройки гибких действий обработки.

Команда	Описание
set aggregator as	Изменяет значение атрибута AS агрегатора маршрутов
set as-path prepend	Добавляет указанное значение атрибута as-path
set as-path replace	Заменяет указанное значение атрибута as-path
set atomic-aggregate	Устанавливает атрибут atomic-aggregate маршрута
set comm-list delete	Удаляет все значения атрибутов сообщества из списка атрибутов сообщества для маршрута, соответствующего правилам соответствия
set community	Устанавливает значение атрибута сообщества маршрута
set dampening	Устанавливает параметры flapping-а маршрута
set extcomm-list delete	Удаляет все значения расширенных атрибутов сообщества из списка атрибутов extcommunity для маршрута, соответствующего правилам соответствия
set extcommunity	Устанавливает значение атрибута расширенного сообщества маршрута
set fast-reroute	Устанавливает резервный выходной интерфейс и следующий hop для быстрого перенаправления

Команда	Описание
set ip default nexthop	Указывает следующий hop маршрута по умолчанию. Эта команда имеет более низкий приоритет, чем общий маршрут, и более высокий приоритет, чем **set default interface**
set ip dscp	Изменяет поле **dscp** IP-пакета
set ip global next-hop	Указывает следующий hop маршрута
set ip global default next-hop	Указывает следующий hop маршрута по умолчанию
set ip nexthop	Указывает следующий hop маршрута. Эта команда имеет более высокий приоритет, чем команда **set interface**
set ip next-hop recursive	Указывает рекурсивный IP-адрес следующего hop-а маршрута
set ip next-hop verify-availability	Указывает IP-адрес следующего hop-а маршрута и проверяет доступность следующего hop-а с помощью BFD
set ip precedence	Изменяет поле **precedence** IP-пакета
set ip tos	Изменяет поле **tos** IP-пакета
set ipv6 default next-hop	Указывает следующий hop маршрута по умолчанию. Эта команда имеет более низкий приоритет, чем общий маршрут, и более высокий приоритет, чем маршрут по умолчанию
set ipv6 global next-hop	Указывает следующий hop IPv6 маршрута
set ipv6 global default next-hop	Указывает следующий hop IPv6 по умолчанию для маршрута
set ipv6 next-hop	Указывает следующий hop IPv6 маршрута. Эта команда имеет более высокий приоритет, чем обычный маршрут
set ipv6 next-hop verify-availability	Указывает IP-адрес следующего hop-а маршрута и проверяет доступность следующего hop-а с помощью BFD
set ipv6 precedence	Устанавливает приоритет заголовка пакета IPv6

Команда	Описание
set level	Устанавливает тип области назначения, к которой будет направлен маршрут
set local-preference	Устанавливает значение атрибута local-preference маршрута
set metric	Изменяет значение метрики (metric) маршрута
set metric-type	Устанавливает тип метрики маршрута
set next-hop	Устанавливает IP-адрес следующего hop-а маршрута
set ip next-hop verify-availability	Указывает IP-адрес следующего hop-а маршрута и проверяет доступность следующего hop-а с помощью стороннего протокола
set origin	Устанавливает атрибут источника маршрута
set originator-id	Устанавливает IP-адрес отправителя (originator) маршрута
set tag	Устанавливает значение тега маршрута
set distance	Устанавливает административное расстояние
set weight	Устанавливает значение веса маршрута

1.4. Конфигурация

Конфигурация	Описание и команда	
Настройка карты маршрутов	(Опционально) Используется для определения политики	
	route-map	Создает политику (карту маршрутов)
	match	Устанавливает условия соответствия политики
Настройка карты маршрутов	**set**	Устанавливает действия обработки политика

Конфигурация	Описание и команда	
Настройка списка фильтрации	(Опционально) Используется для определения списка фильтрации	
	ip as-path	Определяет правила фильтрации AS path
	ip community-list	Определяет список сообщества
	ip extcommunity-list	Определяет список extcommunity
	ip prefix-list	Создает список префиксов
	ip prefix-list description	Добавляет описание к списку префиксов
	ip prefix-list sequence-number	Включает функцию сортировки для списка префиксов
	ipv6 prefix-list	Создает список префиксов IPv6
	ipv6 prefix-list description	Добавляет описание к списку префиксов IPv6
	ipv6 prefix-list sequence-number	Включает функцию сортировки для списка префиксов IPv6

1.4.1. Настройка карты маршрутов

1.4.1.1. Эффект конфигурации

Определите набор политик маршрутизации, которые будут использоваться протоколами маршрутизации или PBR.

1.4.1.2. Примечания

- Если команда **match** использует ACL для определения условий соответствия пакетов, этот ACL необходимо настроить.
- Следующие команды **match** не могут быть настроены одновременно:

Следующие команды match	Невозможно настроить следующие команды match одновременно
match ip address	**match ip prefix-list**
match ipv6 address	**match ipv6 prefix-list**
match ip next-hop	**match ip next-hop prefix-list**
match ipv6 next-hop	**match ipv6 next-hop prefix-list**
match ip route-source	**match ip route-source prefix-list**
match ipv6 route-source	**match ipv6 route-source prefix-list**

- Следующие команды **set** не могут быть настроены одновременно:

Следующие команды set	Невозможно настроить одновременно следующие команды set
set ip next-hop	**set ip next-hop verify-availability**
set ip dscp	**set ip tos**
set ip dscp	**set ip precedence**

1.4.1.3. Шаги настройки

Создание политики (карта маршрутов)

- Обязательный.
- Выполните эту настройку на устройстве, к которому необходимо применить политику.

Установка условий соответствия политики

- Опционально.
- Если правило соответствия не настроено, ни один пакет не будет сопоставлен.
- Если настроено несколько правил соответствия, все правила соответствия должны быть сопоставлены.
- Выполните эту настройку на устройстве, к которому необходимо применить политику.

Настройка действий обработки политики

- Опционально.
- Если установленное правило не настроено, никакие действия по обработке выполняться не будут.

- Если настроено несколько установленных правил, все установленные правила должны выполняться (если установленные правила имеют разные приоритеты, вступает в силу установленное правило с наивысшим приоритетом).
- Выполните эту настройку на устройстве, к которому необходимо применить политику.

1.4.1.4. Проверка

Проверьте настройки карты маршрутов.

1.4.1.5. Связанные команды

Создание политики (карта маршрутов)

Команда	**route-map** *route-map-name* [{ **permit** | **deny** } *sequence*]
Описание параметра	*route-map-name*: указывает название карты маршрутов, содержащее не более 32 символов. **permit**: определяет режим работы этой политики как разрешение (permit), которое является режимом по умолчанию. **deny**: определяет режим работы этой политики как отказ (deny). Режим по умолчанию — permit. *sequence*: указывает порядковый номер этой политики. Меньшее значение означает более высокий приоритет. Значение по умолчанию — 10
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если эта карта маршрутов недоступна, эта команда создаст карту маршрутов и добавит политику в карту маршрутов. Если эта карта маршрутов доступна, эта команда добавит политику в карту маршрутов

Установка условий соответствия политики

Команда	**match as-path** *as-path-acl-list-number* [*as-path-acl-list-number*…..]
Описание параметра	*as-path-acl-list-number*: указывает номер списка AS-PATH в диапазоне от 1 до 500
Командный режим	Режим настройки карты маршрутов

Руководство по использованию	Это правило соответствия используется для соответствия атрибута AS-PATH маршрута BGP. Запустите команду **ip as-path access-list** *path-list-num* { **permit** | **deny** } *regular-expression* для настройки списка AS-PATH

Команда	**match community** { *community-list-number* | *community-list-name* } [**exact-match**] [{ *community-list-number* | *community-list-name* } [**exact-match**] …]
Описание параметра	*community-list-number*: указывает номер списка сообщества. Для стандартного списка сообщества значение находится в диапазоне от 1 до 99. Для списка extcommunity значение находится в диапазоне от 100 до 199. *community-list-name*: указывает имя списка сообщества, содержащее не более 80 символов. **exact-match**: указывает список точных совпадений. По умолчанию это список неточного соответствия, то есть правило соответствия соблюдается до тех пор, пока атрибуты маршрутизации содержат атрибуты, указанные в списке сообщества
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило соответствия используется для соответствия атрибута сообщества, указанного в списке сообществ

Команда	**match extcommunity** { *standard-list-number* | *standard-list-name* | *expanded-list-num* | *expanded-list-name* }
Описание параметра	*standard-list-number*: обозначает идентификатор в диапазоне от 1 до 99. Он используется для идентификации стандартного списка extcommunity. Один список extcommunity может содержать несколько значений extcommunity. *standard-list-name*: указывает имя стандартного списка extcommunity. Он используется для идентификации имени стандартного списка extcommunity. Один список extcommunity может содержать несколько значений extcommunity. *expanded-list-num*: обозначает идентификатор в диапазоне от 100 до 199. Он используется для идентификации списка extcommunity. Один список extcommunity может содержать несколько значений extcommunity.

	expanded-list-name: указывает имя extcommunity. Он используется для идентификации имени списка extcommunity. Один список extcommunity может содержать несколько значений extcommunity
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило соответствия используется для соответствия атрибута расширенного сообщества, указанного в списке extcommunity

Команда	**match interface** *interface-type interface-number* […*interface-type interface-number*]
Описание параметра	*interface-type interface-number*: указывает тип и номер интерфейса
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило соответствия используется для соответствия выходного интерфейса следующего hop-а маршрута или пакета

Команда	**match ip address** { *access-list-number* [*access-list-number*... | *access-list-name*...] | *access-list-name* [*access-list-number*...| *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name*...] }
Описание параметра	*access-list-number*: указывает номер списка доступа. Для стандартного списка доступа диапазоны значений составляют от 1 до 99 и от 1300 до 1999. Для расширенного списка доступа диапазоны значений составляют от 100 до 199 и от 2000 до 2699. *access-list-name*: указывает имя списка доступа. **prefix-list** *prefix-list-name*: указывает имя списка префиксов для соответствия
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило соответствия сопоставляет IPv4-адрес назначения пакета или маршрута с помощью ACL или списка префиксов. ACL и список префиксов не может быть настроен одновременно

Команда	**match ip next-hop** { *access-list-number* [*access-list-number*... | *access-list-name*...] | *access-list-name* [*access-list-number*... | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name*...] }
Описание параметра	*access-list-number*: указывает номер списка доступа. Для стандартного списка доступа диапазоны значений составляют от 1 до 99 и от 1300 до 1999. Для расширенного списка доступа диапазоны значений составляют от 100 до 199 и от 2000 до 2699. *access-list-name*: указывает имя списка доступа. **prefix-list** *prefix-list-name*: указывает имя списка префиксов для соответствия
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило соответствия сопоставляет IPv4-адрес следующего hop-а маршрута с помощью ACL или списка префиксов. ACL и список префиксов не может быть настроен одновременно

Команда	**match ip route-source** { *access-list-number* [*access-list-number*... | *access-list-name*...] | *access-list-name* [*access-list-number*... | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name*...] }
Описание параметра	*access-list-number*: указывает номер списка доступа. Для стандартного списка доступа диапазоны значений составляют от 1 до 99 и от 1300 до 1999. Для расширенного списка доступа диапазоны значений составляют от 100 до 199 и от 2000 до 2699. *access-list-name*: указывает имя списка доступа. **prefix-list** *prefix-list-name*: указывает имя списка префиксов для соответствия
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило соответствия сопоставляет исходный IPv4-адрес маршрута с помощью ACL или списка префиксов. ACL и список префиксов не может быть настроен одновременно

Команда	**match ipv6 address** { *access-list-name* | **prefix-list** *prefix-list-name* }
Описание параметра	*access-list-name*: указывает имя списка доступа. **prefix-list** *prefix-list-name*: указывает имя списка префиксов IPv6 для соответствия
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило соответствия сопоставляет IPv6-адрес назначения пакета или маршрута с помощью ACL или списка префиксов. ACL и список префиксов нельзя настроить одновременно

Команда	**match ipv6 next-hop** { *access-list-name* | **prefix-list** *prefix-list-name* }
Описание параметра	*access-list-name*: указывает имя списка доступа. **prefix-list** *prefix-list-name*: указывает имя списка префиксов IPv6 для соответствия
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило соответствия сопоставляет IPv6-адрес следующего hop-а маршрута с помощью ACL или списка префиксов. ACL и список префиксов не может быть настроен одновременно

Команда	**match ipv6 route-source** { *access-list-name* | **prefix-list** *prefix-list-name* }
Описание параметра	*access-list-name*: указывает имя списка доступа. **prefix-list** *prefix-list-name*: указывает имя списка префиксов IPv6 для соответствия
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило соответствия сопоставляет исходный IPv6-адрес маршрута с помощью ACL или списка префиксов. ACL и список префиксов не может быть настроен одновременно

Команда	**match metric** *metric*
Описание параметра	*metric*: указывает значение метрики маршрута в диапазоне от 0 до 4 294 967 295
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило соответствия используется для соответствия значения метрики маршрута

Команда	**match origin** { **egp** | **igp** | **incomplete** }
Описание параметра	**egp**: указывает, что источником является удаленный EGP. **igp**: указывает, что источником является локальный IGP. **incomplete**: указывает, что источник является неполным типом
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило соответствия используется для соответствия источника маршрута

Команда	**match route-type** { **local** | **internal** | **external** [**type-1** | **type-2**] | **level-1** | **level-2** }
Описание параметра	**local**: указывает маршрут, созданный локально. **internal**: указывает внутренний маршрут OSPF. **external**: указывает внешний маршрут (BGP или OSPF). **type-1** | **type-2**: указывает внешний маршрут OSPF типа 1 или типа 2. **level-1** | **level-2**: указывает маршрут ISIS Level-1 или Level-2
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило соответствия используется для соответствия типа маршрута

Команда	**match tag** *tag* […*tag*]
Описание параметра	*tag*: указывает значение тега маршрута
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило соответствия используется для соответствия значения тега маршрута

Настройка действий обработки политики

Команда	**set aggregator as** *as-number ip-address*
Описание параметра	*as-number*: указывает номер AS агрегатора. Номер AS варьируется от 1 до 4 294 967 295, что может обозначаться от 1 до 65535.65535 в точечном режиме (dot mode). *ip-address*: указывает адрес агрегатора
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для изменения значения атрибута AS агрегатора маршрута

Команда	**set as-path prepend** *as-number*
Описание параметра	*as-number*: указывает номер AS, который нужно добавить к атрибуту AS_PATH. Номер AS варьируется от 1 до 4 294 967 295, что может обозначаться от 1 до 65535.65535 в точечном режиме (dot mode)
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для добавления указанного значения атрибута as-path

Команда	**set as-path replace** *as-number*
Описание параметра	*as-number*: указывает номер AS, который заменит атрибут AS_PATH. Номер AS варьируется от 1 до 4 294 967 295, что может обозначаться от 1 до 65535.65535 в точечном режиме (dot mode)
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для замены указанного значения атрибута as-path

Команда	**set atomic-aggregate**
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки атрибута atomic-aggregate маршрута

Команда	**set comm-list** { *community-list-number* | *community-list-name* } **delete**
Описание параметра	*community-list-number*: указывает номер списка сообщества. Для стандартного списка сообщества значение находится в диапазоне от 1 до 99. Для списка extcommunity значение находится в диапазоне от 100 до 199. *community-list-name*: указывает имя списка сообщества, содержащее не более 80 символов
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило используется для удаления всех значений атрибутов сообщества из списка сообществ для маршрута, соответствующего правилам соответствия

Команда	**set community** { *community-number* [*community-number* …] **additive** | **none** }
Описание параметра	*community-number*: указывает значение атрибута сообщества. **additive**: добавляет номер на основе исходного атрибута сообщества. **none**: атрибут сообщества остается пустым
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки значения атрибута сообщества маршрута

Команда	**set dampening** *half-life reuse suppress max-suppress-time*
Описание параметра	*half-life*: период полураспада, когда маршрут доступен или недоступен, от 1 до 45 минут. Значение по умолчанию — 15 минут. *reuse*: если значение штрафа (пенальти) для маршрута меньше этого значения, подавление маршрута будет отменено. Значение варьируется от 1 до 20000, значение по умолчанию — 750. *suppress*: если значение штрафа (пенальти) для маршрута превышает это значение, маршрут будет подавлен. Значение варьируется от 1 до 20000, значение по умолчанию — 2000. *max-suppress-time*: указывает максимальное время, в течение которого маршрут может быть скрыт, в диапазоне от 1 до 255 минут. Значение по умолчанию составляет 4 × *half-life*
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки параметров flapping-а маршрута

Команда	**set extcomm-list** { *extcommunity-list-number* | *extcommunity-list-name* } **delete**
Описание параметра	*extcommunity-list-number*: указывает номер списка extcommunity. Для стандартного списка extcommunity, значение варьируется от 1 до 99. Для расширенного списка списка extcommunity, значение варьируется от 100 до 199.

	extcommunity-list-name: указывает имя списка extcommunity, содержащее не более 80 символов
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для удаления всех значений атрибутов расширенного сообщества из списка атрибутов extcommunity для маршрута, соответствующего правилам соответствия

Команда	**set extcommunity** { **rt** *extend-community-value* | **soo** *extend-community-value* }
Описание параметра	**rt**: устанавливает значение атрибута RT маршрута. **soo**: устанавливает значение атрибута SOO маршрута. *extend-community-value*: указывает значение расширенного сообщества
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки значения атрибута расширенного сообщества маршрута

Команда	**set fast-reroute backup-interface** *interface-type interface-number* [**backup-nexthop** *ip-address*]
Описание параметра	*interface-type interface-number*: указывает выходной интерфейс резервного копирования. **backup-nexthop** *ip-address*: указывает следующий hop для резервного копирования. Для интерфейса non-point-to-point необходимо указать резервный следующий hop
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки резервного выходного интерфейса и следующего hop-а быстрого перенаправления

Команда	**set ip default next-hop** *ip-address* [*weight*] […*ip-address* [*weight*]]
Описание параметра	*ip-address*: указывает IP-адрес следующего hop-a. *weight*: указывает вес следующего hop-a
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для указания следующего hop-a маршрута по умолчанию

Команда	**set ip dscp** *dscp_value*
Описание параметра	*dscp_value*: устанавливает значение DSCP в IP-заголовке IP-пакета
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для изменения поля dscp IP-пакета

Команда	**set ip next-hop recursive** *ip-address*
Описание параметра	*ip-address*: указывает рекурсивный IP-адрес следующего hop-a
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Эта команда используется только для настройки PBR. Это правило установки (set) используется для указания рекурсивного следующего hop-a маршрута. IP-адрес может повторяться на статическом или динамическом маршруте, который имеет выходной интерфейс и IP-адрес следующего hop-a. Поддерживается максимум 32 следующих hop-a. Если рекурсивный маршрут является статическим, для статического рекурсивного маршрута поддерживается только один следующий hop

Команда	**set ip next-hop verify-availability** *ip-address* [**track** *track-obj-number* | **bfd** *interface-type interface-number gateway*]
Описание параметра	*ip-address*: указывает IP-адрес следующего hop-а. **track**: оценивает эффективность следующего hop-а с помощью *Track*. **bfd**: указывает, что BFD используется для обнаружения соседей. *interface-type*: настраивает тип интерфейса. *interface-number*: настраивает номер интерфейса. *gateway*: настраивает IP-адрес шлюза, который является соседним IP-адресом BFD. Если следующий hop настроен как сосед, BFD будет использоваться для определения доступности пути пересылки
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для указания следующего hop-а маршрута, и BFD используется для быстрого определения эффективности следующего hop-а

Команда	**set ip precedence** { *number* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine** }
Описание параметра	*number*: указывает приоритет IP-заголовка с помощью номера от 0 до 7. 7: critical 6: flash 5: flash-override 4: immediate 3: internet 2: network 1: priority 0: routine **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**: приоритет IP-заголовка
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для изменения поля **precedence** заголовка IP-пакета

Команда	**set ip tos** { *number* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal** }
Описание параметра	*number*: указывает значение TOS IP-заголовка с числом от 0 до 15. 2: max-reliability 4: max-throughput 8: min-delay 1: min-monetary-cost 0: normal **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**: приоритет IP-заголовка
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для изменения поля tos IP-пакета

Команда	**set ipv6 default next-hop** *global-ipv6-address* [*weight*] [*global-ipv6-address* [*weight*] ...]
Описание параметра	*global-ipv6-address*: указывает IPv6-адрес следующего hop-а для пересылки пакетов. Маршрутизатор следующего hop-а должен быть соседним маршрутизатором. *weight*: указывает вес в режиме балансировки нагрузки в диапазоне от 1 до 8. Чем больше значение, тем больший пакетный трафик будет использоваться следующим hop-ом
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для указания IPv6-адреса следующего hop-а по умолчанию для маршрута

Команда	**set ipv6 next-hop** *global-ipv6-address* [*weight*] [*global-ipv6-address* [*weight*] ...]
Описание параметра	*global-ipv6-address*: указывает IPv6-адрес следующего hop-а для пересылки пакетов. Маршрутизатор следующего hop-а должен быть соседним маршрутизатором. *weight*: указывает вес в режиме балансировки нагрузки в диапазоне от 1 до 8. Чем больше значение, тем больший пакетный трафик будет использоваться следующим hop-ом
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для указания IPv6-адреса следующего hop-а маршрута

Команда	**set ipv6 next-hop verify-availability** *global-ipv6-address* **bfd** *interface-type interface-number gateway*
Описание параметра	*global-ipv6-address*: указывает IPv6-адрес следующего hop-а. **bfd**: указывает, что BFD используется для обнаружения соседей. *interface-type*: настраивает тип интерфейса. *interface-number*: настраивает номер интерфейса. *gateway*: настраивает IPv6-адрес шлюза, который является соседним IPv6-адресом BFD. Если следующий hop настроен как сосед, BFD будет использоваться для определения доступности пути пересылки
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для указания следующего hop-а маршрута, и BFD используется для быстрого определения эффективности следующего hop-а

Команда	**set ipv6 precedence** { *number* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine** }
Описание параметра	*number*: указывает приоритет IP-заголовка с помощью номера от 0 до 7. 7: critical

	6: flash 5: flash-override 4: immediate 3: internet 2: network 1: priority 0: routine **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**: приоритет IP-заголовка
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки приоритета заголовка пакета IPv6

Команда	**set level** { **level-1** | **level-2** | **level-1-2** | **stub-area** | **backbone** }
Описание параметра	**level-1**: указывает, что маршрут перераспределения объявляется на уровне ISIS 1. **level-2**: указывает, что маршрут перераспределения объявляется на уровне ISIS 2. **level-1-2**: указывает, что маршрут перераспределения объявляется на уровне ISIS 1 и Level-2. **stub-area**: указывает, что маршрут перераспределения объявляется в тупиковой области OSPF. **backbone**: указывает, что маршрут перераспределения объявляется в магистральной области OSPF
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки типа области назначения, в которую будет перенаправлен маршрут

Команда	**set local-preference** *number*
Описание параметра	*number*: указывает значение метрики локального приоритета в диапазоне от 0 до 4 294 967 295. Большее значение означает более высокий приоритет
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки значения атрибута local-preference маршрута

Команда	**set metric** [+ *metric-value* | - *metric-value* | *metric-value*]
Описание параметра	+: увеличивает (на основе значения метрики маршрута источника). -: уменьшает (на основе значения метрики маршрута источника). *metric-value*: устанавливает значение метрики маршрута перераспределения. Большее значение означает меньший приоритет
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для изменения значения метрики маршрута

Команда	**set metric-type** *type*
Описание параметра	*type*: устанавливает тип маршрута перераспределения. Тип маршрута перераспределения OSPF по умолчанию — тип 2
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки типа метрики

Команда	**set next-hop** *ip-address*
Описание параметра	*ip-address*: указывает IP-адрес следующего hop-а
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки IP-адреса следующего hop-а

Команда	**set origin** { **egp** | **igp** | **incomplete** }
Описание параметра	**egp**: указывает, что источником является удаленный EGP. **igp**: указывает, что источником является локальный IGP. **incomplete**: указывает, что источник имеет неполный тип и обычно относится к маршруту, созданному в результате перераспределения
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки атрибута источника маршрута

Команда	**set originator-id** *ip-address*
Описание параметра	*ip-address*: указывает адрес отправителя (originator)
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки IP-адреса отправителя маршрута

Команда	**set tag** *tag*
Описание параметра	*tag*: устанавливает тег маршрута перераспределения

Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки значения тега маршрута

Команда	**set distance** *number*
Описание параметра	*number*: чем больше значение административного расстояния, тем ниже приоритет
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки административного расстояния

Команда	**set weight** *number*
Описание параметра	*number*: устанавливает вес маршрута в диапазоне от 0 до 65 535. Большее значение означает более высокий приоритет
Командный режим	Режим настройки карты маршрутов
Руководство по использованию	Это правило установки (set) используется для установки веса маршрута

Отображение конфигураций карты маршрутов

Команда	**show route-map** [*name*]
Описание параметра	*name*: указывает карту маршрута
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации

Руководство по использованию	Запустите команду **show route-map**, чтобы отобразить конфигурации карты маршрутов. Если ACL используется при настройке карты маршрутов, вы можете запустить команду **show access-list**, чтобы отобразить конфигурации ACL

1.4.1.6. Пример конфигурации

Использование карты маршрутов при перераспределении маршрутов для фильтрации и изменения информации о маршрутах

Сценарий:

Как показано на Рисунке 1-4, устройство подключено как к домену маршрутизации OSPF, так и к домену маршрутизации RIP.



Рисунок 1-4.

Шаги настройки	• Перераспределите в OSPF только маршруты RIP с 4 hop-ами. В домене маршрутов OSPF, если типом маршрута является внешний тип маршрута 1, установите значение тега маршрута равным 40. • Перераспределите в RIP только маршруты OSPF со значением тега 10. В домене маршрута RIP установите начальное значение метрики этого маршрута равным 10 • Настройте redrip карты маршрута: сопоставьте маршрут с 4 часами, установите начальное значение метрики маршрута на 40, установите тип маршрута на внешний маршрут типа-1 и установите значение тега маршрута на 40. • Настройте redospf карты маршрута: сопоставьте маршрут со значением тега 10 и установите начальное значение метрики маршрута равным 10. • Настройте перераспределение маршрута RIP в OSPF и примените redrip карты маршрутов. • Настройте перераспределение маршрута OSPF на RIP и примените redospf карты маршрута
	QTECH(config)# route-map redrip permit 10 QTECH(config-route-map)# match metric 4 QTECH(config-route-map)# set metric-type type-1 QTECH(config-route-map)# set tag 40 QTECH(config-route-map)# exit

	QTECH(config)# route-map redospf permit 10 QTECH(config-route-map)# match tag 10 QTECH(config-route-map)# set metric 10 QTECH(config-route-map)# exit QTECH(config)# router ospf 1 QTECH(config-router)# redistribute rip subnets route-map redrip QTECH(config-router)# exit QTECH(config)# router rip QTECH(config-router)# redistribute ospf 1 route-map redospf QTECH(config-router)# exit
Проверка	• Проверьте конфигурации карты маршрутов, чтобы проверить правила политики. • Проверьте библиотеку информации о маршрутизации OSPF, чтобы убедиться, что правила, соответствующие правилам политики, перераспределены
	QTECH# show route-map route-map redrip, permit, sequence 10 Match clauses: metric 4 Set clauses: metric 40 metric-type type-1 tag 40 route-map redospf, permit, sequence 10 Match clauses: tag 10 Set clauses: metric 10
	QTECH# show ip ospf database external OSPF Router with ID (192.100.1.9) (Process ID 1) AS External Link States LS age: 5

	Options: 0x2 (-|-|-|-|-|-|E|-) LS Type: AS-external-LSA Link State ID: 192.168.199.0 (External Network Number) Advertising Router: 192.100.1.9 LS Seq Number: 80000001 Checksum: 0x554d Length: 36 Network Mask: /24 Metric Type: 1 TOS: 0 Metric: 4 Forward Address: 0.0.0.0 External Route Tag: 40

Применение карты маршрутов в PBR

Сценарий:

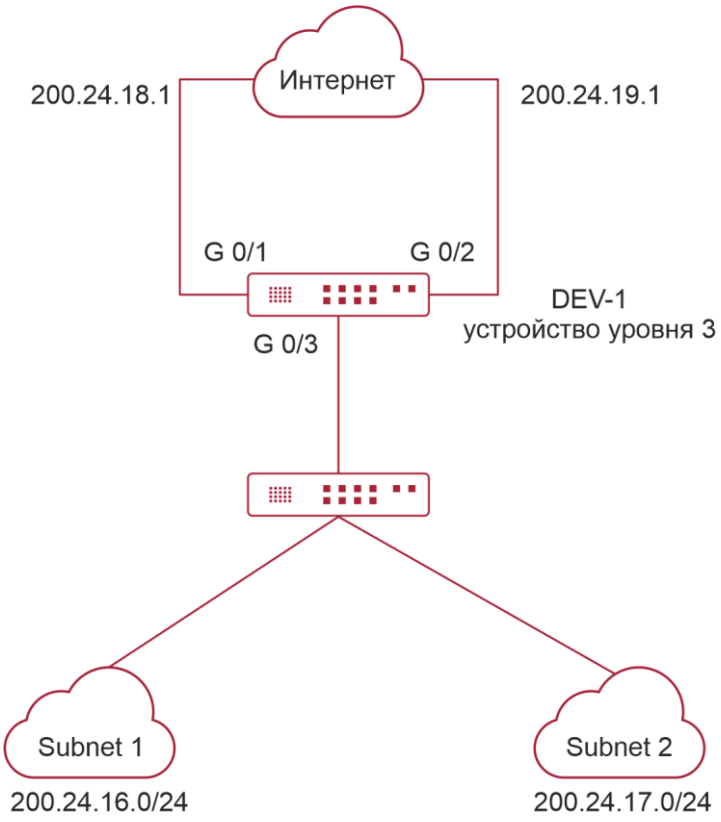


Рисунок 1-5.

Шаги настройки	Настройте PBR на устройстве DEV1 для достижения следующих целей: • Пакеты из подсети 1 (200.24.16.0/24) сначала отправляются из GE0/1. • Пакеты из подсети 2 (200.24.17.0/24) сначала отправляются из GE0/2. • Два выходных канала работают в режиме взаимного резервирования • Настройте два разных списка ACL для соответствия пакетов из подсетей 1 и 2 соответственно. • Настройте карту маршрутов RM_FOR_PBR: политика 10 используется для обеспечения того, чтобы «пакеты из подсети 1 отправлялись сначала из GE0/1»; политика 20 используется для обеспечения того, чтобы «пакеты из подсети 2 сначала отправлялись из GE0/2». • Настройте PBR для пакетов, полученных от GE0/3, и примените карту маршрутов RM_FOR_PBR. • Установите PBR для реализации избыточного резервного копирования между несколькими следующими hop-ами. **ПРИМЕЧАНИЕ:** в режиме избыточного резервирования последовательность нескольких установленных следующих hop-ов представляет собой последовательность приоритетов, вступающих в силу
	QTECH(config)# access-list 1 permit 200.24.16.0 0.0.0.255 QTECH(config)# access-list 2 permit 200.24.17.0 0.0.0.255 QTECH(config)# route-map RM_FOR_PBR 10 QTECH(config-route-map)# match ip address 1 QTECH(config-route-map)# set ip next-hop 200.24.18.1 QTECH(config-route-map)# set ip next-hop 200.24.19.1 QTECH(config-route-map)# exit QTECH(config)# route-map RM_FOR_PBR 20 QTECH(config-route-map)# match ip address 2 QTECH(config-route-map)# set ip next-hop 200.24.19.1 QTECH(config-route-map)# set ip next-hop 200.24.18.1 QTECH(config-route-map)# exit QTECH(config)# interface GigabitEthernet 0/3 QTECH(config-if)# ip policy route-map RM_FOR_PBR QTECH(config)# ip policy redundance

Проверка	• Проверьте конфигурации PBR, чтобы убедиться, что карта маршрутов применяется к интерфейсам. • Проверьте конфигурации карты маршрутов, чтобы проверить правила политики. • Проверьте конфигурации ACL, чтобы проверить правила фильтрации пакетов
	QTECH# show ip policy Balance mode: redundance Interface Route map GigabitEthernet 0/3 RM_FOR_PBR !
	QTECH# show route-map route-map RM_FOR_PBR, permit, sequence 10 Match clauses: ip address 1 Set clauses: ip next-hop 200.24.18.1 ip next-hop 200.24.19.1 route-map RM_FOR_PBR, permit, sequence 20 Match clauses: ip address 2 Set clauses: ip next-hop 200.24.19.1 ip next-hop 200.24.18.1
	QTECH# show access-lists ip access-list standard 1 10 permit 200.24.16.0 0.0.0.255 10 permit 200.24.16.0 0.0.0.255 ip access-list standard 2 10 permit 200.24.17.0 0.0.0.255

1.4.1.7. Распространенные ошибки

После настройки соответствия списков ACL и списков префиксов соответствующие списки ACL и списки префиксов не определяются.

1.4.2. Настройка списка фильтрации

1.4.2.1. Эффект конфигурации

Определите набор правил фильтрации маршрутов, которые будут использоваться протоколами маршрутизации.

1.4.2.2. Примечания

Настроенный список фильтрации может вступить в силу только после того, как он будет связан с протоколом маршрутизации.

1.4.2.3. Шаги настройки

Настройка списка префиксов

- Чтобы фильтровать префиксы адресов, вам следует выполнить эту настройку.
- Если нет особых требований, вам следует выполнить эту настройку на маршруте, для которого необходимо выполнить фильтрацию на основе списка префиксов.

Настройка списка путей AS

- Чтобы фильтровать префиксы адресов, вам следует выполнить эту настройку.
- Если нет особых требований, вам следует выполнить эту настройку на маршруте, для которого необходимо выполнить фильтрацию на основе пути AS.

Настройка списка сообщества

- Чтобы фильтровать атрибуты сообщества, вам следует выполнить эту настройку.
- Если нет особых требований, вам следует выполнить эту настройку на маршруте, для которого необходимо фильтровать атрибуты сообщества.

Настройка списка Extcommunity

- Чтобы фильтровать атрибуты расширенного сообщества, вам следует выполнить эту настройку.
- Если нет особых требований, вам следует выполнить эту настройку на маршруте, для которого необходимо фильтровать атрибутов расширенного сообщества.

1.4.2.4. Проверка

- Проверьте, правильно ли настроен список фильтрации.
- Проверьте таблицу маршрутизации, чтобы убедиться, что маршруты можно правильно фильтровать.

1.4.2.5. Связанные команды

Определение правил фильтрации путей AS

Команда	**ip as-path access-list** *path-list-num* { **permit** | **deny** } *regular-expression*
Описание параметра	*path-list-num*: указывает имя ACL пути AS на основе регулярного выражения (regular expression) и является идентификатором списка путей AS в диапазоне от 1 до 500. **permit**: разрешает доступ. **deny**: запрещает доступ.

	regular-expression: указывает регулярное выражение в диапазоне от 1 до 255
Командный режим	Режим глобальной конфигурации

Определение списка сообщества

Команда	**ip community-list** { { **standard** | **expanded** } *community-list-name* | *community-list-number* } { **permit** | **deny** } [*community-number*..]
Описание параметра	**standard**: обозначает стандартный список сообщества. **expanded**: обозначает расширенный список сообщества. *community-list-name*: указывает название списка сообщества, содержащее не более 80 символов. *community-list-number*: указывает номер списка сообщества. Для стандартного списка сообществ значение находится в диапазоне от 1 до 99. Для списка расширенного сообществ значение находится в диапазоне от 100 до 199. **permit**: разрешает доступ. **deny**: запрещает доступ. *community-number*: указывает значение атрибута сообщества
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду, чтобы определить список сообществ, используемый для BGP

Определение списка Extcommunity

Команда	**ip extcommunity-list** {*expanded-list* | **expanded** *list-name* } { **permit** | **deny** } [*regular-expression*]
Описание параметра	*expanded-list*: указывает расширенный список extcommunity в диапазоне от 100 до 199. Один список extcommunity может содержать несколько правил. *standard-list*: указывает стандартный список extcommunity в диапазоне от 1 до 99. Один список extcommunity может содержать несколько правил. *expanded list-name*: указывает расширенное имя extcommunity, содержащее не более 32 символов. При использовании этого параметра вы входите в режим настройки списка extcommunity.

	standard list-name: указывает имя стандартного списка extcommunity, содержащее не более 32 символов. При использовании этого параметра вы входите в режим настройки списка extcommunity. **permit**: определяет правило extcommunity на разрешение. **deny**: определяет правило extcommunity на отказ. *regular-expression*: (необязательно) определяет соответствующий шаблон, который используется для соответствия с extcommunity. *sequence-number*: (необязательно) определяет порядковый номер правила в диапазоне от 1 до 2 147 483 647. Если порядковый номер не указан, порядковый номер автоматически увеличивается на 10 при добавлении правила по умолчанию. Первоначальное число — 10. **rt**: (необязательно) устанавливает значение атрибута RT. Эту команду можно использовать только для стандартной конфигурации extcommunity, но не для расширенной конфигурации extcommunity. **soo**: (необязательно) устанавливает значение атрибута SOO. Эту команду можно использовать только для стандартной конфигурации extcommunity, но не для расширенной конфигурации extcommunity. *value*: указывает значение расширенного сообщества (extend_community_value)
Командный режим	Режим глобальной конфигурации и режим конфигурации ip extcommunity-list

Создание списка префиксов

Команда	**ip prefix-list** *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]
Описание параметра	*prefix-list-name*: указывает имя списка префиксов. *seq-number*: присваивает порядковый номер записи списка префиксов в диапазоне от 1 до 2 147 483 647. Если эта команда не содержит порядковый номер, система назначит порядковый номер по умолчанию записи списка префиксов. Порядковый номер по умолчанию для первой записи равен 5. В последствии порядковый номер по умолчанию для каждой записи, которой не присвоено значение, будет первое число, кратное 5, превышающее предыдущий порядковый номер. **deny**: запрещает доступ при выполнении определенных условий. **permit**: разрешает доступ при выполнении определенных условий. *ip-prefix*: настраивает IP-адрес и маску в диапазоне от 0 до 32 цифр. *minimum-prefix-length*: указывает минимальный диапазон (а именно, начальную длину диапазона). *maximum-prefix-length*: указывает максимальный диапазон (а именно, конечную длину диапазона)

Командный режим	Режим глобальной конфигурации

Добавление описания в список префиксов

Команда	**ip prefix-list** *prefix-list-name* **description** *descripton-text*
Описание параметра	*prefix-list-name*: указывает имя списка префиксов. *descripton-text*: описывает список префиксов
Командный режим	Режим глобальной конфигурации

Включение функции сортировки для списка префиксов

Команда	**ip prefix-list sequence-number**
Командный режим	Режим глобальной конфигурации

Создание списка префиксов IPv6

Команда	**ipv6 prefix-list** *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv6-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]
Описание параметра	*prefix-list-name*: указывает имя списка префиксов. *seq-number*: присваивает порядковый номер записи списка префиксов в диапазоне от 1 до 2 147 483 647. Если эта команда не содержит порядковый номер, система назначит порядковый номер по умолчанию записи списка префиксов. Порядковый номер по умолчанию для первой записи равен 5. В последствии порядковый номер по умолчанию для каждой записи, которой не присвоено значение, будет первое число, кратное 5, превышающее предыдущий порядковый номер. **deny**: запрещает доступ при выполнении определенных условий. **permit**: разрешает доступ при выполнении определенных условий. *ipv6-prefix*: настраивает IP-адрес и маску в диапазоне от 0 до 128 цифр. *minimum-prefix-length*: указывает минимальный диапазон (а именно, начальную длину диапазона). *maximum-prefix-length*: указывает максимальный диапазон (а именно, конечную длину диапазона)
Командный режим	Режим глобальной конфигурации

Добавление описания в список префиксов IPv6

Команда	**ipv6 prefix-list** *prefix-list-name* **description** *descripton-text*
Описание параметра	*prefix-list-name*: указывает имя списка префиксов. *descripton-text*: описывает список префиксов
Командный режим	Режим глобальной конфигурации

Включение функции сортировки для списка префиксов IPv6

Команда	**ipv6 prefix-list sequence-number**
Командный режим	Режим глобальной конфигурации

1.4.2.6. Пример конфигурации

Настройка списка префиксов

Сценарий:

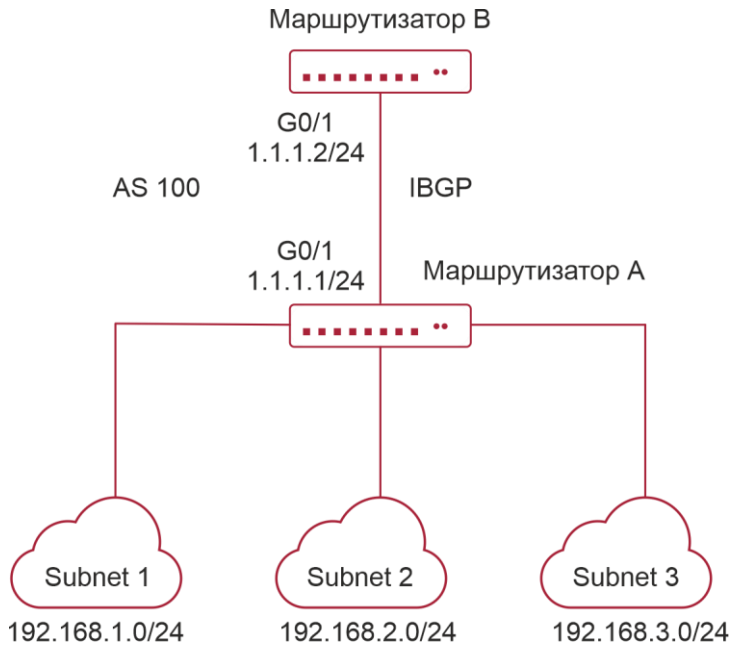


Рисунок 1-6.

Шаги настройки	• Настройте соседа IBGP и объявите его в трех подключенных подсетях. • Настройте список префиксов.

	• Свяжите список префиксов с A для фильтрации отправленных маршрутов
A	A# configure terminal A(config)# ip prefix-list pre1 permit 192.168.1.0/24 A(config)# router bgp 100 A(config-router)# neighbor 1.1.1.2 prefix-list pre1 out A(config-router)# end
Проверка	• Запустите команду **show**, чтобы отобразить список префиксов. • Запустите команду **show**, чтобы отобразить таблицу маршрутизации BGP и проверить правильность поведения фильтрации
A	A# show ip prefix-list ip prefix-list pre1: 1 entries seq 5 permit 192.168.1.0/24 A# show ip bgp BGP table version is 2, local router ID is 1.1.1.1 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale, b - backup entry Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path *> 192.168.1.0 0.0.0.0 0 32768 i *> 192.168.2.0 0.0.0.0 0 32768 i *> 192.168.3.0 0.0.0.0 0 32768 i Total number of prefixes 3
B	B# show ip bgp BGP table version is 4, local router ID is 1.1.1.2 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale Origin codes: i - IGP, e - EGP, ? – incomplete Network Next Hop Metric LocPrf Weight Path

	*>i192.168.1.0 1.1.1.1 0 100 0 i Total number of prefixes 1

Настройка списка путей AS

Сценарий:

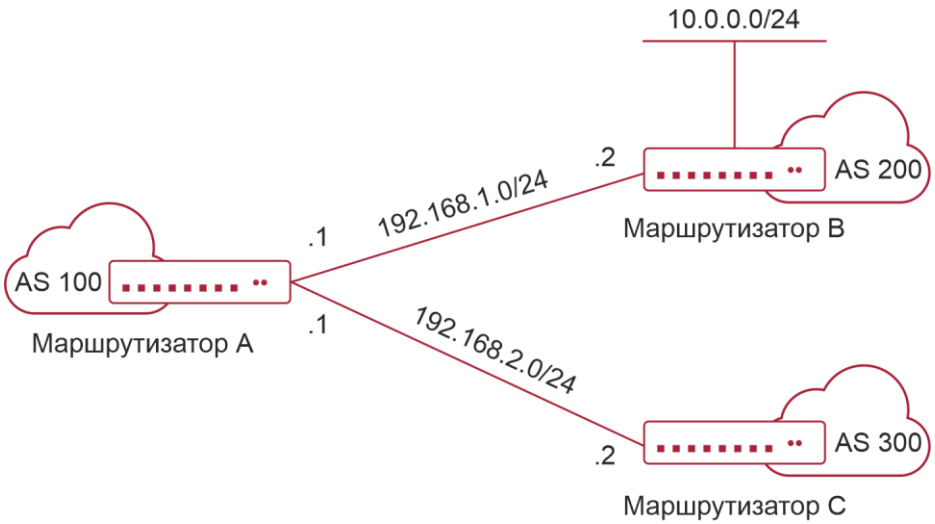


Рисунок 1-7.

Шаги настройки	• Создайте правило фильтрации путей AS для соответствия информации о пути, включая только AS 200. • Установите соседство EBGP на A с B и C. • Свяжите список AS-путей с A, чтобы фильтровать маршруты, полученные от B и C
A	A(config)# ip as-path access-list 123 permit ^200$ A(config)# router bgp 100 A(config)# neighbor 192.168.1.2 filter-list 123 in A(config)# neighbor 192.168.2.2 filter-list 123 in
Проверка	• Запустите команду **show**, чтобы отобразить список путей AS. • Запустите команду **show**, чтобы отобразить таблицу маршрутизации BGP и проверить правильность поведения фильтрации
A	A# show ip as-path-access-list AS path access list 123 permit ^200$

	//When no AS-path list is associated with A, run the show command to check the BGP
	routing table.
	A(config)# show ip bgp
	BGP table version is 1, local router ID is 1.1.1.1
	Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
	S Stale, b - backup entry
	Origin codes: i - IGP, e - EGP, ? - incomplete
	
	Network Next Hop Metric LocPrf Weight Path
	*> 10.0.0.0/24 192.168.1.2 0 0 200 i
	*> 20.0.0.0/24 192.168.2.2 0 0 300 i
	
	Total number of prefixes 2
	
	//When an AS-path list is associated with A, run the show command to display the
	BGP routing table and check whether the filtering behavior is correct.
	A(config)# show ip bgp
	BGP table version is 1, local router ID is 1.1.1.1
	Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
	S Stale, b - backup entry
	Origin codes: i - IGP, e - EGP, ? - incomplete
	
	Network Next Hop Metric LocPrf Weight Path
	*> 10.0.0.0/24 192.168.1.2 0 0 200 i
	Total number of prefixes 1

Настройка списка сообщества

Сценарий:

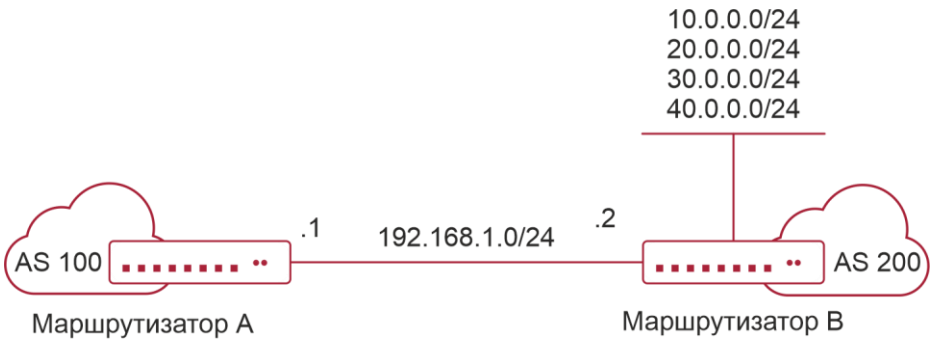


Рисунок 1-8.

Шаги настройки	• Определите стандартный список сообществ, соответствующий атрибуту сообщества 100:20. • Установите соседство EBGP между A и B. • Объявите маршрут с атрибутом сообщества на B. • Свяжите список сообществ с A (BGP можно применять только через карту маршрутов), чтобы фильтровать маршруты, полученные на B
A	A(config)# ip community-list standard test permit 100:20 A(config)# route-map COM A(config-route-map)# match community test A(config-route-map)# exit A(config)# router bgp 100 A(config-router)# neighbor 192.168.1.2 route-map COM in
B	B(config)# route-map comm1 B(config-route-map)# set community 100:20 200:20 B(config-route-map)# route-map comm2 B(config-route-map)# set community 100:20 B(config-route-map)# route-map comm3 B(config-route-map)# set community 200:20 B(config-route-map)# exit B(config)# router bgp 200 B(config-router)# neighbor 192.168.1.1 send-community B(config-router)# network 10.0.0.0 mask 255.255.255.0 route-map comm1 B(config-router)# network 20.0.0.0 mask 255.255.255.0 route-map comm2

	B(config-router)# network 30.0.0.0 mask 255.255.255.0 route-map comm3 B(config-router)# network 40.0.0.0 mask 255.255.255.0
Проверка	• Запустите команду **show**, чтобы отобразить список сообщества. • Запустите команду **show**, чтобы отобразить таблицу маршрутизации BGP и проверить правильность поведения фильтрации
A	A# show ip community-list Named Community standard list test permit 100:20
	//When no community list is associated with A, run the show command to check the BGP routing table. A# show ip bgp BGP table version is 1, local router ID is 192.168.1.1 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale, b - backup entry Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path *> 10.0.0.0/24 192.168.1.2 0 0 200 i *> 20.0.0.0/24 192.168.1.2 0 0 200 i *> 30.0.0.0/24 192.168.1.2 0 0 200 i *> 40.0.0.0/24 192.168.1.2 0 0 200 i Total number of prefixes 4 A# show ip bgp 10.0.0.0 BGP routing table entry for 10.0.0.0/24 Paths: (1 available, best #1, table Default-IP-Routing-Table) Not advertised to any peer 200 192.168.1.2 from 192.168.1.2 (192.168.1.2) Origin IGP, metric 0, localpref 100, valid, external, best Community: 100:20 200:20 Last update: Wed Nov 6 18:58:18 2013 A# show ip bgp 20.0.0.0

	BGP routing table entry for 20.0.0.0/24 Paths: (1 available, best #1, table Default-IP-Routing-Table) Not advertised to any peer 200 192.168.1.2 from 192.168.1.2 (192.168.1.2) Origin IGP, metric 0, localpref 100, valid, external, best Community: 100:20 Last update: Wed Nov 6 18:58:18 2013 A# show ip bgp 30.0.0.0 BGP routing table entry for 30.0.0.0/24 Paths: (1 available, best #1, table Default-IP-Routing-Table) Not advertised to any peer 200 192.168.1.2 from 192.168.1.2 (192.168.1.2) Origin IGP, metric 0, localpref 100, valid, external, best Community: 200:20 Last update: Wed Nov 6 18:58:18 2013 A# show ip bgp 40.0.0.0 BGP routing table entry for 40.0.0.0/24 Paths: (1 available, best #1, table Default-IP-Routing-Table) Not advertised to any peer 200 192.168.1.2 from 192.168.1.2 (192.168.1.2) Origin IGP, metric 0, localpref 100, valid, external, best Last update: Wed Nov 6 18:58:18 2013
	//When a community list is associated with A, run the show command to display the BGP routing table and check whether the filtering behavior is correct. A# show ip bgp BGP table version is 1, local router ID is 192.168.1.1 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale, b - backup entry Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path

```
*> 10.0.0.0/24      192.168.1.2      0          0          200 i
*> 20.0.0.0/24      192.168.1.2      0          0          200 i

Total number of prefixes 2
A#
A# show ip bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Not advertised to any peer
        200
        192.168.1.2 from 192.168.1.2 (192.168.1.2)
        Origin IGP, metric 0, localpref 100, valid, external, best
        Community: 100:20 200:20
        Last update: Wed Nov 6 19:02:49 2013

A# show ip bgp 20.0.0.0
BGP routing table entry for 20.0.0.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Not advertised to any peer
        200
        192.168.1.2 from 192.168.1.2 (192.168.1.2)
        Origin IGP, metric 0, localpref 100, valid, external, best
        Community: 100:20
        Last update: Wed Nov 6 19:02:49 2013
```

Настройка списка Extcommunity

Сценарий:

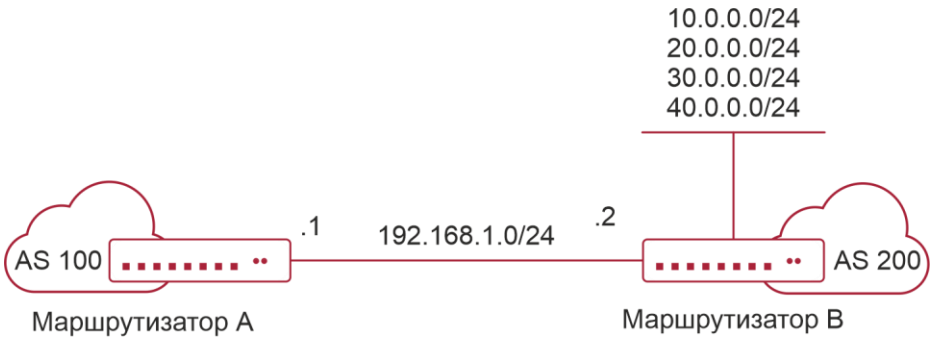


Рисунок 1-9.

Шаги настройки	• Определите список extcommunity, соответствующий атрибуту extcommunity RT 1: 100. • Установите соседство EBGP между A и B. • Объявите маршрут с атрибутом extcommunity на B. • Свяжите список extcommunity с A (BGP можно применять только через карту маршрутов), чтобы фильтровать маршруты, полученные на B
A	A(config)# ip extcommunity-list 10 permit rt 1:100 A(config)# route-map EXTCOM A(config-route-map)# match extcommunity 10 A(config-route-map)# exit A(config)# router bgp 100 A(config-router)# neighbor 192.168.1.2 route-map EXTCOM in
B	B(config)# route-map ecomm1 B(config-route-map)# set extcommunity rt 1:100 2:200 B(config-route-map)# route-map ecomm2 B(config-route-map)# set extcommunity rt 1:100 B(config-route-map)# route-map ecomm3 B(config-route-map)# set extcommunity rt 2:200 B(config-route-map)# exit B(config)# router bgp 200 B(config-router)# neighbor 192.168.1.1 send-community both B(config-router)# network 10.0.0.0 mask 255.255.255.0 route-map ecomm1 B(config-router)# network 20.0.0.0 mask 255.255.255.0 route-map ecomm2 B(config-router)# network 30.0.0.0 mask 255.255.255.0 route-map ecomm3 B(config-router)# network 40.0.0.0 mask 255.255.255.0
Проверка	• Запустите команду **show**, чтобы отобразить список extcommunity. • Запустите команду **show**, чтобы отобразить таблицу маршрутизации BGP и проверить правильность поведения фильтрации
A	A(config)#show ip extcommunity-list Extended community standard list 10 10 permit RT:1:100

//When no extcommunity list is associated with A, run the show command to check

the BGP routing table.

A# show ip bgp

BGP table version is 1, local router ID is 192.168.1.1

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale, b - backup entry

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight Path
*> 10.0.0.0/24	192.168.1.2	0	0	200 i
*> 20.0.0.0/24	192.168.1.2	0	0	200 i
*> 30.0.0.0/24	192.168.1.2	0	0	200 i
*> 40.0.0.0/24	192.168.1.2	0	0	200 i

Total number of prefixes 4

A#

A# show ip bgp 10.0.0.0

BGP routing table entry for 10.0.0.0/24

Paths: (1 available, best #1, table Default-IP-Routing-Table)

Not advertised to any peer

200

192.168.1.2 from 192.168.1.2 (192.168.1.2)

Origin IGP, metric 0, localpref 100, valid, external, best

Extended Community: RT:1:100 RT:2:200

Last update: Wed Nov 6 19:15:12 2013

A# show ip bgp 20.0.0.0

BGP routing table entry for 20.0.0.0/24

Paths: (1 available, best #1, table Default-IP-Routing-Table)

Not advertised to any peer

200

192.168.1.2 from 192.168.1.2 (192.168.1.2)

Origin IGP, metric 0, localpref 100, valid, external, best

Extended Community: RT:1:100

	Last update: Wed Nov 6 19:15:12 2013
	A# show ip bgp 30.0.0.0 BGP routing table entry for 30.0.0.0/24 Paths: (1 available, best #1, table Default-IP-Routing-Table) Not advertised to any peer 200 192.168.1.2 from 192.168.1.2 (192.168.1.2) Origin IGP, metric 0, localpref 100, valid, external, best Extended Community: RT:2:200 Last update: Wed Nov 6 19:15:12 2013 A# show ip bgp 40.0.0.0 BGP routing table entry for 40.0.0.0/24 Paths: (1 available, best #1, table Default-IP-Routing-Table) Not advertised to any peer 200 192.168.1.2 from 192.168.1.2 (192.168.1.2) Origin IGP, metric 0, localpref 100, valid, external, best Last update: Wed Nov 6 19:15:12 2013
	//When an extcommunity list is associated with A, run the show command to display the BGP routing table and check whether the filtering behavior is correct. A# show ip bgp BGP table version is 1, local router ID is 192.168.1.1 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale, b - backup entry Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path *> 10.0.0.0/24 192.168.1.2 0 0 200 i *> 20.0.0.0/24 192.168.1.2 0 0 200 i Total number of prefixes 2 A#

	A# show ip bgp 10.0.0.0 BGP routing table entry for 10.0.0.0/24 Paths: (1 available, best #1, table Default-IP-Routing-Table) Not advertised to any peer 200 192.168.1.2 from 192.168.1.2 (192.168.1.2) Origin IGP, metric 0, localpref 100, valid, external, best Extended Community: RT:1:100 RT:2:200 Last update: Wed Nov 6 19:17:04 2013
	A# show ip bgp 20.0.0.0 BGP routing table entry for 20.0.0.0/24 Paths: (1 available, best #1, table Default-IP-Routing-Table) Not advertised to any peer 200 192.168.1.2 from 192.168.1.2 (192.168.1.2) Origin IGP, metric 0, localpref 100, valid, external, best Extended Community: RT:1:100 Last update: Wed Nov 6 19:17:04 2013

1.4.2.7. Распространенные ошибки

Список фильтрации настроен, но неправильно применен в протоколе маршрутизации, в результате чего список фильтрации не может действовать.

1.5. Мониторинг

1.5.1. Отображение

Описание	Команда
Отображает конфигурации карты маршрутов	**show route-map** [*route-map-name*]
Отображает конфигурации ACL	**show access-lists** [*id* | *name*]
Отображает конфигурации списка префиксов IPv4	**show ip prefix-list** [*prefix-name*]
Отображает конфигурации списка префиксов IPv6	**show ipv6 prefix-list** [*prefix-name*]

Описание	Команда
Отображает конфигурации списка AS-путей	**show ip as-path-access-list** [*num*]
Отображает конфигурации списка сообщества	**show ip community-list** [*community-list-number* | *community-list-name*]
Отображает конфигурации списка extcommunity	**show ip extcommunity-list** [*extcommunity-list-num* | *extcommunity-list-name*]

2. НАСТРОЙКА КЛЮЧЕЙ

2.1. Обзор

Ключи — это своего рода параметры, которые используются в алгоритмах для преобразования обычного текста в зашифрованный текст или из зашифрованного текста в обычный текст.

Аутентификация обычного текста и зашифрованного текста поддерживается для аутентификации пакетов в протоколе маршрутизации, во время которой необходимо использовать ключи.

ПРИМЕЧАНИЕ: в настоящее время ключи используются только для аутентификации пакетов RIP и ISIS.

2.2. Приложения

Приложение	Описание
RIP-аутентификация	RIP использует ключи для аутентификации пакетов

2.2.1. RIP-аутентификация

2.2.1.1. Сценарий

Сетевые устройства используют RIP и режим аутентификации MD5 для повышения безопасности протокола.

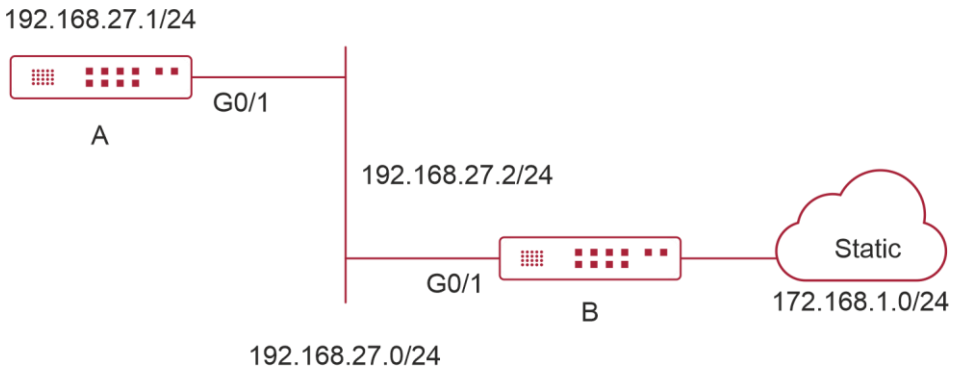


Рисунок 2-1.

2.2.1.2. Развертывание

- Настройте цепочку ключей на A. Настройте RIP для включения аутентификации пакетов и использования цепочки ключей.
- Настройте цепочку ключей на B. Настройте RIP для включения аутентификации пакетов и использования цепочки ключей.

2.3. Функции

2.3.1. Обзор

Особенность	Описание
Цепочка ключей	Предоставьте инструмент для аутентификации в протоколе маршрутизации

2.3.2. Цепочка ключей

2.3.2.1. Принцип работы

Цепочка ключей может содержать несколько разных ключей. Каждый ключ содержит следующие атрибуты:

- Идентификатор ключа: идентифицирует ключ. В текущей цепочке ключей ключи и идентификаторы сопоставляются взаимно однозначно.
- Строка аутентификации: указывает набор ключевых символов, используемых для проверки согласованности строк аутентификации в протоколе маршрутизации.
- Lifetime (время жизни): указывает срок действия текущего ключа для отправки или получения пакетов. В разные периоды могут использоваться разные ключи аутентификации.

2.3.2.2. Сопутствующая конфигурация

Создание цепочки ключей и ключа

В режиме глобальной конфигурации запустите команду **key chain** *key-chain-name*, чтобы определить цепочку ключей и войти в режим настройки цепочки ключей.

В режиме настройки цепочки ключей запустите команду **key** *key-id*, чтобы определить ключ и войти в режим настройки ключей цепочки ключей.

Настройка строки аутентификации

В режиме настройки ключей цепочки ключей запустите текстовую команду **key-string** [**0**|**7**] *text*, чтобы указать строку аутентификации.

- По умолчанию настраивается строка аутентификации в виде обычного текста. Значение **0** указывает, что настроен ключ аутентификации в виде обычного текста.
- Значение **7** указывает, что настроена строка аутентификации зашифрованного текста.
- Служба аутентификации с шифрованием отключена по умолчанию. Вы можете запустить команду **service password-encryption**, чтобы разрешить службе шифрования принудительно преобразовывать аутентификацию в виде обычного текста в зашифрованный текст.

Настройка время жизни

В режиме настройки ключей цепочки ключей вы можете настроить время жизни цепочки ключей в направлениях приема и отправки.

- **accept-lifetime** *start-time* **{ infinite |** *end-time* **| duration** *seconds* **}**: настраивает время жизни цепочки ключей в направлении приема.

- **send-lifetime** *start-time* **{ infinite |** *end-time* **| duration** *seconds* **}**: настраивает время жизни цепочки ключей в направлении отправки.

2.4. Конфигурация

Конфигурация	Описание и команда	
Настройка цепочки ключей	(Обязательно) Используется для создания ключа	
	key chain	Создает цепочку ключей
	key	Настраивает идентификатор ключа
	key-string	Настраивает строку ключа
	accept-lifetime	Настраивает время жизни в принимающем направлении
	send-lifetime	Настраивает время жизни в направлении отправки

2.4.1. Настройка цепочки ключей

2.4.1.1. Эффект конфигурации

Определите цепочку ключей, которая будет использоваться протоколом маршрутизации.

2.4.1.2. Примечания

Цепочка ключей может вступить в силу только после того, как она будет связана с протоколом маршрутизации.

2.4.1.3. Шаги настройки

Создание цепочки ключей

- Эта конфигурация является обязательной, если необходимо использовать цепочку ключей.
- Если нет особых требований, вам следует выполнить эту настройку на всех маршрутизаторах, для которых необходимо выполнить аутентификацию протокола маршрутизации.

Настройка идентификатора ключа

- Эта конфигурация является обязательной, если необходимо использовать цепочку ключей.
- Если нет особых требований, вам следует выполнить эту настройку на всех маршрутизаторах, для которых необходимо выполнить аутентификацию протокола маршрутизации.

Настройка строки ключа

- Эта конфигурация является обязательной, если необходимо использовать цепочку ключей.
- Если нет особых требований, вам следует выполнить эту настройку на всех маршрутизаторах, для которых необходимо выполнить аутентификацию протокола маршрутизации.

Настройте время жизни в направлении приема

- Опционально.
- Если время жизни в направлении отправки не настроено, цепочка ключей будет действовать всегда.

Настройте время жизни в направлении отправки

- Опционально.
- Если время жизни в направлении отправки не настроено, цепочка ключей будет действовать всегда.

2.4.1.4. Проверка

Используйте ключи в протоколе маршрутизации и наблюдайте за соседством, установленным протоколом маршрутизации. Если ключи несовместимы, соседство не может быть установлено.

2.4.1.5. Связанные команды

Настройка цепочки ключей

Команда	**key chain** *key-chain-name*
Описание параметра	*key-chain-name*: указывает название цепочки ключей
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Чтобы цепочка ключей вступила в силу, необходимо настроить хотя бы один ключ

Настройка идентификатора ключа

Команда	**key** *key-id*
Описание параметра	*key-id*: указывает идентификатор ключа аутентификации в цепочке ключей в диапазоне от 0 до 2 147 483 647
Командный режим	Режим настройки цепочки ключей

Настройка строки ключа аутентификации

Команда	**key-string** [**0**|**7**] *text*
Описание параметра	**0**: указывает, что ключ отображается в виде обычного текста. **7**: указывает, что ключ отображается в зашифрованном тексте. *text*: указывает символы строки аутентификации
Командный режим	Режим настройки ключей цепочки ключей

Настройка времени жизни в направлении отправки

Команда	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
Описание параметра	*start-time*: указывает время начала жизни. **infinite**: указывает, что ключ всегда эффективен. *end-time*: указывает время окончания времени жизни, которое должно быть позже времени начала (*start-time*). **duration** *seconds*: указывает продолжительность от времени начала до времени окончания в диапазоне от 1 до 2 147 483 646
Командный режим	Режим настройки ключей цепочки ключей
Руководство по использованию	Запустите эту команду, чтобы определить срок действия ключа в направлении отправки

Настройка времени жизни в направлении приема

Команда	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
Описание параметра	*start-time*: указывает время начала жизни. **infinite**: указывает, что ключ всегда эффективен. *end-time*: указывает время окончания времени жизни, которое должно быть позже времени начала (*start-time*). **duration** *seconds*: указывает продолжительность от времени начала до времени окончания в диапазоне от 1 до 2 147 483 646
Командный режим	Режим настройки ключей цепочки ключей
Руководство по использованию	Запустите эту команду, чтобы определить срок жизни ключа в направлении приема

2.4.1.6. Пример конфигурации

Настройка цепочки ключей и использование цепочки ключей при аутентификации пакетов RIP

Сценарий:

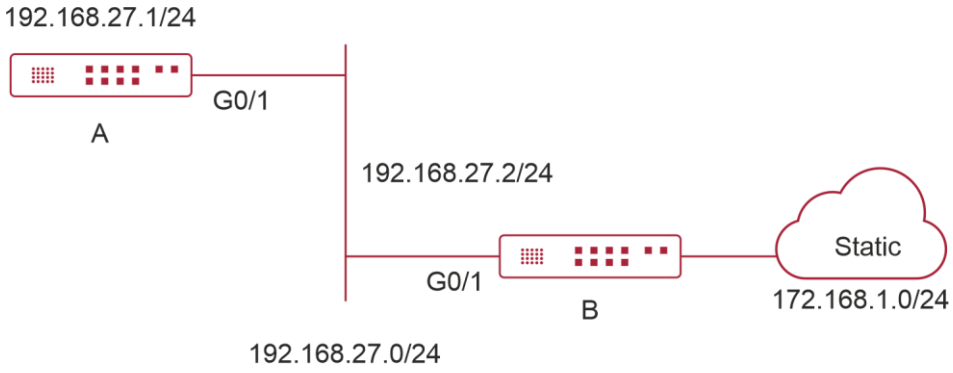


Рисунок 2-2.

Шаги настройки	• Настройте ключ на всех маршрутизаторах. • Настройте RIP на всех маршрутизаторах. • Включите аутентификацию RIP на всех маршрутизаторах
A	A>enable A#configure terminal A(config)#key chain ripchain A(config-keychain)#key 1 A(config-keychain-key)#key-string Hello A(config-keychain-key)#accept-lifetime 16:30:00 Oct 1 2013 duration 43200 A(config-keychain-key)#send-lifetime 16:30:00 Oct 1 2013 duration 43200 A(config-keychain-key)#exit A(config-keychain)#key 2 A(config-keychain-key)#key-string World A(config-keychain-key)#accept-lifetime 04:00:00 Oct 2 2013 infinite A(config-keychain-key)#send-lifetime 04:00:00 Oct 2 2013 infinite A(config-keychain-key)#exit A(config)#interface gigabitEthernet 0/1 A(config-if)#ip address 192.168.27.1 255.255.255.0 A(config-if)#ip rip authentication key-chain ripchain A(config-if)#ip rip authentication mode md5

	A(config-if)#exit A(config)#router rip A(config-router)#version 2 A(config-router)#network 192.168.27.0
B	B>enable B#configure terminal B(config)#key chain ripchain B(config-keychain)#key 1 B(config-keychain-key)#key-string Hello B(config-keychain-key)#accept-lifetime 16:30:00 Oct 1 2013 duration 43200 B(config-keychain-key)#send-lifetime 16:30:00 Oct 1 2013 duration 43200 B(config-keychain-key)#exit B(config-keychain)#key 2 B(config-keychain-key)#key-string World B(config-keychain-key)#accept-lifetime 04:00:00 Oct 2 2013 infinite B(config-keychain-key)#send-lifetime 04:00:00 Oct 2 2013 infinite B(config-keychain-key)#exit B(config)#interface gigabitEthernet 0/1 B(config-if)#ip address 192.168.27.2 255.255.255.0 B(config-if)#ip rip authentication key-chain ripchain B(config-if)#ip rip authentication mode md5 B(config-if)#exit B(config)#router rip B(config-router)#version 2 B(config-router)#network 192.168.27.0 B(config-router)#redistribute static
Проверка	Запустите команду **show ip route rip**, чтобы проверить, может ли маршрутизатор A получить маршрут RIP от маршрутизатора B
A	A(config)#show ip route rip R 172.168.0.0/16 [120/1] via 192.168.27.2, 00:05:16, GigabitEthernet 0/1

2.4.1.7. Распространенные ошибки

- Ключ неправильно связан с протоколом маршрутизации, из-за чего аутентификация не вступает в силу.

- Ключи, настроенные на нескольких маршрутизаторах, не согласованы, что приводит к сбою аутентификации.

2.5. Мониторинг

2.5.1. Отображение

Описание	Команда
Отображает конфигурации цепочки ключей	**show key chain** [*key-chain-name*]

3. НАСТРОЙКА RIP

3.1. Обзор

Routing Information Protocol (RIP) — это протокол unicast-маршрутизации, применяемый в сетях IPv4. Маршрутизаторы с поддержкой RIP обмениваются информацией о маршрутизации для получения маршрутов к удаленным сетям.

Как Interior Gateway Protocol (IGP), RIP может работать только внутри автономной системы (AS) и применим к сетям небольшого размера, самый длинный путь которых включает менее16 hop-ов.

3.1.1.1. Протоколы и стандарты

- RFC1058: определяет RIPv1.
- RFC2453: определяет RIPv2.

3.2. Приложения

Приложение	Описание
Базовое приложение RIP	Информация о маршрутизации автоматически обслуживается через RIP в сети небольшого размера
Взаимодействие между RIP и BGP	Несколько AS связаны между собой. RIP работает внутри каждой AS, а Border Gateway Protocol (BGP) работает между AS

3.2.1. Базовое приложение RIP

3.2.1.1. Сценарий

В сети с простой структурой вы можете настроить RIP для реализации сетевого взаимодействия. Настройка RIP проще, чем настройка других протоколов IGP, таких как Open Shortest Path First (OSPF). По сравнению со статическими маршрутами RIP может динамически адаптироваться к изменениям структуры сети и его легче обслуживать.

Как показано на Рисунке 3-1, чтобы реализовать взаимодействие между ПК1, ПК2 и ПК3, вы можете настроить маршруты RIP на R1, R2 и R3.

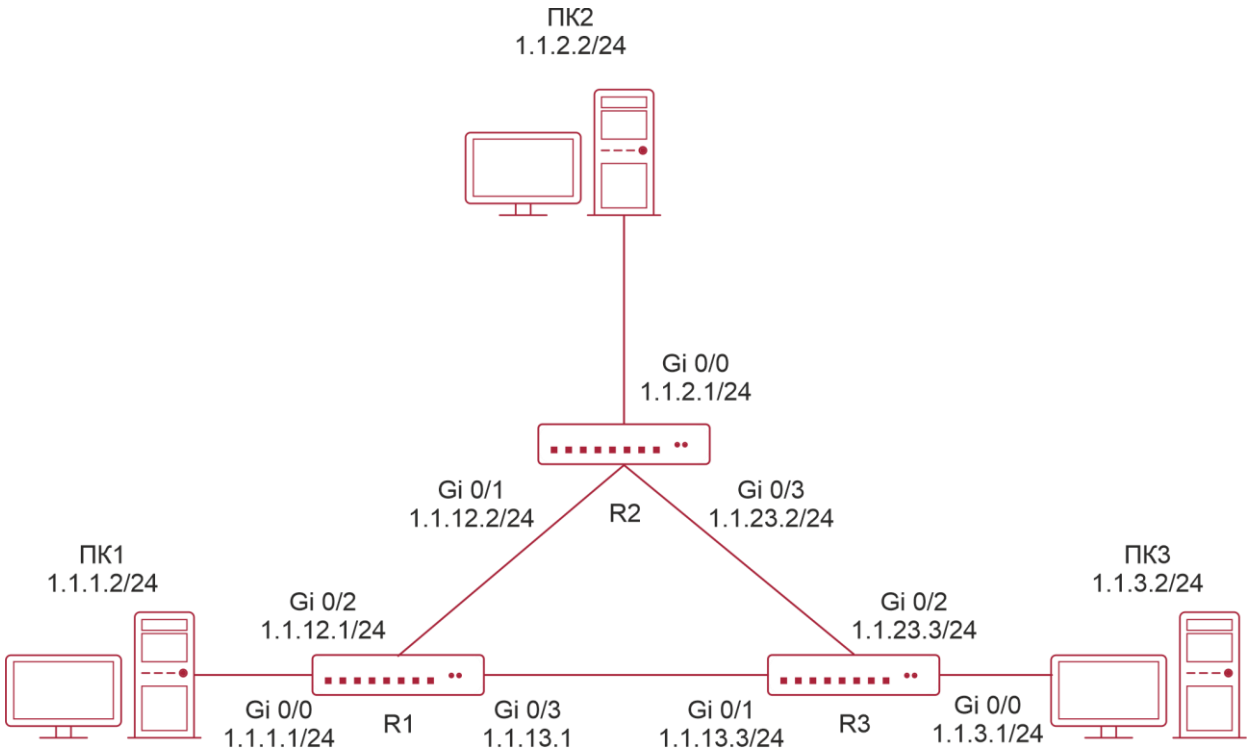


Рисунок 3-1.

3.2.1.2. Развертывание

- Настройте IP-адреса и шлюзы на трех ПК.
- Настройте IP-адреса и маски подсети на трех маршрутизаторах.
- Настройте RIP на трех маршрутизаторах.

3.2.2. Взаимодействие между RIP и BGP

3.2.2.1. Сценарий

Несколько AS связаны между собой. RIP работает внутри каждой AS, а BGP — между AS. Обычно RIP и BGP изучают информацию о маршрутизации друг у друга.

Как показано на Рисунке 3-2, unicast-маршрутизация реализована в AS 100 и AS 200 с помошью RIP, а между двумя AS — BGP.

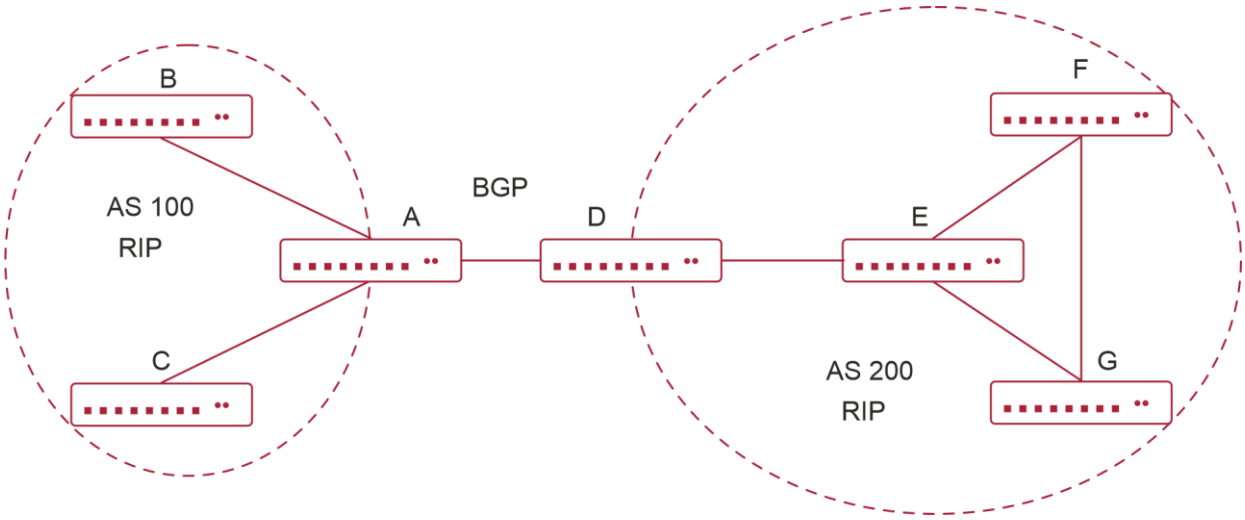


Рисунок 3-2. Взаимодействие между RIP и BGP

RIP и BGP работают одновременно на маршрутизаторах A и D.

3.2.2.2. Развертывание

- RIP работает в AS 100 и AS 200 для реализации unicast-маршрутизации.
- BGP работает между двумя AS для реализации unicast-маршрутизации.

3.3. Функции

3.3.1. Базовые определения

IGP и EGP

IGP работает внутри AS. Например, RIP — это тип IGP.

Exterior Gateway Protocol (EGP) работает между AS. Например, BGP — это тип EGP.

Classful Routing Protocol (протокол классовой маршрутизации) и Classless Routing Protocol (протокол бесклассовой маршрутизации)

Протоколы можно классифицировать по типу поддерживаемых маршрутов:

- Протокол классовой маршрутизации: поддерживает классовые маршруты. Например, RIPv1 — это классовый протокол маршрутизации.
- Протокол бесклассовой маршрутизации: поддерживает бесклассовые маршруты. Например, RIPv2 — это бесклассовый протокол маршрутизации.

3.3.1.1. Обзор

Особенность	Описание
RIPv1 и RIPv2	RIP доступны в двух вариантах: RIPv1 и RIPv2

Особенность	Описание
Обмен информацией о маршрутизации	Обмениваясь информацией о маршрутизации, устройства с включенным RIP могут автоматически получать маршруты к удаленной сети и обновлять маршруты в режиме реального времени
Алгоритм маршрутизации	RIP — это протокол, основанный на алгоритме вектора расстояния. Он использует метод сложения векторов для вычисления информации о маршрутизации
Как избежать петель маршрута	RIP использует функции, такие как split horizon и poison reverse, чтобы избежать петель маршрута
Меры безопасности	RIP использует функции, такие как аутентификация и проверка адреса источника, для обеспечения безопасности протокола
Меры надежности	RIP использует такие функции, как корреляция обнаружения двунаправленной пересылки (BFD), быстрое перенаправление и плавный перезапуск (GR), чтобы повысить надежность протокола
Несколько экземпляров	RIP поддерживает несколько экземпляров и VPN-приложения

3.3.2. RIPv1 и RIPv2

Доступны две версии RIP: RIPv1 и RIPv2.

3.3.2.1. Принцип работы

RIPv1

Пакеты RIPv1 передаются через broadcast. Broadcast-адрес — 255.255.255.255, а идентификатор порта UDP — 520. RIPv1 не может идентифицировать маску подсети и поддерживает только классовые маршруты.

RIPv2

Пакеты RIPv2 являются multicast. Адрес multicast-рассылки — 224.0.0.9, а идентификатор порта UDP — 520. RIPv2 может идентифицировать маску подсети и поддерживает бесклассовые маршруты, суммарный (summarized) маршрут и маршруты supernetting. RIPv2 поддерживает аутентификацию в виде обычного текста и аутентификацию message digest 5 (MD5).

3.3.2.2. Сопутствующая конфигурация

Включение процесса RIP

По умолчанию процесс RIP отключен.

Запустите команду **router rip**, чтобы включить процесс RIP.

Вы должны включить процесс RIP на устройстве; в противном случае все функции, связанные с RIP, не смогут действовать.

Запуск RIP на интерфейсе

По умолчанию RIP не запускается на интерфейсе.

Запустите команду **network**, чтобы определить диапазон адресов. RIP работает на интерфейсах, принадлежащих этому диапазону адресов.

После запуска RIP на интерфейсе можно обмениваться пакетами RIP на интерфейсе, и RIP может изучать маршруты к сегментам сети, напрямую подключенным к устройству.

Определение версии RIP

По умолчанию интерфейс получает пакеты RIPv1 и RIPv2 и отправляет пакеты RIPv1.

Запустите команду **version**, чтобы определить версию пакетов RIP, отправляемых или получаемых на всех интерфейсах.

Запустите команду **ip rip send version**, чтобы определить версию пакетов RIP, отправляемых на интерфейс.

Запустите команду **ip rip receive version**, чтобы определить версию пакетов RIP, получаемых на интерфейсе.

ПРИМЕЧАНИЕ: если версии RIP, работающие на соседних маршрутизаторах, различаются, маршрутизатор с поддержкой RIPv1 изучит неправильные маршруты.

Запрет интерфейса на отправку или получение пакетов

По умолчанию интерфейсу с поддержкой RIP разрешено отправлять и получать пакеты RIP.

Запустите команду **no ip rip receive enable**, чтобы запретить интерфейсу получать пакеты RIP.

Запустите команду **no ip rip send enable**, чтобы запретить интерфейсу отправлять пакеты RIP.

Запустите команду **passive-interface**, чтобы запретить интерфейсу отправлять broadcast- или multicast-пакеты RIP.

Настройка режима отправки RIP-пакетов

По умолчанию отправляются broadcast-пакеты RIPv1 и multicast-пакеты RIPv2.

Запустите команду **ip rip v2-broadcast** для отправки broadcast-пакетов RIPv2 на интерфейс.

Запустите команду **neighbor**, чтобы отправить unicast-пакеты RIP на указанный маршрутизатор соседа.

3.3.3. Обмен информацией о маршрутизации

По сравнению со статической маршрутизацией протокол динамической маршрутизации имеет существенное преимущество, то есть путем обмена информацией о маршрутизации устройства могут автоматически получать маршруты к удаленной сети и обновлять маршруты в режиме реального времени.

3.3.3.1. Принцип работы

Инициализация

После включения RIP на маршрутизаторе маршрутизатор отправляет пакет запроса своему соседнему маршрутизатору, запрашивая всю информацию о маршрутизации, то есть таблицу маршрутизации. После получения сообщения запроса соседний маршрутизатор возвращает ответный пакет, содержащий локальную таблицу маршрутизации. После получения ответного пакета маршрутизатор обновляет локальную таблицу маршрутизации и отправляет пакет обновления соседнему маршрутизатору, информируя соседний маршрутизатор об обновлении маршрута. После получения пакета обновления соседний маршрутизатор обновляет локальную таблицу маршрутизации и отправляет пакет обновления другим соседним маршрутизаторам. После серии обновлений все маршрутизаторы смогут получать и сохранять самую свежую информацию о маршрутизации.

Периодическое обновление

По умолчанию для RIP включено периодическое обновление. Соседние маршрутизаторы обмениваются друг с другом полной информацией о маршрутизации каждые 30 с (таймер обновления), то есть вся таблица маршрутизации отправляется соседним маршрутизаторам. Один пакет обновления содержит не более 25 маршрутов. Поэтому для отправки всей таблицы маршрутизации может потребоваться множество пакетов обновления. Вы можете установить задержку отправки между пакетами обновлений, чтобы избежать потери информации о маршрутизации.

ПРИМЕЧАНИЕ: если для каждого нелокального маршрута маршрут не обновляется в течение 180 с (таймер неработоспособности), метрика маршрута изменяется на 16 (недоступен). Если маршрут по-прежнему не обновляется в течение следующих 120 с (таймер очистки), маршрут удаляется из таблицы маршрутизации.

Триггерные обновления

После включения функции триггерных обновлений периодическое обновление автоматически отключается. При изменении информации о маршрутизации на маршрутизаторе маршрутизатор немедленно отправляет маршруты, связанные с изменением (вместо полной таблицы маршрутизации), соседнему маршрутизатору и использует механизмы подтверждения и повторной передачи, чтобы гарантировать успешное получение маршрутов соседним маршрутизатором. По сравнению с периодическим обновлением, триггерные обновления помогают уменьшить флудинг и ускоряют сходимость маршрутов.

События, которые могут инициировать обновление, включают запуск маршрутизатора, изменение состояния интерфейса, изменения информации о маршрутизации (например, метрики) и прием пакета запроса.

Суммирование маршрутов

При отправке информации о маршрутизации соседнему маршрутизатору маршрутизатор с поддержкой RIP суммирует маршруты подсети, принадлежащие одной и той же классовой сети, в маршрут и отправляет его соседнему маршрутизатору. Например, суммирует 80.1.1.0/24 (метрика=2) и 80.1.2.0/24 (метрика=3) в 80.0.0.0/8 (метрика=2) и установит метрику суммированного маршрута на оптимальную метрику.

Только RIPv2 поддерживает суммирование маршрутов. Суммирование маршрутов позволяет уменьшить размер таблицы маршрутизации и повысить эффективность обмена маршрутной информацией.

Маршрут supernetting

Если длина маски подсети маршрута меньше длины естественной маски, этот маршрут называется маршрутом supernetting. Например, в маршруте 80.0.0.0/6, поскольку 80.0.0.0 является сетевым адресом класса A, а естественная маска равна 8 битам, маршрут 80.0.0.0/6 является маршрутом supernetting.

Только RIPv2 поддерживает маршруты supernetting.

Маршрут по умолчанию

В таблице маршрутизации маршрут к сети назначения 0.0.0.0/0 называется маршрутом по умолчанию.

Маршрут по умолчанию можно изучить от соседнего маршрутизатора или отправить на соседний маршрутизатор.

Перераспределение маршрутов

Для RIP другие типы маршрутов (например, прямые маршруты, статические маршруты и маршруты других протоколов маршрутизации) называются внешними маршрутами.

Внешние маршруты (за исключением маршрута по умолчанию) можно перераспределить в RIP и объявить соседям.

Фильтрация маршрутов

Условия фильтрации можно настроить для ограничения информации о маршрутизации, которой обмениваются соседние маршрутизаторы. Отправлять или получать можно только ту информацию о маршрутизации, которая соответствует условиям фильтрации.

3.3.3.2. Сопутствующая конфигурация

Задержка отправки между пакетами обновлений

По умолчанию пакеты обновлений отправляются непрерывно, без каких-либо задержек.

Запустите команду **output-delay**, чтобы установить задержку отправки между пакетами обновлений.

RIP-таймеры

По умолчанию таймер обновления составляет 30 с, таймер неработоспособности — 180 с, а таймер очистки — 120 с.

Запустите команду **timers basic**, чтобы изменить продолжительность таймеров RIP.

Увеличение продолжительности таймера очистки может уменьшить flapping маршрута. Уменьшение продолжительности таймера очистки помогает ускорить сходимость маршрутов.

Длительность таймеров RIP должна быть одинаковой на соседних маршрутизаторах. Если не требуется иное, не рекомендуется изменять таймеры RIP.

Триггерные обновления

По умолчанию периодическое обновление включено.

Запустите команду **ip rip triggered**, чтобы включить триггерные обновления на интерфейсе и отключить периодическое обновление.

Запустите команду **ip rip triggered retransmit-timer**, чтобы изменить интервал повторной передачи пакетов обновлений. Значение по умолчанию — 5 с.

Запустите команду **ip rip triggered retransmit-count**, чтобы изменить максимальное количество повторных передач пакетов обновлений. Значение по умолчанию — 36.

Суммирование маршрутов

По умолчанию суммирование маршрутов включается автоматически, если интерфейсу разрешено отправлять пакеты RIPv2.

Запустите команду **no auto-summary**, чтобы отключить суммирование маршрутов.

Запустите команду **ip rip summary-address**, чтобы настроить суммирование маршрутов на интерфейсе.

Маршрут supernetting

По умолчанию маршруты supernetting могут быть отправлены, если интерфейсу разрешено отправлять пакеты RIPv2.

Запустите команду **no ip rip send supernet-routes**, чтобы предотвратить отправку маршрутов supernetting.

Маршрут по умолчанию

Запустите команду **ip rip default-information**, чтобы объявить маршрут по умолчанию соседям на интерфейсе.

Запустите команду **default-information originate**, чтобы объявить маршрут по умолчанию соседям со всех интерфейсов.

Перераспределение маршрутов

Запустите команду **redistribute**, чтобы перераспределить внешние маршруты (за исключением маршрута по умолчанию) в RIP и объявить их соседям.

Фильтрация маршрутов

Запустите команду **distribute-list out**, чтобы установить правила фильтрации для ограничения информации о маршрутизации, отправляемой устройством.

Запустите команду **distribute-list in**, чтобы установить правила фильтрации для ограничения информации о маршрутизации, получаемой устройством.

3.3.4. Алгоритм маршрутизации

RIP — это протокол, основанный на алгоритме вектора расстояния. Он использует метод сложения векторов для вычисления информации о маршрутизации.

3.3.4.1. Принцип работы

Алгоритм вектора расстояния

RIP — это протокол, основанный на алгоритме вектора расстояния. Алгоритм вектора расстояния рассматривает маршрут как вектор, состоящий из сети назначения и расстояния (метрики). Маршрутизатор получает маршрут от своего соседа и добавляет к маршруту вектор расстояния от себя до соседа, чтобы сформировать свой собственный маршрут.

RIP использует количество hop-ов для оценки расстояния (метрики) до сети назначения. По умолчанию количество hop-ов от маршрутизатора к сети, к которой он подключен напрямую, равно 0, количество hop-ов от маршрутизатора к сети, к которой можно получить доступ через маршрутизатор, равно 1 и так далее. То есть метрика равна количеству маршрутизаторов из локальной сети в сеть назначения. Чтобы ограничить время сходимости, RIP предусматривает, что метрика должна быть целым числом от 0 до 15. Если метрика равна или больше 16, сеть назначения или хост недоступны. По этой причине RIP не может применяться в крупномасштабной сети.

Как показано на Рисунке 3-3, Маршрутизатор A подключен к сети 10.0.0.0. Маршрутизатор B получает маршрут (10.0.0.0,0) от маршрутизатора A и добавляет к маршруту метрику 1, чтобы получить собственный маршрут ((10.0.0.0,1), а следующий hop указывает на Маршрутизатор A.

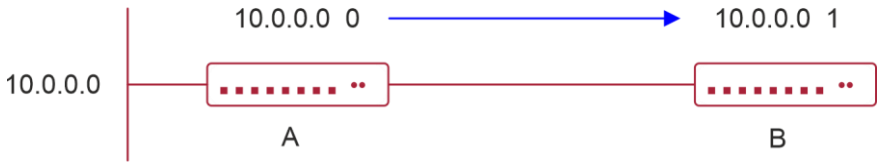


Рисунок 3-3.

Выбор оптимального маршрута

RIP выбирает оптимальный маршрут на основе следующего принципа: если доступно несколько маршрутов к одной и той же сети назначения, маршрутизатор предпочтительно выбирает маршрут с наименьшей метрикой.

Как показано на Рисунке 3-4, Маршрутизатор A подключен к сети 10.0.0.0. Маршрутизатор C получает маршрут (10.0.0.0,0) от маршрутизатора A и маршрут (10.0.0.0,1) от маршрутизатора B. Маршрутизатор C выберет маршрут, полученный от маршрутизатора A, и добавит метрику 1 к этому маршруту, чтобы сформировать собственный маршрут (10.0.0.0,1), а следующий hop указывает на Маршрутизатор A.

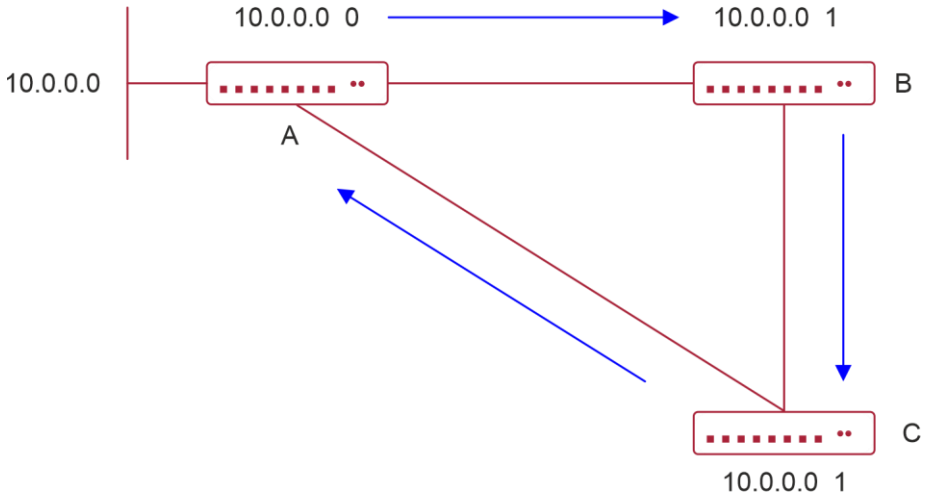


Рисунок 3-4.

ПРИМЕЧАНИЕ: когда на маршрутизаторе существуют маршруты, поступающие из разных источников, предпочтительно выбирается маршрут с наименьшим расстоянием.

Источник маршрута	Расстояние по умолчанию
Сеть с прямым подключением	0

Источник маршрута	Расстояние по умолчанию
Статический маршрут	1
Маршрут OSPF	110
Маршрут IS-IS	115
RIP-маршрут	120
Недоступный маршрут	255

3.3.4.2. Сопутствующая конфигурация

Изменение расстояния

По умолчанию расстояние маршрута RIP составляет 120.

Запустите команду **distance**, чтобы изменить расстояние маршрута RIP.

Изменение метрики

Для маршрута RIP, который заранее обнаруживается устройством, метрика по умолчанию равна количеству hop-ов из локальной сети в сеть назначения. Для маршрутизатора RIP, настроенного вручную (маршрут по умолчанию или перераспределенный маршрут), метрика по умолчанию равна 1.

Запустите команду **offset-list in**, чтобы увеличить метрику полученного маршрута RIP.

Запустите команду **offset-list out**, чтобы увеличить метрику отправленного маршрута RIP.

Запустите команду **default-metric**, чтобы изменить метрику по умолчанию перераспределенного маршрута.

Запустите команду **redistribute**, чтобы изменить метрику маршрута при его перераспределении.

Запустите команду **default-information originate**, чтобы изменить метрику маршрута по умолчанию, когда маршрут по умолчанию введен.

Запустите команду **ip rip default-information**, чтобы изменить метрику маршрута по умолчанию при создании маршрута по умолчанию.

3.3.5. Как избежать петель маршрута

RIP использует такие функции, как split horizon и poison reverse, чтобы избежать петель маршрута.

3.3.5.1. Принцип работы

Петля маршрута

Петля маршрута RIP возникает из-за дефектов, присущих алгоритму вектора расстояния.

Как показано на Рисунке 3-5, маршрутизатор A подключен к сети 10.0.0.0 и отправляет пакет обновления каждые 30 секунд. Маршрутизатор B получает маршрут 10.0.0.0 от маршрутизатора A каждые 30 секунд. Если маршрутизатор A отключен от 10.0.0.0,

маршрут к 10.0.0.0 будет удален из таблицы маршрутизации на маршрутизаторе A. В следующий раз пакет обновления, отправленный маршрутизатором A, больше не будет содержать этот маршрут. Поскольку маршрутизатор B не получает пакет обновления, относящийся к 10.0.0.0, маршрутизатор B определяет, что маршрут к 10.0.0.0 действителен в течение 180 с, и использует пакет обновления для отправки этого маршрута маршрутизатору A. Поскольку маршрут к 10.0.0.0 не существует на маршрутизаторе A, маршрут, полученный от маршрутизатора B, добавляется в таблицу маршрутизации. Маршрутизатор B определяет, что данные могут достичь адреса 10.0.0.0 через маршрутизатор A, а маршрутизатор A определяет, что данные могут достичь адреса 10.0.0.0 через маршрутизатор B. Таким образом формируется петля маршрута.

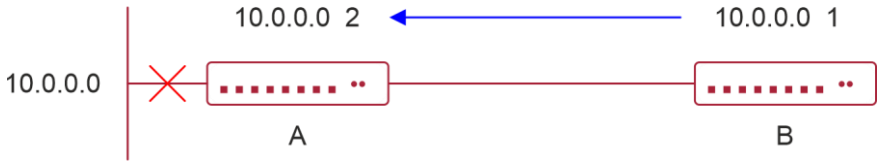


Рисунок 3-5.

Split Horizon

Split Horizon может предотвратить появление петель на маршруте. После включения Split Horizon на интерфейсе маршрут, полученный на этом интерфейсе, не будет отправляться с этого интерфейса.

Как показано на Рисунке 3-6, после того, как Split Horizon включен на интерфейсе между маршрутизаторами A и маршрутизатором B, маршрутизатор B не будет отправлять маршрут 10.0.0.0 обратно маршрутизатору A. Маршрутизатор B узнает через 180 секунд, что 10.0.0.0 недоступен.

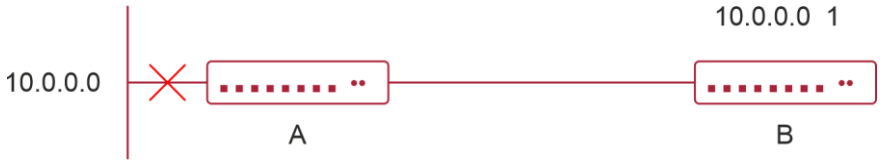


Рисунок 3-6.

Poison Reverse

Poison Reverse также может предотвратить появление петель маршрута. По сравнению со Split Horizon,то Poison Reverse более надежен, но переносит больше пакетов протокола, что делает перегрузку сети более серьезной.

После включения Poison Reverse на интерфейсе маршрут, полученный от этого интерфейса, будет снова отправлен с этого интерфейса, но метрика этого маршрутизатора будет изменена на 16 (недоступен).

Как показано на Рисунке 3-7, после изучения маршрута 10.0.0.0 от маршрутизатора A, маршрутизатор B устанавливает метрику этого маршрута равным 16 и отправляет маршрут обратно маршрутизатору A. После того, как этот маршрут становится недействительным, маршрутизатор B объявляет маршрут 10.0.0.0 (метрика = 16). к

маршрутизатору A, чтобы ускорить процесс удаления маршрута из таблицы маршрутизации.

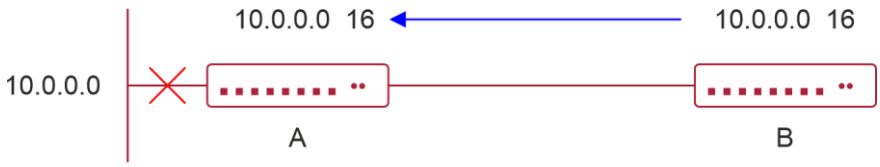


Рисунок 3-7.

3.3.5.2. Сопутствующая конфигурация

Split Horizon

По умолчанию Split Horizon включен.

Запустите команду **no ip rip split-horizon**, чтобы отключить Split Horizon.

Poison Reverse

По умолчанию Poison Reverse отключено.

Запустите команду **ip rip split-horizon poisoned-reverse**, чтобы включить Poison Reverse. (После включения Poison Reverse автоматически отключается Split Horizon.)

3.3.6. Меры безопасности

RIP использует такие функции, как аутентификация и проверка адреса источника, для обеспечения безопасности протокола.

3.3.6.1. Принцип работы

Аутентификация

RIPv2 поддерживает аутентификацию, а RIPv1 — нет.

После включения аутентификации на интерфейсе соседние устройства не могут обмениваться информацией о маршрутизации между собой, если аутентификация не удалась. Функция аутентификации используется для предотвращения доступа неавторизованных устройств к домену маршрутизации RIP.

RIPv2 поддерживает аутентификацию в виде обычного текста и аутентификацию MD5.

Проверка адреса источника

Когда устройство с поддержкой RIP получает пакет обновления, оно проверяет, находятся ли IP-адрес источника в пакете и IP-адрес входящего интерфейса в одном сегменте сети. В противном случае устройство отбрасывает пакет. Проверка адреса источника используется для обеспечения обмена информацией о маршрутизации RIP только между соседними устройствами маршрутизации.

ПРИМЕЧАНИЕ: на ненумерованном IP-интерфейсе, проверка адреса источника не выполняется (не настраивается).

ПРИМЕЧАНИЕ: если функция триггерных обновлений включена, проверка адреса источника включается автоматически (не настраивается).

ПРИМЕЧАНИЕ: если Split Horizon отключен, проверка адреса источника включается автоматически (не настраивается).

3.3.6.2. Сопутствующая конфигурация

Аутентификация

По умолчанию аутентификация отключена.

Запустите команду **ip rip authentication mode text**, чтобы включить аутентификацию в виде обычного текста на интерфейсе.

Запустите команду **ip rip authentication mode md5**, чтобы включить аутентификацию MD5 на интерфейсе.

Запустите команду **ip rip authentication text-password**, чтобы установить пароль для аутентификации в виде обычного текста на интерфейсе.

Запустите команду **ip rip authentication key-chain**, чтобы ссылаться на ключ в настроенной цепочке ключей как на ключ аутентификации на интерфейсе.

Проверка адреса источника

По умолчанию проверка адреса источника включена.

Запустите команду **no validate-update-source**, чтобы отключить проверку адреса источника.

3.3.7. Меры надежности

RIP использует такие функции, как корреляция BFD, быстрое перенаправление и GR, для повышения надежности протокола.

3.3.7.1. Принцип работы

Корреляция BFD и быстрое перенаправление

Если канал или устройство в сети неисправны, пакеты, передаваемые по этому маршруту, будут потеряны до тех пор, пока маршрут снова не будет конвергирован.

Как показано на Рисунке 3-8, после того как соединение (канал) между маршрутизатором A и маршрутизатором S неисправно, маршрутизатор B может подождать 180 секунд, прежде чем сможет обнаружить сбой маршрута (сеть назначения: 10.0.0.0; следующий hop: маршрутизатор A). Позже маршрутизатору B может потребоваться подождать 30 секунд, чтобы повторно получить маршрут (сеть назначения: 10.0.0.0; следующий hop: маршрутизатор C) от маршрутизатора C. Поэтому трафик прерывается на 210 секунд.

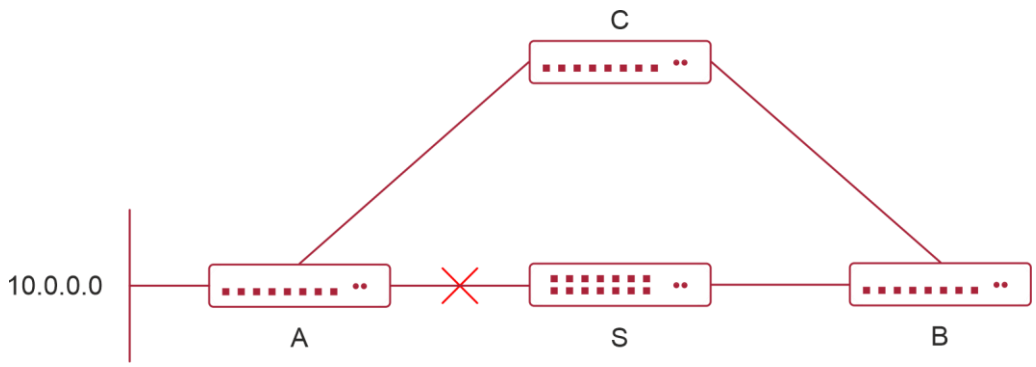


Рисунок 3-8.

Быстрое обнаружение сбоя маршрута или быстрое переключение на резервный маршрут помогают сократить время перерыва трафика.

- Сеанс BFD может быть установлен между маршрутизаторами A и маршрутизатором B и коррелирован с RIP. BFD может быстро проверить соединение между соседними маршрутизаторами. Если канал неисправен, RIP может обнаружить сбой маршрута в течение 1 секунды.
- Можно включить функцию быстрого перенаправления. Резервный маршрут (сеть назначения: 10.0.0.0; следующий hop: маршрутизатор C) можно настроить на маршрутизаторе B заранее. Как только RIP обнаруживает сбой маршрута, резервный маршрут немедленно включается.
- GR

GR обеспечивает бесперебойную передачу данных при перезапуске протокола. Если RIP перезапускается на устройстве с поддержкой GR, таблица пересылки до перезапуска будет сохранена, и пакет запроса будет отправлен соседу, чтобы можно было снова изучить маршрут. В течение периода GR RIP завершает повторную конвергенцию маршрута. По истечении периода GR RIP обновляет запись пересылки и объявляет таблицу маршрутизации соседу.

3.3.7.2. Сопутствующая конфигурация

Корреляция BFD

По умолчанию RIP не коррелирует с BFD.

Запустите команду **bfd all-interfaces**, чтобы настроить корреляцию между RIP и BFD. Эта конфигурация действует на всех интерфейсах.

Запустите команду **ip rip bfd**, чтобы настроить корреляцию между RIP и BFD на текущем интерфейсе.

Быстрое перенаправление

По умолчанию быстрое перенаправление отключено.

Запустите команду **fast-reroute route-map**, чтобы включить быстрое перенаправление и обратиться к карте маршрутов.

Запустите команду **set fast-reroute backup-interface backup-nexthop** для настройки резервного маршрута в карте маршрутов.

3.3.8. Несколько экземпляров

3.3.8.1. Принцип работы

На устройстве может существовать несколько экземпляров VPN.

RIP поддерживает несколько экземпляров. Вы можете включить процесс RIP в режиме семейства адресов VPN-маршрутизации и пересылки (VRF), чтобы запускать RIP на экземплярах VPN. Одно семейство адресов VRF сопоставлено с одним экземпляром VPN.

Экземпляры VPN невозможно отличить друг от друга при выполнении операций RIP с использованием SNMP. Прежде чем операции SNMP начнут действовать на экземпляре VPN, необходимо связать базу управляющей информации (MIB) RIP с экземпляром VPN.

3.3.8.2. Сопутствующая конфигурация

Семейство адресов VRF

По умолчанию процесс RIP запускается в экземпляре общедоступной (публичной) сети.

Запустите команду **address-family**, чтобы создать семейство адресов VRF и войти в режим семейства адресов VRF.

Запустите команду **exit-address-family**, чтобы выйти из режима семейства адресов VRF.

Запустите команду **no address-family**, чтобы удалить семейство адресов VRF.

Привязка MIB

По умолчанию RIP MIB привязан к экземпляру общедоступной (публичной) сети.

Запустите команду **enable mib-binding**, чтобы связать MIB RIP с экземпляром VPN.

3.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций RIP	(Обязательный) Используется для создания домена маршрутизации RIP	
	router rip	Включает процесс маршрутизации RIP и переходит в режим настройки процесса маршрутизации
	network	Запускает RIP на интерфейсах в указанном диапазоне адресов
	version	Определяет версию RIP
	ip rip split-horizon	Включает Split Horizon или Poison Reverse на интерфейсе
	passive-interface	Настраивает пассивный интерфейс
Управление взаимодействием пакетов RIP	(Необязательный) Эта конфигурация необходима, если вы хотите изменить механизм по умолчанию для отправки или получения пакетов RIP	
	neighbor	Отправляет unicast-пакеты RIP указанному соседу
	ip rip v2-broadcast	Отправляет broadcast-пакеты RIPv2 на интерфейс
	ip rip receive enable	Позволяет интерфейсу получать пакеты RIP

Конфигурация	Описание и команда	
	ip rip send enable	Позволяет интерфейсу отправлять пакеты RIP
	ip rip send version	Определяет версию пакетов RIP, отправляемых на интерфейс
	ip rip receive version	Определяет версию пакетов RIP, полученных на интерфейсе
Включение триггерных обновлений	Опционально	
	ip rip triggered	Включает триггерные обновления на интерфейсе
Включение проверки адреса источника	Опционально	
	validate-update-source	Включает проверку адреса источника
Включение аутентификации	(Опционально) Только RIPv2 поддерживает аутентификацию	
	ip rip authentication mode	Включает аутентификацию и устанавливает режим аутентификации на интерфейсе
	ip rip authentication text-password	Настраивает пароль для аутентификации в виде обычного текста на интерфейсе
Включение аутентификации	**ip rip authentication key-chain**	Настраивает цепочку ключей аутентификации на интерфейсе
Включение суммирования маршрутов	(Опционально) Только RIPv2 поддерживает суммирование маршрутов	
	auto-summary	Включает автоматическое суммирование маршрутов RIP
	ip rip summary-address	Настраивает суммирование маршрутов на интерфейсе

Конфигурация	Описание и команда	
Включение маршрутов Supernetting	(Опционально) Только RIPv2 поддерживает маршруты supernetting	
	ip rip send supernet-routes	Включает объявление маршрутов supernetting RIP на интерфейсе
Объявление маршрута по умолчанию или внешних маршрутов	Опционально	
	ip rip default-information	Объявляет маршрут по умолчанию соседям на интерфейсе
	default-information originate	Объявляет маршрут по умолчанию соседям
	redistribute	Перераспределяет маршруты и объявляет внешние маршруты соседям
Настройка правил фильтрации маршрутов	Опционально	
	distribute-list in	Фильтрует полученную информацию о маршрутизации RIP
	distribute-list out	Фильтрует отправленную информацию о маршрутизации RIP
Изменение параметров выбора маршрута	Опционально	
	distance	Изменяет административное расстояние (AD) маршрута RIP
	offset-list	Увеличивает метрику полученного или отправленного маршрута RIP
	default-metric	Настраивает метрику по умолчанию для внешнего маршрута, перераспределенного в RIP

Конфигурация	Описание и команда	
Изменение таймеров	Опционально	
	timers basic	Изменяет таймер обновления, таймер неработоспособности и таймер очистки
	output-delay	Устанавливает задержку отправки между пакетами обновления маршрута RIP
Включение корреляции BFD	Опционально	
	bfd all-interfaces	Сопоставляет RIP с BFD на всех интерфейсах
	ip rip bfd	Сопоставляет RIP с BFD на интерфейсе
Включение быстрого перенаправления	Опционально	
	fast-reroute route-map	Включает быстрое перенаправление маршрута и ссылается на карту маршрута
	set fast-reroute backup-interface backup-nexthop	Настраивает резервный интерфейс и резервный следующий hop для быстрого перенаправления маршрута в карте маршрутов
Включение GR	Опционально	
	graceful-restart	Настраивает возможность перезапуска GR
Включение нескольких экземпляров	(Опционально) Используется для запуска RIP на экземплярах VPN	
	address-family ipv4 vrf	Создает семейство адресов VRF и переходит в режим семейства адресов VRF IPv4

Конфигурация	Описание и команда	
	exit-address-family	Выход из семейства адресов VRF IPv4
	enable mib-binding	Связывает RIP MIB с экземпляром VPN

3.4.1. Настройка основных функций RIP

3.4.1.1. Эффект конфигурации

- Создайте в сети домен маршрутизации RIP.
- Маршрутизаторы в домене получают маршруты к удаленной сети через RIP.

3.4.1.2. Примечания

- IPv4-адреса должны быть настроены.
- Должны быть включены unicast-маршруты IPv4.

3.4.1.3. Шаги настройки

Включение процесса маршрутизации RIP

- Обязательный.
- Если не требуется иное, эту настройку необходимо выполнить на каждом маршрутизаторе в домене маршрутизации RIP.

Связь с локальной сетью

- Обязательный.
- Если не требуется иное, эту настройку необходимо выполнить на каждом маршрутизаторе в домене маршрутизации RIP.
- Если не требуется иное, локальная сеть, связанная с RIP, должна охватывать сетевые сегменты всех интерфейсов L3.

Определение версии RIP

- Если требуются функции RIPv2 (например, маска подсети переменной длины и аутентификация), включите RIPv2.
- Если не требуется иное, вы должны определить одну и ту же версию RIP на каждом маршрутизаторе.

Включение Split Horizon или Poison Reverse

- По умолчанию Split Horizon включен, а Poison Reverse отключен.
- Если не требуется иное, включите Split Horizon на каждом интерфейсе, подключенном к broadcast-сети, например Ethernet. (Сохраните настройки по умолчанию.)
- Если не требуется иное, включите Split Horizon на каждом интерфейсе, подключенном к сети «точка-точка» (P2P), например PPP и HDLC. (Сохраните настройки по умолчанию.)

- Рекомендуется отключить Split Horizon и Poison Reverse на интерфейсе, подключенном к сети non-broadcast multi-access (NBMA), например FR и X.25; в противном случае некоторые устройства могут не получить полную информацию о маршрутизации.
- Если дополнительный IP-адрес настроен для интерфейса, подключенного к non-broadcast-интерфейсу, рекомендуется отключить Split Horizon и Poison Reverse.

Настройка пассивного интерфейса

- Если вы хотите подавить пакеты обновления на интерфейсе RIP, настройте этот интерфейс как пассивный.
- Используйте пассивный интерфейс, чтобы установить границу домена маршрутизации RIP. Сетевой сегмент пассивного интерфейса принадлежит домену маршрутизации RIP, но пакеты RIP не могут отправляться через пассивный интерфейс.
- Если необходимо обмениваться маршрутами RIP на интерфейсе (например, интерфейсе межсоединения маршрутизатора) в домене маршрутизации RIP, этот интерфейс нельзя настроить как пассивный интерфейс.

3.4.1.4. Проверка

Проверьте таблицу маршрутизации маршрутизатора, чтобы убедиться, что маршрут к удаленной сети можно получить через RIP.

3.4.1.5. Связанные команды

Включение процесса маршрутизации RIP

Синтаксис команды	**router rip**
Командный режим	Режим глобальной конфигурации
Использование конфигурации	Эта команда используется для создания процесса маршрутизации RIP и входа в режим настройки процесса маршрутизации

Связь с локальной сетью

Синтаксис команды	**network** *network-number* [*wildcard*]
Описание параметра	*network-number*: указывает номер сети. *wildcard*: определяет бит сравнения IP-адресов. **0** указывает на точное совпадение, а **1** указывает на то, что сравнение не выполняется
Командный режим	Режим настройки процесса маршрутизации

Использование конфигурации	RIP может работать и изучать прямые маршруты, а обмен пакетами RIP может осуществляться только на интерфейсе, покрытом сетью (**network**). Если настроена **network** 0.0.0.0 255.255.255.255, покрываются все интерфейсы. Если *wildcard* не настроен, по умолчанию используется классовый диапазон адресов, то есть интерфейсы, адреса которых попадают в классовый диапазон адресов, участвуют в операциях RIP

Определение версии RIP

Синтаксис команды	**version** { **1** | **2** }
Описание параметра	**1**: указывает RIPv1. **2**: указывает RIPv2
Командный режим	Режим глобальной конфигурации
Использование конфигурации	Эта команда действует на весь маршрутизатор. Вы можете запустить эту команду, чтобы определить версию пакетов RIP, отправляемых или получаемых на всех интерфейсах

Включение Split Horizon

Синтаксис команды	**ip rip split-horizon** [**poisoned-reverse**]
Описание параметра	**poisoned-reverse**: указывает на Poison Reverse
Командный режим	Режим настройки интерфейса
Использование конфигурации	Split Horizon автоматически отключается после включения Poison Reverse

Настройка пассивного интерфейса

Синтаксис команды	**passive-interface** { **default** | *interface-type interface-num* }
Описание параметра	**default**: указывает все интерфейсы. *interface-type interface-num*: указывает интерфейс

Командный режим	Режим настройки процесса маршрутизации
Использование конфигурации	Сначала запустите команду **passive-interface default**, чтобы настроить все интерфейсы как пассивные. Затем запустите команду **no passive-interface** *interface-type interface-num*, чтобы отменить интерфейсы, используемые для соединения между маршрутизаторами в домене

3.4.1.6. Пример конфигурации

Создание домена маршрутизации RIP

Сценарий:

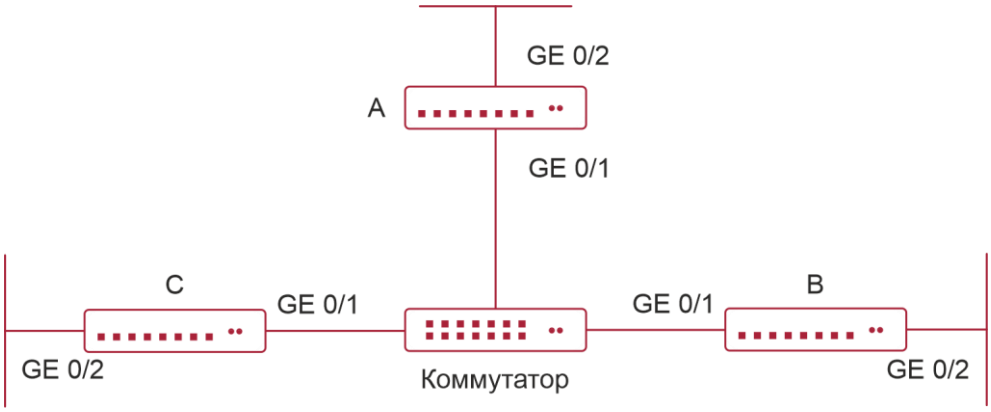


Рисунок 3-9.

IP-адреса интерфейса следующие:

A: GE0/1 110.11.2.1/24 GE0/2 155.10.1.1/24

B: GE0/1 110.11.2.2/24 GE0/2 196.38.165.1/24

C: GE0/1 110.11.2.3/24 GE0/2 117.102.0.1/16

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. • Настройте базовые функции RIP на всех маршрутизаторах
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 110.11.2.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# exit A(config)# interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)# ip address 155.10.1.1 255.255.255.0

	A(config)# router rip A(config-router)# version 2 A(config-router)# network 0.0.0.0 255.255.255.255 A(config-router)# passive-interface default A(config-router)# no passive-interface GigabitEthernet 0/1
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip address 110.11.2.2 255.255.255.0 B(config-if-GigabitEthernet 0/1)# exit B(config)# interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)# ip address 196.38.165.1 255.255.255.0 B(config-if-GigabitEthernet 0/2)# exit B(config)# router rip B(config-router)# version 2 B(config-router)# network 0.0.0.0 255.255.255.255 B(config-router)# passive-interface default B(config-router)# no passive-interface GigabitEthernet 0/1
C	C# configure terminal C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ip address 110.11.2.3 255.255.255.0 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface GigabitEthernet 0/2 C(config-if-GigabitEthernet 0/2)# ip address 117.102.0.1 255.255.0.0 C(config-if-GigabitEthernet 0/2)# exit C(config)# router rip C(config-router)# version 2 C(config-router)#no auto-summary C(config-router)# network 0.0.0.0 255.255.255.255 C(config-router)# passive-interface default C(config-router)# no passive-interface GigabitEthernet 0/1
Проверка	Проверьте таблицы маршрутизации на маршрутизаторе A, маршрутизаторе B и маршрутизаторе C. Убедитесь, что RIP изучает маршруты к удаленным сетям

A	A# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 110.11.2.0/24 is directly connected, GigabitEthernet 0/1 C 110.11.2.1/32 is local host. R 117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1 C 155.10.1.0/24 is directly connected, GigabitEthernet 0/2 C 155.10.1.1/32 is local host. C 192.168.217.0/24 is directly connected, VLAN 1 C 192.168.217.233/32 is local host. R 196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
B	B# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 110.11.2.0/24 is directly connected, GigabitEthernet 0/1 C 110.11.2.2/32 is local host. R 155.10.0.0/16 [120/1] via 110.11.2.1, 00:15:21, GigabitEthernet 0/1 C 196.38.165.0/24 is directly connected, GigabitEthernet 0/2 C 196.38.165.1/32 is local host. R 117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1

C	C# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 110.11.2.0/24 is directly connected, GigabitEthernet 0/1 C 110.11.2.3/32 is local host. C 117.102.0.0/16 is directly connected, GigabitEthernet 0/2 C 117.102.0.1/32 is local host. R 155.10.0.0/16 [120/1] via 110.11.2.1, 00:20:55, GigabitEthernet 0/1 R 196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1

3.4.1.7. Распространенные ошибки

- Адрес IPv4 не настроен на интерфейсе.
- Версия RIP не определена на устройстве, или версия RIP на устройстве отличается от версии на других маршрутизаторах.
- Диапазон адресов, настроенный командой **network**, не охватывает конкретный интерфейс.
- Параметр *wildcard* в команде **network** настроен неправильно. **0** указывает на точное совпадение, а **1** указывает на то, что сравнение не выполняется.
- Интерфейс, используемый для соединения между устройствами, настроен как пассивный интерфейс.

3.4.2. Управление взаимодействием пакетов RIP

3.4.2.1. Эффект конфигурации

Измените механизм запуска RIP по умолчанию посредством конфигурации и вручную управляйте режимом взаимодействия пакетов RIP, включая:

- Разрешение или запрет отправки unicast-пакетов RIP указанному соседу на интерфейсе.
- Разрешение или запрет отправки unicast-пакетов RIPv2 вместо broadcast-пакетов указанному соседу на интерфейсе.
- Разрешение или запрет приема пакетов RIP на интерфейсе.
- Разрешение или запрет отправки пакетов RIP на интерфейсе.
- Разрешение или запрет приема RIP-пакетов указанной версии на интерфейсе.

- Разрешение или запрет отправки пакетов RIP указанной версии на интерфейсе.

3.4.2.2. Примечания

- Необходимо настроить основные функции RIP.
- На интерфейсе, подключающемся к соседнему устройству, настроенная версия отправляемых пакетов RIP должна совпадать с версией полученных пакетов RIP.

3.4.2.3. Шаги настройки

Отправка unicast-пакетов обновления маршрута RIP указанному соседу

- Настройте эту функцию, если вы хотите, чтобы только некоторые устройства, подключенные к интерфейсу, могли получать обновленную информацию о маршрутизации.
- По умолчанию RIPv1 использует broadcast IP-адрес (255.255.255.255) для объявления информации о маршрутизации, тогда как RIPv2 использует multicast-адрес (224.0.0.9) для объявления информации о маршрутизации. Если вы не хотите, чтобы все устройства в broadcast-сети или сети NBMA получали информацию о маршрутизации, настройте соответствующий интерфейс как пассивный интерфейс и укажите соседей, которые могут получать информацию о маршрутизации. Эта команда не влияет на получение пакетов RIP. Пакеты RIPv2 передаются по интерфейсу.
- Если не требуется иное, эта функция должна быть включена на маршрутизаторе, который отправляет unicast-пакеты обновления.

Broadcast-рассылка пакетов RIPv2 на интерфейсе

- Эту функцию необходимо настроить, если соседний маршрутизатор не поддерживает прием multicast-пакетов RIPv2.
- Если не требуется иное, эту функцию необходимо настроить на каждом интерфейсе маршрутизатора, передающем пакеты RIPv2.

Разрешение интерфейсу получать пакеты RIP

- Эта функция включена по умолчанию и должна быть отключена, если интерфейсу не разрешено получать пакеты RIP.
- Если не требуется иное, эту функцию необходимо настроить на каждом интерфейсе маршрутизатора, которому не разрешено принимать пакеты RIP.

Разрешение интерфейсу отправлять пакеты RIP

- Эта функция включена по умолчанию и должна быть отключена, если интерфейсу не разрешено отправлять пакеты RIP.
- Если не требуется иное, эту функцию необходимо настроить на каждом интерфейсе маршрутизатора, которому не разрешено отправлять пакеты RIP.

Разрешение интерфейсу отправлять пакеты RIP указанной версии

- Эту функцию необходимо настроить, если версия пакетов RIP, которые могут быть отправлены на интерфейсе, должна отличаться от глобальной конфигурации.
- Если не требуется иное, эту функцию необходимо настроить на каждом интерфейсе маршрутизатора, которому разрешено отправлять пакеты RIP указанной версии.

Разрешение интерфейсу получать пакеты RIP указанной версии

- Эту функцию необходимо настроить, если версия пакетов RIP, которые могут быть получены на интерфейсе, должна отличаться от глобальной конфигурации.
- Если не требуется иное, эту функцию необходимо настроить на каждом интерфейсе маршрутизатора, которому разрешено принимать пакеты RIP указанной версии.

3.4.2.4. Проверка

Запустите команду **debug ip rip packet**, чтобы проверить результат отправки и тип пакета.

3.4.2.5. Связанные команды

Отправка unicast-пакетов обновления маршрута RIP указанному соседу

Синтаксис команды	**neighbor** *ip-address*
Описание параметра	*ip-address*: указывает IP-адрес соседа. Это должен быть адрес сети, к которой напрямую подключено локальное устройство
Командный режим	Режим настройки процесса маршрутизации
Использование конфигурации	Как правило, вы можете сначала запустить команду **passive-interface** в режиме настройки процесса маршрутизации, чтобы настроить соответствующий интерфейс как пассивный, а затем указать соседей, которые могут получать информацию о маршрутизации. Эта команда не влияет на получение пакетов RIP. После того как интерфейс настроен как пассивный, он не отправляет пакеты запросов даже после перезапуска устройства

Broadcast-рассылка пакетов RIPv2 на интерфейсе

Синтаксис команды	**ip rip v2-broadcast**
Командный режим	Режим настройки интерфейса
Использование конфигурации	Поведение по умолчанию определяется настройкой команды **version**. Результат конфигурации этой команды может перезаписать конфигурацию по умолчанию команды **version**. Эта команда влияет на поведение отправки пакетов RIP на текущем интерфейсе, и этому интерфейсу разрешено отправлять пакеты RIPv1 и RIPv2 одновременно. Если эта команда не содержит каких-либо параметров, поведение приема пакетов RIP определяется конфигурацией команды **version**

Разрешение интерфейсу получать пакеты RIP

Синтаксис команды	**ip rip receive enable**
Командный режим	Режим настройки интерфейса
Использование конфигурации	Чтобы запрещать получении RIP-пакетов на интерфейсе используйте форму **no** этой команды. Эта команда действует только на текущий интерфейс. Вы можете использовать форму команды **default**, чтобы восстановить настройки по умолчанию, то есть разрешить интерфейсу получать пакеты RIP

Разрешение интерфейсу отправлять пакеты RIP

Синтаксис команды	**ip rip send enable**
Командный режим	Режим настройки интерфейса
Использование конфигурации	Чтобы запретить отправку пакетов RIP на интерфейс, используйте форму **no** этой команды в режиме настройки интерфейса. Эта команда действует только на текущий интерфейс. Вы можете использовать форму команды **default**, чтобы восстановить настройки по умолчанию, то есть разрешить интерфейсу отправлять пакеты RIP

Разрешение интерфейсу отправлять пакеты RIP указанной версии

Синтаксис команды	**ip rip send version** [**1**] [**2**]
Описание параметра	**1**: указывает, что отправляются только пакеты RIPv1. **2**: указывает, что отправляются только пакеты RIPv2
Командный режим	Режим настройки интерфейса
Использование конфигурации	Поведение по умолчанию определяется настройкой команды **version**. Результат конфигурации этой команды может перезаписать конфигурацию по умолчанию команды **version**. Эта команда влияет на поведение отправки пакетов RIP на текущем интерфейсе, и этому интерфейсу разрешено отправлять пакеты RIPv1 и RIPv2 одновременно. Если эта команда не содержит каких-либо параметров, поведение приема пакетов RIP определяется конфигурацией команды **version**

Разрешение интерфейсу получать пакеты RIP указанной версии

Синтаксис команды	**ip rip receive version** [**1**] [**2**]
Описание параметра	**1**: указывает, что принимаются только пакеты RIPv1. **2**: указывает, что принимаются только пакеты RIPv2
Командный режим	Режим настройки интерфейса
Использование конфигурации	Поведение по умолчанию определяется настройкой команды **version**. Результат конфигурации этой команды может перезаписать конфигурацию по умолчанию команды **version**. Эта команда влияет на поведение получения пакетов RIP на текущем интерфейсе, и интерфейсу разрешено получать пакеты RIPv1 и RIPv2 одновременно. Если эта команда не содержит каких-либо параметров, поведение приема пакетов RIP определяется конфигурацией команды **version**

3.4.2.6. Пример конфигурации

Запрет интерфейса на отправку пакетов RIP

Сценарий:

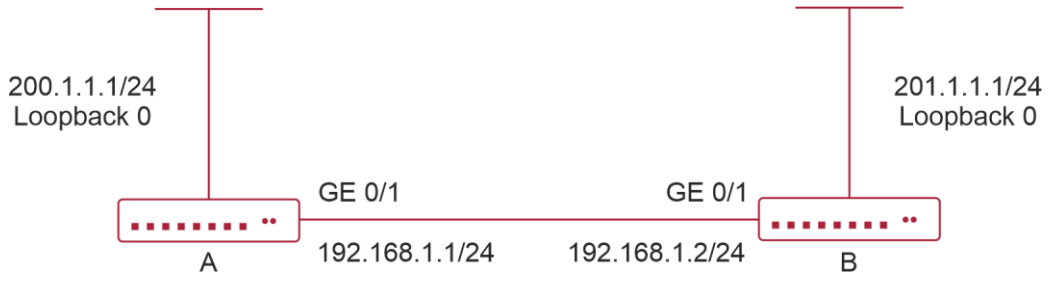


Рисунок 3-10.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • Запретить отправку пакетов RIP на интерфейсе маршрутизатора A
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# no ip rip send enable

Проверка	Запустите команду **debug ip rip packet send** на маршрутизаторе A и убедитесь, что пакеты не могут быть отправлены
A	A# debug ip rip packet recv *Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Prepare to send BROADCAST response... *Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Building update entries on GigabitEthernet 0/1 *Nov 4 08:19:31: %RIP-7-DEBUG: 117.0.0.0/8 via 0.0.0.0 metric 1 tag 0 *Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Interface GigabitEthernet 0/1 is disabled to send RIP packet!

3.4.2.7. Распространенные ошибки

Возникает ошибка совместимости, поскольку версия RIP, настроенная на соседнем устройстве, отличается от версии, настроенной на локальном устройстве.

3.4.3. Включение триггерных обновлений

3.4.3.1. Эффект конфигурации

Включите функцию обновлений, запускаемых RIP, после чего RIP не будет периодически отправлять пакеты обновления маршрута.

3.4.3.2. Примечания

- Необходимо настроить основные функции RIP.
- Рекомендуется включить Split Horizon с Poisoned Reverse; в противном случае может существовать неверная информация о маршрутизации.
- Эту функцию нельзя включить вместе с функцией корреляции RIP с BFD.
- Убедитесь, что функция триггерных обновлений включена на каждом маршрутизаторе в одном канале; в противном случае обмен информацией о маршрутизации невозможен должным образом.

3.4.3.3. Шаги настройки

Включение триггерных обновлений

- Эту функцию необходимо включить, если на интерфейсе WAN настроены demand circuits.
- Функцию триггерного обновления можно включить в любом из следующих случаев: (1) у интерфейса есть только один сосед; (2) интерфейс имеет несколько соседей, но устройство взаимодействует с этими соседями в unicast-режиме.
- Рекомендуется включить триггерные обновления на интерфейсе WAN (работающем по протоколу канала передачи данных PPP, Frame Relay или X.25) для удовлетворения требований demand circuits.
- Если на интерфейсе включена функция триггерных обновлений, проверка адреса источника выполняется независимо от того, включена ли функция проверки адреса источника командой **validate-update-source**.

- Если не требуется иное, запускаемые обновления должны быть включены на demand circuits на каждом маршрутизаторе.

3.4.3.4. Проверка

Если функция обновлений, запускаемых RIP, включена, RIP не может периодически отправлять пакеты обновления маршрута. RIP отправляет пакеты обновления маршрута на интерфейс WAN только в одном из следующих случаев:

- Получен пакет запроса маршрута.
- Информация о маршрутизации RIP изменяется.
- Состояние интерфейса изменяется.
- Маршрутизатор запущен.

3.4.3.5. Связанные команды

Включение триггерных обновлений

Синтаксис команды	**ip rip triggered** { **retransmit-timer** *timer* | **retransmit-count** *count* }
Описание параметра	**retransmit-timer** *timer*: настраивает интервал повторной передачи запроса на обновление или пакета ответа на обновление. Значение по умолчанию — 5 с. Значение варьируется от 1 до 3600. **retransmit-count** *count*: настраивает максимальное количество повторных передач пакета запроса на обновление или пакета ответа на обновление. Значение по умолчанию — 36. Значение находится в диапазоне от 1 до 3600
Командный режим	Режим настройки интерфейса
Использование конфигурации	Можно запустить команду **ip rip triggered**, чтобы включить триггерную функцию RIP. Когда эта функция включена, функция периодического обновления RIP автоматически отключается. Поэтому необходимо использовать механизмы подтверждения и повторной передачи, чтобы гарантировать успешную отправку или получение пакетов обновления в глобальной сети. Вы можете использовать параметры **retransmit-timer** и **retransmit-count**, чтобы указать интервал повторной передачи и максимальное количество повторных передач пакетов запроса и обновления

3.4.3.6. Пример конфигурации

Включение триггерных обновлений

Сценарий:

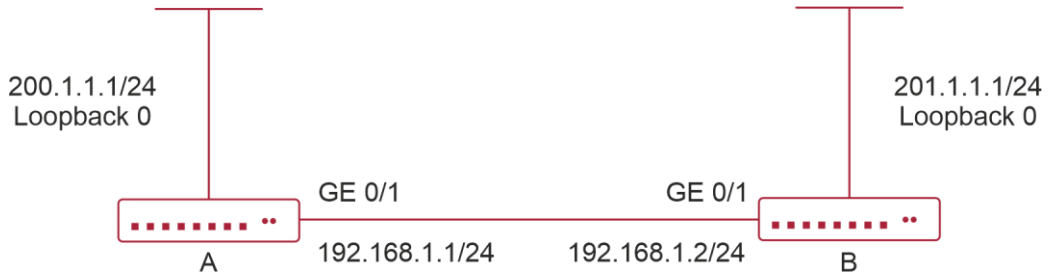


Рисунок 3-11.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • На маршрутизаторе A включите функцию триггерных обновлений RIP и установите интервал повторной передачи и максимальное количество повторных передач пакетов запроса и обновления на 10 с и 18 соответственно
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# encapsulation ppp A(config-if-GigabitEthernet 0/1)# ip rip triggered A(config-if-GigabitEthernet 0/1)# ip rip triggered retransmit-timer 10 A(config-if-GigabitEthernet 0/1)# ip rip triggered retransmit-count 18 A(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse A(config)# router rip A(config-router)# network 192.168.1.0 A(config-router)# network 200.1.1.0
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# encapsulation ppp B(config-if-GigabitEthernet 0/1)# ip rip triggered B(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse B(config)# router rip

	B(config-router)# network 192.168.1.0 B(config-router)# network 201.1.1.0
Проверка	На Маршрутизаторе A и Маршрутизаторе B проверьте базу данных RIP и убедитесь, что соответствующие маршруты являются постоянными
A	A# sho ip rip database 201.1.1.0/24 auto-summary 201.1.1.0/24 [1] via 192.168.12.2 GigabitEthernet 0/1 06:25 permanent
B	B# sho ip rip database 200.1.1.0/24 auto-summary 200.1.1.0/24 [1] via 192.168.12.1 GigabitEthernet 0/1 06:25 permanent

3.4.3.7. Распространенные ошибки

- Функция триггерных обновлений активируется, когда конфигурации RIP на обоих концах канала согласованы.
- Включены как триггерные обновления, так и функции BFD.
- Функция триггерных обновлений включена не на всех маршрутизаторах в одном канале.

3.4.4. Включение проверки адреса источника

3.4.4.1. Эффект конфигурации

Проверяется адрес источника полученного пакета обновления маршрута RIP.

3.4.4.2. Примечания

Необходимо настроить основные функции RIP.

3.4.4.3. Шаги настройки

Включение проверки адреса источника

- Эта функция включена по умолчанию и должна быть отключена, если проверка адреса источника не требуется.
- После отключения Split Horizon на интерфейсе процесс маршрутизации RIP выполнит проверку адреса источника в пакете обновления независимо от того, выполняется ли команда **validate-update-source** в режиме конфигурации процесса маршрутизации.
- Для ненумерованного IP-интерфейса процесс маршрутизации RIP не выполняет проверку адреса источника в пакете обновления независимо от того, выполняется ли команда **validate-update-source** в режиме конфигурации процесса маршрутизации.

- Если не требуется иное, эту функцию необходимо отключить на каждом маршрутизаторе, не требующем проверки адреса источника.

3.4.4.4. Проверка

Принимаются только пакеты обновления маршрута, поступающие от одного и того же соседа по подсети IP.

3.4.4.5. Связанные команды

Синтаксис команды	**validate-update-source**
Командный режим	Режим настройки процесса маршрутизации
Использование конфигурации	Проверка адреса источника пакета обновления включена по умолчанию. После включения этой функции проверяется адрес источника пакета обновления маршрута RIP. Цель состоит в том, чтобы гарантировать, что процесс маршрутизации RIP получает только пакеты обновления маршрута, поступающие от того же соседа по подсети IP

3.4.4.6. Пример конфигурации

Сценарий:

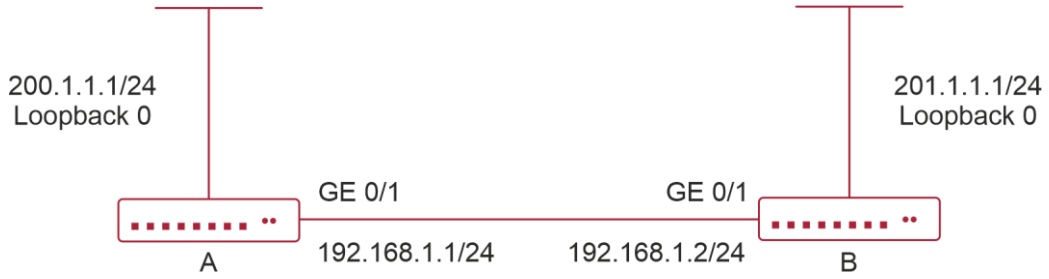


Рисунок 3-12.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • Отключите проверку адреса источника пакетов обновления на всех маршрутизаторах
A	A# configure terminal A(config)# router rip

	A(config-router)# no validate-update-source
B	B# configure terminal B(config)# router rip B(config-router)# no validate-update-source
Проверка	• На маршрутизаторе A проверьте таблицу маршрутизации и убедитесь, что запись 201.1.1.0/24 загружена. • На маршрутизаторе B проверьте таблицу маршрутизации и убедитесь, что запись 200.1.1.0/24 загружена
A	A# show ip route rip R 201.1.1.0/24 [120/1] via 192.168.2.2, 00:06:11, GigabitEthernet 0/1
B	B# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1

3.4.5. Включение аутентификации

3.4.5.1. Эффект конфигурации

Предотвращает изучение неаутентифицированных и недействительных маршрутов и объявление действительных маршрутов неавторизованным устройствам, обеспечивая стабильность системы и защищая ее от вторжений.

3.4.5.2. Примечания

- Необходимо настроить основные функции RIP.
- Только RIPv2 поддерживает аутентификацию пакетов RIP, а RIPv1 — нет.

3.4.5.3. Шаги настройки

Включение аутентификации и указание цепочки ключей, используемой для аутентификации RIP

- Эта конфигурация является обязательной, если необходимо включить аутентификацию.
- Если цепочка ключей уже указана в конфигурации интерфейса, запустите команду **key chain** в режиме глобальной конфигурации, чтобы определить цепочку ключей; в противном случае аутентификация пакетов RIP может завершиться неудачей.
- Если не требуется иное, эту настройку необходимо выполнить на каждом маршрутизаторе, требующем аутентификации.

Определение режима аутентификации RIP

- Эта конфигурация является обязательной, если необходимо включить аутентификацию.
- Режимы аутентификации RIP, настроенные на всех устройствах, которым необходимо напрямую обмениваться информацией о маршрутизации RIP,

должны быть одинаковыми; в противном случае обмен пакетами RIP может оказаться невозможным.

- Если используется аутентификация в виде обычного текста, но цепочка ключей для аутентификации в виде обычного текста не настроена или не связана, аутентификация не выполняется. Аналогично, если используется аутентификация MD5, но цепочка ключей не настроена или не связана, аутентификация не выполняется.
- Если не требуется иное, эту настройку необходимо выполнить на каждом маршрутизаторе, требующем аутентификации.

Включение аутентификации по обычному тексту RIP и настройка цепочки ключей

- Эта конфигурация является обязательной, если необходимо включить аутентификацию.
- Если необходимо включить аутентификацию в виде обычного текста RIP, используйте эту команду для настройки цепочки ключей для аутентификации в виде обычного текста. Альтернативно вы можете получить цепочку ключей для аутентификации в виде обычного текста, связав цепочку ключей. Цепочка ключей, полученная вторым методом, имеет приоритет над полученной первым методом.
- Если не требуется иное, эту настройку необходимо выполнить на каждом маршрутизаторе, требующем аутентификации.

3.4.5.4. Проверка

- Аутентификация по открытому тексту RIP обеспечивает лишь ограниченную безопасность, поскольку пароль, передаваемый через пакет, виден.
- Аутентификация RIP MD5 может обеспечить более высокий уровень безопасности, поскольку пароль, передаваемый через пакет, шифруется с использованием алгоритма MD5.
- Маршруты можно изучить правильно, если настроены правильные параметры аутентификации.
- Маршруты невозможно изучить, если настроены неправильные параметры аутентификации.

3.4.5.5. Связанные команды

Включение проверки адреса источника

Синтаксис команды	**ip rip authentication key-chain** *name-of-keychain*
Описание параметра	*name-of-keychain*: указывает имя цепочки ключей, используемой для аутентификации RIP
Командный режим	Режим настройки интерфейса
Использование конфигурации	Указанная цепочка ключей должна быть заранее определена командой **key chain** в режиме глобальной конфигурации

Определение режима аутентификации RIP

Синтаксис команды	**ip rip authentication mode** { **text** | **md5** }
Описание параметра	**text**: указывает, что режим аутентификации RIP представляет собой аутентификацию в виде обычного текста. **md5**: указывает, что режим аутентификации RIP — это аутентификация MD5
Командный режим	Режим настройки интерфейса
Использование конфигурации	Для всех устройств, которым необходимо напрямую обмениваться информацией о маршрутизации RIP, режим аутентификации RIP этих устройств должен быть одинаковым

Включение аутентификации по обычному тексту RIP и настройка цепочки ключей

Синтаксис команды	**ip rip authentication text-password** [**0** | **7**] *password-string*
Описание параметра	**0**: указывает, что ключ отображается в виде обычного текста. **7**: указывает, что ключ отображается в зашифрованном виде. *password-string*: указывает цепочку ключей, используемую для аутентификации в виде обычного текста. Цепочка ключей представляет собой строку длиной от 1 до 16 байт
Командный режим	Режим настройки интерфейса
Использование конфигурации	Эти команды действуют только в режиме аутентификации с использованием обычного текста

3.4.5.6. Пример конфигурации

Настройка основных функций RIP и включение аутентификации MD5

Сценарий:

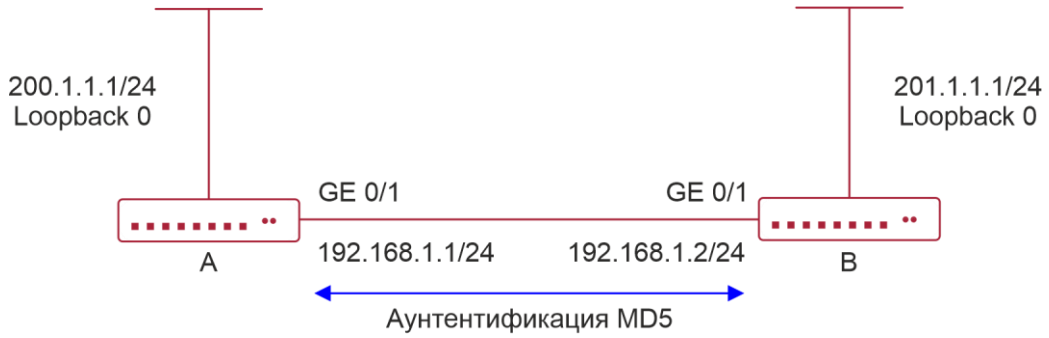


Рисунок 3-13.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • Настройте тип аутентификации и ключ аутентификации MD5 на всех маршрутизаторах
A	A# configure terminal A(config)# key chain hello A(config-keychain)# key 1 A(config-keychain-key)# key-string world A(config-keychain-key)# exit A(config-keychain)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5 A(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain hello
B	B# configure terminal B(config)# key chain hello B(config-keychain)# key 1 B(config-keychain-key)# key-string world B(config-keychain-key)# exit B(config-keychain)# exit B(config)# interface GigabitEthernet 0/1

	B(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5 B(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain hello
Проверка	• На маршрутизаторе A проверьте таблицу маршрутизации и убедитесь, что запись 201.1.1.0/24 загружена. • На маршрутизаторе B проверьте таблицу маршрутизации и убедитесь, что запись 200.1.1.0/24 загружена
A	A# show ip route rip R 201.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1
B	A# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1

3.4.5.7. Распространенные ошибки

- Ключи, настроенные на маршрутизаторах, которым необходимо обмениваться информацией о маршрутизации RIP, различаются.
- Режимы аутентификации, настроенные на маршрутизаторах, которым необходимо обмениваться информацией о маршрутизации RIP, различаются.

3.4.6. Включение суммирования маршрутов

3.4.6.1. Эффект конфигурации

Уменьшает размер таблицы маршрутизации, улучшает эффективность маршрутизации, в некоторой степени избегает flapping-а маршрутов и улучшает масштабируемость и эффективность сети.

ПРИМЕЧАНИЕ: если суммарный маршрут существует, подмаршруты, включенные в суммарный маршрут, не отображаются в таблице маршрутизации, что значительно уменьшает размер таблицы маршрутизации.

ПРИМЕЧАНИЕ: объявление суммарного маршрута более эффективна, чем объявление отдельных маршрутов, потому что:(1) Суммарный маршрут обрабатывается первым, когда RIP просматривает базу данных; (2) Все подмаршруты игнорируются, когда RIP просматривает базу данных, что сокращает необходимое время обработки.

3.4.6.2. Примечания

- Необходимо настроить основные функции RIP.
- Диапазон маршрутов supernetting больше, чем у классовой сети. Таким образом, функция автоматического суммирования маршрутов недействительна для маршрутов supernetting.
- RIPv1 всегда выполняет автоматическое суммирование маршрутов. Если необходимо объявить подробные маршруты, необходимо установить версию RIP на RIPv2.

3.4.6.3. Шаги настройки

Включение автоматического суммирования маршрутов

- Эта функция включена по умолчанию.
- Чтобы изучить конкретные маршруты подсети вместо суммарных сетевых маршрутов, необходимо отключить автоматическое суммирование маршрутов.
- Отключить автоматическое суммирование маршрутов можно только в RIPv2. RIPv1 всегда выполняет автоматическое суммирование маршрутов.

Настройка суммирования маршрутов RIP на интерфейсе

- Эту функцию необходимо настроить, если требуется суммировать классовые подсети.
- Команда **ip rip summary-address** используется для суммирования адреса или подсети в указанном интерфейсе. RIP автоматически суммирует данные до границы классовой сети. Каждую классовую подсеть можно настроить только с помощью команды **ip rip summary-address**.
- Суммарный диапазон, настроенный в этой команде, не может быть маршрутами supernetting, то есть настроенная длина маски подсети не может быть меньше естественной длины маски сети.
- Если не требуется иное, эту настройку следует выполнять на маршрутизаторе, требующем классового суммирования подсетей.

3.4.6.4. Проверка

Убедитесь, что маршруты суммированы в таблице маршрутизации peer end-a.

3.4.6.5. Связанные команды

Включение автоматического суммирования маршрутов

Синтаксис команды	**auto-summary**
Командный режим	Режим настройки процесса маршрутизации
Использование конфигурации	Суммирование маршрутов включено по умолчанию для RIPv1 и RIPv2. Отключить автоматическое суммирование маршрутов можно только в RIPv2. RIPv1 всегда выполняет автоматическое суммирование маршрутов

Настройка суммирования маршрутов RIP на интерфейсе

Синтаксис команды	**ip rip summary-address** *ip-address ip-network-mask*
Описание параметра	*ip-address*: указывает IP-адрес для суммирования. *ip-network-mask*: указывает маску подсети IP-адреса, подлежащего суммированию

Командный режим	Режим настройки интерфейса
Использование конфигурации	Эта команда используется для суммирования адреса или подсети в указанном интерфейсе

3.4.6.6. Пример конфигурации

Настройка суммирования маршрутов

Сценарий:

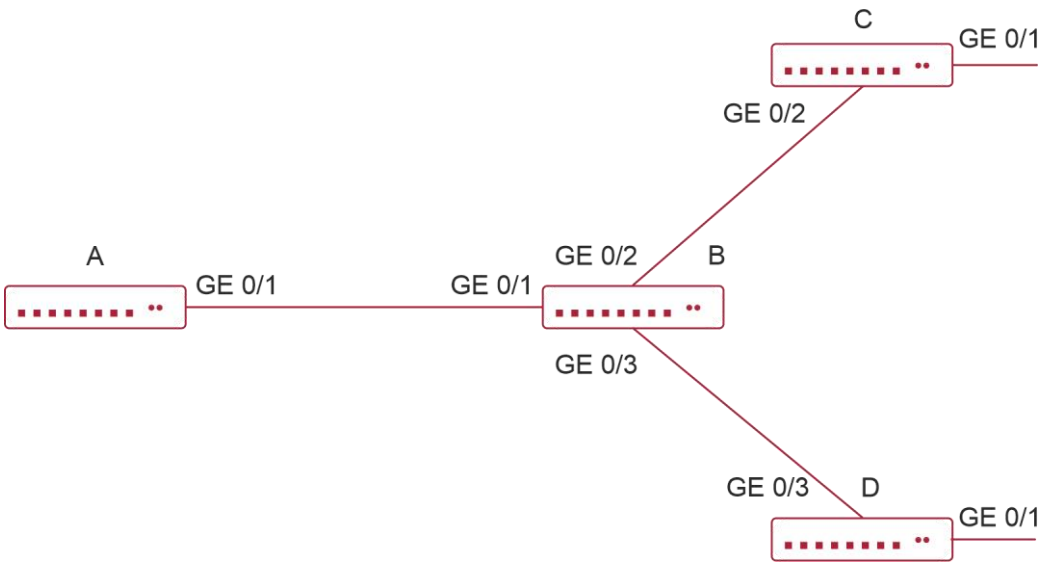


Рисунок 3-14.

IP-адреса интерфейса следующие:

A: GE0/1 192.168.1.1

B: GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1

C: GE0/2 172.16.2.2 GE0/3 172.16.4.2

D: GE0/2 172.16.3.2 GE0/3 172.16.5.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • Настройте суммирование маршрутов на маршрутизаторе B
	B# configure terminal B(config)# interface GigabitEthernet 0/1

	B(config-if-GigabitEthernet 0/1)# ip rip summary-address 172.16.0.0 255.255.0.0 B(config)# router rip B(config-router)# version 2 B(config-router)# no auto-summary
Проверка	Проверьте таблицу маршрутизации на маршрутизаторе A и убедитесь, что создана запись 172.16.0.0/16
	A# show ip route rip R 172.16.0.0/16 [120/2] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1

3.4.6.7. Распространенные ошибки

Основные функции RIP не настроены или не могут быть настроены.

3.4.7. Включение маршрутов Supernetting

3.4.7.1. Эффект конфигурации

Разрешить RIP отправлять маршруты supernetting RIP на указанный интерфейс.

3.4.7.2. Примечания

Необходимо настроить основные функции RIP.

3.4.7.3. Шаги настройки

Включение маршрутов Supernetting

- Если маршрут supernetting обнаружен, когда маршрутизатор с поддержкой RIPv1 отслеживает пакеты ответа маршрута RIPv2, маршрутизатор изучает неправильный маршрут, поскольку RIPv1 игнорирует маску подсети в информации о маршрутизации пакета. В этом случае на маршрутизаторе с поддержкой RIPv2 необходимо использовать форму команды **no**, чтобы запретить объявление маршрутов supernetting на соответствующем интерфейсе. Эта команда действует только на текущий интерфейс.
- Команда эффективна только при отправке пакетов RIPv2 на интерфейс и используется для управления отправкой маршрутов supernetting.

3.4.7.4. Проверка

Убедитесь, что peer-маршрутизатор не может изучить маршрут supernetting.

3.4.7.5. Связанные команды

Синтаксис команды	**ip rip send supernet-routes**
Командный режим	Режим настройки интерфейса

Использование конфигурации	По умолчанию интерфейсу разрешено отправлять маршруты supernetting RIP

3.4.7.6. Пример конфигурации

Отключение маршрутов Supernetting

Сценарий:



Рисунок 3-15.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • Запретите отправку маршрутов supernetting RIP на интерфейсе GigabitEthernet 0/1 маршрутизатора B
	B# configure terminal B(config)# ip route 207.0.0.0 255.0.0.0 Null 0 B(config)# ip route 208.1.1.0 255.255.255.0 Null 0 B(config)# router rip B(config-router)# redistribute static B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# no ip rip send supernet-routes
Проверка	Проверьте таблицу маршрутизации на маршрутизаторе A и убедитесь, что маршрутизатор A может изучить только non-supernetting маршрут 208.1.1.0/24, но не supernetting маршрут 207.0.0.0/8
	A#show ip route rip R 208.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

3.4.8. Объявление маршрута по умолчанию или внешних маршрутов

3.4.8.1. Эффект конфигурации

- В домене RIP введите unicast-маршрут другой AS, чтобы сервис unicast-маршрутизации к этой AS мог предоставляться пользователям в домене RIP.
- В домене RIP внедрите маршрут по умолчанию в другую AS, чтобы сервис unicast-маршрутизации к этой AS мог предоставляться пользователям в домене RIP.

3.4.8.2. Примечания

- Необходимо настроить основные функции RIP.
- Перераспределение маршрутов не может добавлять маршруты по умолчанию для других протоколов в домен маршрутизации RIP.

3.4.8.3. Шаги настройки

Объявление маршрута по умолчанию соседям

Эту функцию необходимо включить, если требуется объявить маршрут по умолчанию соседям.

По умолчанию маршрут по умолчанию не генерируется, а метрика маршрута по умолчанию равна 1.

Если процесс RIP может сгенерировать маршрут по умолчанию с помощью этой команды, RIP не изучает маршрут по умолчанию, объявленный соседом.

Если не требуется иное, эту настройку следует выполнять на маршрутизаторе, которому необходимо объявить маршрут по умолчанию.

Объявление маршрута по умолчанию соседям на интерфейсе

Эту функцию необходимо включить, если требуется объявить маршрут по умолчанию соседям на указанном интерфейсе.

По умолчанию маршрут по умолчанию не настроен, а метрика маршрута по умолчанию равна 1.

После настройки этой команды на интерфейсе маршрут по умолчанию генерируется и объявляется через этот интерфейс.

Если не требуется иное, эту настройку следует выполнять на маршрутизаторе, которому необходимо объявить маршрут по умолчанию.

Перераспределяет маршруты и объявляет внешние маршруты соседям

Эту функцию необходимо включить, если необходимо перераспределить маршруты других протоколов.

По умолчанию:

- Если настроено перераспределение OSPF, перераспределите маршруты всех подтипов процесса OSPF.
- Если настроено перераспределение IS-IS, перераспределите маршруты Level-2 процесса IS-IS.
- В остальных случаях перераспределите все внешние маршруты.
- Метрика перераспределенного маршрута по умолчанию равна 1.

- Карта маршрутов не связана по умолчанию.

При перераспределении маршрутов нет необходимости преобразовывать метрику одного протокола маршрутизации в метрику другого протокола маршрутизации, поскольку разные протоколы маршрутизации используют совершенно разные методы измерения метрики. RIP измеряет метрику на основе количества hop-ов, а OSPF измеряет метрику на основе пропускной способности. Поэтому вычисленные метрики нельзя сравнивать друг с другом. Однако во время перераспределения маршрутов необходимо настроить символическую метрику; в противном случае перераспределение маршрутов не удастся.

Если не требуется иное, эту настройку следует выполнять на маршрутизаторе, которому необходимо перераспределить маршруты.

3.4.8.4. Проверка

- На соседнем устройстве убедитесь, что в таблице маршрутизации RIP существует маршрут по умолчанию.
- На локальном и соседнем устройствах убедитесь, что в таблице маршрутизации RIP существуют внешние маршруты (маршруты к другим AS).

3.4.8.5. Связанные команды

Объявление маршрута по умолчанию соседям

Синтаксис команды	**default-information originate** [**always**] [**metric** *metric-value*] [**route-map** *map-name*]
Описание параметра	**always**: позволяет RIP генерировать маршрут по умолчанию независимо от того, имеет ли локальный маршрутизатор маршрут по умолчанию. **metric** *metric-value*: указывает начальную метрику маршрута по умолчанию. Значение варьируется от 1 до 15. **route-map** *map-name*: указывает название связанной карты маршрута. По умолчанию карта маршрута не привязана
Командный режим	Режим настройки процесса маршрутизации
Использование конфигурации	Если маршрут по умолчанию существует в таблице маршрутизации маршрутизатора, RIP по умолчанию не объявляет маршрут по умолчанию внешним объектам. Вам необходимо запустить команду **default-information originate** в режиме конфигурации процесса маршрутизации, чтобы объявить соседям маршрут по умолчанию. Если выбран параметр **alway**, процесс маршрутизации RIP объявляет соседям маршрут по умолчанию независимо от того, существует ли маршрут по умолчанию, но этот маршрут по умолчанию не отображается в локальной таблице маршрутизации. Чтобы проверить, сгенерирован ли маршрут по умолчанию, запустите команду **show ip rip database**, чтобы проверить базу данных информации о маршрутизации RIP.

	Для дальнейшего управления поведением объявления маршрута по умолчанию RIP используйте параметр **route-map**. Например, запустите правило установки метрики, чтобы установить метрику маршрута по умолчанию. Вы можете использовать параметр **metric**, чтобы установить метрику объявленного значения по умолчанию, но приоритет этой конфигурации ниже, чем у правила установки метрики параметра **route-map**. Если параметр **metric** не настроен, маршрут по умолчанию использует метрику по умолчанию, настроенную для RIP. Еще необходимо запустить команду **default-information originate** для представления маршрута по умолчанию, созданного **ip default-network**, в RIP

Объявление маршрута по умолчанию соседям на интерфейсе

Синтаксис команды	**ip rip default-information** { **only** | **originate** } [**metric** *metric-value*]
Описание параметра	**only**: указывает, что объявляется только маршрут по умолчанию. **originate**: указывает, что объявлен маршрут по умолчанию и другие маршруты. **metric** *metric-value*: указывает метрику маршрута по умолчанию. Значение варьируется от 1 до 15
Командный режим	Режим настройки интерфейса
Использование конфигурации	Если вы настраиваете команду **ip rip default-information** для интерфейса и команду **default-information originate** для процесса RIP, объявляется только маршрут по умолчанию, настроенный для интерфейса. Поскольку **ip rip default-information** настроена для одного интерфейса, RIP не изучает маршрут по умолчанию, объявленный соседом

Перераспределение маршрутов и объявление внешних маршрутов соседям

Синтаксис команды	**redistribute** { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static** } [{ **level-1** | **level-1-2** | **level-2** }] [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] [**metric** *metric-value*] []
Описание параметра	**bgp**: указывает на перераспределение из BGP. **connected**: указывает на перераспределение из прямых маршрутов. **isis** *area-tag*: указывает на перераспределение из IS-IS. *area-tag* указывает идентификатор процесса IS-IS.

	ospf *process-id*: указывает на перераспределение из OSPF. *process-id* указывает идентификатор процесса OSPF. Значение варьируется от 1 до 65 535. **static**: указывает на перераспределение из статических маршрутов. **level-1** | **level-1-2** | **level-2**: используется только при перераспределении маршрутов IS-IS. Перераспределяются только маршруты указанного уровня. **match**: используется только при перераспределении маршрутов OSPF. Перераспределяются только маршруты, соответствующие условиям фильтрации. **metric** *metric-value*: устанавливает метрику перераспределяемого маршрута. Значение варьируется от 1 до 16. **route-map** *route-map-name*: устанавливает правила фильтрации перераспределения
Командный режим	Режим настройки процесса маршрутизации
Использование конфигурации	Если вы настраиваете перераспределение маршрутов IS-IS без указания параметра уровня, по умолчанию можно перераспределять только маршруты Level-2. Если при первоначальной настройке перераспределения указать параметр **level**, то маршруты указанного уровня могут быть перераспределены. Если настроены и **level-1**, и **level-2**, для удобства эти два уровня объединяются и сохраняются как **level-1-2**. Если вы настроите перераспределение маршрутов OSPF без указания параметра **match**, маршруты OSPF всех подтипов могут распределяться по умолчанию. Последняя настройка параметра **match** используется в качестве начального параметра **match**. Перераспределять можно только маршруты, соответствующие подтипам. Вы можете использовать форму команды **no**, чтобы восстановить значение соответствия по умолчанию. Правила конфигурации для формы **no** команды **redistribute** следующие: 1. Если некоторые параметры указаны в форме **no** команды, значения этих параметров по умолчанию будут восстановлены. 2. Если в форме **no** команды не указан ни один параметр, вся команда будет удалена. Например, если настроено **redistribute isis 112 level-2**, вы можете запустить команду **no redistribute isis 112 level-2**, чтобы восстановить значение Level-2 по умолчанию. Поскольку уровень 2 сам по себе является значением параметра по умолчанию, сохраненная конфигурация по-прежнему перераспределяет isis 112 level-2 после выполнения предыдущей формы **no** команды.

	Чтобы удалить всю команду, выполните команду **no redistribute isis 112**

3.4.8.6. Пример конфигурации

Перераспределение маршрутов и объявление внешних маршрутов соседям

Сценарий:

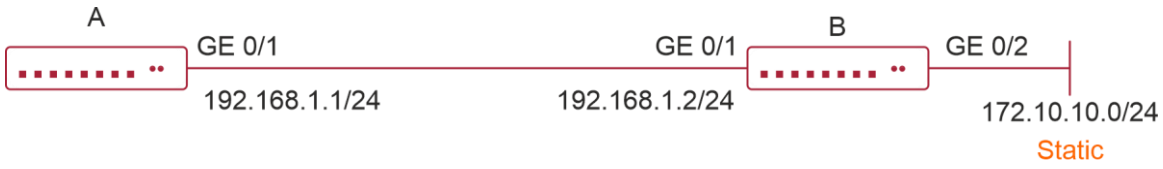


Рисунок 3-16.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • На маршрутизаторе B настройте перераспределение статических маршрутов
B	B# configure terminal B(config)# router rip B(config-router)# redistribute static
Проверка	На маршрутизаторе A проверьте таблицу маршрутизации и убедитесь, что запись 172.10.10.0/24 загружена
	A# show ip route rip R 172.10.10.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

3.4.9. Настройка правил фильтрации маршрутов

3.4.9.1. Эффект конфигурации

Маршруты, не соответствующие критериям фильтрации, не могут быть загружены в таблицу маршрутизации или объявлены соседям. Таким образом, пользователям внутри сети можно запретить доступ к указанным сетям назначения.

3.4.9.2. Примечания

- Необходимо настроить основные функции RIP.

- Что касается правил фильтрации отправляемых маршрутов, то сначала необходимо настроить перераспределение маршрутов, а затем фильтровать перераспределяемые маршруты.

3.4.9.3. Шаги настройки

Фильтрация полученной информации о маршрутизации RIP

- Эту функцию необходимо настроить, если требуется фильтровать полученную информацию маршрута.
- Чтобы отказаться от получения некоторых указанных маршрутов, вы можете настроить список управления распределением маршрутов для обработки всех полученных пакетов обновления маршрута. Если интерфейс не указан, будут обработаны пакеты обновления маршрута, полученные на всех интерфейсах.
- Если не требуется иное, эту настройку следует выполнять на маршрутизаторе, требующем фильтрации маршрутов.

Фильтрация отправляемой маршрутной информации RIP

- Эту функцию необходимо настроить, если требуется фильтровать перераспределяемую информацию о маршрутизации, которая отправляется.
- Если эта команда не содержит каких-либо дополнительных параметров, управление объявлением обновления маршрута вступает в силу на всех интерфейсах. Если команда содержит параметр интерфейса, управление объявлением обновления маршрута действует только на указанном интерфейсе. Если команда содержит другие параметры процесса маршрутизации, управление объявлением обновления маршрута действует только на указанный процесс маршрутизации.
- Если не требуется иное, эту настройку следует выполнять на маршрутизаторе, требующем фильтрации маршрутов.

3.4.9.4. Проверка

Запустите команду **show ip route rip**, чтобы убедиться, что отфильтрованные маршруты не загружены в таблицу маршрутизации.

3.4.9.5. Связанные команды

Фильтрация полученной информации о маршрутизации RIP

Синтаксис команды	**distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]
Описание параметра	*access-list-number* | *name*: определяет список доступа. Могут быть получены только маршруты, разрешенные списком доступа. **prefix** *prefix-list-name*: использует список префиксов для фильтрации маршрутов. **gateway** *prefix-list-name*: использует список префиксов для фильтрации источников маршрутов. *interface-type interface-number*: указывает, что список рассылки применен к указанному интерфейсу

Командный режим	Режим настройки процесса маршрутизации

Фильтрация отправляемой маршрутной информации RIP

Синтаксис команды	**distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* | [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]]
Описание параметра	*access-list-number* | *name*: определяет список доступа. Могут быть отправлены только маршруты, разрешенные списком доступа. **prefix** *prefix-list-name*: использует список префиксов для фильтрации маршрутов. *interface*: применяет управление объявлением об обновлении маршрута только на указанном интерфейсе. **bgp**: применяет управление объявлением об обновлении маршрутов только к маршрутам, введенным из BGP. **connected**: применяет управление объявлением об обновлении маршрута только к прямым маршрутам, введеным путем перераспределения. **isis** [*area-tag*]: применяет управление объявлением об обновлении маршрута только на маршрутах, введенных из IS-IS. *area-tag* определяет процесс IS-IS. **ospf** *process-id*: применяет управление объявлением об обновлении маршрута только к маршрутам, введенным из OSPF. *process-id* указывает процесс OSPF. **rip**: применяет управление объявлением об обновлении маршрута только на маршрутах RIP. **static**: применяет управление объявлением об обновлении маршрута только к статическим маршрутам, введеным путем перераспределения
Командный режим	Режим настройки процесса маршрутизации

3.4.9.6. Пример конфигурации

Фильтрация полученной информации о маршрутизации RIP

Сценарий:

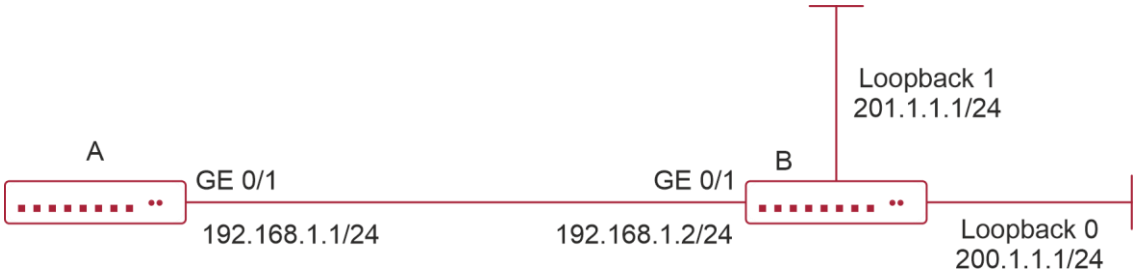


Рисунок 3-17.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • Включите процесс маршрутизации RIP, чтобы контролировать маршруты, полученные через порт GigabitEthernet 0/1, и получать только маршрут 200.1.1.0
A	A# configure terminal A(config)# router rip A(config-router)# distribute-list 10 in GigabitEthernet 0/1 A(config-router)# no auto-summary A(config)# access-list 10 permit 200.1.1.0 0.0.0.255
Проверка	На маршрутизаторе A проверьте таблицу маршрутизации и убедитесь, что существует только запись 200.1.1.0/24
A	A# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

Фильтрация отправляемой маршрутной информации RIP

Сценарий:



Рисунок 3-18.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • Включите процесс маршрутизации RIP, чтобы объявлять только маршрут 200.1.1.0/24
B	B# configure terminal B(config)# router rip B(config-router)# redistribute connected B(config-router)# distribute-list 10 out B(config-router)# version 2 B(config)# access-list 10 permit 200.1.1.0 0.0.0.255
Проверка	Проверьте таблицу маршрутизации на маршрутизаторе A и убедитесь, что маршрут в сегменте сети 200.1.1.0 существует
A	A# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

3.4.9.7. Распространенные ошибки

Фильтрация не удалась, поскольку правила фильтрации списка доступа настроены неправильно.

3.4.10. Изменение параметров выбора маршрута

3.4.10.1. Эффект конфигурации

- Измените маршруты RIP, чтобы разрешить прохождение трафика через указанные узлы или избежать прохождения через указанные узлы.

- Измените последовательность выбора маршрутизатором различных типов маршрутов, чтобы изменить приоритеты маршрутов RIP.

3.4.10.2. Примечания

Необходимо настроить основные функции RIP.

3.4.10.3. Шаги настройки

Изменение административного расстояния маршрута RIP

- Опционально.
- Эта конфигурация является обязательной, если вы хотите изменить приоритеты маршрутов RIP на маршрутизаторе, который использует несколько протоколов unicast-маршрутизации.

Увеличение метрики полученного или отправленного маршрута RIP

- Опционально.
- Если не указано иное, эту настройку следует выполнять на маршрутизаторе, на котором необходимо настроить метрики маршрутов.

Настройка метрики по умолчанию для внешнего маршрута, перераспределенного в RIP

- Опционально.
- Если не требуется иное, эту настройку необходимо выполнить на ASBR, к которому введены внешние маршруты.

3.4.10.4. Проверка

Запустите команду **show ip rip**, чтобы отобразить настроенное в данный момент административное расстояние. Запустите команду **show ip rip data**, чтобы отобразить метрики перераспределенных маршрутов и убедиться, что конфигурация вступила в силу.

3.4.10.5. Связанные команды

Изменение административного расстояния маршрута RIP

Синтаксис команды	**distance** *distance* [*ip-address wildcard*]
Описание параметра	*distance*: устанавливает административное расстояние маршрута RIP. Значение представляет собой целое число от 1 до 255. *ip-address*: указывает префикс исходного IP-адреса маршрута. *wildcard*: определяет бит сравнения IP-адресов. **0** указывает на точное совпадение, а **1** указывает на то, что сравнение не выполняется
Командный режим	Режим настройки процесса маршрутизации
Использование конфигурации	Запустите эту команду, чтобы настроить административное расстояние маршрута RIP

Увеличение метрики полученного или отправленного маршрута RIP

Синтаксис команды	**offset-list** { *access-list-number* | *name* } { **in** | **out** } *offset* [*interface-type interface-number*]
Описание параметра	*access-list-number* | *name*: определяет список доступа. **in**: использует ACL для изменения метрики полученного маршрута. **out**: использует ACL для изменения метрики отправленного маршрута. *offset*: указывает смещение измененной метрики. Значение варьируется от 0 до 16. *interface-type*: использует ACL на указанном интерфейсе. *interface-number*: указывает номер интерфейса
Командный режим	Режим настройки процесса маршрутизации
Использование конфигурации	Запустите эту команду, чтобы увеличить метрику полученного или отправленного маршрута RIP. Если указан интерфейс, конфигурация вступает в силу только для указанного интерфейса; в противном случае конфигурация вступит в силу глобально

Настройка метрики по умолчанию для внешнего маршрута, перераспределенного в RIP

Синтаксис команды	**default-metric** *metric-value*
Описание параметра	*metric-value*: указывает метрику по умолчанию. Допустимое значение находится в диапазоне от 1 до 16. Если значение равно или больше 16, ПО определяет, что этот маршрут недоступен
Командный режим	Режим настройки процесса маршрутизации
Использование конфигурации	Эту команду необходимо использовать вместе с командой **redistribute** конфигурации протокола маршрутизации

3.4.10.6. Пример конфигурации

Увеличение метрики полученного или отправленного маршрута RIP

Сценарий:



Рисунок 3-19.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • Увеличьте на 7 метрику каждого маршрута RIP в диапазоне, указанном ACL 7. • Увеличьте на 7 метрику каждого изученного маршрута RIP в диапазоне, указанном ACL 8
A	A# configure terminal A(config)# access-list 7 permit host 200.1.1.0 A(config)# access-list 8 permit host 201.1.1.0 A(config)# router rip A(config-router)# offset-list 7 out 7 A(config-router)# offset-list 8 in 7
Проверка	Проверьте таблицу маршрутизации на маршрутизаторе A и маршрутизаторе B, чтобы убедиться, что метрика маршрутов RIP равна 8
A	A# show ip route rip R 201.1.1.0/24 [120/8] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1
B	B# show ip route rip R 200.1.1.0/24 [120/8] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1

3.4.11. Изменение таймеров

3.4.11.1. Эффект конфигурации

Изменяйте длительность таймеров RIP, чтобы ускорить или замедлить изменение состояния протокола или возникновение события.

3.4.11.2. Примечания

- Необходимо настроить основные функции RIP.
- Изменение параметров управления протоколом может привести к сбоям в работе протокола. Поэтому не рекомендуется изменять таймеры.

3.4.11.3. Шаги настройки

Изменение таймера обновления, таймера неработоспособности и таймера очистки

Эту настройку необходимо выполнить, если вам необходимо настроить таймеры RIP.

Настраивая таймеры, можно сократить время сходимости и время устранения ошибок протокола маршрутизации. Для маршрутизаторов, подключенных к одной сети, значения трех таймеров RIP должны быть одинаковыми. Как правило, не рекомендуется изменять таймеры RIP, если не требуется иное.

Установка небольших значений таймеров на низкоскоростном канале сопряжена с риском, поскольку множество пакетов обновления потребляют полосу пропускания. Вы можете установить таймеры на небольшие значения, как правило, в Ethernet или канале со скоростью 2 Мбит/с (или выше), чтобы сократить время сходимости сетевых маршрутов.

Если не требуется иное, эту настройку следует выполнять на маршрутизаторе, на котором необходимо изменить таймеры RIP.

Настройка задержки отправки между пакетами обновления маршрута RIP

Эту настройку необходимо выполнить, если вам нужно настроить задержку отправки между пакетами обновления RIP.

Запустите команду **output-delay**, чтобы увеличить задержку отправки между пакетами на высокоскоростном устройстве, чтобы низкоскоростное устройство могло получать и обрабатывать все пакеты обновления.

Если не требуется иное, эту настройку следует выполнять на маршрутизаторе, на котором необходимо настроить задержку отправки.

3.4.11.4. Проверка

Запустите команду **show ip rip**, чтобы отобразить текущие настройки таймеров RIP.

3.4.11.5. Связанные команды

Изменение таймера обновления, таймера неработоспособности и таймера очистки

Синтаксис команды	**timers basic** *update invalid flush*
Описание параметра	*update*: указывает время обновления маршрута в секундах. Он определяет интервал, с которым устройство отправляет пакет обновления маршрута. Каждый раз при получении пакета обновления таймер неработоспособности и таймер очистки сбрасываются. По умолчанию пакет обновления маршрутизации отправляется каждые 30 секунд. *invalid*: указывает время неработоспособности маршрута в секундах, отсчитываемое от последнего момента получения действительного пакета обновления. Он определяет время, по истечении которого маршрут в списке маршрутизации становится недействительным, поскольку маршрут не обновляется. Длительность таймера неработоспособности должна быть как минимум в три раза больше длительности таймера обновления. Если пакет обновления не получен до истечения таймера неработоспособности, соответствующий маршрут переходит в недопустимое (invalid) состояние. Если пакет обновления получен до истечения срока действия таймера неработоспособности, таймер сбрасывается. По умолчанию продолжительность таймера неработоспособности составляет 180 с. *flush*: указывает время очистки маршрута в секундах, отсчитываемое с момента, когда маршрут RIP переходит в недопустимое состояние. По истечении времени таймера очистки маршрут в недопустимом состоянии будет удален из таблицы маршрутизации. По умолчанию продолжительность таймера очистки составляет 120 с
Командный режим	Режим настройки процесса маршрутизации
Использование конфигурации	По умолчанию таймер обновления составляет 30 с, таймер неработоспособности — 180 с, а таймер очистки — 120 с

Настройка задержки отправки между пакетами обновления маршрута RIP

Синтаксис команды	**output-delay** *delay*
Описание параметра	*delay*: устанавливает задержку отправки между пакетами в мс. Значение варьируется от 8 до 50
Командный режим	Режим настройки интерфейса

Использование конфигурации	Обычно пакет обновления маршрута RIP имеет длину 512 байт и может содержать 25 маршрутов. Если количество обновляемых маршрутов превышает 25, более одного пакета обновления будет отправлено как можно быстрее. Когда высокоскоростное устройство отправляет много пакетов обновлений низкоскоростному устройству, низкоскоростное устройство может не успеть обработать все пакеты обновлений вовремя, что приведет к потере информации о маршрутизации. В этом случае вам необходимо запустить команду **output-delay**, чтобы увеличить задержку отправки между пакетами на высокоскоростном устройстве, чтобы низкоскоростное устройство могло получать и обрабатывать все пакеты обновления

3.4.11.6. Пример конфигурации

Настройка задержки отправки между пакетами обновления маршрута RIP

Сценарий:



Рисунок 3-20.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • Настройте задержку отправки пакетов обновлений на маршрутизаторе A
A	A# configure terminal A(config)# router rip A(config-router)# output-delay 30
Проверка	Перехватите пакеты на маршрутизаторе A и сравните время отправки пакетов обновления до и после настройки и убедитесь, что введена задержка в 30 мс

3.4.11.7. Распространенные ошибки

Для маршрутизаторов, подключенных к одной сети, значения трех таймеров RIP не совпадают.

3.4.12. Включение корреляции BFD

3.4.12.1. Эффект конфигурации

Если канал неисправен, RIP может быстро обнаружить сбой маршрута. Эта конфигурация помогает сократить время прерывания трафика.

3.4.12.2. Примечания

- Необходимо настроить основные функции RIP.
- Корреляция BFD, настроенная в режиме конфигурации интерфейса, имеет приоритет над глобальной конфигурацией.

3.4.12.3. Шаги настройки

Корреляция RIP с BFD на всех интерфейсах

- Эту настройку необходимо выполнить, если вам нужно включить корреляцию BFD.
- После включения BFD в RIP будет настроен сеанс BFD для источника информации о маршрутизации RIP (то есть адреса источника пакетов обновления маршрута RIP). При выходе из строя соседа BFD соответствующий маршрут RIP напрямую переходит в недопустимое состояние и не пересылается.
- Вы также можете запустить команду **ip ospf bfd** [**disable**] в режиме конфигурации интерфейса, чтобы включить или отключить функцию BFD на указанном интерфейсе, и эта конфигурация имеет приоритет над командой **bfd all-interfaces**, используемой в режиме конфигурации процесса маршрутизации.
- Если не требуется иное, эту настройку следует выполнять на каждом маршрутизаторе.

Корреляция RIP с BFD на интерфейсе

- Эту настройку необходимо выполнить, если вам нужно включить или отключить корреляцию BFD на указанном интерфейсе.
- Конфигурация на основе интерфейса имеет приоритет над командой **bfd all-interfaces**, используемой в режиме настройки процесса маршрутизации.
- В зависимости от реальной среды вы можете запустить команду **ip ospf bfd**, чтобы включить BFD на указанном интерфейсе для обнаружения каналов, или запустить команду **bfd all-interfaces** в режиме конфигурации процесса RIP, чтобы включить BFD на всех интерфейсах процесса OSPF, или запустите команду **ospf bfd disable**, чтобы отключить BFD на указанном интерфейсе.
- Если не требуется иное, настройте эту функцию на интерфейсе маршрутизатора, где корреляция BFD должна быть настроена отдельно.

3.4.12.4. Проверка

- Убедитесь, что сеанс BFD правильно настроен с помощью RIP.
- После сбоя соединения маршрут RIP может быстро сходиться.

3.4.12.5. Связанные команды

Корреляция RIP с BFD на всех интерфейсах

Синтаксис команды	**bfd all-interfaces**
Командный режим	Режим настройки процесса маршрутизации

Корреляция RIP с BFD на интерфейсе

Синтаксис команды	**ip rip bfd** [**disable**]
Описание параметра	**disable**: отключает BFD для обнаружения канала на указанном интерфейсе с поддержкой RIP
Командный режим	Режим настройки интерфейса
Использование конфигурации	По умолчанию корреляция BFD не настроена для указанного интерфейса, и конфигурация зависит от конфигурации, настроенной в режиме настройки процесса маршрутизации

3.4.12.6. Пример конфигурации

Включение корреляции BFD с RIP

Сценарий:



Рисунок 3-21.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • Настройте параметры BFD для интерфейсов всех маршрутизаторов. • Сопоставьте RIP с BFD на всех маршрутизаторах

A	A# configure terminal
	A(config)# interface GigabitEthernet 0/1
	A(config-if-GigabitEthernet 0/1)# bfd interval 200 min_rx 200 multiplier 5
	A(config)# router rip
	A(config-router)

B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# bfd interval 200 min_rx 200 multiplier 5 B(config)# router rip B(config-router)# bfd all-interfaces
Проверка	• На маршрутизаторах A и B убедитесь, что сеанс BFD находится в состоянии Up. • Отключите маршрутизатор B от коммутатора и убедитесь, что маршрут RIP удален на маршрутизаторе A
A	A# show ip rip peer Peer 192.168.1.2: Local address: 192.168.1.1 Input interface: GigabitEthernet 0/1 Peer version: RIPv2 Received bad packets: 0 Received bad routes: 0 BFD session state up
B	A# show ip rip peer Peer 192.168.1.1: Local address: 192.168.1.2 Input interface: GigabitEthernet 0/1 Peer version: RIPv2 Received bad packets: 0 Received bad routes: 0 BFD session state up

3.4.12.7. Распространенные ошибки

Две предыдущие команды выполняются в RIP до включения функции BFD.

3.4.13. Включение быстрого перенаправления

3.4.13.1. Эффект конфигурации

Как только RIP обнаруживает сбой маршрута, маршрутизатор может немедленно переключиться на второй лучший маршрут. Эта конфигурация помогает сократить время прерывания трафика.

3.4.13.2. Примечания

- Необходимо настроить основные функции RIP.
- Необходимо настроить карту маршрутов и резервный следующий hop.
- Чтобы ускорить конвергенцию, установите задержка пересылки интерфейса на 0 и включите корреляцию BFD с RIP.

3.4.13.3. Шаги настройки

Включение быстрого перенаправления и привязка к карте маршрута

Эту настройку необходимо выполнить, если вам нужно включить быстрое перенаправление.

Если **route-map** настроен, резервный путь может быть указан для успешно сопоставленного маршрута через карту маршрутов.

При использовании функции быстрого перенаправления RIP рекомендуется одновременно включить BFD, чтобы устройство могло быстро обнаружить любой сбой канала и, следовательно, сократить время прерывания пересылки. Если интерфейс включен или выключен, чтобы сократить время прерывания пересылки во время быстрого перенаправления RIP, вы можете настроить **carrier-delay 0** в режиме конфигурации интерфейса, чтобы достичь максимальной скорости переключения.

Если не требуется иное, эту настройку следует выполнять на каждом маршрутизаторе.

3.4.13.4. Проверка

- Резервный маршрут может быть правильно рассчитан и сгенерирован.
- При выходе из строя активного канала данные можно быстро переключить на резервный канал для пересылки.

3.4.13.5. Связанные команды

Включение быстрого перенаправления и привязка к карте маршрута

Синтаксис команды	**fast-reroute route-map** *route-map-name*
Описание параметра	*route-map-name*: указывает резервный путь на карте маршрутов
Командный режим	Режим настройки процесса маршрутизации

Использование конфигурации	В настоящее время функция быстрого перенаправления RIP подвержена следующим ограничениям: (1) для одного маршрута может быть сгенерирован только один резервный следующий hop; (2) для equal и equal-cost multi-path (ECMP) маршрутизации не может быть создан резервный следующий hop

3.4.13.6. Пример конфигурации

Включение быстрого перенаправления и привязка к карте маршрута

Сценарий:

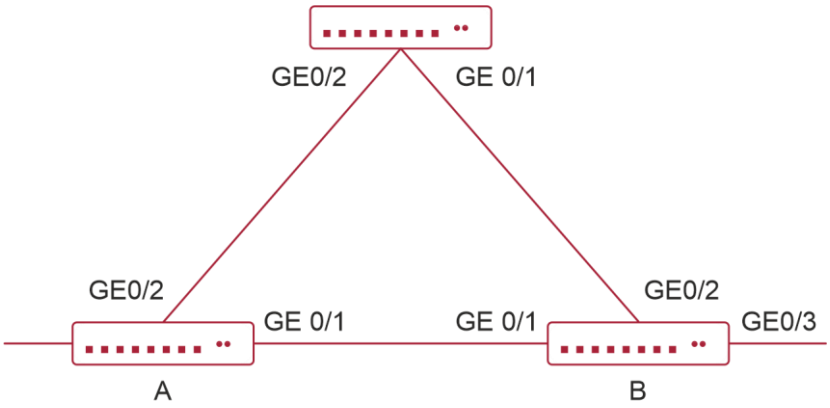


Рисунок 3-22.

IP-адреса интерфейса следующие:

A: GE0/1 192.168.1.1 GE0/2 192.168.2.1]

B: GE0/1 192.168.1.2 GE0/2 192.168.3.1 GE0/3 192.168.4.1

C: GE0/1 192.168.3.2 GE 0/2 192.168.2.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • Настройте быстрое перенаправление на маршрутизаторе A. • Настройте **carrier-delay 0** для интерфейса маршрутизатора A
A	A# configure terminal A(config)# route-map fast-reroute A(config-route-map)# match interface GigabitEthernet 0/2 A(config-route-map)# set fast-reroute backup-interface GigabitEthernet 0/1 backupnexthop 192.168.1.1 A(config)# router rip

	A(config-router)# fast-reroute route-map fast-reroute A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# carrier-delay 0 A(config-if-GigabitEthernet 0/1)# exit A(config)# interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)# carrier-delay 0
Проверка	На маршрутизаторе A проверьте таблицу маршрутизации и убедитесь, что существует резервный маршрут для записи 192.168.4.0/24
A	A# show ip route fast-reroute | begin 192.168.4.0 R 192.168.4.0/24 [ma] via 192.168.1.2, 00:39:28, GigabitEthernet 0/1 [b] via 192.168.2.2, 00:39:28, GigabitEthernet 0/2

3.4.13.7. Распространенные ошибки

- Резервный следующий hop неправильно настроен для карты маршрутов.
- Задержка пересылки не настроена для интерфейса или корреляция BFD не настроена. Следовательно, скорость переключения линии пересылки низкая.

3.4.14. Включение GR

3.4.14.1. Эффект конфигурации

- Когда распределенный маршрут переключает сервисы с активной платы на резервную, пересылка трафика продолжается и не прерывается.
- При перезапуске процесса RIP пересылка трафика продолжается и не прерывается.

3.4.14.2. Примечания

- Необходимо настроить основные функции RIP.
- Период GR как минимум в два раза превышает период обновления маршрута RIP.
- Во время процесса RIP GR убедитесь, что сетевая среда стабильна.

3.4.14.3. Шаги настройки

Настройка возможности перезапуска GR

Эту настройку необходимо выполнить, если необходимо корректно перезапустить RIP, чтобы обеспечить пересылку данных во время переключения на «горячий» резерв.

Функция GR настраивается на основе процесса RIP. Вы можете настроить разные параметры для разных процессов RIP в зависимости от фактических условий.

Период GR — это максимальное время от перезапуска процесса RIP до завершения GR. В течение этого периода таблица пересылки до перезапуска сохраняется, а маршрут RIP восстанавливается, чтобы восстановить состояние RIP перед перезапуском. По истечении периода перезапуска RIP выходит из состояния GR и выполняет общие операции RIP.

Если не требуется иное, эту настройку следует выполнять на каждом маршрутизаторе, который необходимо корректно перезапустить.

3.4.14.4. Проверка

- Запустите команду **show ip rip**, чтобы отобразить состояние GR и настроенное время.
- Запустите переключение на «горячий» резерв и убедитесь, что пересылка данных не прерывается.

3.4.14.5. Связанные команды

Настройка возможности перезапуска GR

Синтаксис команды	**graceful-restart** [**grace-period** *grace-period*]
Описание параметра	**graceful-restart**: включает функцию GR. **grace-period**: явно настраивает grace-период. *grace-period*: указывает период GR. Значение варьируется от 1 до 1800 с. Значение по умолчанию — удвоенное время обновления или 60 с, в зависимости от того, что меньше
Командный режим	Режим настройки процесса маршрутизации
Использование конфигурации	Эта команда позволяет явно изменить период GR. Обратите внимание, что GR должен быть завершен после истечения таймера обновления маршрута RIP и до истечения срока действия таймера неработоспособности маршрута RIP. Неподходящий период GR не может гарантировать бесперебойную передачу данных во время процесса GR. Типичный случай выглядит следующим образом: если период GR превышает продолжительность таймера неработоспособности, GR не завершается по истечении срока действия таймера неработоспособности. Маршрут не объявляется повторно соседу, и пересылка маршрута соседа прекращается после истечения таймера неработоспособности, что приводит к прерыванию пересылки данных в сети. Если не требуется иное, не рекомендуется корректировать период GR. Если необходимо настроить период GR, убедитесь, что период GR длиннее, чем продолжительность таймера обновления, но короче, чем продолжительность таймера неработоспособности, на основе конфигурации команды **timers basic**

3.4.14.6. Пример конфигурации

Настройка возможности перезапуска GR

Сценарий:

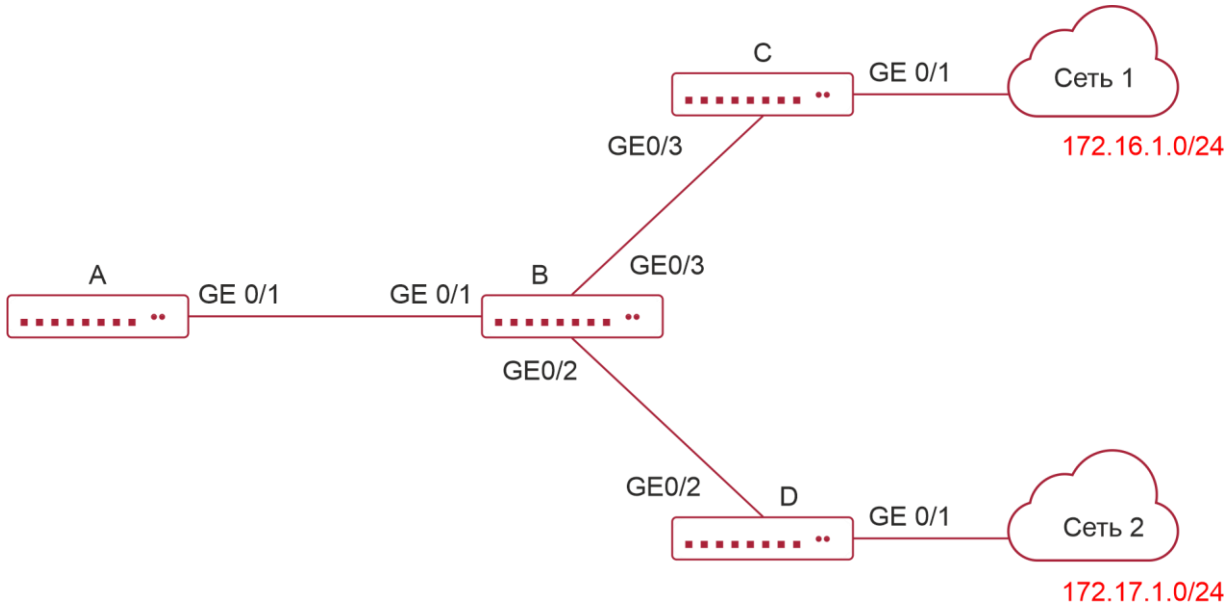


Рисунок 3-23.

IP-адреса интерфейса следующие:

A: GE 0/1 192.168.1.1

B: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 GE 0/3 192.168.3.1

C: GE 0/1 192.168.4.2 GE 0/3 192.168.3.2

D: GE 0/1 192.168.5.2 GE 0/2 192.168.2.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • На маршрутизаторе B включите функцию GR
	B# configure terminal B(config)# router rip B(config-router)# graceful-restart grace-period 90
Проверка	• Запустите переключение на горячий резерв на маршрутизаторе B и убедитесь, что таблицы маршрутизации целевой сети 1 и сети 2 остаются неизменными на маршрутизаторе A во время переключения.

	• Запустите переключение на горячий резерв на маршрутизаторе B, пропингуйте сеть назначения 1 от маршрутизатора A и убедитесь, что пересылка трафика не прерывается во время переключения

3.4.15. Включение нескольких экземпляров

3.4.15.1. Эффект конфигурации

Запустите RIP на экземплярах VPN.

3.4.15.2. Примечания

Базовые функции RIP (с параметром VRF) должны быть настроены.

3.4.15.3. Шаги настройки

Создание экземпляра VRF и ввод семейства адресов VRF IPv4

- Эту настройку необходимо выполнить, если вам нужно настроить несколько экземпляров RIP и связать эти экземпляры RIP с VRF.
- Если не требуется иное, эту настройку следует выполнять на каждом маршрутизаторе, которому требуется несколько экземпляров RIP.

Связывание RIP MIB с экземпляром VPN

- Эту настройку необходимо выполнить, если вы настраиваете несколько экземпляров RIP и хотите управлять экземплярами RIP, отличными от стандартных, с помощью MIB.
- MIB RIP не содержит информации об экземпляре RIP. Поэтому вам необходимо выполнять операции только на одном экземпляре через SNMP. По умолчанию MIB RIP связан с экземпляром RIP VRF по умолчанию, и все пользовательские операции применяются к этому экземпляру.
- Если вы хотите выполнять операции с указанным экземпляром RIP через SNMP, запустите эту команду, чтобы связать MIB с экземпляром.
- Если не требуется иное, эту настройку следует выполнять на маршрутизаторе, где экземпляр управляется с помощью MIB.

3.4.15.4. Проверка

- Проверьте таблицу маршрутизации VRF на маршрутизаторе, чтобы убедиться, что маршрут к удаленной сети можно получить через RIP.
- Используйте программное обеспечение управления MIB для управления связанным экземпляром.

3.4.15.5. Связанные команды

Создание экземпляра VRF и ввод семейства адресов VRF IPv4

Синтаксис команды	**address-family ipv4 vrf** *vrf-name*
Описание параметра	**vrf** *vrf-name*: указывает имя VRF, связанное с подрежимом конфигурации семейства адресов

Командный режим	Режим настройки процесса маршрутизации
Использование конфигурации	Запустите команду **address-family**, чтобы войти в подрежим конфигурации семейства адресов, пояснительный текст которого — (config-router-af)#. Когда VRF, связанный с подрежимом конфигурации семейства адресов, указан впервые, будет создан экземпляр RIP, соответствующий VRF. В этом подрежиме вы можете настроить информацию о маршрутизации RIP для соответствующего VRF. Чтобы выйти из подрежима конфигурации семейства адресов и вернуться в режим настройки процесса маршрутизации, выполните команду **exit-address-family** или **exit**

Выход из семейства адресов IPv4 VRF

Синтаксис команды	**exit-address-family**
Командный режим	Режим настройки семейства адресов
Использование конфигурации	Запустите эту команду в режиме настройки семейства адресов, чтобы выйти из этого режима конфигурации. Эту команду можно сократить до **exit**

Связывание RIP MIB с экземпляром VPN

Синтаксис команды	**enable mib-binding**
Командный режим	Режим настройки процесса маршрутизации

3.4.15.6. Пример конфигурации

Создание экземпляра VRF и включение сетевого управления этим экземпляром

Сценарий:



Рисунок 3-24.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции RIP на всех маршрутизаторах. (опущено) • Создайте VRF с именем «vpn1» и создайте экземпляр RIP для этого VRF. • На маршрутизаторе A свяжите MIB с экземпляром RIP vpn1
	A# configure terminal A(config)# snmp-server community public rw A(config)# ip vrf vpn1 A(config-vrf)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet0/1)# ip vrf forwarding vpn1 A(config-if-GigabitEthernet0/1)# ip address 192.168.1.1 255.255.255.0 A(config)# router rip A(config-router)# address-family ipv4 vrf vpn1 A(config-router)# enable mib-binding A(config-router-af)# network 192.168.1.0 A(config-router-af)# exit-address-family
Проверка	• Проверьте таблицу маршрутизации на маршрутизаторе A и убедитесь, что маршрут VRF 201.1.1.0/24 может быть изучен. • Прочтите и настройте параметры экземпляра RIP vpn1 с помощью инструмента MIB

	A# show ip route vrf vpn1 rip R 201.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

3.5. Мониторинг

3.5.1. Отображение

Описание	Команда
Отображает основную информацию о процессе RIP	**show ip rip**
Отображает таблицу маршрутизации RIP	**show ip rip database** [**vrf** *vrf-name*] [*network-number network-mask*] [**count**]
Отображает информацию о внешних маршрутах, перераспределяемых RIP	**show ip rip external** [**bgp** | **connected** | **isis** [*process-id*] | **ospf** *process-id* | **static**] [**vrf** *vrf-name*]
Отображает информацию об интерфейсе RIP	**show ip rip interface** [**vrf** *vrf-name*] [*interface-type interface-number*]
Отображает информацию о соседе RIP	**show ip rip peer** [*ip-address*] [**vrf** *vrf-name*]

3.5.1.1. Отладка

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

Описание	Команда
Отладка событий, происходящих во время работы процесса RIP	**debug ip rip event**
Отладка взаимодействия с процессом NSM	**debug ip rip nsm**
Отладка отправленных и полученных пакетов	**debug ip rip packet** [**interface** *interface-type interface-number* | **recv** | **send**]
Отладка процесса RIP GR	**debug ip rip restart**

Описание	Команда
Отладка изменений маршрута процесса RIP	**debug ip rip route**

4. НАСТРОЙКА OSPFV2

4.1. Обзор

Open Shortest Path First (OSPF) — это Interior Gateway Protocol (IGP), который используется в автономной системе (AS), чтобы позволить маршрутизаторам получать маршрут к удаленной сети.

ПРИМЕЧАНИЕ: OSPF версии 2 (OSPFv2) применимо к IPv4 и OSPF версии 3 (OSPFv3) применимо к IPv6. Механизм работы протокола и большинство конфигураций одинаковы.

OSPF имеет следующие характеристики:

- Широкая сфера применения: OSPF применим к более крупной сети, поддерживающей сотни маршрутизаторов.
- Быстрая конвергенция: при изменении топологии сети между маршрутизаторами можно быстро отправлять уведомления для обновления маршрутов.
- Отсутствие самозацикливания (self-loop): между маршрутизаторами синхронизируется только информация о состоянии канала. Каждый маршрутизатор самостоятельно вычисляет маршруты, поэтому самозацикливания не возникает.
- Разделение областей: большой домен маршрутизации делится на несколько небольших областей для экономии системных ресурсов и пропускной способности сети, а также обеспечения стабильности и надежности маршрутов.
- Классификация маршрутов. Маршруты подразделяются на несколько типов для обеспечения гибкого управления.
- Эквивалентные маршруты: OSPF поддерживает эквивалентные маршруты.
- Аутентификация: OSPF поддерживает аутентификацию пакетов для обеспечения безопасности взаимодействия протоколов.
- Multicast-передача: пакеты протокола отправляются с использованием multicast-адреса, чтобы избежать взаимодействия с посторонними объектами и сэкономить системные ресурсы.

ПРИМЕЧАНИЕ: в этой главе термин «маршрутизатор» относится к любому сетевому устройству, поддерживающему функцию маршрутизации. Этими сетевыми устройствами могут быть коммутаторы L3, маршрутизаторы или фаервол.

ПРИМЕЧАНИЕ: если не указано иное, «OSPF» в следующих описаниях относится к OSPFv2.

4.1.1. Протоколы и стандарты

RFC2328	В этом документе описывается версия 2 протокола OSPF. OSPF — это протокол маршрутизации состояния канала
RFC2370	В этом документе определены усовершенствования протокола OSPF для поддержки нового класса объявлений о состоянии канала (LSA), называемых непрозрачными LSA (Opaque LSA). Непрозрачные LSA предоставляют обобщенный механизм, обеспечивающий будущую расширяемость OSPF

RFC3137	В этом документе описывается техника обратной совместимости, которая может использоваться реализациями OSPF (OpenShortest Path First) для объявления о недоступности для пересылки транзитного трафика или для понижения уровня предпочтений для путей, проходящих через такой маршрутизатор
RFC3623	В этом документе описывается усовершенствование протокола маршрутизации OSPF, благодаря которому маршрутизатор OSPF может оставаться на пути пересылки даже после перезапуска его программного обеспечения OSPF
RFC3630	В этом документе описываются расширения протокола OSPF версии 2 для поддержки внутри области Traffic Engineering (TE) с использованием непрозрачных объявлений состояния канала (Opaque Link State Advertisements)
RFC3682	Использование времени жизни пакета (TTL) (IPv4) или Hop Limit (IPv6) для защиты стека протоколов от атак, основанных на загрузке ЦП, предлагалось во многих настройках
RFC3906	В этом документе описывается, как обычные протоколы маршрутизации состояния канала "hop-by-hop" взаимодействуют с новыми возможностями Traffic Engineering для создания ярлыков Interior Gateway Protocol (IGP)
RFC4576	Этот документ определяет необходимую процедуру, используя один из битов опций в LSA (Link State Advertisements), чтобы указать, что LSA уже было перенаправлено PE-ом и должно игнорироваться любыми другими PE, которые его видят
RFC4577	Этот документ расширяет эту спецификацию, позволяя использовать протокол маршрутизации на интерфейсе PE/CE в качестве протокола OSPF
RFC4750	В этом документе определяется часть базы Management Information Base (MIB) для использования с протоколами сетевого управления в сетях Интернет на основе TCP/IP. В частности, в нем определяются объекты для управления версией 2 протокола маршрутизации Open Shortest Path First. Версия 2 протокола OSPF определена для семейства адресов IPv4

4.2. Приложения

Приложение	Описание
Внутридоменное взаимодействие	OSPF работает внутри AS, которая разделена на несколько областей

Приложение	Описание
Междоменное взаимодействие	Несколько AS связаны между собой. OSPF работает внутри каждой AS, а протокол пограничного шлюза (BGP) работает между AS

4.2.1. Внутридоменное взаимодействие

4.2.1.1. Сценарий

OSPF работает внутри AS. Если количество маршрутизаторов превышает 40, рекомендуется разделить AS на несколько областей. Как правило, устройства высокого уровня, обладающие надежной производительностью и высокой скоростью обработки, развертываются в магистральной области, а устройства низкого или среднего уровня с относительно низкой производительностью могут быть развернуты в обычной области. Все обычные области должны быть подключены к магистральной области. Рекомендуется настроить обычную область, расположенную на тупиковом сетевом устройстве, как тупиковую область. Как показано на Рисунке 4-1, сеть разделена на четыре области. Связь между этими областями должна проходить через магистраль, то есть область 0.

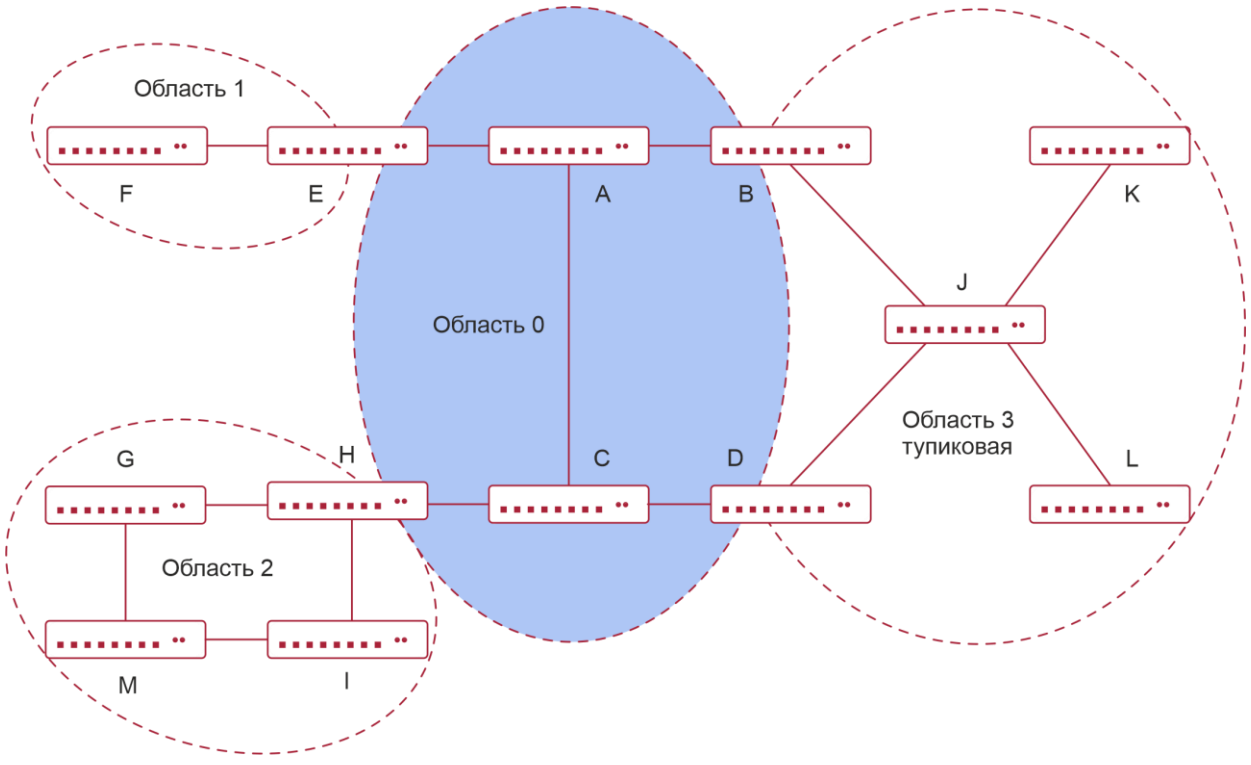


Рисунок 4-1. Отдел территорий OSPF

A, B, C, D, E и H расположены в магистральной области и являются магистральными маршрутизаторами.

Область 3 настроена как тупиковая область.

4.2.1.2. Развертывание

OSPF работает на всех маршрутизаторах в пределах AS для реализации unicast-маршрутизации.

4.2.2. Междоменное взаимодействие

4.2.2.1. Сценарий

Несколько AS связаны между собой. OSPF работает внутри каждой AS, а BGP работает между AS. Обычно OSPF и BGP изучают информацию о маршрутизации друг у друга.

Как показано на Рисунке 4-2, unicast-маршрутизация реализована в AS 100 и AS 200 использует OSPF, а между двумя AS использует BGP.

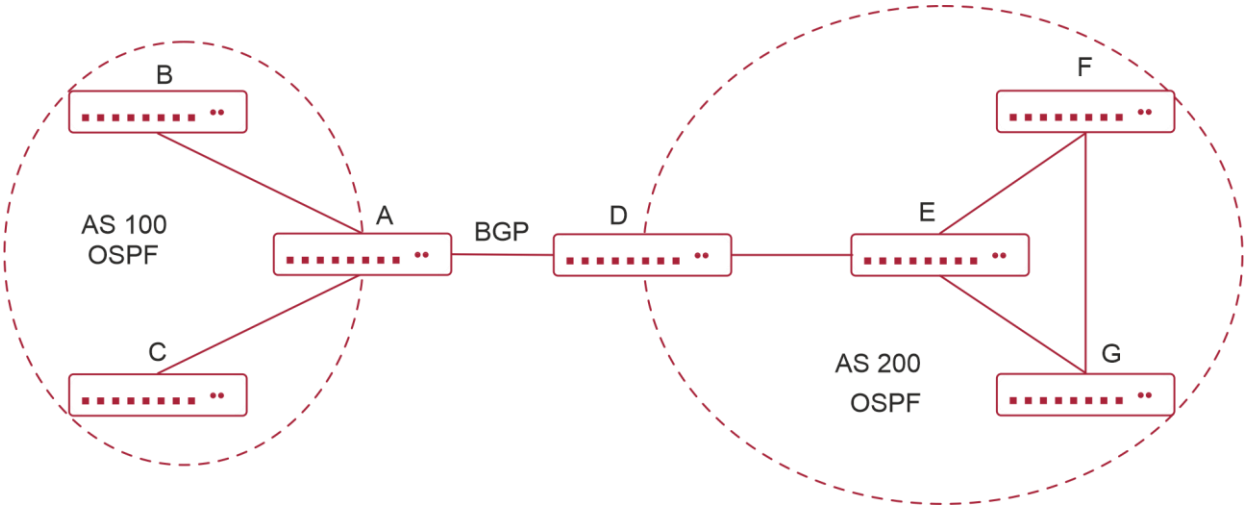


Рисунок 4-2. Взаимодействие между OSPF и BGP

OSPF и BGP работают одновременно на маршрутизаторах A и D.

4.2.2.2. Развертывание

- OSPF работает в AS 100 и AS 200 для реализации unicast-маршрутизации.
- BGP работает между двумя AS для реализации unicast-маршрутизации.

4.3. Функции

4.3.1. Базовые определения

Домен маршрутизации

Все маршрутизаторы в AS должны быть связаны между собой и использовать один и тот же протокол маршрутизации. Поэтому AS также называют доменом маршрутизации.

AS, на которой работает OSPF, также называется доменом маршрутизации OSPF или сокращенно доменом OSPF.

Процесс OSPF

OSPF поддерживает несколько экземпляров, и каждый экземпляр соответствует процессу OSPF.

На маршрутизаторе можно запустить один или несколько процессов OSPF. Каждый процесс OSPF запускает OSPF независимо, и процессы взаимно изолированы.

Идентификатор процесса действует только на локальном маршрутизаторе и не влияет на обмен пакетами OSPF на соседних интерфейсах.

Идентификатор маршрутизатора

Идентификатор маршрутизатора однозначно идентифицирует маршрутизатор в домене OSPF. Идентификаторы любых двух маршрутизаторов не могут быть одинаковыми.

Если на маршрутизаторе существует несколько процессов OSPF, каждый процесс OSPF использует один идентификатор маршрутизатора. Идентификаторы маршрутизаторов любых двух процессов OSPF не могут быть одинаковыми.

Область

OSPF поддерживает несколько областей. Домен OSPF разделен на несколько областей, чтобы облегчить вычислительную нагрузку в крупномасштабной сети.

Область представляет собой логическую группу маршрутизаторов, каждая группа идентифицируется идентификатором области. Границей между областями является маршрутизатор. Маршрутизатор может принадлежать одной или нескольким областям. Один сегмент сети (канал) может принадлежать только одной области, либо каждый интерфейс с поддержкой OSPF должен принадлежать определенной области.

Область 0 — это магистральная область, а остальные области — обычные области. Обычные области должны быть напрямую подключены к магистральной области.

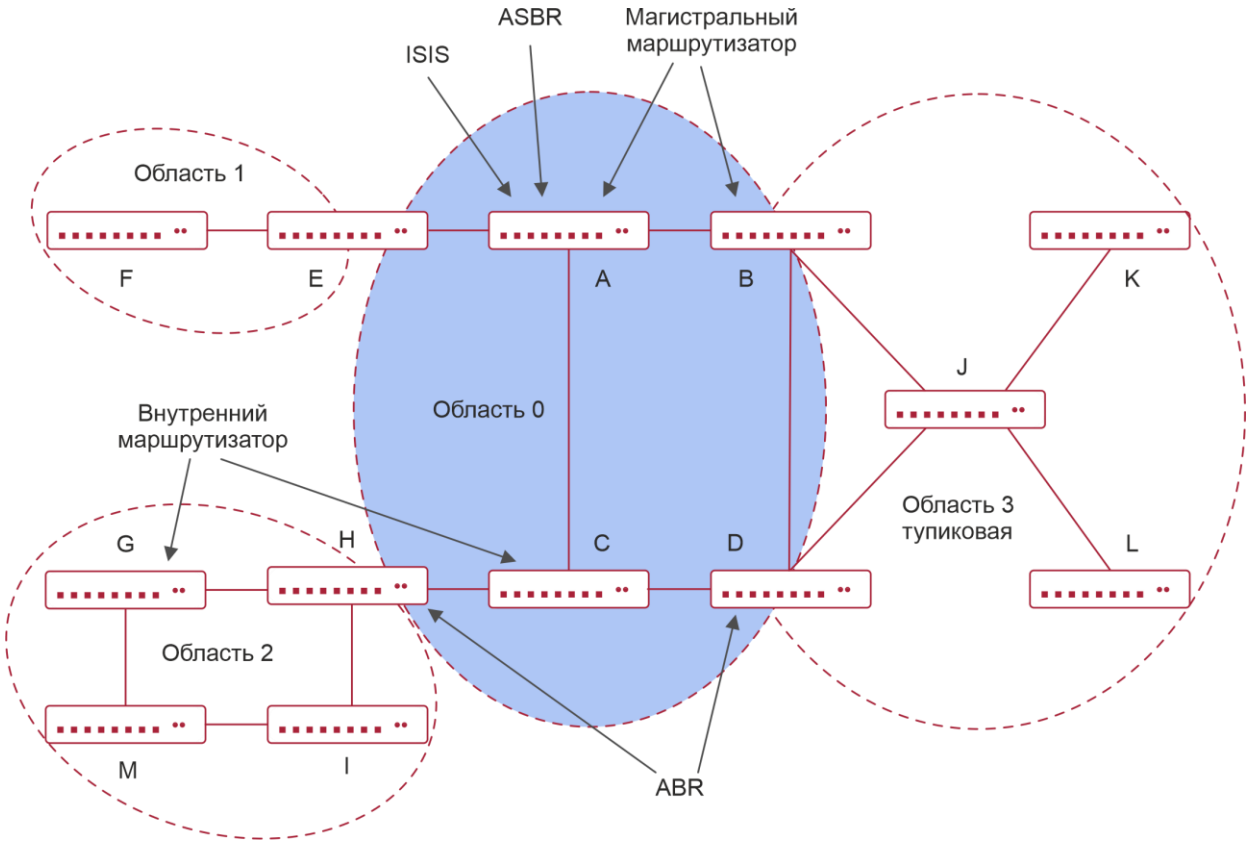


Рисунок 4-3. Разделение на области OSPF

OSPF-маршрутизатор

Следующие типы маршрутизаторов определены в OSPF и на них возложены различные обязанности:

- Внутренний маршрутизатор. Все интерфейсы интервального маршрутизатора принадлежат одной и той же области OSPF. Как показано на Рисунке 4-3, A, C, F, G, I, M, J, K и L — внутренние маршрутизаторы.
- Граничный маршрутизатор области (ABR). ABR используется для соединения магистральной области с обычной областью. ABR принадлежит двум или более областям, причем одна из областей должна быть магистральной. Как показано на Рисунке 4-3, B, D, E и H представляют собой ABR.
- Магистральный маршрутизатор. Магистральный маршрутизатор имеет по крайней мере один интерфейс, принадлежащий магистральной области. Все ABR и все маршрутизаторы в области 0 являются магистральными маршрутизаторами. Как показано на Рисунке 4-3, A, B, C, D, E и H — магистральные маршрутизаторы.
- Граничный маршрутизатор AS (ASBR). ASBR используется для обмена информацией о маршрутизации с другими AS. ASBR не обязательно расположен на границе AS. Это может быть маршрутизатор внутри области или ABR. Как показано на Рисунке 4-3, A представляет собой ASBR.

Виртуальный канал

OSPF поддерживает виртуальные каналы. Виртуальный канал — это логический канал, принадлежащий магистральной области. Он используется для решения таких проблем, как прерывистая магистральная область или невозможность прямого подключения обычной области к магистральной области в физической сети. Виртуальный канал поддерживает прохождение только одной обычной области, и эта область называется транзитной областью. Маршрутизаторы на обоих концах виртуального канала являются ABR.

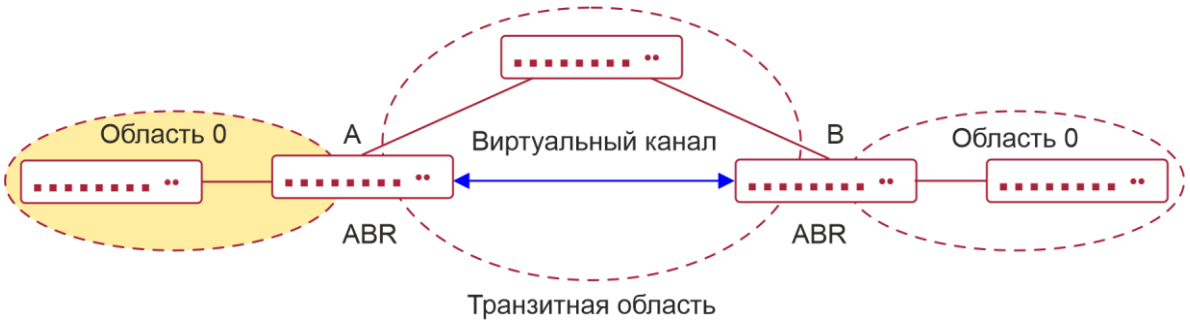


Рисунок 4-4. Прерывистая магистральная область в физической сети

Как показано на Рисунке 4-4, между A и B устанавливается виртуальный канал для соединения двух отдельных областей 0. Область 1 является транзитной областью, а A и B являются ABR области 1.

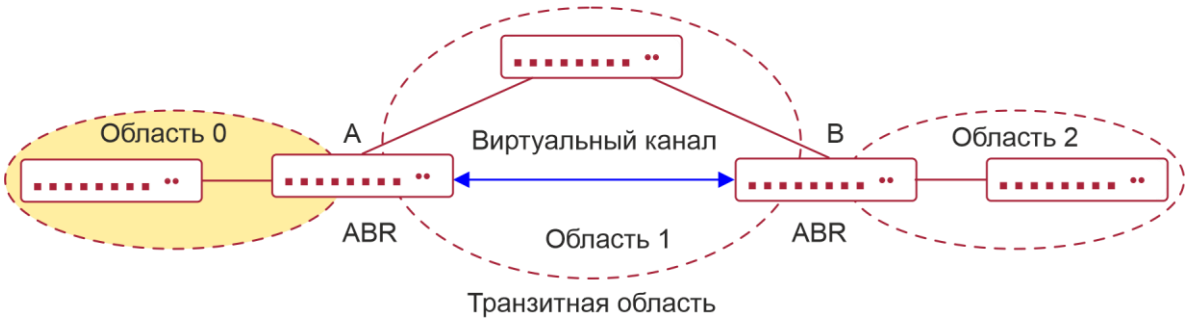


Рисунок 4-5. Невозможность прямого подключения обычной области к магистральной области физической сети

Как показано на Рисунке 4-5 между A и B устанавливается виртуальный канал для расширения области 0 до B, чтобы область 0 могла быть напрямую соединена с областью 2 на B. Область 1 — транзитная область, A — ABR области 1, а B — ABR области 0 и области 2.

LSA

OSPF описывает информацию о маршрутизации посредством объявления состояния канала (LSA).

Тип LSA	Описание
Router-LSA (тип 1)	Этот LSA создается каждым маршрутизатором. Он описывает состояние соединения и стоимость маршрутизатора и объявляется только в пределах области, где расположен исходный маршрутизатор
Network-LSA (тип 2)	Этот LSA генерируется назначенным маршрутизатором (DR) в сети NBMA. Он описывает состояние соединения в текущем сегменте сети и объявляется только в пределах области, где находится DR
Network-summary-LSA (тип 3)	Это LSA создано ABR. Он описывает маршрут в другую область и объявляется областям, за исключением полностью тупиковых или Not-So-Stubby Area (NSSA)
ASBR-summary-LSA (тип 4)	Это LSA создано ABR. Он описывает маршрут к ASBR и объявляются областям, за исключением областей, где расположен ASBR
AS-external-LSA (тип 5)	Это LSA создано ABR. Он описывает маршрут к пункту назначения за пределами AS и объявляются всем областям, за исключением тупиковых областей и NSSA

Тип LSA	Описание
NSSA LSA (тип 7)	Это LSA создано ABR. Он описывает маршрут к пункту назначения за пределами AS и объявляются только в пределах областей NASSA
Opaque LSA (тип 9/ тип 10/тип 11)	Непрозрачные LSA предоставляют обобщенный механизм, обеспечивающий будущую расширяемость OSPF, при этом: • LSA типа 9 объявляются только в том сегменте сети, где расположены интерфейсы. Grace LSA используется для поддержки плавной перезагрузки (GR) и является одним из LSA типа 9. • LSA типа 10 объявляются в пределах области. LSA, используемый для поддержки Traffic Engineering (TE), является одним из LSA типа 10. • LSA типа 11 объявляются в рамках AS. В настоящее время примеров применения LSA типа 11 нет

ПРИМЕЧАНИЕ: тупиковые области, области NSSA, полностью тупиковые области и полностью NSSA-области представляют собой особые формы обычных областей и помогают снизить нагрузку на маршрутизаторы и повысить надежность маршрутов OSPF.

Пакет OSPF

В следующей таблице перечислены пакеты протоколов, которые использует OSPF. Эти пакеты OSPF инкапсулируются в IP-пакеты и передаются в multicast- или unicast-режиме.

Тип пакета	Описание
Hello	Пакеты Hello периодически отправляются для обнаружения и поддержания отношений соседства OSPF
Database Description (DD)	Пакеты DD содержат краткую информацию о локальной базе данных состояния каналов (LSDB) и используются для синхронизации LSDB между соседями OSPF
Link State Request (LSR)	Пакеты LSR используются для запроса необходимых LSA от соседей. Пакеты LSR отправляются только после успешного обмена пакетами DD между соседями OSPF
Link State Update (LSU)	Пакеты LSU используются для отправки требуемых LSA peer-ам
Link State Acknowledgment (LSAck)	Пакеты LSAck используются для подтверждения полученных LSA

4.3.2. Обзор

Особенность	Описание
Протоколы маршрутизации по состоянию канала	Запустите OSPF на маршрутизаторе для получения маршрутов к различным пунктам назначения в сети
Управление маршрутами OSPF	Планируйте или оптимизируйте маршруты OSPF с помощью ручной настройки для реализации управления маршрутами OSPF
Повышенная безопасность и надежность	Используйте такие функции, как аутентификация и корреляция обнаружения двунаправленной пересылки (BFD) для повышения безопасности, стабильности и надежности OSPF
Управление сетью	Используйте такие функции, как база данных управления (MIB) и системный журнал (Syslog), для облегчения управления OSPF

4.3.3. Протоколы маршрутизации по состоянию канала

OSPF — это тип протоколов маршрутизации по состоянию канала. Процесс его работы следующий:

- Обнаружение соседей → Двунаправленная связь

Между соседними маршрутизаторами устанавливаются отношения соседства OSPF, и поддерживается двунаправленная связь.

- Синхронизация базы данных → Полная смежность (полное соседство)

Маршрутизатор использует LSA для объявления всех состояний своих каналов. Между соседями происходит обмен LSA, а база данных состояний каналов (LSDB) синхронизируется для достижения полной смежности.

- Вычисление Shortest Path Tree (SPT) → Формирование таблицы маршрутизации

Маршрутизатор вычисляет кратчайший путь до каждой сети назначения на основе LSDB и формирует таблицу маршрутизации OSPF.

4.3.3.1. Принцип работы

Обнаружение соседей → Двунаправленная связь

Маршрутизаторы отправляют пакеты Hello через все интерфейсы с поддержкой OSPF (или виртуальные каналы). Если два маршрутизатора могут обмениваться пакетами Hello и параметры, передаваемые в пакетах Hello, могут быть успешно согласованы, два маршрутизатора становятся соседями. Маршрутизаторы, являющиеся взаимно соседями, находят свои собственные идентификаторы маршрутизаторов из пакетов Hello, отправленных от соседей, и устанавливается двусторонняя связь.

Пакет Hello включает в себя, помимо прочего, следующую информацию:

- Идентификатор исходного маршрутизатора
- Идентификатор области интерфейса исходного маршрутизатора (или виртуального канала)

- Маска подсети исходного интерфейса маршрутизатора (или виртуального канала)
- Информация аутентификации интерфейса исходного маршрутизатора (или виртуального канала)
- Интервал Hello интерфейса исходного маршрутизатора (или виртуального канала)
- Интервал dead соседа интерфейса исходного маршрутизатора (или виртуального канала)
- Приоритет интерфейса исходного маршрутизатора (используется для выбора DR/BDR)
- IP-адреса DR и назначенного резервного маршрутизатора (BDR)
- Идентификатор маршрутизатора соседа исходного маршрутизатора

Синхронизация базы данных → Полная смежность

После установки двунаправленной связи между соседними маршрутизаторами пакеты DD, LSR, LSU и LSAck используются для обмена LSA и настройки смежности. Краткий процесс выглядит следующим образом:

- Маршрутизатор генерирует LSA для описания всех состояний каналов на маршрутизаторе.
- LSA обменивается между соседями. Когда маршрутизатор получает LSA от своего соседа, он копирует LSA и сохраняет копию в локальной базе данных LSDB, а затем объявляет LSA другим соседям.
- Когда маршрутизатор и его соседи получают один и тот же LSDB, достигается полная смежность.

ПРИМЕЧАНИЕ: OSPF будет работать очень тихо без изменений в стоимости канала или добавления или удаления сети. Если происходят какие-либо изменения, измененные состояния каналов объявляются для быстрой синхронизации LSDB.

SPT-вычисление → Формирование таблицы маршрутизации

После получения полной LSDB от маршрутизатора запускается алгоритм Dijkstra для генерации SPT от локального маршрутизатора к каждой сети назначения. SPT записывает сети назначения, адреса следующего hop-а и стоимость. OSPF генерирует таблицу маршрутизации на основе SPT.

Если произойдут изменения в стоимости каналов, добавлении или удалении сети, LSDB будет обновлена. Маршрутизатор снова запускает алгоритм Dijkstra, генерирует новый SPT и обновляет таблицу маршрутизации.

ПРИМЕЧАНИЕ: алгоритм Dijkstra используется для поиска кратчайшего пути от вершины (вертекса) к другим вершинам (вертексам) во взвешенном ориентированном графе.

Типы сетей OSPF

Маршрутизатору не обязательно обмениваться LSA с каждым соседом и настраивать смежность с каждым соседом. Чтобы повысить эффективность, OSPF классифицирует сети, использующие различные протоколы канального уровня, на пять типов, чтобы обмен LSA осуществлялся разными способами для настройки смежности:

- Broadcast

Соседи обнаружены, выбраны DR и BDR. DR (или BDR) обменивается LSA со всеми другими маршрутизаторами для настройки смежности. За исключением DR и BDR, все остальные маршрутизаторы не обмениваются LSA друг с другом, и смежность не настроена. Ethernet и оптоволоконный распределенный интерфейс данных (FDDI) по умолчанию относятся к типу сети broadcast.

- Non-broadcast multiple access (NBMA)

Соседи настраиваются вручную, и выбираются DR и BDR. DR (или BDR) обменивается LSA со всеми другими маршрутизаторами для настройки смежности. За исключением DR и BDR, все остальные маршрутизаторы не обмениваются LSA друг с другом, и смежность не настроена. X.25, Frame Relay и ATM по умолчанию принадлежат сетям NBMA.

- Point-to-point («точка-точка») (P2P)

Соседи обнаруживаются автоматически, а DR или BDR не выбираются. LSA обмениваются между маршрутизаторами на обоих концах канала и устанавливается смежность. PPP, HDLC и LAPB по умолчанию относятся к типу сети P2P.

- Point-to-multipoint («точка-многоточка») (P2MP)

Соседи обнаруживаются автоматически, а DR или BDR не выбираются. Между любыми двумя маршрутизаторами происходит обмен LSA и устанавливается смежность. Сети без какого-либо протокола канального уровня относятся к типу сети P2MP по умолчанию.

- P2MP broadcast

Соседи настраиваются вручную, а DR или BDR не выбираются. Между любыми двумя маршрутизаторами происходит обмен LSA, и устанавливается смежность. Сети без какого-либо протокола канального уровня по умолчанию относятся к типу сети P2MP.

Типы маршрутов OSPF

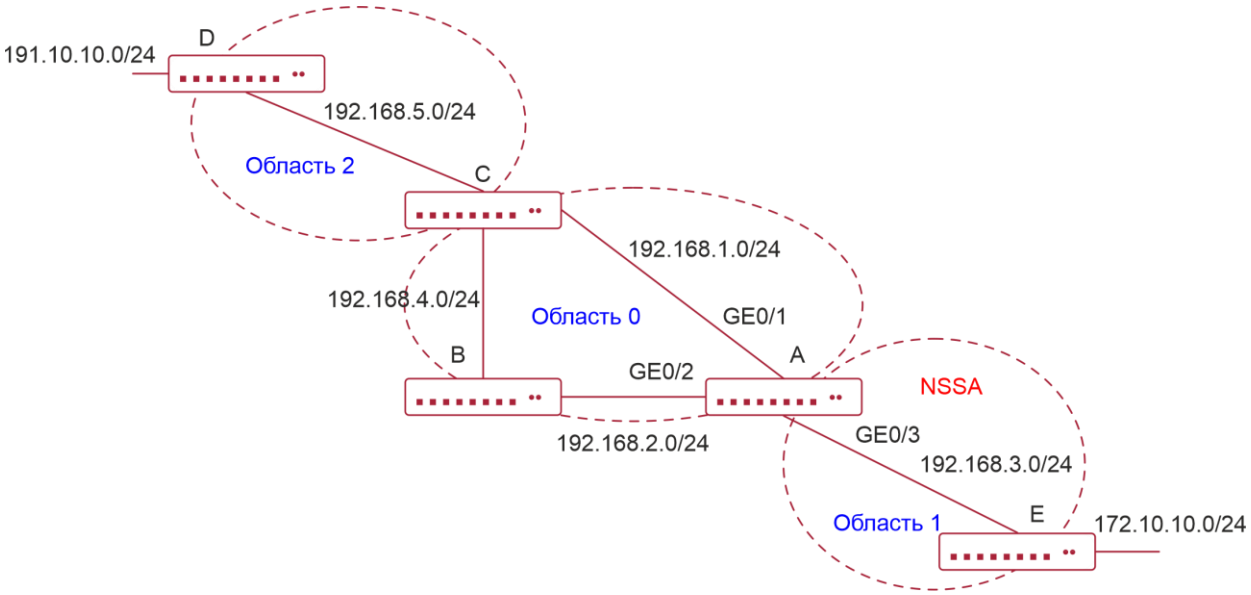


Рисунок 4-6.

Отобразите маршруты OSPF (отмечены красным) в таблице маршрутизации маршрутизатора A.

```
A#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
O N2 172.10.10.0/24 [110/20] via 192.168.3.2, 00:01:00,GigabitEthernet 0/3
O E2 191.10.10.0/24 [110/20] via 192.168.1.2, 01:11:26,GigabitEthernet 0/1
C 192.168.1.0/24 is directly connected,GigabitEthernet 0/1
C 192.168.1.1/32 is local host.
C 192.168.2.0/24 is directly connected,GigabitEthernet 0/2
C 192.168.2.1/32 is local host.
C 192.168.3.0/24 is directly connected,GigabitEthernet 0/3
C 192.168.3.1/32 is local host.
O 192.168.4.0/24 [110/2] via 192.168.2.2, 00:00:02,GigabitEthernet 0/2
O IA 192.168.5.0/24 [110/3] via 192.168.1.2, 00:01:02,GigabitEthernet 0/1
```

Перед каждым маршрутом OSPF отображается метка, указывающая тип маршрута. Существует шесть типов маршрутов OSPF:

- O: внутриобластной маршрут. Этот тип маршрута описывает, как добраться до сети назначения в локальной области. Стоимость этого типа маршрута равна стоимости маршрута от локального маршрутизатора до сети назначения.
- IA: маршрут между областями. Этот тип маршрута описывает, как добраться до сети назначения в другой области. Стоимость этого типа маршрута равна стоимости маршрута от локального маршрутизатора до сети назначения.
- E1: внешний маршрут типа 1. Этот тип маршрута описывает, как добраться до сети назначения за пределами AS. Стоимость этого типа маршрута равна стоимости маршрута от локального маршрутизатора до ASBR плюс стоимость маршрута от ASBR до сети назначения. Этот тип маршрута не существует на маршрутизаторах в тупиковой области или области NSSA.
- E2: внешний маршрут типа 2. Этот тип маршрута описывает, как добраться до сети назначения за пределами AS. Стоимость этого типа маршрута равна стоимости маршрута от ASBR до сети назначения. Этот тип маршрута не существует на маршрутизаторах в тупиковой области или области NSSA.
- N1: внешний маршрут типа 1 области NSSA. Этот тип маршрута описывает, как добраться до сети назначения за пределами AS через ASBR в области NSSA. Стоимость этого типа маршрута равна стоимости маршрута от локального маршрутизатора до ASBR плюс стоимость маршрута от ASBR до сети назначения. Этот тип маршрута существует только на маршрутизаторах в области NSSA.
- N2: внешний маршрут типа 2 области NSSA. Этот тип маршрута описывает, как добраться до сети назначения за пределами AS через ASBR в области NSSA. Стоимость этого типа маршрута равна стоимости маршрута от ASBR до сети назначения. Этот тип маршрута существует только на маршрутизаторах в области NSSA.

ПРИМЕЧАНИЕ: надежность маршрутов E2 и N2 низкая. OSPF считает, что стоимость маршрута от ASBR до пункта назначения за пределами AS намного превышает стоимость маршрута к ASBR внутри AS. Таким образом, при вычислении стоимости маршрута учитывается только стоимость маршрута от ASBR до пункта назначения за пределами AS.

4.3.3.2. Сопутствующая конфигурация

Включение OSPF

OSPF отключен по умолчанию.

Запустите команду **router ospf** 1, чтобы создать процесс OSPF на маршрутизаторе.

Запустите команду **network area**, чтобы включить OSPF на интерфейсе, и укажите идентификатор области.

Запустите команду **area virtual-link**, чтобы создать виртуальный канал на маршрутизаторе. Виртуальный канал можно рассматривать как логический интерфейс.

Идентификатор маршрутизатора

По умолчанию процесс OSPF выбирает наибольший IP-адрес среди IP-адресов всех loopback-интерфейсов в качестве идентификатора маршрутизатора. Если loopback-интерфейсы, настроенные с IP-адресами, недоступны, процесс OSPF выбирает наибольший IP-адрес среди IP-адресов всех loopback-интерфейсов в качестве идентификатора маршрутизатора.

Альтернативно вы можете запустить команду **router-id**, чтобы вручную указать идентификатор маршрутизатора.

Параметры управления протоколом

Запустите команду **ip ospf hello-interval**, чтобы изменить интервал Hello на интерфейсе. Значение по умолчанию — 10 с (или 30 с для сетей NBMA).

Запустите команду **ip ospf dead-interval**, чтобы изменить dead-интервал соседа на интерфейсе. Значение по умолчанию в четыре раза превышает интервал Hello.

Используйте параметр **poll-interval** в команде **neighbor**, чтобы изменить интервал опроса соседей на интерфейсе NBMA. Значение по умолчанию — 120 с.

Запустите команду **ip ospf transmit-delay**, чтобы изменить задержку передачи пакетов LSU на интерфейсе. Значение по умолчанию — 1 с.

Запустите команду **ip ospf retransmit-interval**, чтобы изменить интервал повторной передачи пакетов LSU на интерфейсе. Значение по умолчанию — 5 с.

Используйте параметр **hello-interval** в команде **area virtual-link**, чтобы изменить интервал Hello для виртуального канала. Значение по умолчанию — 10 с.

Используйте параметр **dead-interval** в команде **area virtual-link**, чтобы изменить dead-интервал соседа в виртуальном канале. Значение по умолчанию в четыре раза превышает интервал Hello.

Используйте параметр **transmit-delay** в команде **area virtual-link**, чтобы изменить задержку передачи пакетов LSU по виртуальному каналу. Значение по умолчанию — 1 с.

Используйте параметр **retransmit-interval** в команде **area virtual-link**, чтобы изменить интервал повторной передачи пакетов LSU по виртуальному каналу. Значение по умолчанию — 5 с.

Запустите команду **timers throttle lsa all**, чтобы изменить параметры алгоритма экспоненциальной задержки, генерирующего LSA. Значения этих параметров по умолчанию: 0 мс, 5000 мс и 5000 мс.

Запустите команду **timerspacinglsa-group**, чтобы изменить интервал обновления группы LSA. Значение по умолчанию — 30 с.

Запустите команду **timers pacing lsa-transmit**, чтобы изменить интервал отправки пакетов LS-UPD и количество отправленных пакетов LS-UPD. Значения по умолчанию: 40 мс и 1.

Запустите команду **timers lsa arrival**, чтобы изменить задержку, после которой будет получен тот же LSA. Значение по умолчанию — 1000 мс.

Запустите команду **timers throttle spf**, чтобы изменить задержку вычислений SPT, минимальный интервал между двумя вычислениями SPT и максимальный интервал между двумя вычислениями SPT. Значения по умолчанию: 1000 мс, 5000 мс и 10 000 мс.

Типы сетей OSPF

По умолчанию Ethernet и FDDI относятся к типу broadcast, X.25, Frame Relay и ATM относятся к типу NBMA, а PPP, HDLC и LAPB относятся к типу P2P.

Запустите команду **ip ospf network**, чтобы вручную указать тип сети интерфейса.

Запустите команду **neighbor**, чтобы вручную указать соседа. Для типов NBMA и P2MP non-broadcast необходимо вручную указать соседей.

Запустите команду **ip ospf priority**, чтобы настроить приоритеты интерфейсов, которые используются для выбора DR/BDR. Выбор DR/BDR необходим для типов broadcast и NBMA. В выборах побеждает маршрутизатор с наивысшим приоритетом, а маршрутизатор с приоритетом 0 в выборах не участвует. Значение по умолчанию — 1.

4.3.4. Управление маршрутами OSPF

Планируйте или оптимизируйте маршруты OSPF с помощью ручной настройки для реализации управления маршрутами OSPF.

4.3.4.1. Принцип работы

(Полностью) Тупиковая область и (Полностью) Область NSSA

Области (полностью) тупиковые и (полностью) NSSA помогают снизить нагрузку на взаимодействие протоколов и размер таблицы маршрутизации.

- Если соответствующая область настроена как (полностью) тупиковая область или область NSSA, можно избежать объявления большого количества LSA типа 5 и типа 3 внутри этой области.

Область	LSA тип1 и тип2	LSA типа 3	LSA типа 4	LSA типа 5	LSA тип 7
Не (полностью) тупиковая область и область NSSA	Допускается	Допускается	Допускается	Допускается	Не допуска-ется

Область	LSA тип1 и тип2	LSA типа 3	LSA типа 4	LSA типа 5	LSA тип 7
Тупиковая область	Допускается	Допускается (содержит один маршрут по умолчанию)	Не допускается	Не допускается	Не допуска-ется
Полностью тупиковая область	Допускается	Разрешен только один маршрут по умолчанию	Не допускается	Не допускается	Не допуска-ется
Область NSSA	Допускается	Допускается (содержит один маршрут по умолчанию)	Допускается	Не допускается	Допуска-ется
Полностью область NSSA	Допускается	Разрешен только один маршрут по умолчанию	Допускается	Не допускается	Допуска-ется

ПРИМЕЧАНИЕ: ABR использует LSA типа 3 для объявления маршрута по умолчанию к (полностью) тупиковой области или области NSSA.

ПРИМЕЧАНИЕ: ABR преобразует LSA типа 7 в области NSSA в LSA типа 5 и объявляет LSA типа 5 в магистральной области.

- Если область соответствующим образом настроена как (полностью) тупиковая область или область NSSA, большое количество маршрутов E1, E2 и IA не будет добавлено в таблицу маршрутизации маршрутизатора в этой области.

Область	Маршруты, доступные в таблице маршрутизации маршрутизатора внутри области
Не (полностью) тупиковая область и область NSSA	O: маршрут к сети назначения в локальной области. IA: маршрут к сети назначения в другой области. E1 или E2: маршрут или маршрут по умолчанию к целевому сегменту сети за пределами AS (через любой ASBR в AS)
Тупиковая область	O: маршрут к сети назначения в локальной области. IA: маршрут или маршрут по умолчанию к сети назначения в другой области

Область	Маршруты, доступные в таблице маршрутизации маршрутизатора внутри области
Полностью тупиковая область	O: маршрут к сети назначения в локальной области. IA: маршрут по умолчанию
Область NSSA	O: маршрут к сети назначения в локальной области. IA: маршрут или маршрут по умолчанию к сети назначения в другой области. N1 или N2: маршрут или маршрут по умолчанию к целевому сегменту сети за пределами AS (через любой ASBR в локальной области)
Полностью Область NSSA	O: маршрут к сети назначения в локальной области. IA: маршрут по умолчанию. N1 или N2: маршрут или маршрут по умолчанию к целевому сегменту сети за пределами AS (через любой ASBR в локальной области)

Перераспределение маршрутов

Перераспределение маршрутов — это процесс введения маршрутов других протоколов маршрутизации, маршрутов других процессов OSPF, статических маршрутов и прямых маршрутов, существующих на устройстве, в процесс OSPF, чтобы эти маршруты можно было объявлять соседям с использованием LSA типов 5 и 7. Маршрут по умолчанию не может быть введен во время перераспределения маршрута.

Перераспределение маршрутов часто используется для взаимодействия между AS. Вы можете настроить перераспределение маршрутов в ASBR для объявления маршрутов за пределами AS внутрь AS или маршрутов внутри AS во внешнюю часть AS.

Введение маршрута по умолчанию

Настроив команду в ASBR, вы можете ввести маршрут по умолчанию для процесса OSPF, чтобы этот маршрут можно было объявлять соседям с помощью LSA типа 5 и типа 7.

Введение маршрута по умолчанию часто используется для взаимодействия между AS. Один маршрут по умолчанию используется для замены всех маршрутов за пределами AS.

Суммирование маршрутов

Суммирование маршрутов — это процесс объединения информации о маршрутах с одним и тем же префиксом в один маршрут и объявления суммированного маршрута соседям (замена большого количества отдельных маршрутов). Суммирование маршрутов помогает снизить нагрузку на взаимодействие протоколов и размер таблицы маршрутизации.

По умолчанию ABR объявляет информацию о маршрутизации между областями с помощью LSA типа 3 в сегменте сети и объявляет информацию о перераспределенной маршрутизации с помощью LSA типа 5 и 7. Если существуют непрерывные сегменты сети, рекомендуется настроить суммирование маршрутов.

При настройке суммирования маршрутов диапазон суммирования может превышать фактическую сеть маршрутов. Если данные отправляются в сеть за пределами диапазона суммирования, может образоваться петля маршрутизации и увеличиться нагрузка на обработку маршрутизатора. Чтобы предотвратить эти проблемы, ABR или ASBR автоматически добавляет отброшенный маршрут в таблицу маршрутизации. Этот маршрут не будет объявляться.

Фильтрация маршрутов

OSPF поддерживает фильтрацию маршрутов для обеспечения безопасности и облегчения контроля при изучении, обмене или использовании информации о маршрутизации.

С помощью команд конфигурации вы можете настроить фильтрацию маршрутов для следующих элементов:

- Интерфейс: интерфейсу запрещено отправлять информацию о маршрутизации (любые LSA) или обмениваться информацией о маршрутизации (любые LSA) с соседями.
- Информация о маршрутизации, объявляемая между областями: в другую область может быть объявлена только та информация о маршрутизации, которая соответствует условиям фильтрации (LSA типа 3).
- Информация о маршрутизации вне AS: только та информация о маршрутизации, которая соответствует условиям фильтрации, может быть перераспределена в процесс OSPF (LSA типа 5 и типа 7).
- LSA, полученные маршрутизатором: в таблице маршрутизации OSPF могут объявляться только те маршруты, которые рассчитываются на основе LSA, соответствующих условиям фильтрации.

Стоимость маршрута

Если в сети существуют резервные каналы или устройства, может существовать несколько путей от локального устройства к сети назначения. OSPF выбирает путь с минимальной общей стоимостью для формирования маршрута OSPF. Общая стоимость пути равна сумме стоимостей отдельных каналов на этом пути. Общую стоимость пути можно минимизировать путем изменения стоимости отдельных каналов на этом пути. Таким образом, OSPF выбирает этот путь для формирования маршрута.

Используя команды конфигурации, вы можете изменить стоимость канала:

- Стоимость перехода от интерфейса к напрямую подключенному сегменту сети и стоимость от интерфейса к соседу.
- Стоимость перехода от ABR к сегменту сети межобластного суммирования и стоимость от ABR к сегменту сети по умолчанию.
- Стоимость перехода от ASBR к сегменту внешней сети и стоимость от ASBR к сегменту сети по умолчанию.

ПРИМЕЧАНИЕ: и стоимость, и метрика указывают стоимость и не отличаются друг от друга.

Административное расстояние OSPF

Административное расстояние (AD) оценивает надежность маршрута. Его значение представляет собой целое число от 0 до 255. Меньшее значение AD указывает на то, что маршрут заслуживает большего доверия. Если к одному и тому же пункту назначения существует несколько маршрутов, маршрут предпочтительно выбирает маршрут с меньшим значением AD. Маршрут с большим значением AD становится плавающим маршрутом, то есть резервным маршрутом оптимального маршрута.

По умолчанию маршрут, исходящий из одного источника, соответствует значению AD. Значение AD является местным понятием. Изменение значения AD влияет на выбор маршрута только на текущем маршрутизаторе.

Источник маршрута	AD по умолчанию
Напрямую подключенная сеть	0
Статический маршрут	1
EBGP-маршрут	20
Маршрут OSPF	110
IS-IS-маршрут	115
RIP-маршрут	120
IBGP-маршрут	200
Недоступный маршрут	255

4.3.4.2. Сопутствующая конфигурация

Тупиковая область и область NSSA

По умолчанию тупиковая область или область NSSA не настроены.

Запустите команду **area stub**, чтобы настроить указанную область как тупиковую.

Запустите команду **area nssa**, чтобы настроить указанную область как область NSSA.

ПРИМЕЧАНИЕ: магистральную область нельзя настроить как тупик или область NSSA.

ПРИМЕЧАНИЕ: транзитную область (с проходящими сквозь виртуальными каналами) нельзя настроить как тупиковую или как зону NSSA.

ПРИМЕЧАНИЕ: область, содержащая ASBR, не может быть настроена как тупиковая область.

Перераспределение маршрутов и введение маршрута по умолчанию

По умолчанию маршруты не перераспределяются и маршрут по умолчанию не вводится.

Запустите команду **redistribute**, чтобы настроить перераспределение маршрутов.

Запустите команду **default-information originate**, чтобы ввести маршрут по умолчанию.

После настройки перераспределения маршрутов и введения маршрута по умолчанию маршрут автоматически становится ASBR.

Суммирование маршрутов

По умолчанию маршруты не суммируются. Если настроено суммирование маршрутов, автоматически будет добавлен отброшенный маршрут.

Запустите команду **arearange**, чтобы суммировать маршруты, распределенные между областями (LSA типа 3) на ABR.

Запустите команду **summary-address**, чтобы суммировать перераспределенные маршруты (LSA типа 5 и типа 7) на ASBR.

Запустите команду **discard-route**, чтобы добавить отброшенный маршрут в таблицу маршрутизации.

Фильтрация маршрутов

По умолчанию маршруты не фильтруются.

Запустите команду **passive-interface**, чтобы настроить пассивный интерфейс. Информацией о маршрутизации (любые LSA) нельзя обмениваться на пассивном интерфейсе.

Запустите команду **ip ospfdatabase-filter all out**, чтобы запретить интерфейсу отправлять информацию о маршрутизации (любые LSA).

Запустите команду **area filter-list**, чтобы отфильтровать информацию о маршрутизации, объявленную между областями на ABR. Только та информация о маршрутизации, которая соответствует условиям фильтрации, может быть объявлена в другую область (LSA типа 3).

Используйте параметр **area filter-list** в команде **redistribute** или используйте команду **area filter-list** для фильтрации внешней информации о маршрутизации AS на ASBR. Только та информация о маршрутизации, которая соответствует условиям фильтрации, может быть перераспределена в процесс OSPF (LSA типа 5 и типа 7).

Запустите команду **distribute-list in**, чтобы отфильтровать LSA, полученные маршрутизатором. В таблице маршрутизации OSPF могут объявляться только те маршруты, которые рассчитываются на основе LSA, соответствующих условиям фильтрации.

Стоимость маршрута

- Стоимость от интерфейса до сегмента сети с прямым подключением (стоимость на интерфейсе). Значением по умолчанию является автоматическая стоимость. Автоматическая стоимость = эталонная полоса пропускания/пропускная способность интерфейса. Запустите команду **auto-costreference-bandwidth**, чтобы установить эталонную полосу пропускания для автоматической стоимости. Значение по умолчанию — 100 Мбит/с. Запустите команду **ip ospf cost**, чтобы вручную установить стоимость интерфейса. Приоритет конфигурации этого элемента выше, чем у автоматической стоимости.
- Стоимость от интерфейса до указанного соседа (то есть стоимость от локального устройства до указанного соседа). Значением по умолчанию является автоматическая стоимость. Используйте параметр **cost** в команде **neighbor**, чтобы изменить стоимость от интерфейса до указанного соседа. Приоритет конфигурации этого пункта выше, чем стоимость интерфейса. Этот элемент конфигурации применим только к интерфейсам типа P2MP.
- Стоимость от ABR до сегмента сети межобластного суммирования (то есть стоимость суммированного межобластного маршрута). Если маршрутизация OSPF совместима с RFC1583, значением по умолчанию — это минимальная стоимость среди всех стоимостей суммированных каналов; в противном случае значением по умолчанию будет максимальная стоимость среди всех стоимостей суммированных каналов. Запустите команду **compatible rfc1583**, чтобы сделать маршрутизацию OSPF совместимой с RFC1583. По умолчанию маршрутизация

OSPF совместима с RFC1583. Используйте параметр **cost** в команде **area range**, чтобы изменить стоимость суммирования маршрутов между областями.

- Стоимость от ABR до сегмента сети по умолчанию (то есть стоимость маршрута по умолчанию, который автоматически объявляется ABR до тупиковой области или области NSSA). Значение по умолчанию — 1. Запустите команду **area default-cost**, чтобы изменить стоимость маршрута по умолчанию, который ABR автоматически объявляет тупиковым областям или NSSA.
- Стоимость от ASBR до сегмента внешней сети (то есть метрика внешнего маршрута) По умолчанию метрика перераспределяемого маршрута BGP равна 1, метрика других типов перераспределяемых маршрутов равна 20, а тип маршрута — Внешний тип 2. Запустите команду **default-metric**, чтобы изменить метрику по умолчанию внешнего маршрута. Используйте параметры **metric**,**metric-type** и **route-map** в команде **redistribute**, чтобы изменить метрику и тип маршрута внешнего маршрута.
- Стоимость от ASBR до сегмента сети по умолчанию (то есть метрика маршрута по умолчанию, введенная вручную). По умолчанию метрика равна 1, а тип маршрута — Внешний тип 2. Используйте параметры **metric**,**metric-type** и **route-map** в команде **default-information originate**, чтобы изменить метрику и тип маршрута маршрута по умолчанию, который вводится вручную. Используйте параметры **metric** и **metric-type** в **default-information originate** в команде **area nssa**, чтобы изменить метрику и тип маршрута по умолчанию, который вручную вводится в область NSSA.
- Запустите команду **max-metric router-lsa**, чтобы установить метрики всех маршрутов, объявляемых на маршрутизаторе, на максимальное значение. Таким образом, общая стоимость любого пути, проходящего через этот маршрутизатор, станет очень большой, и этот путь вряд ли сможет стать кратчайшим.

Административное расстояние OSPF

По умолчанию OSPF AD равен 110.

Запустите команду **distance**, чтобы установить AD маршрута OSPF.

4.3.5. Повышенная безопасность и надежность

Используйте такие функции, как аутентификация и корреляция BFD, чтобы повысить безопасность, стабильность и надежность OSPF.

4.3.5.1. Принцип работы

Аутентификация

Аутентификация не позволяет маршрутизаторам, осуществляющим незаконный доступ к сети, и узлам, подделывающим пакет OSPF, участвовать в процессе OSPF. Пакеты OSPF, полученные на интерфейсе OSPF (или на обоих концах виртуального канала), аутентифицируются. Если аутентификация не удалась, пакеты отбрасываются и смежность не может быть установлена.

Включение аутентификации позволяет избежать изучения неаутентифицированных или недействительных маршрутов, тем самым предотвращая объявление действительных маршрутов неаутентифицированным устройствам. В сети broadcast типа аутентификация также предотвращает превращение неаутентифицированных устройств в назначенные устройства, обеспечивая стабильность системы маршрутизации и защиту системы маршрутизации от вторжений.

Проверка MTU

При получении пакета DD OSPF проверяет, совпадает ли MTU соседнего интерфейса с MTU локального интерфейса. Если MTU интерфейса, указанного в полученном пакете DD, больше, чем MTU интерфейса, который получает пакет, то смежность настроить невозможно. Отключение проверки MTU позволяет избежать этой проблемы.

Проверка адреса источника

Обычно адрес источника пакета, полученного OSPF, находится в том же сегменте сети, что и принимающий интерфейс. Адреса на обоих концах P2P-канала настраиваются отдельно и не обязательно находятся в одном сегменте сети. В этом сценарии, поскольку информация об адресе peer-а будет сообщена во время процесса согласования канала P2P, OSPF проверяет, является ли адрес источника пакета адресом, объявленным peer-ом во время согласования. В противном случае OSPF определяет, что пакет недействителен, и отбрасывает его. В частности, OSPF не проверяет адрес ненумерованного интерфейса.

В некоторых сценариях адрес источника пакета, полученного OSPF, может не находиться в том же сегменте сети, что и принимающий интерфейс, и поэтому проверка адреса OSPF завершается неудачно. Например, согласованный адрес peer-а не может быть получен по каналу P2P. В этом сценарии проверка адреса источника должна быть отключена, чтобы обеспечить правильную настройку смежности OSPF.

Двустороннее обслуживание

Маршрутизаторы OSPF периодически отправляют друг другу пакеты Hello для поддержания смежности. В большой сети может быть отправлено или получено много пакетов, занимающих слишком много процессора и памяти. В результате некоторые пакеты задерживаются или отбрасываются. Если время обработки пакетов Hello превышает dead-интервал, смежность будет нарушена.

Если включена функция двустороннего обслуживания, в дополнение к пакетам Hello для поддержания двунаправленной связи между соседями могут также использоваться пакеты DD, LSU, LSR и LSAck, что делает смежность более стабильной.

Ограничение одновременного взаимодействия с соседями

Когда маршрутизатор одновременно обменивается данными с несколькими соседями, это может повлиять на его производительность. При максимальном количестве соседей, которые одновременно инициируют или принимают взаимодействие с процессом OSPF, маршрутизатор может взаимодействовать с соседями пакетно, что обеспечивает пересылку данных и другие ключевые сервисы.

Переполнение

OSPF требует, чтобы маршрутизаторы в одной области хранили одну и ту же LSDB. Количество маршрутизаторов в сети продолжает расти. Однако некоторые маршрутизаторы не могут хранить столько информации о маршрутизации из-за ограниченности системных ресурсов. Большой объем информации о маршрутизации может истощить системные ресурсы маршрутизаторов, что приведет к сбоям в работе маршрутизаторов.

Функция переполнения ограничивает количество внешних маршрутов в LSDB, чтобы контролировать размер LSDB.

Когда количество внешних маршрутов на маршрутизаторе превышает верхний предел, маршрутизатор переходит в состояние переполнения. Маршрутизатор удаляет из LSDB внешние маршруты, созданные им самим, и не генерирует новые внешние маршруты. Кроме того, маршрутизатор отбрасывает вновь полученные внешние маршруты. По

истечении таймера состояния переполнения (5 с), если количество внешних маршрутов меньше верхнего предела, нормальное состояние восстанавливается.

GR

Технология разделения управления и пересылки широко используется среди маршрутизаторов. В относительно стабильной топологии сети, когда маршрутизатор с поддержкой GR перезапускается на control plane, пересылка данных может продолжаться на forwarding plane. Кроме того, действия (такие как изменение смежности и вычисление маршрута), выполняемые на control plane, не влияют на функции forwarding plane. Таким образом, можно избежать прерывания обслуживания, вызванного изменением маршрута, что повышает надежность всей сети.

В настоящее время функция GR используется только во время переключения активный/резервный режим и обновления системы.

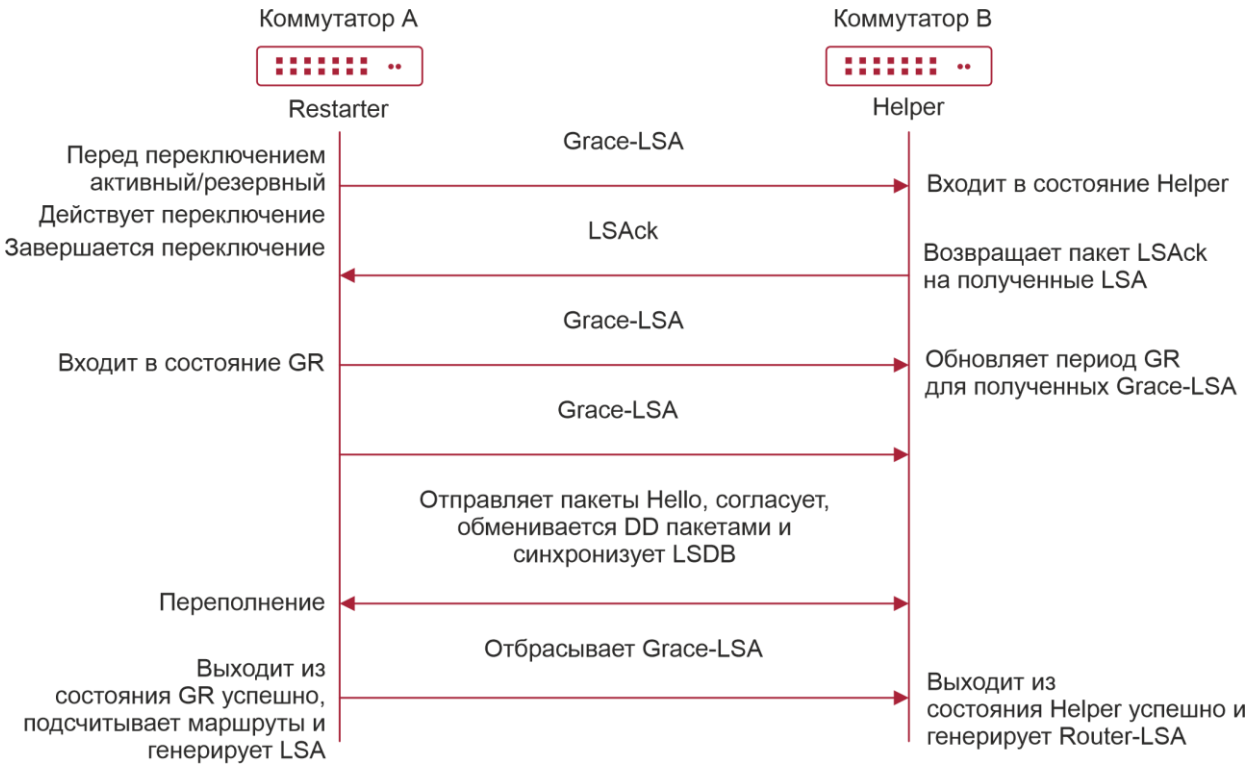


Рисунок 4-7. Обычный процесс GR OSPF

- Процесс GR требует сотрудничества между restarter-ом и helper-ом. Restarter — это маршрутизатор, на котором происходит GR. Helper является соседом restarter-a.
- При входе в процесс GR или выходе из него restarter отправляет Grace-LSA соседу, уведомляя соседа о необходимости войти в состояние helper- a или выйти из него.
- Когда смежность между restarter-ом и helper-ом достигает состояния Full, маршрутизатор может успешно выйти из процесса GR.

NSR

Во время непрерывной маршрутизации (NSR) информация, связанная с OSPF, копируется из активного модуля супервизора распределенного устройства в резервный модуль

супервизора. Таким образом, устройство может автоматически восстанавливать состояние соединения и заново генерировать маршруты без помощи соседних устройств во время переключения активный/резервный режим. Информация, подлежащая резервному копированию, включает сведения о смежности и состоянии канала.

Fast Hello, корреляция BFD и быстрое перенаправление

После возникновения сбоя канала OSPF обнаруживает отключение соседа только через некоторое время (около 40 с). Затем OSPF объявляет информацию и повторно вычисляет SPT. В этот период трафик прерывается.

- После включения функции Fast Hello (то есть интервал dead соседа установлен на 1 с) OSPF может обнаружить отключение соседа в течение 1 с, если канал неисправен. Это значительно ускоряет сходимость маршрутов и предотвращает прерывание трафика.
- BFD используется для проверки связи между устройствами. Неисправность канала может быть обнаружена всего за 150 мс. После того как OSPF коррелирует с BFD, OSPF может обнаружить отключение соседа всего за 150 мс, если канал неисправен. Это значительно ускоряет сходимость маршрутов и предотвращает прерывание трафика.
- Быстрое перенаправление подготавливает резервный маршрут для OSPF. Как только OSPF обнаруживает отключение соседа, трафик немедленно переключается на резервный маршрут, что предотвращает прерывание трафика.

iSPF

- Топология OSPF основана на областях. Алгоритм SPF запускается для независимых вычислений в каждой области. Стандартный алгоритм SPF каждый раз пересчитывает топологию всей области, даже если в топологии области изменяются только leave-узлы.
- При вычислении топологии сети инкрементальный SPF (iSPF) корректирует только те узлы SPT, на которые влияют топологические изменения, и не перестраивает весь SPT. Это может эффективно снизить нагрузку на процессоры маршрутизаторов в большой сети, особенно если сеть нестабильна.

4.3.5.2. Сопутствующая конфигурация

Аутентификация пакетов OSPF

По умолчанию аутентификация отключена.

- Запустите команду **area authentication**, чтобы включить функцию аутентификации во всей области, чтобы функция вступила в силу на всех интерфейсах в этой области. Если аутентификация включена в области 0, функция действует на виртуальном канале.
- Запустите команду **ip ospf authentication**, чтобы включить аутентификацию на интерфейсе. Эта конфигурация имеет приоритет над конфигурацией на основе области.
- Запустите команду **ip ospf authentication-key**, чтобы установить текстовый ключ аутентификации на интерфейсе.
- Запустите команду **ip ospfmessage-digest-key**, чтобы установить ключ аутентификации message digest 5 (MD5) на интерфейсе.
- Используйте параметр **authentication** в команде **area virtual-link**, чтобы включить аутентификацию на обоих концах виртуального канала. Эта конфигурация имеет приоритет над конфигурацией на основе области.

- Используйте параметр **authentication-key** в команде **area virtual-link**, чтобы установить текстовый ключ аутентификации на обоих концах виртуального канала.
- Используйте параметр **message-digest-key** в команде **area virtual-link**, чтобы установить ключ аутентификации MD5 на обоих концах виртуального канала.

Проверка MTU

По умолчанию проверка MTU отключена.

Запустите команду **ip ospf mtu-ignore**, чтобы отключить проверку MTU на интерфейсе.

Проверка адреса источника

По умолчанию проверка адреса источника включена на P2P-интерфейсе.

Запустите команду **ip ospf source-check-ignore**, чтобы отключить проверку адреса источника на интерфейсе.

Двустороннее обслуживание

По умолчанию двустороннее обслуживание включено.

Запустите команду **two-way-maintain**, чтобы включить двустороннее обслуживание.

Ограничение одновременного взаимодействия с соседями

Запустите команду **max-concurrent-dd**, чтобы изменить максимальное количество соседей, одновременно взаимодействующих с текущим процессом OSPF. Значение по умолчанию — 5.

Запустите команду **ipv6 router ospf max-concurrent-dd**, чтобы изменить максимальное количество соседей, которые одновременно взаимодействуют со всеми процессами OSPF на маршрутизаторе. Значение по умолчанию — 10.

Переполнение

Запустите команду **overflow memory-lack**, чтобы позволить маршрутизатору перейти в состояние переполнения, когда памяти недостаточно. По умолчанию маршрутизатору разрешено переходить в состояние переполнения, когда памяти недостаточно.

Запустите команду **overflow database**, чтобы позволить маршрутизатору перейти в состояние переполнения, когда количество LSA слишком велико. По умолчанию маршрутизатору не разрешено переходить в состояние переполнения, когда количество LSA слишком велико.

Запустите команду **overflow database external**, чтобы разрешить маршрутизатору переходить в состояние переполнения, когда количество внешних LSA слишком велико. По умолчанию маршрутизатору не разрешено переходить в состояние переполнения, когда количество внешних LSA слишком велико.

GR

По умолчанию функция restarter-а отключена, а функция helper-а включена.

Запустите команду **graceful-restart**, чтобы настроить функцию restarter-а.

Запустите команду **graceful-restart helper**, чтобы настроить функцию helper-а.

NSR

По умолчанию NSR отключен.

Запустите команду **nsr**, чтобы включить NSR в текущем процессе OSPF.

Fast Hello

По умолчанию интервал dead соседа на интерфейсе составляет 40 с.

Запустите команду **ip ospf dead-intervalminimal hello-multiplier**, чтобы включить функцию Fast Hello на интерфейсе, то есть dead-интервал соседа равен 1 с.

Корреляция OSPF с BFD

По умолчанию OSPF не коррелирует с BFD.

Запустите команду **bfd interval min_rx multiplier**, чтобы установить параметры BFD.

Запустите команду **bfd all-interfaces**, чтобы сопоставить OSPF с BFD на всех интерфейсах.

Запустите команду **ip ospf bfd**, чтобы сопоставить OSPF с BFD на текущем интерфейсе.

Быстрое перенаправление

По умолчанию быстрое перенаправление отключено.

Запустите команду **fast-reroute route-map**, чтобы включить быстрое перенаправление в процессе OSPF, чтобы можно было использовать резервный маршрут, определенный в карте маршрутов.

Запустите команду **fast-reroute lfa**, чтобы включить быстрое перенаправление в процессе OSPF, чтобы резервный маршрут можно было вычислить с использованием резервного пути без петель.

Запустите команду **fast-reroute lfadownstream-paths**, чтобы включить быстрое перенаправление для процесса OSPF, чтобы резервный маршрут можно было вычислить с использованием downstream-пути.

Запустите команду **set fast-reroute backup-interfacebackup-nexthop**, чтобы определить резервный маршрут в карте маршрутов.

Запустите команду **ip ospf fast-reroute protection**, чтобы указать альтернативный режим защиты без петель (LFA) интерфейса.

Запустите команду **ip ospf fast-reroute no-eligible-backup**, чтобы предотвратить превращение интерфейса в резервный интерфейс.

iSPF

По умолчанию iSPF отключен.

Запустите команду **ispf enable**, чтобы включить iSPF в процессе OSPF.

4.3.6. Управление сетью

Используйте такие функции, как MIB и Syslog, для облегчения управления OSPF.

4.3.6.1. Принцип работы

MIB

MIB — это набор информации о состоянии устройства, поддерживаемый устройством. Вы можете использовать программу управления для просмотра и настройки узла MIB.

На маршрутизаторе можно одновременно запустить несколько процессов OSPF, но MIB OSPF можно связать только с одним процессом OSPF.

Trap

Сообщение Trap — это уведомление, генерируемое, когда система обнаруживает неисправность. Это сообщение содержит соответствующую информацию о неисправности.

Если функция Trap включена, маршрутизатор может заранее отправлять сообщения Trap на устройство управления сетью.

Syslog (системный журнал)

Системный журнал записывает операции (например, настройку команд), выполняемые пользователями на маршрутизаторах, а также определенные события (например, сбои сетевого подключения).

Если системному журналу разрешено записывать изменения смежности, сетевой администратор может просматривать журналы, чтобы узнать весь процесс настройки и поддержки смежности OSPF.

4.3.6.2. Сопутствующая конфигурация

MIB

По умолчанию MIB привязан к процессу OSPF с наименьшим идентификатором процесса.

Запустите команду **enable mib-binding**, чтобы связать MIB с текущим процессом OSPF.

Trap

По умолчанию все Trap отключены, и устройству не разрешено отправлять Trap OSPF.

Запустите команду **enable traps**, чтобы включить указанный Trap для процесса OSPF.

Запустите команду **snmp-server enable traps ospf**, чтобы разрешить устройству отправлять Trap OSPF.

Syslog (системный журнал)

По умолчанию системному журналу разрешено записывать изменения смежности.

Запустите команду **log-adj-changes**, чтобы системный журнал мог записывать изменения смежности.

4.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций OSPF	(Обязательно) Используется для создания домена маршрутизации OSPF	
	router ospf	Создает процесс OSPF
Настройка основных функций OSPF	**router-id**	Настраивает идентификатор маршрутизатора
	network area	Включает OSPF на интерфейсе и указывает идентификатор области
	area virtual-link	Создает виртуальный канал

Конфигурация	Описание и команда	
Установка типа сети	(Опционально) Конфигурации являются обязательными, если физическая сеть представляет собой сеть X.25, Frame Relay или ATM	
	ip ospf network	Определяет тип сети
	neighbor	Указывает соседа
	ip ospf priority	Настраивает приоритет DR
Настройка перераспределения маршрутов и маршрута по умолчанию	(Опционально) Эти конфигурации рекомендуются, если домен маршрутизации OSPF подключен к внешней сети	
	redistribute	Настраивает перераспределение маршрутов
	default-information originate	Представляет маршрут по умолчанию
Настройка тупиковой области и области NSSA	(Опционально) Используется для уменьшения взаимодействия информации о маршрутизации и размера таблицы маршрутизации, а также для повышения стабильности маршрутов	
	area stub	Настраивает тупиковую область
	area nssa	Настраивает область NSSA
Настройка суммирования маршрутов	(Опционально) Используется для уменьшения взаимодействия информации о маршрутизации и размера таблицы маршрутизации, а также для повышения стабильности маршрутов	
	area range	Суммирует маршруты, объявляемые между областями
	summary-address	Суммирует маршруты, которые вводятся посредством перераспределения

Конфигурация	Описание и команда	
	discard-route	Добавляет отброшенный маршрут в таблицу маршрутизации
Настройка фильтрации маршрутов	(Опционально) Используется для ручного управления взаимодействием информации о маршрутизации и фильтрации доступных маршрутов OSPF	
	passive-interface	Настраивает пассивный интерфейс
	ip ospfdatabase-filter all out	Запрещает интерфейсу отправлять LSA
	area filter-list	Фильтрует маршруты, которые объявляются между областями
	distribute-list out	Фильтрует маршруты, введенные в результате перераспределения
	distribute-listin	Фильтрует маршруты, рассчитываемые на основе полученных LSA
Изменение стоимости маршрута и AD	(Опционально) Используется для ручного управления кратчайшим маршрутом, вычисленным OSPF, и определения предпочтительности выбора маршрута OSPF	
	auto-costreference-bandwidth	Изменяет базовую полосу пропускания автоматической стоимости
	ip ospf cost	Изменяет стоимость в исходящем направлении интерфейса
	areadefault-cost	Изменяет стоимость маршрута по умолчанию в тупиковой области или области NSSA

Конфигурация	Описание и команда	
	default-metric	Изменяет метрику по умолчанию перераспределенного маршрута
	max-metric router-lsa	Настраивает максимальную метрику
	compatible rfc1583	Обеспечивает совместимость правил маршрутизации с RFC1583
	distance	Изменяет OSPF AD
Включение аутентификации	(Опционально) Используется для предотвращения участия в процессе протокола OSPF маршрутизаторов, осуществляющих незаконный доступ к сети, и узлов, подделывающих пакеты OSPF	
	area authentication	Включает аутентификацию и устанавливает режим аутентификации в области
	ip ospf authentication	Включает аутентификацию и устанавливает режим аутентификации на интерфейсе
Включение аутентификации	**ip ospf authentication-key**	Устанавливает текстовый ключ аутентификации на интерфейсе
	ip ospf message-digest-keymd5	Устанавливает ключ аутентификации MD5 на интерфейсе
Включение переполнения	(Опционально) Используется для предотвращения проблемы, связанной с прекращением работы процессов OSPF из-за чрезмерного потребления памяти	
	overflow memory-lack	Позволяет маршрутизатору переходить в состояние переполнения, когда памяти недостаточно

Конфигурация	Описание и команда	
	overflow database	Позволяет маршрутизатору переходить в состояние переполнения, когда количество LSA превышает заданный предел
	overflow database external	Позволяет маршрутизатору переходить в состояние переполнения, когда количество внешних LSA превышает заданный предел
Изменение максимального количества одновременных соседей	(Опционально) Используется для предотвращения проблемы ухудшения производительности, вызванной чрезмерным потреблением ресурсов ЦП	
	max-concurrent-dd	Изменяет максимальное количество одновременных соседей в текущем процессе OSPF
	router ospf max-concurrent-dd	Изменяет максимальное количество одновременных соседей во всех процессах OSPF
Отключение проверки адреса источника	(Опционально) Используется для предотвращения проблемы, связанной с невозможностью установки смежности из-за невозможности получить адрес peer-а	
	ip ospf source-check-ignore	Отключает проверку адреса источника на интерфейсе
Отключение проверки MTU	(Опционально) Используется для предотвращения проблемы, связанной с невозможностью настройки смежности из-за несоответствия MTU на соседнем интерфейсе	
	ip ospf mtu-ignore	Отключает проверку MTU на интерфейсе

Конфигурация	Описание и команда	
Включение двустороннего обслуживания	(Опционально) Используется для предотвращения прекращения соединения из-за задержки или потери пакетов Hello	
	two-way-maintain	Обеспечивает двустороннее обслуживание
Включение GR	(Опционально) Используется для сохранения пересылки маршрутизации OSPF во время перезапуска или переключения между активным и резервным процессами OSPF, чтобы предотвратить прерывание трафика	
	graceful-restart	Настраивает функцию restarter-a
	graceful-restart helper	Настраивает функцию helper-a
Включение NSR	(Опционально) Используется для сохранения пересылки маршрутизации OSPF во время переключения между активным и резервным процессами OSPF, чтобы предотвратить прерывание трафика	
	nsr	Включает NSR
Включение Fast Hello	(Опционально) Используется для быстрого обнаружения отключения соседа и предотвращения прерывания трафика в случае неисправности канала	
	ip ospf dead-intervalminimal hello-multiplier	Включение Fast Hello
Корреляция OSPF с BFD	(Опционально) Используется для быстрого обнаружения отключения соседа и предотвращения прерывания трафика в случае неисправности канала	
	bfd interval min_rx multiplier	Устанавливает параметры BFD
	bfd all-interfaces	Коррелирует OSPF с BFD на всех интерфейсах
	ip ospf bfd	Коррелирует OSPF с BFD на текущем интерфейсе

Конфигурация	Описание и команда	
Включение быстрого перенаправления	(Опционально) Используется для быстрого переключения сервисов на резервный маршрут во избежание прерывания трафика	
	fast-reroute route-map	Включает быстрое перенаправление процесса OSPF, чтобы можно было использовать резервный маршрут, определенный в карте маршрутов
	fast-reroute lfa	Обеспечивает быстрое перенаправление процесса OSPF, чтобы резервный маршрут мог быть вычислен с использованием резервного пути без петель
	fast-reroute lfa downstream-paths	Обеспечивает быстрое перенаправление процесса OSPF, чтобы резервный маршрут можно было вычислить, используя downstream-путь
	set fast-reroute backup-interface backup-nexthop	Определяет резервный маршрут на карте маршрутов
	ip ospf fast-reroute protection	Указывает режим защиты LFA интерфейса
Включение быстрого перенаправления	**ip ospf fast-reroute no-eligible-backup**	Предотвращает превращение интерфейса в резервный интерфейс
Включение iSPF	(Опционально) Используется для обеспечения возможности инкрементного вычисления топологии, чтобы снизить нагрузку на процессор	
	ispf enable	Включает iSPF в процессе OSPF

Конфигурация	Описание и команда	
Настройка функции управления сетью	(Опционально) Конфигурации позволяют пользователям использовать программное обеспечение управления сетью SNMP для управления OSPF	
	enable mib-binding	Связывает MIB с текущим процессом OSPF
	enable traps	Включает указанный Trap для процесса OSPF
	snmp-server enable traps ospf	Позволяет устройству отправлять Trap OSPF
	log-adj-changes	Позволяет системному журналу записывать изменения смежности
Изменение параметров управления протоколом	(Опционально) Рекомендуется не изменять параметры управления протоколом без необходимости	
	ip ospf hello-interval	Изменяет интервал Hello
	ip ospf dead-interval	Изменяет интервал отключения соседа
	timers throttle lsa all	Изменяет параметры алгоритма экспоненциального отката, который генерирует LSA
	timers throttle route inter-area	Изменяет задержку расчета маршрута между областями
Изменение параметров управления протоколом	**timers throttle route ase**	Изменяет задержку расчета внешнего маршрута
	timers pacing lsa-group	Изменяет интервал обновления группы LSA
	timers pacing lsa-transmit	Изменяет интервал отправки пакетов LS-UPD

Конфигурация	Описание и команда	
	timers pacing lsa-transmit	Изменяет задержку передачи пакетов LSU
	ip ospf retransmit-interval	Изменяет интервал повторной передачи пакетов LSU
	timers lsa arrival	Изменяет задержку, после которой принимается тот же LSA
	timers throttle spf	Изменяет таймер вычислений SPT

4.4.1. Настройка основных функций OSPF

4.4.1.1. Эффект конфигурации

Настройте домен маршрутизации OSPF в сети, чтобы предоставить пользователям в сети сервис unicast-маршрутизации IPv4.

4.4.1.2. Примечания

- Убедитесь, что функция IP-маршрутизации включена, то есть IP-маршрутизация не отключена; в противном случае OSPF невозможно будет включить.
- Настоятельно рекомендуется вручную настроить идентификатор маршрутизатора.
- После настройки **ip ospf disable all** интерфейс не отправляет и не получает пакеты OSPF и не участвует в вычислениях OSPF, даже если интерфейс принадлежит сети.

4.4.1.3. Шаги настройки

Создание процесса OSPF

- Обязательный.
- Конфигурация обязательна для каждого маршрутизатора.

Настройка идентификатора маршрутизатора

- (Опционально) Настоятельно рекомендуется вручную настроить идентификатор маршрутизатора.
- Если идентификатор маршрутизатора не настроен, OSPF выбирает IP-адрес интерфейса. Если IP-адрес не настроен ни для одного интерфейса или настроенные IP-адреса использовались другими экземплярами OSPF, необходимо вручную настроить идентификатор маршрутизатора.

Включение OSPF на интерфейсе и указание идентификатора области

- Обязательный.
- Конфигурация обязательна для каждого маршрутизатора.

4.4.1.4. Проверка

- Запустите команду **show ip route ospf**, чтобы убедиться, что записи таблицы маршрутизации OSPF загружены правильно.
- Запустите команду **ping**, чтобы убедиться, что сервис unicast IPv4 настроен правильно.

4.4.1.5. Связанные команды

Создание процесса OSPF

Команда	**router ospf** *process-id* [**vrf** *vrf-name*]
Описание параметра	*process-id*: указывает идентификатор процесса OSPF. Если идентификатор процесса не указан, идентификатор процесса равен 1. *vrf-name*: указывает маршрутизацию и пересылку VPN (VRF), к которой принадлежит процесс OSPF
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Различные процессы OSPF независимы друг от друга и могут рассматриваться как разные протоколы маршрутизации, работающие независимо

Настройка идентификатора маршрутизатора

Команда	**router-id** *router-id*
Описание параметра	*router-id*: указывает идентификатор маршрутизатора, который необходимо настроить. Это выражается в IP-адресе
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Различные процессы OSPF независимы друг от друга и могут рассматриваться как разные протоколы маршрутизации, работающие независимо. Каждый процесс OSPF использует уникальный идентификатор маршрутизатора

Включение OSPF на интерфейсе и указание идентификатора области

Команда	**network** *ip-address wildcard* **area** *area-id*
Описание параметра	*ip-address*: указывает IP-адрес интерфейса.

	wildcard: указывает режим сравнения IP-адресов. **0** означает точное сопоставление, а **1** означает, что сравнение не выполняется. *area-id*: указывает идентификатор области OSPF. Область OSPF всегда связана с диапазоном адресов. Чтобы облегчить управление, вы можете использовать подсеть в качестве идентификатора области OSPF
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Указав *ip-address* и *wildcard*, вы можете использовать одну команду для связывания нескольких интерфейсов с одной областью OSPF. Чтобы запустить OSPF на одном интерфейсе, необходимо включить основной (primary) IP-адрес интерфейса в диапазон IP-адресов, определенный в **network area**. Если диапазон IP-адресов, определенный в **network area**, содержит только дополнительный (secondary) IP-адрес интерфейса, OSPF не работает на этом интерфейсе. Если адрес интерфейса соответствуют диапазону IP-адресов, определенным в командах **network** нескольких процессов OSPF, процесс OSPF, с которым связан интерфейс, определяется на основе метода наилучшего соответствия

Создание виртуального канала

Команда	**area** *area-id* **virtual-link** *router-id* [**authentication** [**message-digest** | **null**]] [**dead-interval** { *seconds* | **minimal hello-multiplier** *multiplier* }] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [[**authentication-key** [**0** | **7**] *key*] | [**message-digest-key** *key-id* **md5** [**0** | **7**] *key*]]
Описание параметра	*area-id*: указывает идентификатор транзитной области OSPF. Идентификатор области может быть десятичным целым числом или IP-адресом. *router-id*: указывает идентификатор соседнего маршрутизатора виртуального канала. **dead-interval** *seconds*: указывает время, когда сосед объявлен потерянным. Указывается в секундах. Значение находится в диапазоне от 0 до 2 147 483 647. Настройка этого параметра должна соответствовать настройке соседнего узла. **minimal**: указывает, что функция Fast Hello включена и устанавливает dead-интервал равным 1 с. **hello-multiplier**: указывает результат интервала dead, кратного интервалу Hello в функции Fast Hello. *multiplier*: указывает количество пакетов Hello, отправляемых в секунду с помощью функции Fast Hello. Значение варьируется от 3 до 20. **hello-interval** *seconds*: указывает интервал, с которым OSPF отправляет пакет Hello по виртуальному каналу. Указывается в

	секундах. Значение варьируется от 1 до 65 535. Настройка этого параметра должна соответствовать настройке соседнего узла. **retransmit-interval** *seconds*: указывает время повторной передачи LSA OSPF. Указывается в секундах. Значение варьируется от 1 до 65 535. **transmit-delay** *seconds*: указывает задержку, после которой OSPF отправляет LSA. Указывается в секундах. Значение варьируется от 1 до 65 535. **authentication-key** [**0** | **7**] *key*: определяет ключ для простой текстовой аутентификации OSPF. **message-digest-key** *key-id* **md5** [**0** | **7**] *key*: определяет идентификатор ключа и ключ для аутентификации OSPF MD5. **authentication**: устанавливает тип аутентификации: обычная текстовая аутентификация. **message-digest**: устанавливает тип аутентификации на аутентификацию MD5. **null**: указывает, что аутентификация отключена
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	В домене маршрутизации OSPF все области должны быть подключены к магистральной области. Если магистральная область отключена, необходимо настроить виртуальный канал для подключения к магистральной области; в противном случае возникнут проблемы с сетевой связью. Между двумя ABR должен быть создан виртуальный канал, а область, которой принадлежат оба ABR, является транзитной областью. Тупиковая область или область NSSA не могут использоваться в качестве транзитной области. Виртуальный канал также можно использовать для подключения других немагистральных областей. **router-id** — идентификатор соседнего маршрутизатора OSPF. Если вы уверены в значении **router-id**, запустите команду **show ip ospf neighbor**, чтобы подтвердить значение. Вы можете настроить loopback-адрес в качестве идентификатора маршрутизатора. Команда **area virtual-link** определяет только ключ аутентификации виртуального канала. Чтобы включить пакетную аутентификацию OSPF в областях, подключенных к виртуальному каналу, необходимо запустить команду **area authentication**. OSPF поддерживает функцию Fast Hello. После включения функции OSPF Fast Hello OSPF быстрее находит соседей и обнаруживает их сбои. Вы можете включить функцию OSPF Fast Hello, указав ключевые слова **minimal** и **hello-multiplier**, а также параметр **multiplier**. Ключевое слово **minimal** указывает, что интервал отключения установлен на 1 с, а **hello-multiplier** указывает количество

	пакетов Hello, отправляемых в секунду. Таким образом, интервал отправки пакета Hello уменьшается как минимум до 1 с. Если функция Fast Hello настроена для виртуального канала, поле интервала Hello пакета Hello, объявляемого по виртуальному каналу, устанавливается в 0, а поле интервала Hello пакета Hello, полученного по этому виртуальному каналу, игнорируется. Независимо от того, включена ли функция Fast Hello, интервал отключения должен быть постоянным, а значения **hello-multiplier** могут быть несовместимыми на маршрутизаторах на обоих концах виртуального канала. Убедитесь, что хотя бы один пакет Hello может быть получен в течение интервала отключения. Запустите команду **show ip ospf virtual-links**, чтобы отслеживать интервал отключения и интервал Fast Hello, настроенные для виртуального канала. Параметры **dead-interval minimal hello-multiplier** и **hello-interval**, введенные для функции Fast Hello, не могут быть настроены одновременно

4.4.1.6. Пример конфигурации

Сценарий:

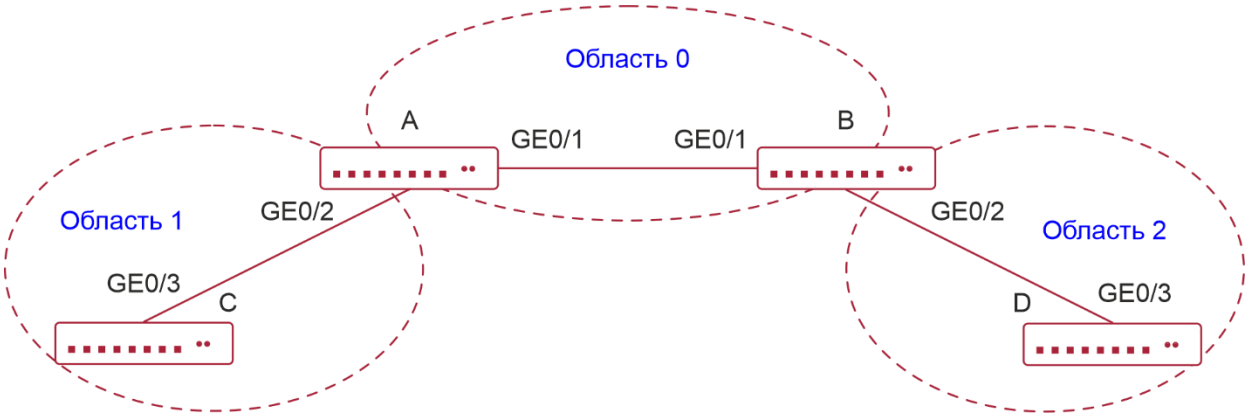


Рисунок 4-8.

IP-адреса интерфейса следующие:

A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1

B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1

C: GE 0/3 192.168.2.2

D: GE 0/3 192.168.3.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. • Включите функцию unicast-маршрутизации IPv4 на всех маршрутизаторах. (Эта функция включена по умолчанию.) • Настройте экземпляры OSPF и идентификаторы маршрутизаторов на всех маршрутизаторах. • Включите OSPF на интерфейсах, настроенных на всех маршрутизаторах
A	A#configure terminal A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)#exit A(config)#interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#ip address 192.168.2.1 255.255.255.0 A(config-if-GigabitEthernet 0/2)#exit A(config)#router ospf 1 A(config-router)#router-id192.168.1.1 A(config-router)#network 192.168.1.0 0.0.0.255 area 0 A(config-router)#network 192.168.2.0 0.0.0.255 area 1
B	B#configure terminal B(config)#interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ip address 192.168.1.2 255.255.255.0 B(config-if-GigabitEthernet 0/1)#exit B(config)#interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)#ip address 192.168.3.1 255.255.255.0 B(config-if-GigabitEthernet 0/2)#exit B(config)#router ospf 1 B(config-router)#router-id192.168.1.2 B(config-router)#network 192.168.1.0 0.0.0.255 area 0 B(config-router)#network 192.168.3.0 0.0.0.255 area 2
C	C#configure terminal C(config)#interface GigabitEthernet 0/3 C(config-if-GigabitEthernet 0/3)#ip address 192.168.2.2 255.255.255.0 C(config-if-GigabitEthernet 0/3)#exit C(config)#router ospf 1

	C(config-router)#router-id192.168.2.2 C(config-router)#network 192.168.2.0 0.0.0.255 area 1
D	D#configure terminal D(config)#interface GigabitEthernet 0/3 D(config-if-GigabitEthernet 0/3)#ip address 192.168.3.2 255.255.255.0 D(config-if-GigabitEthernet 0/3)#exit D(config)#router ospf 1 D(config-router)#router-id192.168.3.2 D(config-router)#network 192.168.3.0 0.0.0.255 area 2
Проверка	• Убедитесь, что соседи OSPF указаны правильно на всех маршрутизаторах. • Убедитесь, что таблица маршрутизации правильно загружена на всех маршрутизаторах. • На маршрутизаторе D убедитесь, что IP-адрес 192.168.2.2 может быть успешно пропингован
A	A# show ip ospf neighbor OSPF process 1, 2 Neighbors, 2 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/DR 00:00:40192.168.1.2 GigabitEthernet 0/1 192.168.2.2 1 Full/BDR00:00:34 192.168.2.2 GigabitEthernet 0/2 A# show ip route ospf O IA 192.168.3.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
B	B# show ip ospf neighbor OSPF process 1, 2 Neighbors, 2 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/BDR 00:00:32 192.168.1.1 GigabitEthernet 0/1 192.168.3.2 1 Full/BDR00:00:30 192.168.3.2 GigabitEthernet 0/2 B# show ip route ospf O IA 192.168.2.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
C	C# show ip ospf neighbor OSPF process 1,1 Neighbors,1 is Full:

	Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/BDR 00:00:32 192.168.2.1 GigabitEthernet 0/3 C# show ip route ospf O IA 192.168.1.0/24 [110/2] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3 O IA 192.168.3.0/24 [110/3] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3
D	D# show ip ospf neighbor OSPF process 1,1 Neighbors,1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.21 Full/BDR00:00:30 192.168.3.1 GigabitEthernet 0/3 D# show ip route ospf O IA 192.168.1.0/24 [110/2] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3 O IA 192.168.2.0/24 [110/3] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3 D# ping 192.168.2.2 Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds: < press Ctrl+C to break > !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

4.4.1.7. Распространенные ошибки

- OSPF невозможно включить, поскольку функция IP unicast-маршрутизации отключена.
- Сегмент сети, настроенный командой **network**, не включает IP-адреса интерфейсов.
- Идентификаторы областей, включенные на соседних интерфейсах, несовместимы.
- Один и тот же идентификатор маршрутизатора настроен на нескольких маршрутизаторах, что приводит к конфликту идентификаторов маршрутизатора.
- Один и тот же IP-адрес интерфейса настроен на нескольких маршрутизаторах, что приводит к ошибке работы сети OSPF.

4.4.2. Установка типа сети

4.4.2.1. Эффект конфигурации

Запустите OSPF, чтобы предоставить сервис unicast-маршрутизации IPv4, если физическая сеть — X.25, Frame Relay или ATM.

4.4.2.2. Примечания

- Необходимо настроить основные функции OSPF.
- Broadcast-сеть отправляет пакеты OSPF в multicast-режиме. Соседи обнаруживаются автоматически, и требуется выбор DR/BDR.
- Сеть P2P отправляет пакеты OSPF в multicast-режиме. Соседи обнаруживаются автоматически.
- Сеть NBMA отправляет пакеты OSPF в unicast-режиме. Соседей необходимо указать вручную, а также необходимо выбрать DR/BDR.
- Сеть P2MP (без параметра **non-broadcast**) отправляет пакеты OSPF в multicast-режиме. Соседи обнаруживаются автоматически.
- Сеть P2MP (с параметром **non-broadcast**) отправляет пакеты OSPF в unicast-режиме. Соседей необходимо указывать вручную.

4.4.2.3. Шаги настройки

Настройка типа сети интерфейса

- Опционально.
- Конфигурация требуется на маршрутизаторах на обоих концах канала.

Настройка соседей

- (Опционально) Если тип сети интерфейса установлен на NBMA или P2MP (с параметром **non-broadcast**), необходимо настроить соседей.
- Соседи настраиваются на маршрутизаторах на обоих концах сети NBMA или P2MP (с параметром **non-broadcast**).

Настройка приоритета интерфейса

- (Опционально) Необходимо настроить приоритет интерфейса, если маршрутизатор должен быть указан как DR, или если маршрутизатор не может быть указан как DR.
- Настройте приоритет интерфейса на маршрутизаторе, который должен быть указан как DR или не может быть указан как DR.

4.4.2.4. Проверка

Запустите команду **show ip ospf interface**, чтобы убедиться, что тип сети каждого интерфейса правильный.

4.4.2.5. Связанные команды

Настройка типа сети интерфейса

Команда	**ip ospf network** { **broadcast** | **non-broadcast** | **point-to-multipoint** [**non-broadcast**] | **point-to-point**}
Описание параметра	**broadcast**: устанавливает тип сети интерфейса как broadcast. **non-broadcast**: устанавливает тип сети интерфейса как non-broadcast. **point-to-multipoint** [**non-broadcast**]: устанавливает тип сети интерфейса как P2MP. Если интерфейс не поддерживает возможность broadcast, должен быть доступен параметр non-broadcast.

	point-to-point: устанавливает тип сети интерфейса как P2P
Командный режим	Режим настройки интерфейса
Руководство по использованию	Тип broadcast требует, чтобы интерфейс имел возможность broadcast-передачи. Тип P2P требует, чтобы интерфейсы были соединены между собой по принципу one-to-one. Тип NBMA требует full-meshed соединений, и все соединенные между собой маршрутизаторы могут напрямую взаимодействовать друг с другом. Тип P2MP не предъявляет никаких требований

Настройка соседей

Команда	**neighbor** *ip-address* [**poll-interval** *seconds*] [**priority** *priority*] [**cost** *cost*]
Описание параметра	*ip-address*: указывает IP-адрес соседнего интерфейса. **poll-interval** *seconds*: указывает интервал опроса соседей. Указывается в секундах. Значение находится в диапазоне от 0 до 2 147 483 647. Этот параметр применим только к интерфейсу NBMA. **priority** *priority*: указывает приоритет соседа. Значение находится в диапазоне от 0 до 255. Этот параметр применим только к интерфейсу NBMA. **cost** *cost*: указывает стоимость, необходимую для достижения каждого соседа. Нет значения по умолчанию. Значение варьируется от 0 до 65 535. Этот параметр применим только к интерфейсу P2MP
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Соседи должны быть указаны для интерфейсов NBMA или P2MP (non-broadcast). IP-адрес соседа должен быть основным IP-адресом этого интерфейса соседа. Если соседний маршрутизатор становится неактивным в сети NBMA, OSPF по-прежнему отправляет пакеты Hello этому соседу, даже если в течение времени отключения маршрутизатора не получен ни один пакет Hello. Интервал отправки пакета Hello называется интервалом опроса. При первом запуске OSPF отправляет пакеты Hello только соседям, чьи приоритеты не равны 0. Таким образом, соседи с приоритетами, установленными на 0, не участвуют в выборе DR/BDR. После выбора DR/BDR он отправляет пакеты Hello всем соседям для настройки смежности.

	Сеть P2MP (non-broadcast) не может динамически обнаруживать соседей, поскольку у нее нет возможности broadcast-передачи. Поэтому вы должны использовать эту команду для ручной настройки соседей для сети P2MP (non-broadcast). Кроме того, вы можете использовать параметр **cost**, чтобы указать стоимость для достижения каждого соседа в сети P2MP

Настройка приоритета интерфейса

Команда	**ip ospf priority** *priority*
Описание параметра	*priority*: указывает приоритет OSPF интерфейса. Значение варьируется от 0 до 255
Командный режим	Режим настройки интерфейса
Руководство по использованию	Приоритет интерфейса OSPF содержится в пакете Hello. Когда выборы DR/BDR происходят в broadcast-сети OSPF, маршрутизатор с наивысшим приоритетом становится DR или BDR. Если приоритеты одинаковы, маршрутизатор с наибольшим идентификатором становится DR или BDR. Маршрутизатор с приоритетом, установленным на 0, не участвует в выборе DR/BDR. Эта команда применима только к интерфейсам OSPF broadcast и NBMA

4.4.2.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Установка типа сети интерфейса на P2MP

Сценарий:

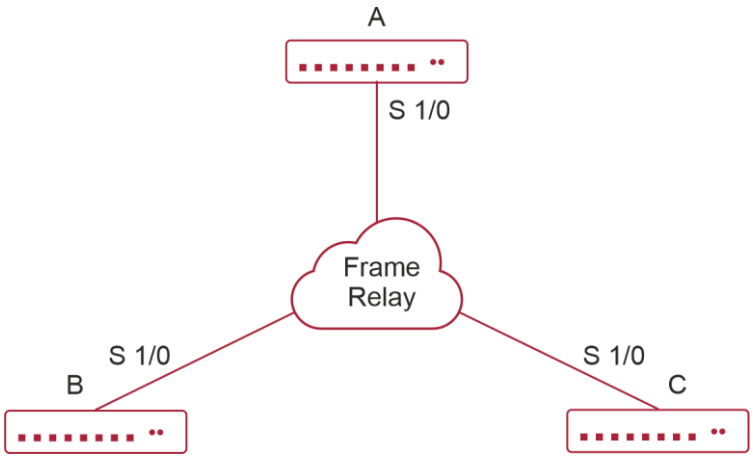


Рисунок 4-9.

IP-адреса интерфейса следующие:

A: S1/0 192.168.1.2

B: S1/0 192.168.1.3

C: S1/0 192.168.1.4

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • Установите тип сети интерфейса на P2MP на всех маршрутизаторах
A	A#configure terminal A(config)# interface Serial1/0 A(config-Serial1/0)# encapsulation frame-relay A(config-Serial1/0)# ip ospf network point-to-multipoint
B	B#configure terminal B(config)# interface Serial1/0 B(config-Serial1/0)# encapsulation frame-relay B(config-Serial1/0)# ip ospf network point-to-multipoint
C	C#configure terminal C(config)# interface Serial1/0 C(config-Serial1/0)# encapsulation frame-relay C(config-Serial1/0)# ip ospf network point-to-multipoint
Проверка	Убедитесь, что тип сети интерфейса — P2MP. A# show ip ospf interface Serial1/0 Serial1/0 is up, line protocol is up Internet Address 192.168.1.2/24, Ifindex 2, Area 0.0.0.1, MTU 1500 Matching network config: 192.168.1.0/24 Process ID 1, Router ID 192.168.1.2, Network Type POINTOMULTIPOINT, Cost: 1 Transmit Delay is 1 sec, State Point-To-Point Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:02 Neighbor Count is 1, Adjacent neighbor count is 0 Crypt Sequence Number is 4787 Hello received 465 sent 466, DD received 8 sent 8

	LS-Req received 2 sent 2, LS-Upd received 8 sent 21 LS-Ack received 14 sent 7, Discarded 3

4.4.2.7. Распространенные ошибки

- Типы сетей, настроенные на интерфейсах на двух концах, несовместимы, что приводит к ненормальному изучению маршрута.
- Тип сети установлен на NBMA или P2MP (с параметром **non-broadcast**), но соседи не указаны.

4.4.3. Настройка перераспределения маршрутов и маршрута по умолчанию

4.4.3.1. Эффект конфигурации

- В домене OSPF введите unicast-маршрут к другим доменам AS, чтобы сервис unicast-маршрутизации в других доменах AS мог предоставляться пользователям в домене OSPF.
- В домене OSPF внедрите маршрут по умолчанию в другие домены AS, чтобы сервис unicast-маршрутизации в других доменах AS мог быть предоставлен пользователям в домене OSPF.

4.4.3.2. Примечания

Необходимо настроить основные функции OSPF.

4.4.3.3. Шаги настройки

Настройка внешнего перераспределения маршрутов

- (Опционально) Эта конфигурация требуется, если внешние маршруты домена OSPF должны быть добавлены в ASBR.
- Эта конфигурация выполняется на ASBR.

Создание маршрута по умолчанию

- (Опционально) Эта конфигурация требуется, если маршрут по умолчанию должен быть введен в ASBR, чтобы другие маршрутизаторы в домене OSPF получали доступ по умолчанию к другим доменам AS через этот ASBR.
- Эта конфигурация выполняется на ASBR.

4.4.3.4. Проверка

- На маршрутизаторе внутри домена OSPF запустите команду **show ip route**, чтобы убедиться, что загружены unicast-маршруты к другим доменам AS.
- На маршрутизаторе внутри домена OSPF запустите команду **show ip route**, чтобы убедиться, что загружен маршрут по умолчанию к ASBR.
- Запустите команду **ping**, чтобы убедиться, что сервис unicast IPv4 к другим доменам AS работает правильно.

4.4.3.5. Связанные команды

Настройка внешнего перераспределения маршрутов

Команда	**redistribute** { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **arp-host** | **static** }[{ **level-1** | **level-1-2** | **level-2**}] [**match** { **internal** | **external** [**1**|**2**]| **nssa-external** [**1**|**2**]}] [**metric** *metric-value*] [**metric-type** {**1**|**2**}] [**route-map** *route-map-name*] [**subnets**] [**tag** *tag-value*]
Описание параметра	**bgp**: указывает на перераспределение из BGP. **connected**: указывает на перераспределение с прямых маршрутов. **isis** [*area-tag*]: указывает на перераспределение из IS-IS. *area-tag* указывает IS-IS. **ospf** *process-id*: указывает на перераспределение из OSPF. *process-id* определяет процесс OSPF. Значение варьируется от 1 до 65 535. **rip**: указывает на перераспределение из RIP. **static**: указывает на перераспределение со статических маршрутов. **arp-host**: указывает на перераспределение из маршрутов arp. **level-1** | **level-1-2** | **level-2**: используется только при перераспределении маршрутов IS-IS. Перераспределяются только маршруты указанного уровня. По умолчанию перераспределять можно только маршруты IS-IS Level-2. **match**: используется только при перераспределении маршрутов OSPF. Перераспределяются только маршруты, удовлетворяющие условиям фильтрации. По умолчанию все маршруты OSPF могут быть перераспределены. **metric** *metric-value*: указывает метрику внешнего LSA OSPF. *metric-value* указывает размер метрики. Значение находится в диапазоне от 0 до 16 777 214. **metric-type** {**1**|**2**}: задает тип внешнего маршрута, который может быть E-1 или E-2. **route-map** *route-map-name*: задает правила фильтрации перераспределения. **subnets**: указывает нестандартные сети перераспределения. **tag** *tag-value*: указывает значение тега маршрута, который перераспределяется в домен маршрутизации OSPF. Значение варьируется от 0 до 4 294 967 295
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	После настройки этой команды маршрутизатор становится ASBR, импортирует соответствующую информацию о маршрутизации в домен OSPF и объявляет информацию о маршрутизации как LSA типа 5 другим маршрутизаторам OSPF в домене.

	Если вы настраиваете перераспределение маршрутов IS-IS без указания параметра **level**, по умолчанию можно перераспределять только маршруты Level-2. Если при первоначальной настройке перераспределения указать параметр **level**, то маршруты указанного уровня могут быть перераспределены. Если настроены и **level-1**, и **level-2**, эти два уровня объединяются и сохраняются как **level-1-2**. Подробности смотрите в примере конфигурации. Если вы настроите перераспределение маршрутов OSPF без указания параметра **match**, маршруты OSPF всех подтипов могут распределяться по умолчанию. Последняя настройка параметра **match** используется в качестве начального параметра **match**. Перераспределять можно только маршруты, соответствующие подтипам. Вы можете использовать форму команды **no**, чтобы восстановить значение **match** по умолчанию. Подробности смотрите в примере конфигурации. Если указан **route-map**, правила фильтрации, указанные в **route-map**, применимы к исходным параметрам перераспределения. Для перераспределения маршрутов OSPF или IS-IS, карта маршрутов используется для фильтрации только в том случае, если перераспределенные маршруты соответствуют критериям, заданным **match** или **level**. Значение **set metric**, связанное с **route-map**, должно находиться в диапазоне от 0 до 16 777 214. Если значение превышает этот диапазон, маршруты невозможно ввести. Правила конфигурации для формы **no** команды **redistribute** следующие: 1. Если некоторые параметры указаны в форме **no** команды, значения этих параметров по умолчанию будут восстановлены. 2. Если в форме **no** команды не указан ни один параметр, вся команда будет удалена. Например, если настроено **redistribute isis 112 level-2**, вы можете запустить команду **no redistribute isis 112 level-2**, чтобы восстановить значение Level-2 по умолчанию. Поскольку уровень 2 сам по себе является значением параметра по умолчанию, сохраненная конфигурация по-прежнему **redistribute isis 112 level-2** после выполнения предыдущей формы команды **no**. Чтобы удалить всю команду, выполните команду **no redistribute isis 112**

Предоставление маршрута по умолчанию

Команда	**default-information originate** [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]
Описание параметра	**always**: позволяет OSPF генерировать маршрут по умолчанию независимо от того, имеет ли локальный маршрутизатор маршрут по умолчанию.

	metric *metric*: указывает начальную метрику маршрута по умолчанию. Значение варьируется от 0 до 16 777 214. **metric-type** *type*: указывает тип маршрута по умолчанию. Внешние маршруты OSPF подразделяются на два типа: Тип 1: метрика зависит от маршрутизатора; Тип 2: Метрика одинакова для всех маршрутизаторов. Внешние маршруты типа 1 более надежны, чем внешние маршруты типа 2. **route-map** *map-name*: указывает связанное имя карты маршрутов. По умолчанию карта маршрутов не связана
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	При выполнении команды **redistribute** или **default-information** маршрутизатор OSPF автоматически становится ASBR. Однако ASBR не генерирует и не объявляет автоматически маршрут по умолчанию для всех маршрутизаторов в домене маршрутизации OSPF. Чтобы ASBR генерировал маршрут по умолчанию, настройте команду **default-information originate**. Если указан **always**, процесс маршрутизации OSPF объявляет соседям внешний маршрут по умолчанию независимо от того, существует ли маршрут по умолчанию. Однако этот маршрут по умолчанию не отображается на локальном маршрутизаторе. Чтобы убедиться, что маршрут по умолчанию создан, запустите команду **show ip ospf database**, чтобы отобразить базу данных состояния каналов OSPF. Внешний канал с идентификатором 0.0.0.0 описывает маршрут по умолчанию. На соседе OSPF вы можете запустить команду **show ip route**, чтобы увидеть маршрут по умолчанию. Метрику внешнего маршрута по умолчанию можно определить только в команде **default-information originate**, а не в команде **default-metric**. OSPF имеет два типа внешних маршрутов. Метрика внешнего маршрута типа 1 изменится, но метрика внешнего маршрута типа 2 останется неизменной. Если два параллельных пути к одному и тому же пункту назначения имеют одинаковую метрику маршрута, приоритет маршрута типа 1 выше, чем приоритет маршрута типа 2. Таким образом, команда **show ip route** отображает только маршрут типа 1. Маршрутизатор в тупиковой области не может генерировать внешний маршрут по умолчанию. Установленное значение метрики, связанное с картой маршрутов, должно находиться в диапазоне от 0 до 16 777 214. Если значение превышает этот диапазон, маршруты невозможно ввести

4.4.3.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Настройка статического перераспределения маршрутов

Сценарий:

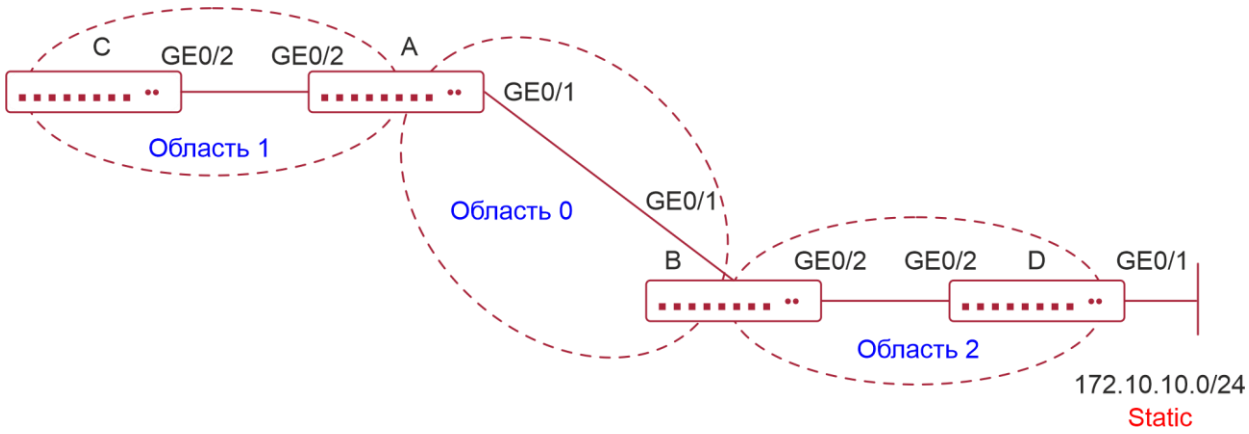


Рисунок 4-10.

IP-адреса интерфейса следующие:

A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1

B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1

C: GE 0/2 192.168.2.2

D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • Введите внешний статический маршрут к маршрутизатору D
D	D# configure terminal D(config)# ip route 172.10.10.0 255.255.255.0 192.168.6.3 D(config)#router ospf 1 D(config-router)# redistribute staticsubnets
Проверка	• На маршрутизаторе D запустите команду **show ip ospf database external brief**, чтобы убедиться, что генерируется LSA, соответствующий внешнему маршруту. • На маршрутизаторе C выполните команду **show ip route ospf**, чтобы убедиться, что внешний статический маршрут введен
D	D# show ip ospf database external brief OSPF Router with ID (192.168.22.30) (Process ID 1)

	AS External Link States Link ID ADV Router Age Seq# CkSum Route Tag 172.10.10.0 192.168.22.30 11 0x80000001 0xa4bb E2 172.10.10.0/24 0
C	C# show ip route ospf O E2 172.10.10.0/24 [110/20] via 192.168.2.1, 00:18:03, GigabitEthernet 0/2

Настройка маршрута по умолчанию

Сценарий:

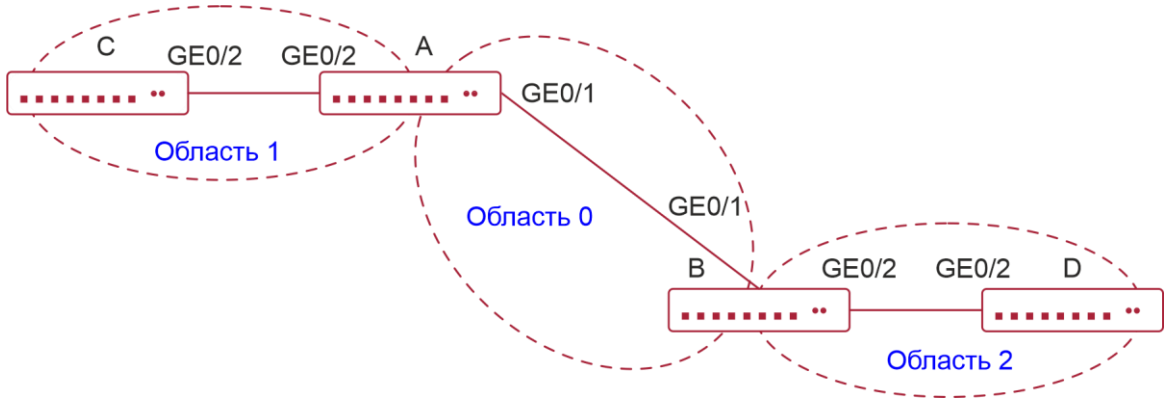


Рисунок 4-11.

IP-адреса интерфейса следующие:

A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1

B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1

C: GE 0/2 192.168.2.2

D: GE 0/2 192.168.3.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • Настройте маршрут по умолчанию на маршрутизаторе D
D	D# configure terminal D(config)#router ospf 1 D(config-router)#default-information originate always

Проверка	• На маршрутизаторе D запустите команду **show ip ospf database external brief**, чтобы убедиться, что создан LSA, соответствующий маршруту по умолчанию. • На маршрутизаторе C выполните команду **show ip route ospf**, чтобы убедиться, что существует маршрут по умолчанию OSPF
D	D#show ip ospf database external brief OSPF Router with ID (192.168.22.30) (Process ID 1)www.qtech.ru AS External Link States Link ID ADV Router Age Seq# CkSum Route Tag 0.0.0.0 192.168.22.30 565 0x80000002 0xa190 E2 0.0.0.0/0 1
C	C# show ip route ospf O E20.0.0.0/0 [110/20] via 192.168.2.1, 00:18:03, GigabitEthernet 0/2

4.4.3.7. Распространенные ошибки

- Маршрут подсети не введен, поскольку параметр **subnets** в команде **redistribute** не настроен.
- Петля маршрутизации формируется из-за того, что команда **default-information originate always** настроена на нескольких маршрутизаторах.
- Маршруты ввести невозможно, поскольку на маршрутизаторе в тупиковой области настроено перераспределение маршрутов.

4.4.4. Настройка тупиковой области и области NSSA

4.4.4.1. Эффект конфигурации

Настройте область, расположенную в тупике, как тупиковую область, чтобы уменьшить взаимодействие информации о маршрутизации и размер таблицы маршрутизации, а также повысить стабильность маршрутов.

4.4.4.2. Примечания

- Необходимо настроить основные функции OSPF.
- Магистральную или транзитную область нельзя настроить как тупиковую область или область NSSA.
- Маршрутизатор в тупиковой области не может вводить внешние маршруты, но маршрутизатор в области NSSA может вводить внешние маршруты.

4.4.4.3. Шаги настройки

Настройка тупиковой области

- (Опционально) Эта конфигурация необходима, если вы хотите уменьшить размер таблицы маршрутизации на маршрутизаторах в этой области.

- Область должна быть настроена как тупиковая на всех маршрутизаторах в этой области.

Настройка области NSSA

- (Опционально) Эта конфигурация необходима, если вы хотите уменьшить размер таблицы маршрутизации на маршрутизаторах в области и ввести в эту область внешние маршруты OSPF.
- Область должна быть настроена как область NSSA на всех маршрутизаторах в этой области.

4.4.4.4. Проверка

Проверка тупиковой области

На маршрутизаторе в тупиковой области запустите команду **show ip route**, чтобы убедиться, что маршрутизатор не загружен какими-либо внешними маршрутами.

Проверка области NSSA

- На маршрутизаторе в области NSSA выполните команду **show ip ospf database**, чтобы убедиться, что введенный внешний маршрут генерирует LSA типа 7.
- На маршрутизаторе в магистральной области запустите команду **show ip route**, чтобы убедиться, что маршрутизатор загружен внешними маршрутами, введенными из области NSSA.

4.4.4.5. Связанные команды

Настройка тупиковой области

Команда	**area** *area-id* **stub** [**no-summary**]
Описание параметра	*area-id*: указывает идентификатор тупиковой области. **no-summary**: запрещает ABR отправлять суммарные сетевые LSA. В это время тупиковую область можно назвать полностью тупиковой областью. Этот параметр настраивается только в том случае, если маршрутизатор является ABR
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Вы должны запустить команду **area stub** на всех маршрутизаторах в тупиковой области OSPF. ABR отправляет в тупиковую область только три типа LSA: (1) Тип 1: LSA маршрутизатора; (2) Тип 2: Сетевой LSA; (3) Тип 3: Суммарный сетевой LSA. С точки зрения таблицы маршрутизации маршрутизатор в тупиковой области может изучать только внутренние маршруты домена маршрутизации OSPF, включая внутренний маршрут по умолчанию, созданный ABR. Маршрутизатор в тупиковой области не может изучать внешние маршруты домена маршрутизации OSPF. Чтобы настроить полностью тупиковую область, добавьте ключевое слово **no-summary** при запуске команды **area stub** на ABR. Маршрутизатор в полностью тупиковой области может изучать только

	внутренние маршруты локальной области, включая внутренний маршрут по умолчанию, созданный ABR. Вы можете запустить команду **area stub** или **area default-cost**, чтобы настроить область OSPF как тупиковую область. Если используется **area stub**, необходимо настроить эту команду на всех маршрутизаторах, подключенных к тупиковой области. Если используется **area default-cost**, запускайте эту команду только на ABR в тупиковой области. Команда **area default-cost** определяет начальную стоимость (метрику) внутреннего маршрута по умолчанию

Настройка области NSSA

Команда	**area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate**[**metric** *value*] [**metric-type** *type*]] [**no-summary**] [**translator** [**stability-interval** *seconds* | **always**]]
Описание параметра	*area-id*: указывает идентификатор области NSSA. **no-redistribution**: выберите эту опцию, если маршрутизатор является NSSA ABR, и вы хотите использовать только команду **redistribute** для внесения информации о маршрутизации в общую область, а не в область NSSA. **default-information-originate**: указывает, что LSA типа 7 по умолчанию создается и вводится в область NSSA. Этот параметр действует только для NSSA ABR или ASBR. **metric** *value*: указывает метрику созданного LSA по умолчанию. Значение находится в диапазоне от 0 до 16 777 214. Значение по умолчанию — 1. **metric-type** *type*: указывает тип маршрута созданного LSA по умолчанию. Значения включают 1 и 2. **1** представляет N-1, а **2** представляет N-2. Значение по умолчанию — 2. **no-summary**: запрещает ABR в области NSSA отправлять суммарные LSA (LSA типа 3). **translator**: указывает, что NSSA ABR является транслятором. **stability-interval** *seconds*: указывает интервал стабильности после того, как NSSA ABR переключается с транслятора на нетранслятор. Указывается в секундах. Значение по умолчанию — 40. Значение находится в диапазоне от 0 до 2 147 483 647. **always**: указывает, что текущий ABR NSSA всегда действует как транслятор. Значение по умолчанию — резервный транслятор
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Параметр **default-information-originate** используется для создания LSA типа 7 по умолчанию. Этот параметр имеет разные функции в ABR и ASBR в области NSSA. В ABR создается маршрут по умолчанию LSA

	типа 7 независимо от того, существует ли маршрут по умолчанию в таблице маршрутизации. В ASBR (не ABR) маршрут по умолчанию LSA типа 7 генерируется только в том случае, если маршрут по умолчанию существует в таблице маршрутизации. Если в ASBR настроен параметр **no-redistribution**, другие внешние маршруты, введенные OSPF с помощью команды **redistribute**, не могут быть объявлены в области NSSA. Этот параметр обычно используется, когда маршрутизатор в области NSSA действует и как ASBR, и как ABR. Это предотвращает попадание внешней информации о маршрутизации в область NSSA. Чтобы еще больше сократить количество LSA, отправляемых в область NSSA, вы можете настроить параметр **no-summary** в ABR, чтобы запретить ABR отправлять суммарные LSA (LSA типа 3) в область NSSA. **area default-cost** используется на ABR или ASBR, подключенном к области NSSA. Эта команда настраивает стоимость маршрута по умолчанию, отправляемого из ABR/ASBR в область NSSA. По умолчанию стоимость маршрута по умолчанию, отправленного в область NSSA, равна 1. Если область NSSA имеет два или более ABR, ABR с наибольшим идентификатором маршрутизатора выбирается по умолчанию в качестве транслятора для преобразования LSA типа 7 в LSA типа 5. Если текущее устройство всегда является транслятором ABR для преобразования LSA типа 7 в LSA типа 5, используйте параметр **translator always**. Если роль транслятора текущего устройства заменяется другим ABR, возможность преобразования сохраняется в течение времени, указанного в **stability-interval**. Если маршрутизатор снова не станет транслятором в течение **stability-interval**, LSA, преобразованные из типа 7 в тип 5, будут удалены из AS после истечения **stability-interval**. Чтобы предотвратить петлю маршрутизации, LSA, преобразованные из типа 7 в тип 5, будут удалены из AS сразу после того, как текущее устройство потеряет роль транслятора, даже если **stability-interval** не истечет. В одной и той же области NSSA рекомендуется настраивать **translator always** только на одном ABR

4.4.4.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Настройка тупиковой области

Сценарий:

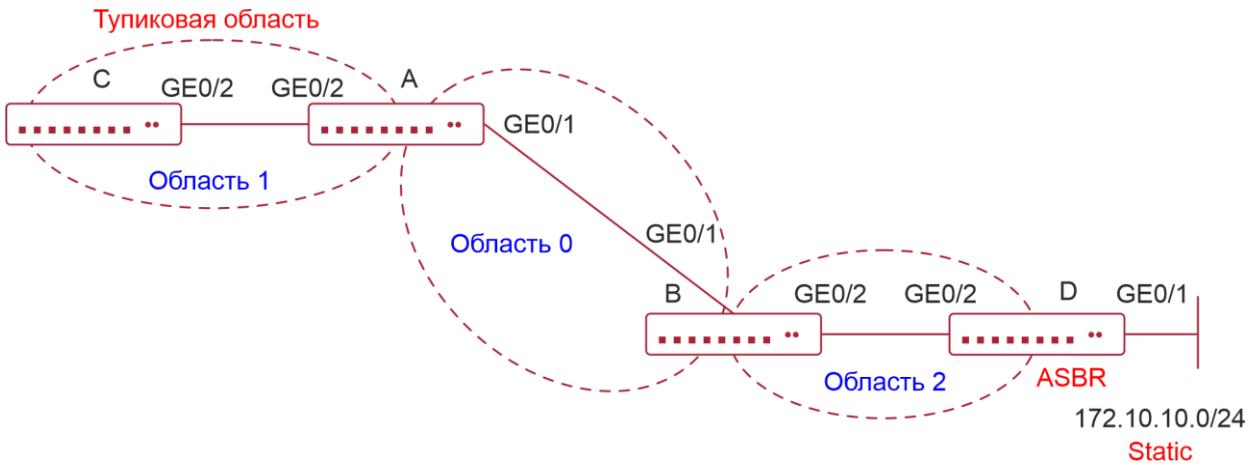


Рисунок 4-12.

IP-адреса интерфейса следующие:

A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1

B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1

C: GE 0/2 192.168.2.2

D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • Введите внешний статический маршрут к маршрутизатору D. • Настройте область 1 как тупиковую область на маршрутизаторах A и C
D	D# configure terminal D(config)#router ospf 1 D(config-router)# redistribute staticsubnets
A	A# configure terminal A(config)#router ospf 1 A(config-router)#area 1 stubno-summary
C	C# configure terminal C(config)#router ospf 1

	C(config-router)#area 1 stub
Проверка	На маршрутизаторе C выполните команду **show ip route ospf**, чтобы отобразить таблицу маршрутизации. Убедитесь, что существует только один межобластной маршрут по умолчанию и не введен внешний статический маршрут от маршрутизатора D
	C#show ip route ospf O*IA 0.0.0.0/0 [110/2] via 192.168.2.1, 00:30:53, GigabitEthernet 0/2

Настройка области NSSA

Сценарий:

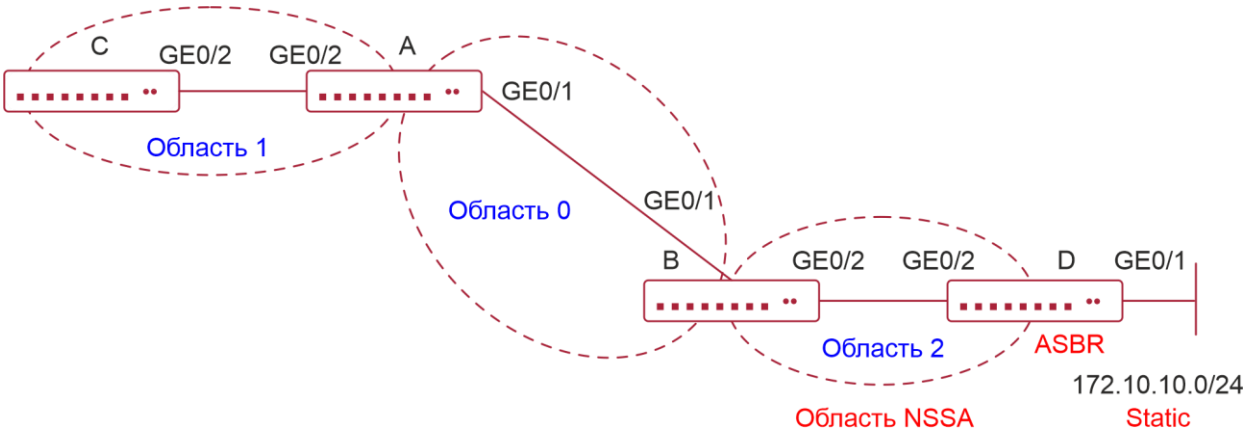


Рисунок 4-13.

IP-адреса интерфейса следующие:

A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1

B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1

C: GE 0/2 192.168.2.2

D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • Введите внешний статический маршрут к маршрутизатору D. • Настройте область 2 как область NSSA на маршрутизаторах B и D
B	B# configure terminal B(config)#router ospf 1

	B(config-router)#area 2 nssa
D	D# configure terminal D(config)#ip route 172.10.10.0 255.255.255.0 192.168.6.2 D(config)#router ospf 1 D(config-router)#redistribute static subnets D(config-router)#area 2 nssa
Проверка	• На маршрутизаторе D убедитесь, что генерируется LSA типа 7, 172.10.10.0/24. • На маршрутизаторе B убедитесь, что LSA типа 5 и типа 7 сосуществуют на 172.10.10.0/24. • На маршрутизаторе B убедитесь, что создан маршрут N-2 172.10.10.0/24
D	D# show ip ospf database nssa-external OSPF Router with ID (192.168.6.2) (Process ID 1) NSSA-external Link States (Area 0.0.0.1 [NSSA]) LS age: 61 Options: 0x8 (-|-|-|-|N/P|-|-|-) LS Type: AS-NSSA-LSA Link State ID: 172.10.10.0 (External Network Number For NSSA) Advertising Router: 192.168.6.2 LS Seq Number: 80000001 Checksum: 0xc8f8 Length: 36 Network Mask: /24 Metric Type: 2 (Larger than any link state path) TOS: 0 Metric: 20 NSSA: Forward Address: 192.168.6.2 External Route Tag: 0
B	B# show ip ospf database nssa-external OSPF Router with ID (192.168.3.1) (Process ID 1) NSSA-external Link States (Area 0.0.0.1 [NSSA]) LS age: 314 Options: 0x8 (-|-|-|-|N/P|-|-|-)

	LS Type: AS-NSSA-LSA Link State ID: 172.10.10.0 (External Network Number For NSSA) Advertising Router: 192.168.6.2 LS Seq Number: 80000001 Checksum: 0xc8f8 Length: 36 Network Mask: /24 Metric Type: 2 (Larger than any link state path) TOS: 0 Metric: 20 NSSA: Forward Address: 192.168.6.2 External Route Tag: 0 B# show ip ospf database external OSPF Router with ID (192.168.3.1) (Process ID 1) AS External Link States LS age: 875 Options: 0x2 (-|-|-|-|-|-|E|-) LS Type: AS-external-LSA Link State ID: 172.10.10.0 (External Network Number) Advertising Router: 192.168.3.1 LS Seq Number: 80000001 Checksum: 0xd0d3 Length: 36 Network Mask: /24 Metric Type: 2 (Larger than any link state path) TOS: 0 Metric: 20 Forward Address: 192.168.6.2 External Route Tag: 0 B# show ip route ospf O N2 172.10.10.0/24 [110/20] via 192.168.3.2, 00:06:53, GigabitEthernet 0/2

4.4.4.7. Распространенные ошибки

- Конфигурации типа области несовместимы на маршрутизаторах в одной и той же области.

- Внешние маршруты ввести невозможно, так как на маршрутизаторе в тупиковой области настроено перераспределение маршрутов.

4.4.5. Настройка суммирования маршрутов

4.4.5.1. Эффект конфигурации

- Суммируйте маршруты, чтобы уменьшить взаимодействие информации о маршрутизации и размер таблицы маршрутизации, а также повысить стабильность маршрутов.
- Экранируйте или фильтруйте маршруты.

4.4.5.2. Примечания

- Необходимо настроить основные функции OSPF.
- Диапазон адресов суммарных маршрутов может превышать фактический диапазон сети в таблице маршрутизации. Если данные отправляются в сеть за пределами диапазона суммирования, может образоваться петля маршрутизации и нагрузка на обработку маршрутизатора может увеличиться. Чтобы предотвратить эти проблемы, необходимо добавить отброшенный маршрут в таблицу маршрутизации или экранировать, или фильтровать маршруты.

4.4.5.3. Шаги настройки

Настройка суммирования межобластных маршрутов

- (Опционально) Эта конфигурация требуется, когда необходимо суммировать маршруты области OSPF.
- Если не требуется иное, эту настройку следует выполнять на ABR в области, где расположены суммируемые маршруты.

Настройка суммирования внешних маршрутов

- (Опционально) Эта конфигурация требуется, когда необходимо суммировать маршруты, внешние по отношению к домену OSPF.
- Если не требуется иное, эту настройку следует выполнять на ASBR, в который вводятся суммируемые маршруты.

4.4.5.4. Проверка

Запустите команду **show ip route ospf**, чтобы убедиться, что индивидуальные маршруты не существует и только суммарный маршрут существует.

4.4.5.5. Связанные команды

Настройка суммирования межобластных маршрутов

Команда	**area** *area-id* **range** *ip-address net-mask* [**advertise** | **not-advertise**] [**cost** *cost*]
Описание параметра	*area-id*: указывает идентификатор области OSPF, в которую следует внедрить суммарный маршрут. Идентификатор области может быть десятичным целым числом или IP-адресом.

	ip-address net-mask: определяет сетевой сегмент суммарного маршрута. **advertise** | **not-advertise**: указывает, следует ли объявлять суммарный маршрут. **cost** *cost*: указывает метрику суммарного маршрута. Значение варьируется от 0 до 16 777 215
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Эту команду можно выполнить только на ABR. Он используется для объединения или суммирования нескольких маршрутов области в один маршрут и объявления маршрута в других областях. Объединение маршрутной информации происходит только на границе области. Маршрутизаторы внутри области могут изучать конкретную информацию о маршрутизации, тогда как маршрутизаторы в других областях могут изучать только один суммарный маршрут. Кроме того, вы можете настроить **advertise** или **not-advertise**, чтобы определить, следует ли объявлять суммарный маршрут для защиты и фильтрации маршрутов. По умолчанию объявляется суммарный маршрут. Вы можете использовать параметр **cost**, чтобы задать метрику суммарного маршрута. Вы можете настроить команды суммирования маршрутов для нескольких областей. Это упрощает маршруты во всем домене маршрутизации OSPF и повышает производительность переадресации сети, особенно для сетей большого размера. Если настроено несколько команд суммирования маршрутов и имеются инклюзивные отношения друг с другом, диапазон суммируемых областей определяется по принципу максимального соответствия

Настройка суммирования внешних маршрутов

Команда	**summary-address** *ip-address net-mask* [**not-advertise** | **tag** *value*]
Описание параметра	*ip-address*: указывает IP-адрес суммарного маршрута. *net-mask*: указывает маску подсети суммарного маршрута. **not-advertise**: указывает, что суммарный маршрут не объявляется. Если этот параметр не указан, объявляется суммарный маршрут. **tag** *value*: указывает тег суммарного маршрута. Значение варьируется от 0 до 4 294 967 295
Командный режим	Режим конфигурации процесса маршрутизации OSPF

Руководство по использованию	Когда маршруты перераспределяются из других процессов маршрутизации и вводятся в процесс маршрутизации OSPF, каждый маршрут объявляется маршрутизаторам OSPF с использованием внешнего LSA. Если внедренные маршруты представляют собой непрерывное адресное пространство, ABR может объявлять только один суммарный маршрут, чтобы значительно уменьшить размер таблицы маршрутизации. **area range** суммирует маршруты между маршрутами OSPF, тогда как **summary-address** суммирует внешние маршруты домена маршрутизации OSPF. При настройке на трансляторе NSSA ABR **summary-address** суммирует перераспределенные маршруты и маршруты, полученные на основе LSA, которые преобразуются из типа 7 в тип 5. При настройке на ASBR (не трансляторе ABR NSSA) **summary-address** суммирует только перераспределенные маршруты

Настройка отброшенного маршрута

Команда	**discard-route** { **internal** | **external** }
Описание параметра	**internal**: указывает, что можно добавить отброшенный маршрут, созданный командой **area range**. **external**: указывает, что можно добавить отброшенный маршрут, созданный командой **summary-address**
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Диапазон адресов суммарных маршрутов может превышать фактический диапазон сети в таблице маршрутизации. Если данные отправляются в сеть за пределами диапазона суммирования, может образоваться петля маршрутизации и нагрузка на обработку маршрутизатора может увеличиться. Чтобы предотвратить эти проблемы, в таблицу маршрутизации на ABR или ASBR необходимо добавить отброшенный маршрут. Этот маршрут генерируется автоматически и не объявляется

4.4.5.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF."

Сценарий:

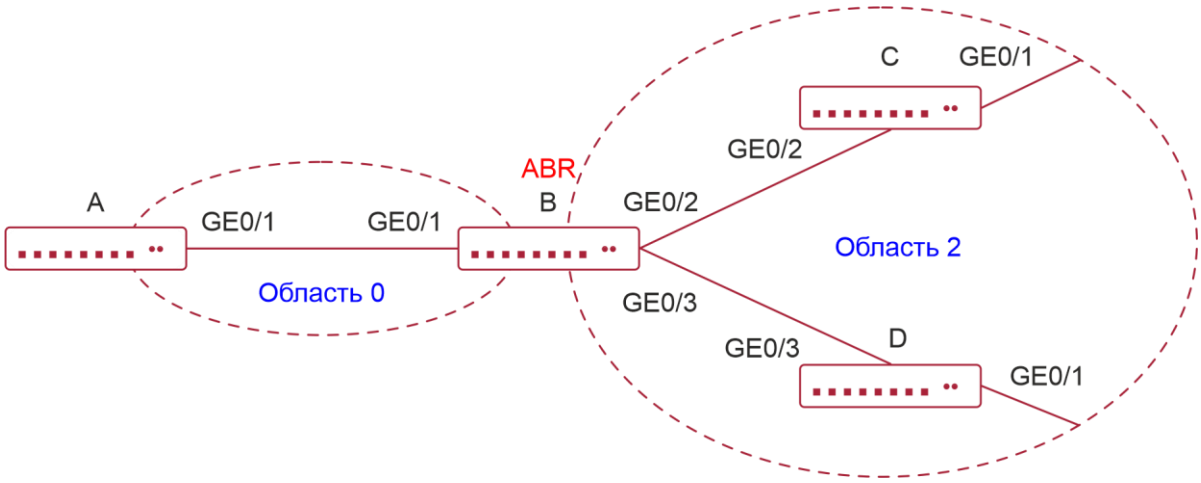


Рисунок 4-14.

IP-адреса интерфейса следующие:

A: GE0/1 192.168.1.1

B: GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1

C: GE0/2 172.16.2.2 GE0/1 172.16.4.2

D: GE0/2 172.16.3.2 GE0/1 172.16.5.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • Суммируйте маршруты области 2 на маршрутизаторе B
B	B# configure terminal B(config)#router ospf 1 B(config-router)#area 2 range 172.16.0.0 255.255.0.0
Проверка	На маршрутизаторе A убедитесь, что запись 172.16.0.0/16 добавлена в таблицу маршрутизации
A	A#show ip route ospf O IA 172.16.0.0/16 [110/2] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1

4.4.5.7. Распространенные ошибки

Суммирование маршрутов между областями невозможно реализовать, поскольку команда **area range** настроена на устройстве, не поддерживающем ABR.

4.4.6. Настройка фильтрации маршрутов

4.4.6.1. Эффект конфигурации

Маршруты, не соответствующие условиям фильтрации, не могут быть загружены в таблицу маршрутизации или объявлены соседям. Пользователи сети не могут получить доступ к указанной сети назначения.

4.4.6.2. Примечания

- Необходимо настроить основные функции OSPF.
- Фильтрация маршрутов с помощью команды **distribute-list in** влияет на пересылку локальных маршрутов, но не влияет на вычисление маршрутов на основе LSA. Таким образом, если на ABR настроена фильтрация маршрутов, LSA типа 3 по-прежнему будут генерироваться и объявляться в других областях, поскольку маршруты по-прежнему можно рассчитывать на основе LSA. В результате генерируются маршруты black-hole. В этом случае вы можете запустить команду **area filter-list** или **area range** (содержащую параметр **not-advertise**) на ABR, чтобы предотвратить создание маршрутов black-hole.

4.4.6.3. Шаги настройки

Настройка фильтрации межобластных маршрутов

- (Опционально) Эту конфигурацию рекомендуется использовать, если пользователям необходимо ограничить доступ к сети в определенной области OSPF.
- Если не требуется иное, эту настройку следует выполнять на ABR в районе расположения фильтруемых маршрутов.

Настройка фильтрации перераспределенных маршрутов

- (Опционально) Эта конфигурация требуется, если необходимо фильтровать внешние маршруты, введенные ASBR.
- Если не требуется иное, эту настройку следует выполнять на ASBR, в который введены фильтруемые маршруты.

Настройка фильтрации изученных маршрутов

- (Опционально) Эта конфигурация требуется, если пользователям необходимо ограничить доступ к указанной целевой сети.
- Если не требуется иное, эту настройку следует выполнять на маршрутизаторе, требующем фильтрации маршрутов.

4.4.6.4. Проверка

- Запустите команду **show ip route**, чтобы убедиться, что маршрутизатор не загружен отфильтрованными маршрутами.
- Запустите команду **ping**, чтобы убедиться, что указанная сеть назначения недоступна.

4.4.6.5. Связанные команды

Настройка пассивного интерфейса

Команда	**passive-interface**{ **default** | *interface-type interface-number* | *interface-type interface-number ip-address*}
Описание параметра	*interface-type interface-number*: указывает интерфейс, который следует настроить как пассивный интерфейс. **default**: указывает, что все интерфейсы будут настроены как пассивные интерфейсы. *interface-type interface-number ip-address*: указывает адрес интерфейса как пассивный адрес
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Чтобы другие маршрутизаторы в сети не узнали информацию о маршрутизации локального маршрутизатора, вы можете настроить указанный сетевой интерфейс локального маршрутизатора в качестве пассивного интерфейса или указанный IP-адрес сетевого интерфейса в качестве пассивного адреса

Настройка фильтрации пакетов обновлений LSA

Команда	**ip ospf database-filter all out**
Командный режим	Режим настройки интерфейса
Руководство по использованию	Включите эту функцию на интерфейсе, чтобы предотвратить отправку пакета обновления LSA на этот интерфейс. После включения этой функции локальный маршрутизатор не объявляет пакет обновления LSA соседям, но по-прежнему устанавливает смежность с соседями и получает LSA от соседей

Настройка фильтрации межобластных маршрутов

Команда	**area** *area-id* **filter-list** {**access** *acl-name*| **prefix** *prefix-name*} {**in** | **out**}
Описание параметра	*area-id*: указывает идентификатор области. **access** *acl-name*: указывает связанный список ACL. **prefix** *prefix-name*: указывает связанный список префиксов. **in** | **out**: фильтрует маршруты, получаемые или отправляемые из области

Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Эту команду можно настроить только на ABR. Используйте эту команду, когда необходимо настроить условия фильтрации для межобластных маршрутов на ABR

Настройка фильтрации перераспределенных маршрутов

Команда	**distribute-list { [** *access-list-number* **|** *name* **]	prefix** *prefix-list-name* **} out [bgp	connected |isis[***area-tag***]	ospf** *process-id* **| rip	arp-host	static]**
Описание параметра	*access-list-number*	*name*: использует ACL для фильтрации. **prefix** *prefix-list-name*: использует список префиксов для фильтрации. **bgp**	**connected** |**isis**[*area-tag*]	**ospf** *process-id*	**rip**	**arp-host**	**static**: указывает источник маршрутов для фильтрации
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	**distribute-list out** аналогичен **redistribute route-map** и используется для фильтрации маршрутов, перераспределяемых из других протоколов в OSPF. Сама команда **distribute-list out** не перераспределяет маршруты и обычно используется вместе с командой **redistribute**. ACL и правила фильтрации списка префиксов в конфигурации являются взаимоисключающими. То есть, если ACL используется для фильтрации маршрутов, поступающих из определенного источника, список префиксов нельзя настроить для фильтрации одних и тех же маршрутов

Настройка фильтрации изученных маршрутов

Команда	**distribute-list** {[*access-list-number*	*name*]	**prefix** *prefix-list-name* [**gateway** *prefix-list-name*]	**route-map** *route-map-name* } **in** [*interface-type interface-number*]
Описание параметра	*access-list-number*	*name*: использует ACL для фильтрации. **gateway** *prefix-list-name*: использует шлюз для фильтрации. **prefix** *prefix-list-name*: использует список префиксов для фильтрации. **route-map** *route-map-name*: использует карту маршрута для фильтрации. *interface-type interface-number*: указывает интерфейс, для которого фильтруются маршруты LSA

Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Фильтруйте маршруты, вычисляемые на основе полученных LSA. Пересылаться могут только маршруты, соответствующие условиям фильтрации. Команда не влияет на LSDB или таблицы маршрутизации соседей. ACL, список префиксов и правила фильтрации карты маршрутов являются взаимоисключающими в конфигурации. То есть, если ACL используется для фильтрации маршрутов указанного интерфейса, список префиксов или карта маршрутизаторов не могут быть настроены для фильтрации маршрутов того же интерфейса

4.4.6.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Сценарий:

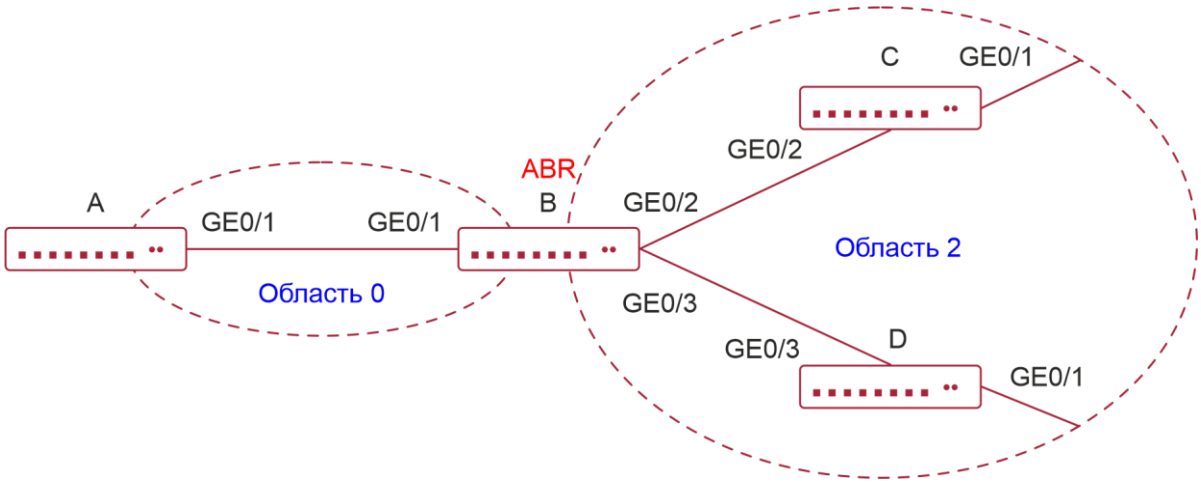


Рисунок 4-15.

IP-адреса интерфейса следующие:

A: GE0/1 192.168.1.1

B: GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1

C: GE0/2 172.16.2.2 GE0/3 172.16.4.2

D: GE0/2 172.16.3.2 GE0/3 172.16.5.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (пропущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (пропущено)

	• На маршрутизаторе A настройте фильтрацию маршрутов
A	A# configure terminal A(config)#access-list 3 permit host 172.16.5.0 A(config)#router ospf 1 A(config-router)#distribute-list 3 in GigabitEthernet 0/1
Проверка	На маршрутизаторе A проверьте таблицу маршрутизации. Убедитесь, что загружена только запись 172.16.5.0/24
A	A# show ip route ospf O 172.16.5.0/24 [110/2] via 192.168.1.2, 10:39:40, GigabitEthernet 0/1

4.4.6.7. Распространенные ошибки

Фильтрация маршрутов с помощью команды **distribute-list in** влияет на пересылку локальных маршрутов, но не влияет на вычисление маршрутов на основе LSA. Таким образом, если на ABR настроена фильтрация маршрутов, LSA типа 3 по-прежнему будут генерироваться и объявляться в других областях, поскольку маршруты по-прежнему можно рассчитывать на основе LSA. В результате генерируются маршруты black-hole.

4.4.7. Изменение стоимости маршрута и AD

4.4.7.1. Эффект конфигурации

- Измените маршруты OSPF, чтобы разрешить прохождение трафика через указанные узлы или избежать прохождения через указанные узлы.
- Измените последовательность выбора маршрутов маршрутизатором, чтобы изменить приоритеты маршрутов OSPF.

4.4.7.2. Примечания

- Необходимо настроить основные функции OSPF.
- Если вы запустите команду **ip ospf cost** для настройки стоимости интерфейса, настроенная стоимость автоматически перезапишет стоимость, рассчитанную на основе автоматической стоимости.

4.4.7.3. Шаги настройки

Настройка эталонной полосы пропускания

- Опционально.
- Маршрутизатор подключен к линиям связи с разной полосой пропускания. Эту конфигурацию рекомендуется использовать, если вы хотите преимущественно выбрать линию связи с большей полосой пропускания.

Настройка стоимости интерфейса

- Опционально.

- Маршрутизатор подключен по нескольким линиям связи. Эту конфигурацию рекомендуется использовать, если вы хотите вручную указать приоритетную линию связи.

Настройка метрики по умолчанию для перераспределения

- Опционально.
- Эта конфигурация является обязательной, если стоимость внешних маршрутов домена OSPF должна быть указана при введении внешних маршрутов в ASBR.

Настройка максимальной метрики

- Опционально.
- Маршрутизатор может работать нестабильно во время процесса перезапуска или в течение определенного периода времени после перезапуска маршрутизатора, и пользователи не хотят пересылать данные через этот маршрутизатор. В этом случае рекомендуется использовать данную конфигурацию.

Настройка AD

- Опционально.
- Эта конфигурация обязательна, если вы хотите изменить приоритеты маршрутов OSPF на маршрутизаторе, который использует несколько протоколов unicast-маршрутизации.

4.4.7.4. Проверка

- Запустите команду **show ip ospf interface**, чтобы убедиться в правильности стоимости интерфейсов.
- Запустите команду **show ip route**, чтобы убедиться, что стоимость внешних маршрутов, введенных в ASBR, верна.
- Перезагрузите маршрутизатор. В течение заданного периода времени данные не пересылаются через перезапущенный маршрутизатор.

4.4.7.5. Связанные команды

Настройка эталонной полосы пропускания

Команда	**auto-costreference-bandwidth** *ref-bw*
Описание параметра	*ref-bw*: указывает эталонную полосу пропускания. Единица измерения — Мбит/с. Значение варьируется от 1 до 4 294 967
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	По умолчанию стоимость интерфейса OSPF равна эталонному значению автоматической стоимости, деленному на пропускную способность интерфейса. Запустите команду **auto-cost**, чтобы получить эталонное значение автоматической стоимости. Значение по умолчанию — 100 Мбит/с. Запустите команду **bandwidth**, чтобы установить пропускную способность интерфейса.

	Стоимость интерфейсов OSPF по нескольким типовым линиям связи следующая: 64 кбит/с серийная линия связи: стоимость 1562. Линия связи E1: стоимость — 48. 10M Ethernet: стоимость 10. 100M Ethernet: стоимость 1. Если вы запустите команду **ip ospf cost** для настройки стоимости интерфейса, настроенная стоимость автоматически перезапишет стоимость, рассчитанную на основе автоматической стоимости

Настройка стоимости интерфейса

Команда	**ip ospf cost** *cost*
Описание параметра	*cost*: указывает стоимость интерфейса OSPF. Значение варьируется от 0 до 65 535
Командный режим	Режим настройки интерфейса
Руководство по использованию	По умолчанию стоимость интерфейса OSPF равна эталонному значению автоматической стоимости, деленному на пропускную способность интерфейса. Запустите команду **auto-cost**, чтобы получить эталонное значение автоматической стоимости. Значение по умолчанию — 100 Мбит/с. Запустите команду **bandwidth**, чтобы установить пропускную способность интерфейса. Стоимость интерфейсов OSPF по нескольким типовым линиям связи следующая: 64 кбит/с серийная линия связи: стоимость 1562. Линия связи E1: стоимость — 48. 10M Ethernet: стоимость 10. 100M Ethernet: стоимость 1. Если вы запустите команду **ip ospf cost** для настройки стоимости интерфейса, настроенная стоимость автоматически перезапишет стоимость, рассчитанную на основе автоматической стоимости

Настройка стоимости маршрута по умолчанию в тупиковой области или области NSSA

Команда	**area** *area-id* **default-cost** *cost*
Описание параметра	*area-id*: указывает идентификатор тупиковой области или области NSSA. *cost*: указывает стоимость суммарного маршрута по умолчанию, введенного в тупиковую область или область NSSA. Значение находится в диапазоне от 0 до 16 777 215
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Эта команда действует только на ABR в тупиковой области или на ABR/ASBR в области NSSA. ABR в тупиковой области или ABR/ASBR в области NSSA разрешено объявлять LSA, указывающее маршрут по умолчанию в тупиковой области или области NSSA. Вы можете запустить команду **area default-cost**, чтобы изменить стоимость объявленного LSA

Настройка метрики по умолчанию для перераспределения

Команда	**default-metric** *metric*
Описание параметра	*metric*: указывает метрику по умолчанию для перераспределенного маршрута OSPF. Значение варьируется от 1 до 16 777 214
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Команда **default-metric** должна использоваться вместе с командой **redistribute** для изменения исходных метрик всех перераспределяемых маршрутов. Команда **default-metric** не действует на внешние маршруты, которые вводятся в домен маршрутизации OSPF командой **default-information originate**

Настройка максимальной метрики

Команда	**max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup**[*seconds*]] [**summary-lsa** [*max-metric-value*]]
Описание параметра	**router-lsa**: устанавливает метрики не тупиковых (non-stub) каналов в LSA маршрутизатора на максимальное значение (0xFFFF).

	external-lsa: позволяет маршрутизатору заменять метрики внешних LSA (включая LSA типа 5 и типа 7) на максимальную метрику. *max-metric-value*: указывает максимальную метрику LSA. Значение по умолчанию — 16 711 680. Значение находится в диапазоне от 1 до 16 777 215. **include-stub**: устанавливает метрики тупиковых каналов в LSA маршрутизатора, объявляемые маршрутизатором, на максимальное значение. **on-startup**: позволяет маршрутизатору объявлять максимальную метрику при запуске. *seconds*: указывает интервал, с которым объявляется максимальная метрика. Значение по умолчанию — 600 с. Значение варьируется от 5 до 86 400. **summary-lsa**: позволяет маршрутизатору заменять метрики суммарных LSA (включая LSA типа 3 и типа 4) максимальной метрикой
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	После выполнения команды **max-metric router-lsa** метрики не тупиковых (non-stub) каналов в LSA маршрутизатора, генерируемые маршрутизатором, будут установлены на максимальное значение (0xFFFF). Если вы отмените эту настройку или истечет таймер, нормальные метрики каналов будут восстановлены. По умолчанию, если выполняется команда **max-metric router-lsa**, тупиковые ссылки по-прежнему объявляют общие метрики, то есть стоимость исходящих интерфейсов. Если настроен параметр **include-stub**, тупиковые каналы будут объявлять максимальную метрику. Если ABR не желает передавать трафик между областями, используйте параметр **summary-lsa**, чтобы установить для метрики суммарного LSA максимальную метрику. Если ASBR не желает передавать внешний трафик, используйте параметр **external-lsa**, чтобы установить максимальную метрику внешнего LSA. Команда **max-metric router-lsa** обычно используется в следующих сценариях: Перезагрузите устройство. После перезапуска устройства IGP обычно сходится (конвергируется) быстрее, и другие устройства пытаются перенаправить трафик через перезапущенное устройство. Если текущее устройство все еще создает таблицу маршрутизации BGP и некоторые маршруты BGP еще не изучены, пакеты, отправленные в эти сети, будут отброшены. В этом случае вы можете использовать параметр **on-startup**, чтобы установить задержку, после которой перезапущенное устройство будет действовать в режиме передачи.

	• Добавляет устройство в сеть, но устройство не используется для передачи трафика. Устройство добавлено в сеть. Если путь-кандидат существует, текущее устройство не используется для передачи трафика. Если путь-кандидат не существует, текущее устройство по-прежнему используется для передачи трафика. • Удалите устройство из сети корректно. После выполнения команды **max-metric router-lsa** текущее устройство объявляет максимальную метрику.среди всех метрик маршрутов. Таким образом, другие устройства в сети смогут выбрать резервный путь для передачи данных до выключения устройства. В более ранней версии OSPF (RFC1247 или более ранней) каналы с максимальной метрикой (0xFFFF) в LSA не участвуют в вычислении SPF, то есть трафик не отправляется на маршрутизаторы, генерирующие эти LSA

Настройка совместимости RFC1583

Команда	**compatible rfc1583**
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Если существует несколько путей к ASBR или адресу пересылки внешнего маршрута, RFC1583 и RFC2328 определяют разные правила маршрутизации. Если настроена совместимость с RFC1583, предпочтительно выбирается путь в магистральной области или путь между областями. Если совместимость с RFC1583 не настроена, предпочтительно выбирается путь в немагистральной области

Настройка AD

Команда	**distance** { *distance* [**route-map** *map-name*] | **ospf**{ **intra-area** *distance* [**route-map** *map-name*] |**inter-area** *distance* [**route-map** *map-name*] |**external** *distance* [**route-map** *map-name*] } }
Описание параметра	*distance*: указывает AD маршрута. Значение варьируется от 1 до 255. **intra-area** *distance*: указывает AD внутриобластного маршрута. Значение варьируется от 1 до 255. **inter-area** *distance*: указывает AD межобластного маршрута. Значение варьируется от 1 до 255. **external** *distance*: указывает AD внешнего маршрута. Значение варьируется от 1 до 255. **route-map** *map-name*: указывает AD указанного маршрута согласно политике

Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Используйте эту команду, чтобы указать разные AD для разных типов маршрутов OSPF. Настройте параметр **route-map**, чтобы установить AD для указанного маршрута с помощью политики. Если **route-map** настроила **set distance** через согласованный маршрут: AD устанавливается с помощью **set distance** через несогласованный маршрут: AD устанавливается командой **distance**

4.4.7.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Настройка стоимости интерфейса

Сценарий:

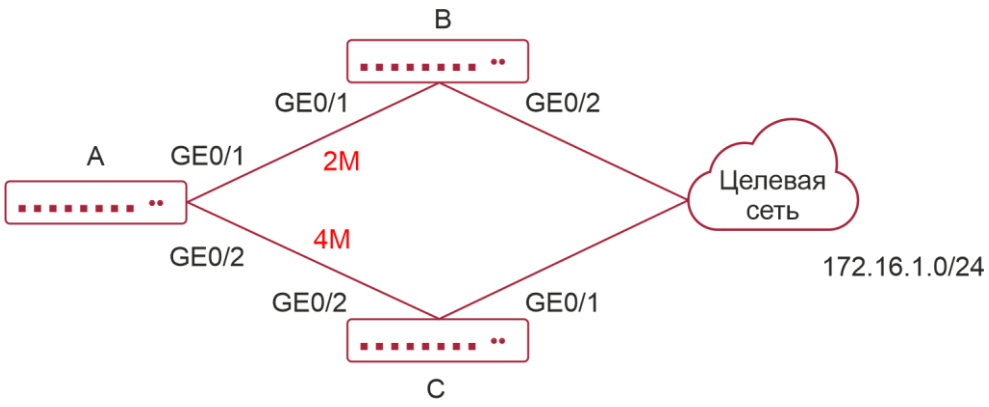


Рисунок 4-16.

IP-адреса интерфейса следующие:

A: GE0/1 192.168.1.1 GE0/2 192.168.2.1

B: GE0/1 192.168.1.2 GE0/2 192.168.3.2

C: GE0/1 192.168.4.2 GE0/2 192.168.2.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено)

	• На маршрутизаторе A настройте стоимость каждого интерфейса
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip ospf cost 10 A(config)# interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)# ip ospf cost 20
Проверка	На маршрутизаторе A проверьте таблицу маршрутизации. Следующий hop оптимального пути к 172.16.1.0/24 — это маршрутизатор B
A	A# show ip route ospf O E2172.16.1.0/0 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1

4.4.7.7. Распространенные ошибки

Если в команде **ip ospf cost** стоимость интерфейса установлена равной 0, может возникнуть ошибка расчета маршрута. Например, получается петля маршрутизации.

4.4.8. Включение аутентификации

4.4.8.1. Эффект конфигурации

Все маршрутизаторы, подключенные к сети OSPF, должны пройти аутентификацию, чтобы обеспечить стабильность OSPF и защитить OSPF от вторжений.

4.4.8.2. Примечания

- Необходимо настроить основные функции OSPF.
- Если для области настроена аутентификация, конфигурация вступает в силу на всех интерфейсах, принадлежащих этой области.
- Если аутентификация настроена как для интерфейса, так и для области, к которой принадлежит интерфейс, конфигурация интерфейса вступает в силу преимущественно.

4.4.8.3. Шаги настройки

Настройка типа аутентификации области

- (Опционально) Эту конфигурацию рекомендуется использовать, если на всех интерфейсах в одной области должен использоваться один и тот же тип аутентификации.
- Эта конфигурация необходима, если маршрутизатор получает доступ к сети, требующей аутентификации.

Настройка типа аутентификации интерфейса

- (Опционально) Эту конфигурацию рекомендуется использовать, если разные типы аутентификации должны использоваться на разных интерфейсах в одной и той же области.

- Эта конфигурация необходима, если маршрутизатор получает доступ к сети, требующей аутентификации.

Настройка ключа аутентификации в виде обычного текста для интерфейса

- Опционально.
- Эта конфигурация необходима, если маршрутизатор получает доступ к сети, требующей аутентификации в виде обычного текста.

Настройка ключа аутентификации MD5 для интерфейса

- (Опционально) Аутентификация MD5 обеспечивает высокий уровень безопасности, поэтому рекомендуется. Вам необходимо настроить либо аутентификацию в виде обычного текста, либо аутентификацию MD5.
- Эта конфигурация необходима, если маршрутизатор получает доступ к сети, требующей аутентификации MD5.

4.4.8.4. Проверка

- Если маршрутизаторы настроены с разными ключами аутентификации, запустите команду **show ip ospf neighbor**, чтобы убедиться в отсутствии соседа OSPF.
- Если маршрутизаторы настроены с одним и тем же ключом аутентификации, запустите команду **show ip ospf neighbor**, чтобы проверить наличие соседей OSPF.

4.4.8.5. Связанные команды

Настройка типа аутентификации области

Команда	**area** *area-id* **authentication** [**message-digest**]
Описание параметра	*area-id*: указывает идентификатор области, в которой включена аутентификация OSPF. Идентификатор области может быть десятичным целым числом или IP-адресом. **message-digest**: включает аутентификацию MD5
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Поддерживается три типа аутентификации: (1) Тип 0: аутентификация не требуется. Если эта команда не настроена, чтобы включить аутентификацию OSPF, тип аутентификации в пакете данных OSPF равен 0. (2) Тип 1: тип аутентификации — аутентификация в виде обычного текста. Если эта команда настроена, но не содержит параметра **message-digest**. (3) Тип 3: тип аутентификации — аутентификация MD5, если эта команда настроена и содержит параметр **message-digest**. Все маршрутизаторы в одной и той же области OSPF должны использовать один и тот же тип аутентификации. Если аутентификация

	включена, ключ аутентификации должен быть настроен на интерфейсах, подключенных к соседям. Вы можете запустить команду конфигурации интерфейса **ip ospf authentication-key**, чтобы настроить текстовый ключ аутентификации, или **ip ospf message-digest-key**, чтобы настроить ключ аутентификации MD5

Настройка типа аутентификации интерфейса

Команда	**ip ospf authentication** [**message-digest** | **null**]
Описание параметра	**message-digest**: указывает, что аутентификация MD5 включена на текущем интерфейсе. **null**: указывает, что аутентификация не включена
Командный режим	Режим настройки интерфейса
Руководство по использованию	Если команда **ip ospf authentication** не содержит каких-либо параметров, это означает, что аутентификация в виде обычного текста включена. Если вы используете форму **no** команды для восстановления режима аутентификации по умолчанию, то, включена ли аутентификация, определяется типом аутентификации, настроенным в области, к которой принадлежит интерфейс. Если для типа аутентификации установлено значение **null**, аутентификация отключается принудительно. Если аутентификация настроена как для интерфейса, так и для области, к которой принадлежит интерфейс, предпочтительно используется тип аутентификации, настроенный для интерфейса

Настройка ключа аутентификации в виде обычного текста для интерфейса

Команда	**ip ospf authentication-key**[**0** |**7**]*key*
Описание параметра	**0**: указывает, что ключ отображается в виде обычного текста. **7**: указывает, что ключ отображается в зашифрованном виде. *key*: указывает ключ. Ключ представляет собой строку длиной до восьми символов
Командный режим	Режим настройки интерфейса
Руководство по использованию	Ключ, настроенный с помощью команды **ip ospf authentication-key**, будет вставлен в заголовки всех пакетов OSPF. Если ключи несовместимы, два напрямую подключенных устройства не смогут настроить смежность OSPF и, следовательно, не смогут обмениваться информацией о маршрутизации.

	Для разных интерфейсов можно настроить разные ключи, но все маршрутизаторы, подключенные к одному физическому сегменту сети, должны быть настроены с использованием одного и того же ключа. Вы можете включить или отключить аутентификацию в области OSPF, выполнив команду **area authentication** в режиме настройки процесса маршрутизации OSPF. Вы также можете включить аутентификацию на отдельном интерфейсе, выполнив команду **ip ospf authentication** в режиме конфигурации интерфейса. Если аутентификация настроена как для интерфейса, так и для области, к которой принадлежит интерфейс, предпочтительно используется тип аутентификации, настроенный для интерфейса

Настройка ключа аутентификации MD5 для интерфейса

Команда	**ip ospf message-digest-key** *key-id* **md5**[**0** |**7**]*key*
Описание параметра	*key-id*: указывает идентификатор ключа. Значение варьируется от 1 до 255. **0**: указывает, что ключ отображается в виде обычного текста. **7**: указывает, что ключ отображается в зашифрованном виде. *key*: указывает ключ. Ключ представляет собой строку длиной до 16 символов
Командный режим	Режим настройки интерфейса
Руководство по использованию	Ключ, настроенный с помощью команды **ip ospf message-digest-key**, будет вставлен в заголовки всех пакетов OSPF. Если ключи несовместимы, два напрямую подключенных устройства не смогут настроить смежность OSPF и, следовательно, не смогут обмениваться информацией о маршрутизации. Для разных интерфейсов можно настроить разные ключи, но все маршрутизаторы, подключенные к одному физическому сегменту сети, должны быть настроены с использованием одного и того же ключа. Один и тот же идентификатор ключа на соседних маршрутизаторах должен соответствовать одному и тому же ключу. Вы можете включить или отключить аутентификацию в области OSPF, выполнив команду **area authentication** в режиме настройки процесса маршрутизации OSPF. Вы также можете включить аутентификацию на отдельном интерфейсе, выполнив команду **ip ospf authentication** в режиме конфигурации интерфейса. Если аутентификация настроена как для интерфейса, так и для области, к которой принадлежит интерфейс, предпочтительно используется тип аутентификации, настроенный для интерфейса.

	Программное обеспечение поддерживает плавную модификацию ключа аутентификации MD5. Прежде чем старый ключ можно будет удалить, необходимо сначала добавить новый ключ аутентификации MD5. Когда к маршрутизатору добавляется ключ аутентификации OSPF MD5, маршрутизатор определяет, что другие маршрутизаторы еще не используют новый ключ, и поэтому использует разные ключи для отправки нескольких пакетов OSPF, пока не подтвердит, что новый ключ настроен на соседях. После настройки нового ключа на всех роутерах вы можете удалить старый ключ

4.4.8.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Сценарий:

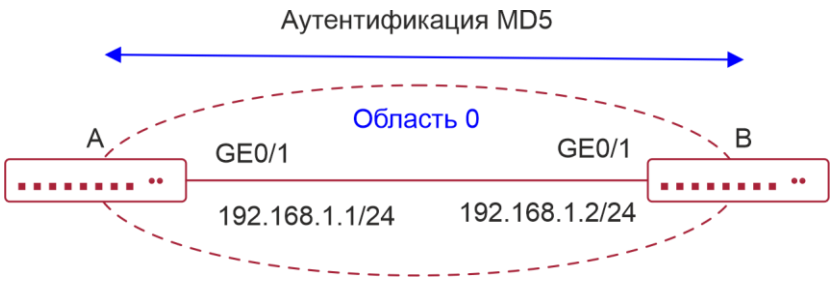


Рисунок 4-17.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (пропущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (пропущено) • Настройте тип аутентификации и ключ аутентификации MD5 на всех маршрутизаторах
A	A# configure terminal A(config)#router ospf 1 A(config-router)#area 0 authentication message-digest A(config-router)#exit A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ip ospf message-digest-key 1 md5 hello
B	B# configure terminal B(config)#router ospf 1

	B(config-router)#area 0 authentication message-digest B(config-router)#exit B(config)#interface GigabitEthernet 0/3 B(config-if-GigabitEthernet 0/3)#ip ospf message-digest-key 1 md5 hello
Проверка	На маршрутизаторе A и маршрутизаторе B убедитесь, что статус соседа OSPF правильный
A	A#show ip ospf neighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/DR 00:00:32 192.168.1.2 GigabitEthernet 0/1
A	#show ip ospf neighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/DR 00:00:32 192.168.1.1 GigabitEthernet 0/1

4.4.8.7. Распространенные ошибки

- Режимы аутентификации, настроенные на маршрутизаторах, несовместимы.
- Ключи аутентификации, настроенные на маршрутизаторах, несовместимы.

4.4.9. Включение переполнения

4.4.9.1. Эффект конфигурации

- Новые маршруты не загружаются в маршрутизаторы, если памяти маршрутизатора недостаточно.
- Новые маршруты не загружаются на маршрутизаторы, когда использование пространства базы данных достигает верхнего предела.

4.4.9.2. Примечания

- Необходимо настроить основные функции OSPF.
- После того, как маршрутизатор перейдет в состояние переполнения, вы можете запустить команду **clear ip ospf process** или остановить, а затем перезапустить OSPF, чтобы выйти из состояния переполнения.

4.4.9.3. Шаги настройки

Настройка функции переполнения памяти

- Опционально.
- Данная конфигурация рекомендуется, если в домене существует большое количество маршрутов и это может привести к нехватке памяти маршрутизатора.

Настройка функции переполнения базы данных

- Опционально.
- Данная конфигурация рекомендуется, если в домене существует большое количество маршрутов и это может привести к нехватке памяти маршрутизатора.

Настройка функции переполнения внешней базы данных LSA

- Опционально.
- Эту конфигурацию рекомендуется использовать, если ASBR вводит большое количество внешних маршрутов и памяти маршрутизатора может быть недостаточно.

4.4.9.4. Проверка

- Когда памяти станет недостаточно, добавьте в сеть новые маршрутизаторы и запустите команду **show ip route**, чтобы убедиться, что новые маршруты не загружены.
- После того, как использование пространства базы данных достигнет верхнего предела, добавьте в сеть новые маршрутизаторы и запустите команду **show ip route**, чтобы убедиться, что новые маршруты не загружены.

4.4.9.5. Связанные команды

Настройка функции переполнения памяти

Команда	**overflow memory-lack**
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Процесс OSPF переходит в состояние переполнения, чтобы отбросить вновь изученные внешние маршруты. Такое поведение может эффективно гарантировать, что использование памяти не увеличится. После включения функции переполнения процесс OSPF переходит в состояние переполнения и отбрасывает вновь изученные внешние маршруты, что может вызвать петлю маршрутизации во всей сети. Чтобы снизить вероятность возникновения этой проблемы, OSPF генерирует маршрут по умолчанию к нулевому (пустому) интерфейсу, и этот маршрут всегда существует в состоянии переполнения. Вы можете запустить команду **clear ip ospf process**, чтобы сбросить процесс OSPF, чтобы процесс OSPF мог выйти из состояния переполнения. Вы можете использовать форму команды **no**, чтобы предотвратить переход процесса OSPF в состояние переполнения, когда памяти недостаточно. Однако это может привести к перерасходу ресурса памяти, после чего процесс OSPF остановится и удалит все изученные маршруты

Настройка функции переполнения базы данных

Команда	**overflow database** *number* [**hard** | **soft**]
Описание параметра	*number*: указывает максимальное количество LSA. Значение варьируется от 1 до 4 294 967 294. **hard**: указывает, что процесс OSPF будет остановлен, если количество LSA превысит ограничение. **soft**: указывает, что будет получено предупреждение, если количество LSA превысит лимит
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Если количество LSA превышает ограничение, используйте параметр **hard**, если процесс OSPF должен быть остановлен, и параметр **soft**, если предупреждение должно быть сгенерировано без остановки процесса OSPF

Настройка функции переполнения базы данных внешними LSA

Команда	**overflow database external** *max-dbsize wait-time*
Описание параметра	*max-dbsize*: указывает максимальное количество внешних LSA. Это значение должно быть одинаковым на всех маршрутизаторах в одной AS. Значение варьируется от 0 до 2 147 483 647. *wait-time*: указывает время ожидания после того, как маршрутизатор в состоянии переполнения попытается восстановить нормальное состояние. Значение находится в диапазоне от 0 до 2 147 483 647
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Когда количество внешних LSA маршрутизатора превышает настроенный **max-dbsize**, маршрутизатор переходит в состояние переполнения. В этом состоянии маршрутизатор больше не загружает внешние LSA и удаляет внешние LSA, созданные локально. По истечении времени *wait-time* устройство восстанавливает нормальное состояние и снова загружает внешние LSA. При использовании функции переполнения убедитесь, что на всех маршрутизаторах в магистральной области OSPF и общих областях настроен один и тот же **max-dbsize**; в противном случае могут возникнуть следующие проблемы: • Непоследовательные LSDB через сети несовместимы, и неспособность достичь полной смежности • Неправильные маршруты, включая петли маршрутизации

	• Частая повторная передача внешних LSA AS

4.4.9.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Настройка функции переполнения базы данных внешними LSA

Сценарий:

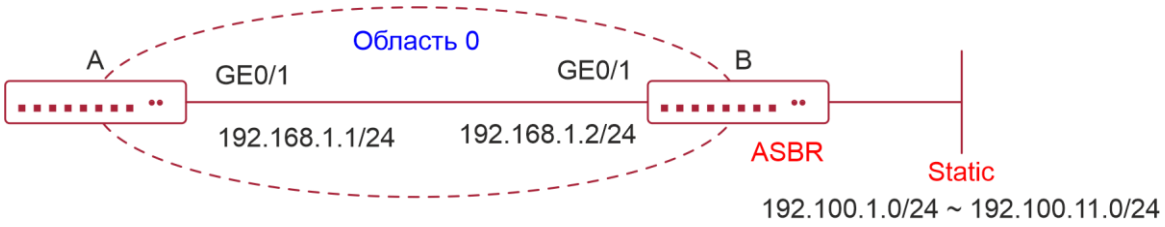


Рисунок 4-18.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • На маршрутизаторе B настройте перераспределение и введите внешние статические маршруты. • На маршрутизаторе B настройте максимальное количество внешних LSA
B	B# configure terminal B(config)# router ospf 1 B(config-router)# redistribute static subnets
A	A# configure terminal A(config)# router ospf 1 A(config-router)# overflow database external 10 3
Проверка	На маршрутизаторе B настройте 11 статических маршрутов (от 192.100.1.0/24 до 192.100.11.0/24). На маршрутизаторе A убедитесь, что загружено только 10 статических маршрутов
A	A# show ip route ospf O E2 192.100.1.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1

	O E2 192.100.2.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.3.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.4.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.5.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.6.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.7.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.8.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.9.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.10.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1

4.4.9.7. Распространенные ошибки

Смежность OSPF является ненормальной, поскольку максимальное количество LSA несовместимо на разных маршрутизаторах.

4.4.10. Изменение максимального количества одновременных соседей

4.4.10.1. Эффект конфигурации

Управляйте максимальным количеством одновременных соседей в процессе OSPF, чтобы снизить нагрузку на устройство.

4.4.10.2. Примечания

Необходимо настроить основные функции OSPF.

4.4.10.3. Шаги настройки

Настройка максимального количества одновременных соседей в процессе OSPF

- (Опционально) Эту конфигурацию рекомендуется использовать, если вы хотите быстрее настроить смежность OSPF, когда маршрутизатор подключен к множеству других маршрутизаторов.
- Эта конфигурация выполняется на маршрутизаторе ядра.

4.4.10.4. Проверка

Запустите команду **show ip ospf neighbor**, чтобы отобразить количество соседей, одновременно взаимодействующих с процессом OSPF.

4.4.10.5. Связанные команды

Настройка максимального количества одновременных соседей в текущем процессе

Команда	**max-concurrent-dd** *number*
Описание параметра	*number*: указывает максимальное количество соседей, одновременно взаимодействующих с процессом OSPF. Значение варьируется от 1 до 65 535
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Если на производительность маршрутизатора влияет обмен данными с несколькими соседями, вы можете настроить эту команду, чтобы ограничить максимальное количество соседей, с которыми один процесс OSPF может одновременно инициировать или принимать взаимодействие

Настройка максимального количества одновременных соседей для всех процессов

Команда	**router ospf max-concurrent-dd** *number*
Описание параметра	*number*: указывает максимальное количество соседей, одновременно взаимодействующих с процессом OSPF. Значение варьируется от 1 до 65 535
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если производительность маршрутизатора снижается из-за того, что маршрутизатор обменивается данными с несколькими соседями, вы можете настроить эту команду, чтобы ограничить максимальное количество соседей, с помощью которой все процессы OSPF могут одновременно инициировать или принимать взаимодействие

4.4.10.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Настройка максимального количества одновременных соседей в процессе OSPF

Сценарий:

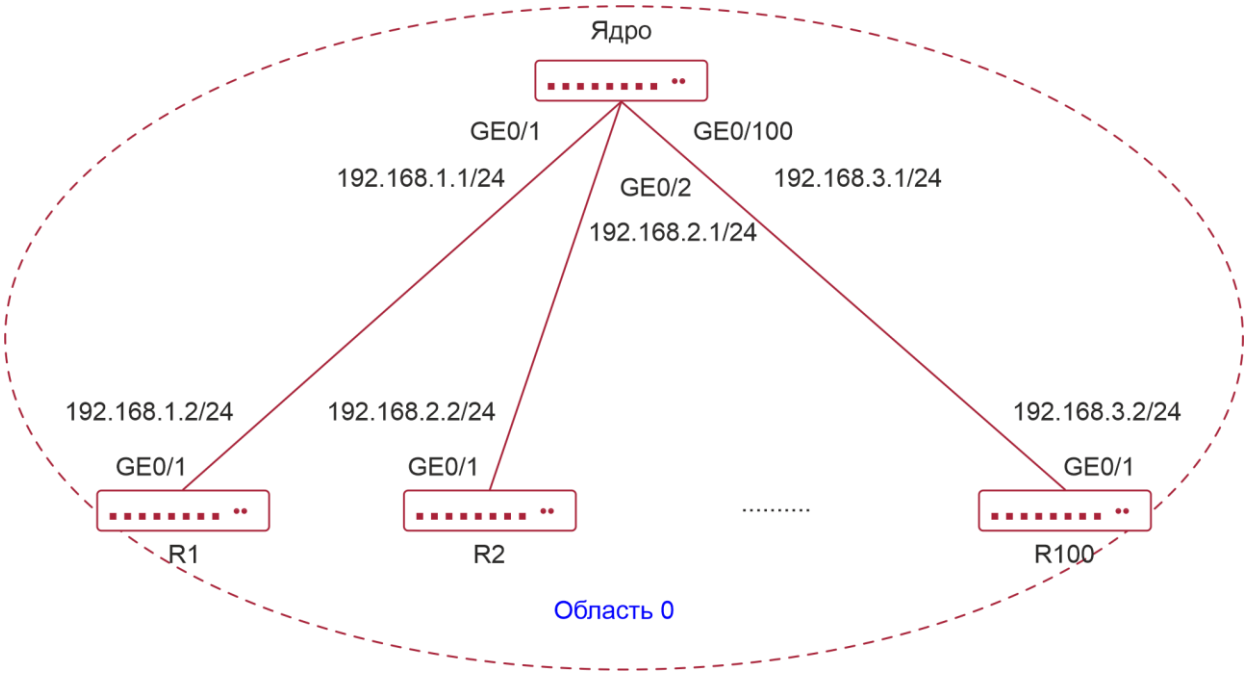


Рисунок 4-19.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • На маршрутизаторе ядра (core) установите максимальное количество одновременных соседей равным 4
Core	Core# configure terminal Core(config)# router ospf max-concurrent-dd 4
Проверка	На маршрутизаторе ядра проверьте состояние соседа и убедитесь, что не более восьми соседей одновременно взаимодействуют с процессом OSPF

4.4.11. Отключение проверки адреса источника

4.4.11.1. Эффект конфигурации

Сервис unicast-маршрутизации может предоставляться, даже если IP-адреса интерфейсов соседних маршрутизаторов не находятся в одном сегменте сети.

4.4.11.2. Примечания

- Необходимо настроить основные функции OSPF.
- Проверка адреса источника не может быть отключена в broadcast-сети или сети NBMA.

4.4.11.3. Шаги настройки

Отключение проверки адреса источника

- (Опционально) Эта конфигурация является обязательной, если необходимо настроить смежность между маршрутизаторами с IP-адресами интерфейсов в разных сегментах сети.
- Данная настройка выполняется на маршрутизаторах с IP-адресами интерфейсов в разных сегментах сети.

4.4.11.4. Проверка

Смежность может быть настроена между маршрутизаторами в разных сегментах сети.

4.4.11.5. Связанные команды

Отключение проверки адреса источника

Команда	**ip ospf source-check-ignore**
Командный режим	Режим настройки интерфейса
Руководство по использованию	Обычно адрес источника пакета, полученного OSPF, находится в том же сегменте сети, что и принимающий интерфейс. Адреса на обоих концах P2P-канала настраиваются отдельно и не обязательно находятся в одном сегменте сети. В этом сценарии, поскольку информация об адресе peer-а будет сообщена во время процесса согласования канала P2P, OSPF проверяет, является ли адрес источника пакета адресом, объявленным peer-ом во время согласования. В противном случае OSPF определяет, что пакет недействителен, и отбрасывает его. В частности, OSPF не проверяет адрес ненумерованного интерфейса. В некоторых сценариях адрес источника может не соответствовать предыдущему требованию, и поэтому проверка адреса OSPF завершается неудачно. Например, согласованный адрес peer-а не может быть получен по каналу P2P. В этом сценарии проверка адреса источника должна быть отключена, чтобы обеспечить правильную настройку смежности OSPF

4.4.11.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Отключение проверки адреса источника

Сценарий:

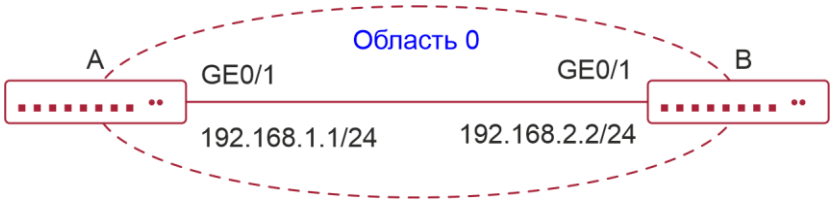


Рисунок 4-20.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • Установите тип сетевых интерфейсов на всех маршрутизаторах как P2P. • Отключите проверку адреса источника на всех маршрутизаторах
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip ospf network point-to-point A(config-if-GigabitEthernet 0/1)# ip ospf source-check-ignore
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip ospf network point-to-point B(config-if-GigabitEthernet 0/1)# ip ospf source-check-ignore
Проверка	На маршрутизаторе A проверьте правильность информации о соседе OSPF
A	A# show ip ospfneighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.100.2.2 1 Full/- 00:00:34 192.100.2.2 GigabitEthernet 0/1

4.4.12. Отключение проверки MTU

4.4.12.1. Эффект конфигурации

Сервис unicast-маршрутизации может предоставляться, даже если MTU интерфейсов соседних маршрутизаторов различны.

4.4.12.2. Примечания

Необходимо настроить основные функции OSPF.

4.4.12.3. Шаги настройки

Отключение проверки MTU

- (Опционально) Проверка MTU отключена по умолчанию. Рекомендуется сохранить конфигурацию по умолчанию.
- Эта настройка выполняется на двух маршрутизаторах с разными MTU интерфейса.

4.4.12.4. Проверка

Смежность можно настроить между маршрутизаторами с разными MTU.

4.4.12.5. Связанные команды

Отключение проверки MTU

Команда	**ip ospf mtu-ignore**
Командный режим	Режим настройки интерфейса
Руководство по использованию	При получении пакета описания базы данных OSPF проверяет, совпадает ли MTU интерфейса соседа с MTU его собственного интерфейса. Если MTU интерфейса, указанный в полученном пакете описания базы данных, больше, чем MTU локального интерфейса, установить смежность невозможно. Чтобы решить эту проблему, вы можете отключить проверку MTU

4.4.12.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Сценарий:



Рисунок 4-21.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено)

	• Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • Настройте разные MTU для интерфейсов на двух маршрутизаторах. • Отключите проверку MTU на всех маршрутизаторах. (По умолчанию функция отключения проверки MTU включена.)
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip mtu 1400 A(config-if-GigabitEthernet 0/1)# ip ospf mtu-ignore
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip mtu 1600 B(config-if-GigabitEthernet 0/1)# ip ospf mtu-ignore
Проверка	На маршрутизаторе A проверьте правильность информации о соседе OSPF
A	A# show ip ospfneighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/DR 00:00:34 192.168.1.2 GigabitEthernet 0/1

4.4.13. Включение двустороннего обслуживания

4.4.13.1. Эффект конфигурации

Пакеты, отличные от Hello, также могут использоваться для поддержания смежности.

4.4.13.2. Примечания

Необходимо настроить основные функции OSPF.

4.4.13.3. Шаги настройки

Включение двустороннего обслуживания

- (Опционально) Эта функция включена по умолчанию. Рекомендуется сохранить конфигурацию по умолчанию.
- Эта настройка выполняется на всех маршрутизаторах.

4.4.13.4. Проверка

Пакеты, отличные от Hello, также могут использоваться для поддержания смежности.

4.4.13.5. Связанные команды

Включение двустороннего обслуживания

Команда	**two-way-maintain**
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	В большой сети может быть отправлено или получено множество пакетов, занимающих слишком много процессора и памяти. В результате некоторые пакеты задерживаются или отбрасываются. Если время обработки пакетов Hello превышает dead-интервал, смежность будет нарушена из-за тайм-аута. Если включена функция двустороннего обслуживания, в дополнение к пакетам Hello также пакеты DD, LSU, LSR и LSAck могут использоваться для поддержания двусторонней связи между соседями, когда в сети существует большое количество пакетов. Это предотвращает прекращение смежности, вызванное задержкой или отклонением пакетов Hello

4.4.13.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Сценарий:



Рисунок 4-22.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • На маршрутизаторе A включите функцию двустороннего обслуживания. (Эта функция включена по умолчанию.)
A	A# configure terminal A(config)#routerospf 1 A(config-router)#two-way-maintain

Проверка	Во время настройки смежности маршрутизатор A проверяет dead-интервал соседа и обновляет dead-интервал не дожидаясь, пока маршрутизатор B отправит пакет Hello
A	A# show ip ospfneighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/BDR 00:00:40 192.168.1.2 GigabitEthernet 0/1

4.4.14. Включение GR

4.4.14.1. Эффект конфигурации

- Когда распределенный маршрутизатор переключает сервисы с активной платы на резервную, пересылка данных продолжается и не прерывается.
- При перезапуске процесса OSPF пересылка данных продолжается и не прерывается.

4.4.14.2. Примечания

- Необходимо настроить основные функции OSPF.
- Соседний маршрутизатор должен поддерживать функцию helper GR.
- Период отсрочки (grace) не может быть короче времени dead соседнего маршрутизатора.

4.4.14.3. Шаги настройки

Настройка функции GR OSPF

- (Опционально) Эта функция включена по умолчанию. Рекомендуется сохранить конфигурацию по умолчанию.
- Эта настройка выполняется на всех маршрутизаторах.

Настройка функции OSPF GR Helper

- (Опционально) Эта функция включена по умолчанию. Рекомендуется сохранить конфигурацию по умолчанию.
- Эта настройка выполняется на всех маршрутизаторах.

4.4.14.4. Проверка

- Когда распределенный маршрутизатор переключает сервисы с активной платы на резервную, пересылка данных продолжается и не прерывается.
- При перезапуске процесса OSPF пересылка данных продолжается и не прерывается.

4.4.14.5. Связанные команды

Настройка функции GR OSPF

Команда	**graceful-restart** [**grace-period** *grace-period* | **inconsistent-lsa-checking**]
Описание параметра	**grace-period** *grace-period*: указывает период отсрочки, который представляет собой максимальное время от возникновения сбоя OSPF до завершения GR OSPF. Значение периода отсрочки варьируется от 1 до 1800 секунд. Значение по умолчанию — 120 с. **inconsistent-lsa-checking**: включает обнаружение изменений топологии. Если обнаружено какое-либо топологическое изменение, OSPF завершает процесс GR для завершения конвергенции. После включения GR обнаружение топологических изменений включается по умолчанию
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Функция GR настроена на основе процесса OSPF. Вы можете настроить разные параметры для разных процессов OSPF в зависимости от реальных условий. Эта команда используется для настройки возможности перезапуска устройства GR. Период отсрочки — это максимальное время всего процесса GR, в течение которого состояние канала перестраивается таким образом, чтобы восстанавливалось исходное состояние процесса OSPF. По истечении периода отсрочки OSPF выходит из состояния GR и выполняет общие операции OSPF. Запустите команду **graceful-restart**, чтобы устанавить период отсрочки на 120 секунд. Команда **graceful-restart grace-period** позволяет вам явно изменить период отсрочки. Предпосылкой успешного выполнения GR и бесперебойной пересылки является стабильность топологии. При изменении топологии OSPF быстро сходится, не дожидаясь дальнейшего выполнения GR, избегая тем самым продолжительной пересылки black-hole. Отключение обнаружения топологии: если OSPF не может сходиться вовремя при изменении топологии во время процесса горячего резерва, через долгое время может возникнуть black-hole пересылки. Включение обнаружения топологии: пересылка может быть прервана, когда обнаружение топологии включено, но время прерывания намного короче, чем когда обнаружение топологии отключено. В большинстве случаев рекомендуется включить определение топологии. В особых сценариях обнаружение топологии можно отключить, если топология изменится после процесса горячего резерва, но можно гарантировать, что пересылающая black-hole не появится в течение длительного времени. Это может минимизировать время прерывания пересылки во время процесса горячего резерва.

	Если функция Fast Hello включена, функцию GR включить невозможно

Настройка функции OSPF GR Helper

Команда	**graceful-restart helper** { **disable** | **strict-lsa-checking** | **internal-lsa-checking**}
Описание параметра	**disable**: запрещает устройству выступать в качестве GR helper-а для другого устройства. **strict-lsa-checking**: указывает, что изменения в LSA от типа 1 до типа 5 и типа 7 будут проверяться в течение периода, в течение которого устройство действует как GR helper для определения изменений в сети. Если сеть изменится, устройство перестанет выступать в роли GR helper-а. **internal-lsa-checking**: указывает, что изменения в LSA от типа 1 до типа 3 будут проверяться в течение периода, в течение которого устройство действует как GR helper для определения изменений в сети. Если сеть изменится, устройство перестанет выступать в роли GR helper-а
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Эта команда используется для настройки функции GR helper-а маршрутизатора. Когда соседний маршрутизатор реализует GR, он отправляет Grace-LSA для уведомления всех соседних маршрутизаторов. Если функция GR helper включена на локальном маршрутизаторе, локальный маршрутизатор становится GR helper-ом при получении Grace-LSA и помогает соседу завершить GR. Опция **disable** указывает, что GR helper не предоставляется ни для одного устройства, реализующего GR. После того как устройство становится GR helper-ом, изменения в сети по умолчанию не обнаруживаются. Если в сети происходят какие-либо изменения, топология сети сходится после завершения GR. Если вы хотите, чтобы изменения в сети могли быть быстро обнаружены во время процесса GR, вы можете настроить **strict-lsa-checking** для проверки LSA типов от 1 до 5 и типа 7, которые указывают сетевую информацию, или **internal-lsa-checking** для проверки типов от 1 до 3. LSA, указывающие внутренние маршруты домена AS. Если масштаб сети велик, рекомендуется отключить параметры проверки LSA (**strict-lsa-checking** и **internal-lsa-checking**), поскольку изменения в региональной сети могут привести к прекращению работы GR и, как следствие, к снижению конвергенции всей сети

4.4.14.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Сценарий:

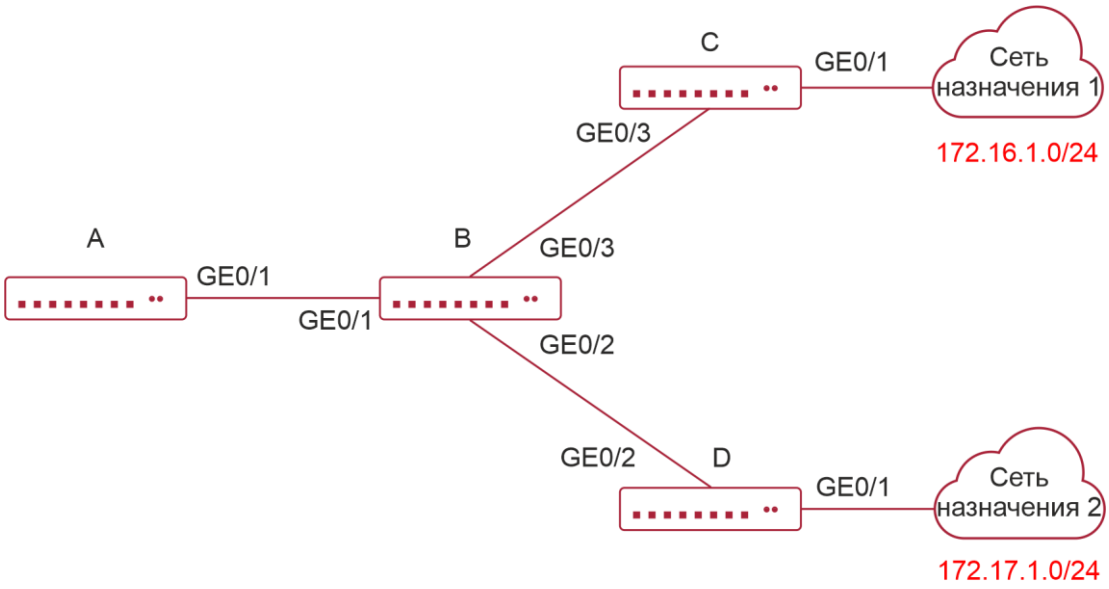


Рисунок 4-23.

IP-адреса интерфейса следующие:

A: GE 0/1 192.168.1.1

B: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 GE 0/3 192.168.3.1

C: GE 0/1 192.168.4.2 GE 0/3 192.168.3.2

D: GE 0/1 192.168.5.2 GE 0/2 192.168.2.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (пропущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • На маршрутизаторе A, маршрутизаторе C и маршрутизаторе D включите функцию GR helper. (Эта функция включена по умолчанию.) • На маршрутизаторе B включите функцию GR
B	B# configure terminal B(config)# router ospf1 B(config-router)# graceful-restart

Проверка	• Запустите переключение горячего резерва на маршрутизаторе B и убедитесь, что таблицы маршрутизации сетей назначения 1 и 2 остаются неизменными на маршрутизаторе A во время переключения. • Запустите переключение на горячий резерв на маршрутизаторе B, пропингуйте сеть назначения 1 с маршрутизатора A и убедитесь, что пересылка данных не прерывается во время переключения

4.4.14.7. Распространенные ошибки

Пересылка трафика прерывается во время процесса GR, поскольку настроенный период отсрочки короче, чем время dead соседнего маршрутизатора.

4.4.15. Включение NSR

4.4.15.1. Эффект конфигурации

Во время переключения активный/резервный маршрутизатор распределенного маршрутизатора пересылка данных продолжается и не прерывается.

4.4.15.2. Примечания

Необходимо настроить основные функции OSPF.

4.4.15.3. Шаги настройки

Включение функции OSPF NSR

(Опционально) Эта функция отключена по умолчанию и включается только тогда, когда эту функцию необходимо использовать.

4.4.15.4. Проверка

Во время переключения активный/резервный маршрутизатор распределенного маршрутизатора пересылка данных продолжается и не прерывается.

4.4.15.5. Связанные команды

Включение NSR

Команда	**nsr**
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Эта команда используется для включения функции NSR. Включите NSR или GR для одного и того же процесса OSPF. То есть, когда GR включен, NSR автоматически отключается. Когда NSR включен, GR автоматически отключается, но возможности GR helper-а не затрагиваются. Переключение распределенного маршрутизатора занимает некоторое время. Если время dead соседа OSPF короче времени переключения, смежность OSPF будет нарушена, что приведет к прерыванию

	обслуживания во время переключения. Поэтому при включении функции NSR рекомендуется настроить время dead соседа OSPF, равное или превышающее значение по умолчанию. Когда функция Fast Hello включена, время dead соседа OSPF меньше 1 с, поэтому рекомендуется отключить функцию NSR

4.4.15.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Сценарий:

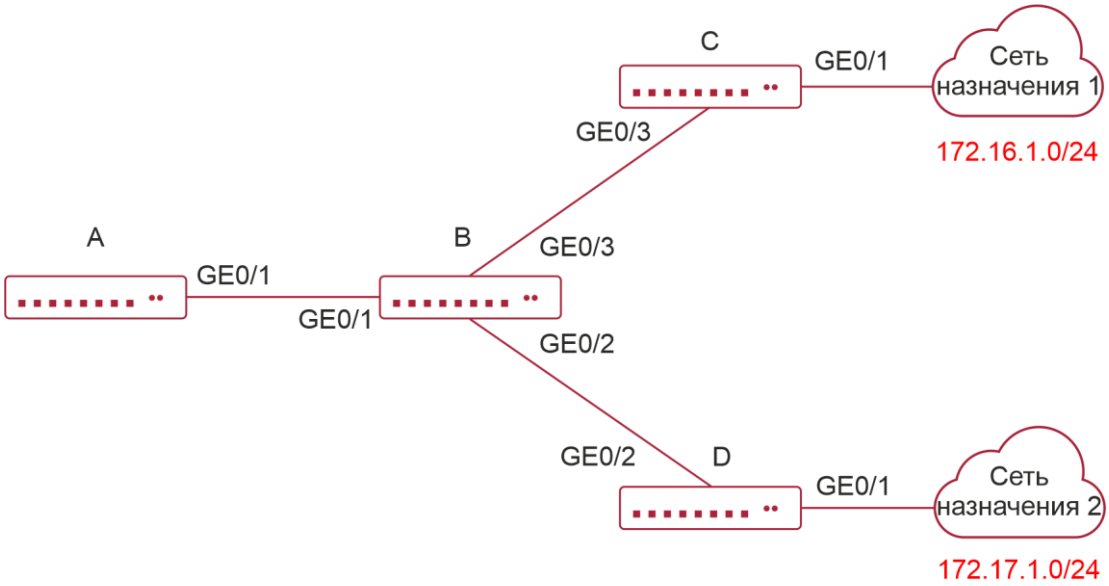


Рисунок 4-24.

IP-адреса интерфейса следующие:

A: GE 0/1 192.168.1.1

B: GE 0/1 192.168.1.2 GE 0/2 192.168.2.1 GE 0/3 192.168.3.1

C: GE 0/1 192.168.4.2 GE 0/3 192.168.3.2

D: GE 0/1 192.168.5.2 GE 0/2 192.168.2.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (пропущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (пропущено) • На маршрутизаторе B включите функцию NSR
B	B# configure terminal

	B(config)# router ospf1 B(config-router)# nsr
Проверка	• Запустите переключение горячего резерва на маршрутизаторе B и убедитесь, что таблицы маршрутизации сетей назначения 1 и 2 остаются неизменными на маршрутизаторе A во время переключения. • Запустите переключение на горячий резерв на маршрутизаторе B, пропингуйте сеть назначения 1 с маршрутизатора A и убедитесь, что пересылка данных не прерывается во время переключения

4.4.15.7. Распространенные ошибки

Настроенный dead-интервал соседа OSPF слишком мал. Если функция Fast Hello включена, смежность OSPF будет разрушена во время переключения, что приведет к прерыванию пересылки данных.

4.4.16. Корреляция OSPF с BFD

4.4.16.1. Эффект конфигурации

Если канал неисправен, OSPF может быстро обнаружить сбой маршрута. Эта конфигурация помогает сократить время прерывания трафика.

4.4.16.2. Примечания

- Необходимо настроить основные функции OSPF.
- Параметры BFD должны быть настроены для интерфейса заранее.
- Если BFD настроен как для процесса, так и для интерфейса, конфигурация интерфейса вступает в силу преимущественно.

4.4.16.3. Шаги настройки

Корреляция OSPF с BFD

- (Опционально) Эта конфигурация необходима, если вы хотите ускорить конвергенцию сети OSPF.
- Конфигурацию необходимо выполнить на маршрутизаторах на обоих концах канала.

4.4.16.4. Проверка

Запустите команду **show bfd neighbor**, чтобы убедиться, что соседи BFD в порядке.

4.4.16.5. Связанные команды

Корреляция интерфейса OSPF с BFD

Команда	**ip ospf bfd** [**disable**]
Описание параметра	**disable**: отключает BFD для обнаружения канала на указанном интерфейсе с включенным OSPF
Командный режим	Режим настройки интерфейса
Руководство по использованию	Конфигурация на основе интерфейса имеет приоритет над командой **bfd all-interfaces**, используемой в режиме конфигурации процесса. В зависимости от реальной среды вы можете запустить команду **ip ospf bfd,** чтобы включить BFD на указанном интерфейсе для обнаружения каналов или запустите команду **bfd all-interfaces** в режиме конфигурации процесса OSPF, чтобы включить BFD на всех интерфейсах процесса OSPF, или запустите команду **ospf bfd disable**, чтобы отключить BFD на указанном интерфейсе

Корреляция процесса OSPF с BFD

Команда	**bfd all-interfaces**
Командный режим	Режим конфигурации процесса OSPF
Руководство по использованию	OSPF динамически обнаруживает соседей с помощью пакетов Hello. После того, как OSPF включит функцию BFD, будет настроен сеанс BFD для достижения полной смежности и использования механизма BFD для определения статуса соседа. Как только с помощью BFD обнаруживается сбой соседа, OSPF немедленно выполняет конвергенцию сети. Вы также можете запустить команду **ip ospf bfd** [**disable**] в режиме конфигурации интерфейса, чтобы включить или отключить функцию BFD на указанном интерфейсе, и эта конфигурация имеет приоритет над командой **bfd all-interfaces**, которая применяется в режиме конфигурации процесса OSPF

4.4.16.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Сценарий:

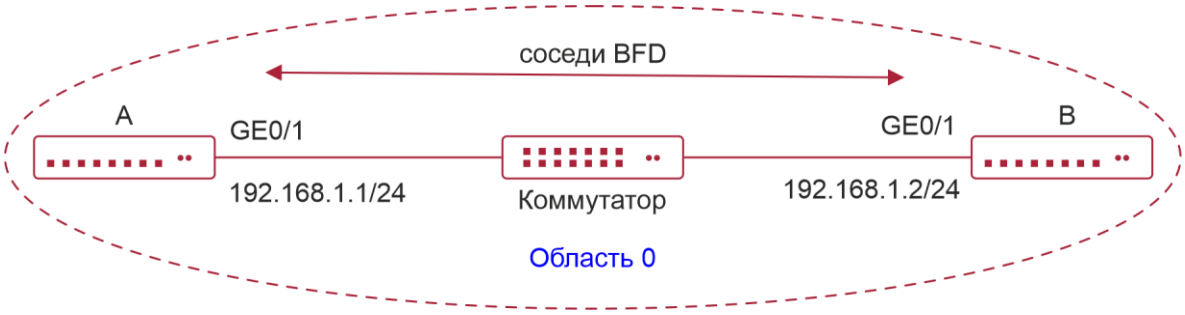


Рисунок 4-25.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (пропущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (пропущено) • Настройте параметры BFD для интерфейсов всех маршрутизаторов. • Сопоставьте OSPF с BFD на всех маршрутизаторах
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#bfd interval 200 min_rx 200 multiplier 5 A(config)# router ospf 1 A(config-router)#bfd all-interfaces
B	B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 2/1)#bfd interval 200 min_rx 200 multiplier 5 B(config)# router ospf 1 B(config-router)#bfd all-interfaces
Проверка	• На маршрутизаторе A и маршрутизаторе B убедитесь, что состояние BFD — Up («Включено»). • Отключите маршрутизатор A от коммутатора. На маршрутизаторе A убедитесь, что сосед отключен во время BFD, а соответствующий маршрут OSPF удален
A	A# show ip ospf neighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State BFD State Dead Time Address Interface

	192.168.1.2 1 Full/BDR Up 00:00:40 192.168.1.2 GigabitEthernet 0/1
B	B# show ip ospf neighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State BFD State DeadTime Address Interface 192.168.1.1 1 Full/BDR Up 00:00:40 192.168.1.1 GigabitEthernet 0/1

4.4.17. Включение быстрого перенаправления

4.4.17.1. Эффект конфигурации

Как только OSPF обнаруживает сбой маршрута, маршрутизатор может немедленно переключиться на второй лучший маршрут. Эта конфигурация помогает сократить время прерывания трафика.

4.4.17.2. Примечания

- Необходимо настроить основные функции OSPF.
- Конфигурация LAF для быстрого перенаправления является взаимоисключающей с конфигурацией виртуального канала.
- Вы должны установить задержку **carrier-delay** интерфейса на 0.

4.4.17.3. Шаги настройки

Настройка быстрого перенаправления

- (Опционально) Эта конфигурация необходима, если вы хотите увеличить скорость конвергенции сети OSPF до уровня миллисекунд.
- Эта настройка выполняется на маршрутизаторе, который имеет несколько путей к сети назначения.

Предотвращение превращения интерфейса в резервный интерфейс

- (Опционально) Эта конфигурация является обязательной, если вы хотите, чтобы трафик данных не переключался на указанный путь после сбоя лучшего пути. После сбоя лучшего пути трафик будет переключен на другой, второй лучший путь, но новый лучший путь будет выбран на основе стоимости интерфейса после повторной конвергенции OSPF.
- Эта настройка выполняется на устройстве, на котором включено быстрое перенаправление.

4.4.17.4. Проверка

Запустите команду **show ip route fast-reroute**, чтобы убедиться, что существуют как лучший, так и второй лучший пути.

4.4.17.5. Связанные команды

Настройка быстрого перенаправления

Команда	**fast-reroute**{ **lfa** [**downstream-paths**] | **route-map** *route-map-name* }
Описание параметра	**lfa**: позволяет вычислить резервный путь без петель. **downstream-paths**: включает расчет downstream-пути. **route-map** *route-map-name*: указывает резервный путь через карту маршрутов
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Если параметр **lfa** настроен, то включен расчет резервного пути без петель. В этом случае вы можете использовать команду режима интерфейса, чтобы указать режим защиты пути интерфейса. Рекомендуется отключить вычисление резервного пути без петель, если в сети существует любой из следующих случаев: 1. Виртуальные каналы существуют. 2. Существуют альтернативные ABR. 3. ASBR также является ABR. 4. Несколько ABSR объявляют один и тот же внешний маршрут. Если оба **lfa** и **downstream-paths** настроены, включен расчет downstream-пути. Если **route-map** настроена, резервный путь может быть указан для соответствующего маршрута через карту маршрутов. При использовании функции быстрого перенаправления OSPF рекомендуется одновременно включить BFD, чтобы устройство могло быстро обнаружить любой сбой канала и, следовательно, сократить время прерывания пересылки. Если интерфейс включен или выключен, чтобы сократить время прерывания пересылки во время быстрого перенаправления OSPF, вы можете настроить задержку **carrier-delay** на 0 в режиме конфигурации интерфейса L3, чтобы достичь максимальной скорости переключения

Настройка защиты LFA интерфейса

Команда	**ip ospf fast-reroute protection** { **node** | **link-node** | **disable**}
Описание параметра	**node**: включает защиту узла LFA. **link-node**: включает защиту узла канала LFA. **disable**: отключает защиту LFA

Командный режим	Режим настройки интерфейса
Руководство по использованию	Если команда **fast-reroute lfa** выполняется в режиме конфигурации процесса маршрутизации OSPF, будет сгенерирована функция вычисления быстрого перенаправления OSPF, и для активного маршрута будет сгенерирован резервный маршрут на основе режима защиты LFA, указанного в режиме конфигурации интерфейса. Защита канала включена по умолчанию для каждого интерфейса OSPF. В этом режиме защиты отказ активного канала не влияет на данные, передаваемые по резервному маршруту. Используйте параметр **node**, чтобы включить защиту узла для интерфейса, то есть, сбой в работе соседнего узла, соответствующего активному каналу, не повлияет на пересылку данных по резервному маршруту. Используйте параметр **link-node** для защиты как канала, так и соседнего узла, соответствующего активному каналу. Используйте параметр **disable**, чтобы отключить функцию защиты LFA интерфейса, то есть не создавать резервную запись для маршрута, следующим hop-ом которого является интерфейс. Эта команда не действует, если настроена **fast-rerotue route-map**

Предотвращение превращения интерфейса в резервный интерфейс

Команда	**ip ospf fast-reroute no-eligible-backup**
Командный режим	Режим настройки интерфейса
Руководство по использованию	Если оставшаяся пропускная способность интерфейса мала или если интерфейс и его активный интерфейс могут выйти из строя одновременно, интерфейс нельзя использовать в качестве резервного интерфейса. Поэтому вам необходимо запустить эту команду в режиме настройки интерфейса, чтобы этот интерфейс не стал резервным интерфейсом во время вычисления быстрого перенаправления OSPF. После выполнения этой команды резервный интерфейс выбирается из других интерфейсов. Эта команда не действует, если настроена **fast-rerotue route-map**

4.4.17.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Настройка быстрого перенаправления

Сценарий:

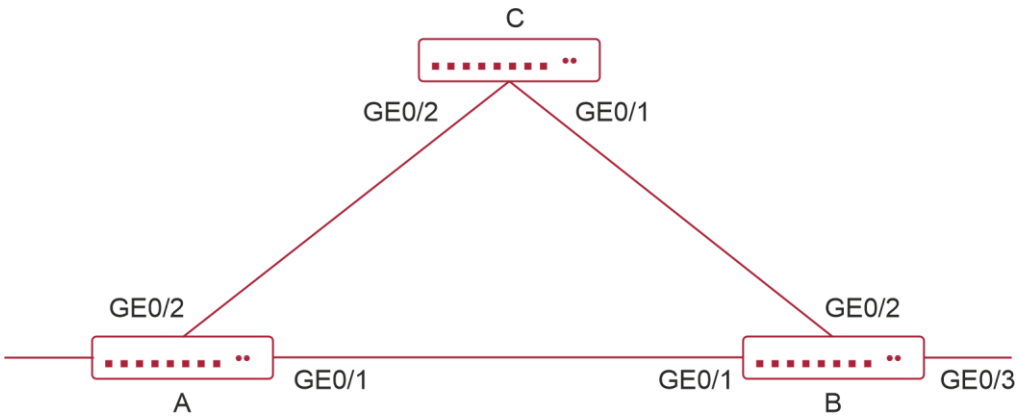


Рисунок 4-26.

IP-адреса интерфейса следующие:

A: GE0/1 192.168.1.1 GE0/2 192.168.2.1

B: GE0/1 192.168.1.2 GE0/2 192.168.3.1 GE0/3 192.168.4.1

C: GE0/1 192.168.3.2 GE 0/2 192.168.2.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (пропущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (пропущено) • Настройте быстрое перенаправление на маршрутизаторе A. • Настройте задержку **carrier-delay 0** для интерфейса маршрутизатора A
A	A# configure terminal A(config)# router ospf 1 A(config-router)# fast-reroute lfa A(config-router)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#carrier-delay 0 A(config-if-GigabitEthernet 0/1)# exit A(config)# interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#carrier-delay 0
Проверка	На маршрутизаторе A проверьте таблицу маршрутизации и убедитесь, что существует резервный маршрут для записи 192.168.4.0/24

	A# show ip route fast-reroute | begin 192.168.4.0 O 192.168.4.0/24 [ma] via 192.168.1.2, 00:39:28, GigabitEthernet 0/1 [b] via 192.168.2.2, 00:39:28, GigabitEthernet 0/2

4.4.18. Включение iSPF

4.4.18.1. Эффект конфигурации

OSPF использует алгоритм iSPF для расчета топологии сети.

4.4.18.2. Примечания

Необходимо настроить основные функции OSPF.

4.4.18.3. Шаги настройки

Настройка iSPF

- (Опционально) Эту конфигурацию рекомендуется использовать, если вы хотите ускорить сходимость маршрутов в одной области с более чем 100 маршрутизаторами.
- Эта настройка выполняется на всех маршрутизаторах в этой области.

4.4.18.4. Проверка

Запустите команду **show ip ospf**, чтобы убедиться, что iSPF включен.

4.4.18.5. Связанные команды

Настройка iSPF

Команда	**ispf enable**
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	После включения iSPF OSPF будет использовать алгоритм iSPF для расчета топологии сети. То есть после изменения топологии сети OSPF исправляет только узлы, затронутые топологическим изменением, а не перестраивает заново полную SPT. Функция iSPF обычно используется в сетях большого размера, чтобы снизить нагрузку на процессоры маршрутизатора

4.4.18.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Настройка iSPF

Сценарий:

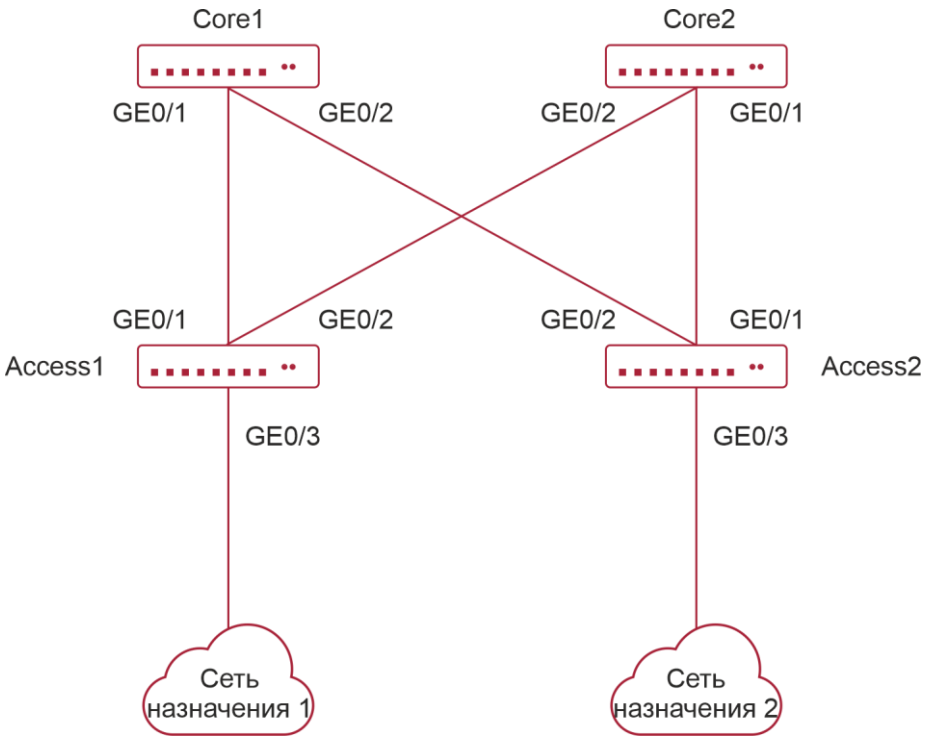


Рисунок 4-27.

IP-адреса интерфейса следующие:

Core1: GE0/1 192.168.1.1 GE0/2 192.168.2.1

Core2: GE0/1 192.168.3.1 GE0/2 192.168.4.1

Access1: GE0/1 192.168.1.2 GE 0/2 192.168.3.2

Access2: GE0/1 192.168.4.2 GE 0/2 192.168.2.2

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (пропущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (пропущено) • Настройте iSPF на всех маршрутизаторах
Core1	Core1# configure terminal Core1(config)# router ospf 1 Core1(config-router)# ispf enable
Core2	Core2# configure terminal Core2(config)# router ospf 1

	Core2(config-router)# ispf enable
Access1	Access1# configure terminal Access1(config)# router ospf 1 Access1(config-router)# ispf enable
Access2	Access2# configure terminal Access2(config)# router ospf 1 Access2(config-router)# ispf enable
Проверка	На маршрутизаторе Core1 убедитесь, что iSPF включен
	Core1# show ip ospf Routing Process "ospf 1" with ID 1.1.1.1 Process uptime is 17 hours 48 minutes Process bound to VRF default Memory Overflow is enabled. Router is not in overflow state now. Conforms to RFC2328, and RFC1583Compatibility flag is enabled Supports only single TOS(TOS0) routes Supports opaque LSA Enable two-way-maintain Enable ispf Initial SPF schedule delay 1000 msecs Minimum hold time between two consecutive SPFs 5000 msecs Maximum wait time between two consecutive SPFs 10000 msecs Initial LSA throttle delay 0 msecs Minimum hold time for LSA throttle 5000 msecs Maximum wait time for LSA throttle 5000 msecs Lsa Transmit Pacing timer 40 msecs, 1 LS-Upd Minimum LSA arrival 1000 msecs Pacing lsa-group: 30 secs Number of incomming current DD exchange neighbors 0/5 Number of outgoing current DD exchange neighbors 0/5 Number of external LSA 0. Checksum 0x000000 Number of opaque AS LSA 0. Checksum 0x000000

	Number of non-default external LSA 0 External LSA database is unlimited. Number of LSA originated 2 Number of LSA received 93 Log Neighbor Adjency Changes : Enabled Graceful-restart disabled Graceful-restart helper support enabled Number of areas attached to this router: 1: 1 normal 0 stub 0 nssa Area 1 Number of interfaces in this area is 1(1) Number of fully adjacent neighbors in this area is 0 Number of fully adjacent virtual neighbors through this area is 0 Area has no authentication SPF algorithm executed 0 times iSPF algorithm last executed 00:04:14.534 ago iSPF algorithm executed 12 times Number of LSA 1. Checksum 0x0029b3

4.4.19. Настройка функции управления сетью

4.4.19.1. Эффект конфигурации

Используйте программное обеспечение управления сетью для управления параметрами OSPF и мониторинга рабочего состояния OSPF.

4.4.19.2. Примечания

- Необходимо настроить основные функции OSPF.
- Перед включением функции OSPF MIB необходимо включить функцию MIB SNMP-сервера.
- Перед включением функции Trap OSPF необходимо включить функцию Trap SNMP-сервера.
- Вы должны включить функцию ведения журнала устройства перед выводом журналов OSPF.

4.4.19.3. Шаги настройки

Связывание MIB с процессом OSPF

- (Опционально) Эта конфигурация необходима, если вы хотите использовать программное обеспечение управления сетью для управления параметрами указанного процесса OSPF.
- Эта настройка выполняется на всех маршрутизаторах.

Включение функции Trap

- (Опционально) Эта конфигурация необходима, если вы хотите использовать программное обеспечение управления сетью для мониторинга рабочего состояния OSPF.
- Эта настройка выполняется на всех маршрутизаторах.

Настройка функции ведения журнала

- (Опционально) Эта функция включена по умолчанию. Рекомендуется сохранить конфигурацию по умолчанию. Если вы хотите уменьшить вывод журнала, отключите эту функцию.
- Эта настройка выполняется на всех маршрутизаторах.

4.4.19.4. Проверка

- Используйте программное обеспечение управления сетью для управления параметрами OSPF.
- Используйте программное обеспечение управления сетью для мониторинга рабочего состояния OSPF.

4.4.19.5. Связанные команды

Связывание MIB с процессом OSPF

Команда	**enable mib-binding**
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	MIB OSPFv2 не содержит информации о процессе OSPFv2. Поэтому вам необходимо выполнять операции на одном процессе OSPFv2 через SNMP. По умолчанию MIB OSPFv2 привязан к процессу OSPFv2 с наименьшим идентификатором процесса, и все пользовательские операции применяются к этому процессу. Если вы хотите выполнять операции с указанным OSPFv2 через SNMP, запустите эту команду, чтобы связать MIB с процессом

Включение функции Trap

Команда	**enable traps[error [IfAuthFailure | IfConfigError | IfRxBadPacket | VirtIfAuthFailure | VirtIfConfigError | VirtIfRxBadPacket] | lsa [LsdbApproachOverflow | LsdbOverflow | MaxAgeLsa | OriginateLsa] | retransmit [IfTxRetransmit | VirtIfTxRetransmit] | state-change[IfStateChange | NbrRestartHelperStatusChange | NbrStateChange | NssaTranslatorStatusChange | RestartStatusChange | VirtIfStateChange | VirtNbrRestartHelperStatusChange| VirtNbrStateChange]]**
Описание параметра	**IfAuthFailure**: указывает, что произошел сбой аутентификации интерфейса.

	IfConfigError: указывает на то, что произошла ошибка настройки параметров интерфейса. **IfRxBadPacket**: указывает, что интерфейс получил неверный пакет. **VirtIfAuthFailure**: указывает, что произошел сбой аутентификации виртуального интерфейса. **VirtIfConfigError**: указывает на то, что произошла ошибка настройки параметров виртуального интерфейса. **VirtIfRxBadPacket**: указывает, что виртуальный интерфейс получил неверный пакет. **LsdbApproachOverflow**: указывает, что количество внешних LSA достигло 90 % от верхнего предела. **LsdbOverflow**: указывает, что количество внешних LSA достигло верхнего предела. **MaxAgeLsa**: указывает, что истекает срок действия таймера устаревания LSA. **OriginateLsa**: указывает, что создан новый LSA. **IfTxRetransmit**: указывает, что пакет повторно передается на интерфейс. **VirtIfTxRetransmit**: указывает, что пакет повторно передается на виртуальный интерфейс. **IfStateChange**: указывает на изменение состояния интерфейса. **NbrRestartHelperStatusChange**: указывает на изменение состояния процесса GR соседа. **NbrStateChange**: указывает на изменение состояния соседа. **NssaTranslatorStatusChange**: указывает на изменение состояния трансляции NSSA. **RestartStatusChange**: указывает на изменение состояния GR локального устройства. **VirtIfStateChange**: указывает на изменение состояния виртуального интерфейса. **VirtNbrRestartHelperStatusChange**: указывает на изменение состояния GR виртуального соседа. **VirtNbrStateChange**: указывает на изменение состояния виртуального соседа
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Функция, настроенная этой командой, ограничена командой **snmp-server**. Вы можете настроить **snmp-server enable traps ospf**, а затем команду **enable traps**, прежде чем соответствующие Trap OSPF смогут быть правильно отправлены.

	Эта команда не ограничена MIB, связанным с процессом. Функцию Trap можно включить одновременно для разных процессов

Настройка функции регистрации

Команда	**log-adj-changes**[**detail**]
Описание параметра	**detail**: записывает всю информацию об изменении статуса
Командный режим	Режим конфигурации процесса маршрутизации OSPF

4.4.19.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе4.4.1 Настройка основных функций OSPF.

Сценарий:

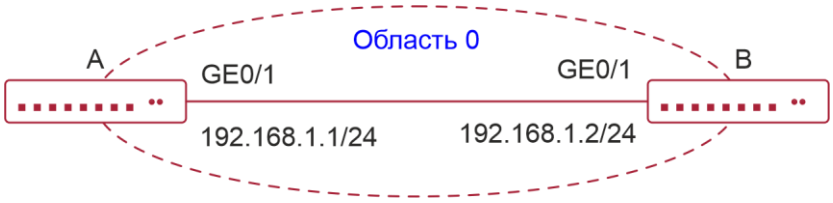


Рисунок 4-28.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • Свяжите MIB с процессом OSPF на маршрутизаторе A. • Включите функцию Trap на маршрутизаторе A
A	A# configure terminal A(config)# snmp-server host 192.168.2.2 traps version 2c public A(config)# snmp-server community public rw A(config)# snmp-server enable traps A(config)# router ospf 10 A(config-router)# enable mib-binding A(config-router)# enable traps

Проверка	Используйте инструмент MIB для чтения и установки параметров OSPF, а также отображения рабочего состояния OSPF

4.4.19.7. Распространенные ошибки

Конфигурации SNMP-сервера неверна. Например, функция MIB или Trap не включена.

4.4.20. Изменение параметров управления протоколом

4.4.20.1. Эффект конфигурации

Измените параметры управления протоколом, чтобы изменить статус работы протокола.

4.4.20.2. Примечания

- Необходимо настроить основные функции OSPF.
- Время dead соседа не может быть короче интервала Hello.

4.4.20.3. Шаги настройки

Настройка интервала Hello

- (Опционально) Рекомендуется сохранить конфигурацию по умолчанию.
- Эта конфигурация выполняется на маршрутизаторах на обоих концах канала.

Настройка интервала dead

- (Опционально) Рекомендуется сохранить конфигурацию по умолчанию. Эту конфигурацию можно изменить, если вы хотите ускорить конвергенцию OSPF при сбое канала.
- Эта конфигурация выполняется на маршрутизаторах на обоих концах канала.

Настройка интервала повторной передачи LSU

(Опционально) Рекомендуется изменить эту конфигурацию, если в пользовательской среде существует много маршрутов и перегрузка сети серьезна.

Настройка времени генерации LSA

(Опционально) Рекомендуется сохранить конфигурацию по умолчанию.

Настройка времени обновления группы LSA

- (Опционально) Рекомендуется сохранить конфигурацию по умолчанию. Эту конфигурацию можно настроить, если в пользовательской среде существует много маршрутов.
- Эта конфигурация выполняется на ASBR или ABR.

Настройка задержки повторного приема LSA

(Опционально) Рекомендуется сохранить конфигурацию по умолчанию.

Настройка задержки вычисления SPF

(Опционально) Эту конфигурацию можно изменить, если часто происходит flapping сети.

Настройка задержки расчета межобластного маршрута

- (Опционально) Рекомендуется сохранить конфигурацию по умолчанию.
- Эта настройка выполняется на всех маршрутизаторах.

Настройка задержки вычисления внешнего маршрута

- (Опционально) Рекомендуется сохранить конфигурацию по умолчанию.
- Эта настройка выполняется на всех маршрутизаторах.

4.4.20.4. Проверка

Запустите команду **show ip ospfandshow ip ospf neighbor**, чтобы отобразить параметры и состояние работы протокола.

4.4.20.5. Связанные команды

Настройка интервала Hello

Команда	**ip ospf hello-interval** *seconds*
Описание параметра	*seconds*: указывает интервал, с которым OSPF отправляет пакет Hello. Измеряется в секундах. Значение варьируется от 1 до 65 535
Командный режим	Режим настройки интерфейса
Руководство по использованию	Интервал Hello содержится в пакете Hello. Более короткий интервал Hello указывает на то, что OSPF может быстрее обнаруживать топологические изменения, но сетевой трафик увеличивается. Интервал Hello должен быть одинаковым на всех маршрутизаторах в одном сегменте сети. Если вы хотите вручную изменить интервал dead соседа, убедитесь, что интервал dead соседа длиннее интервала Hello

Настройка интервала dead

Команда	**ip ospf dead-interval** *seconds*
Описание параметра	*seconds*: указывает время, когда сосед объявлен потерянным. Измеряется в секундах. Значение находится в диапазоне от 0 до 2 147 483 647
Командный режим	Режим настройки интерфейса
Руководство по использованию	Dead-интервал OSPF содержится в пакете Hello. Если OSPF не получает пакет Hello от соседа в течение интервала dead, он объявляет соседа недействительным и удаляет эту запись соседа из списка соседей. По умолчанию dead-интервал в четыре раза превышает интервал Hello. Если интервал Hello изменяется, dead-интервал изменяется автоматически. Когда вы используете эту команду, чтобы вручную изменить dead-интервал, обратите внимание на следующие проблемы: 1. Dead-интервал не может быть короче интервала Hello.

	2. Dead-интервал должен быть одинаковым на всех маршрутизаторах в одном сегменте сети

Настройка задержки передачи LSU

Команда	**ip ospf transmit-delay** *seconds*
Описание параметра	*seconds*: указывает задержку передачи LSU на интерфейсе OSPF. Измеряется в секундах. Значение варьируется от 1 до 65 535
Командный режим	Режим настройки интерфейса
Руководство по использованию	Перед передачей пакета LSU поля Age во всех LSA в этом пакете будут увеличиваться в зависимости от величины, указанной командой **ip ospf transmit-delay**. Учитывая задержку передачи и задержку line propagation на интерфейсе, необходимо установить задержку передачи LSU на большее значение для низкоскоростной линии связи или интерфейса. Задержка передачи LSU виртуального канала определяется параметром **transmit-delay** в команде **area virtual-link**. Если значение поля Age LSA достигает 3600, пакет будет передан повторно или будет запрошена повторная передача. Если LSA не будет обновлено вовремя, LSA с истекшим сроком действия будет удалено из LSDB

Настройка интервала повторной передачи LSU

Команда	**ip ospf retransmit-interval** *seconds*
Описание параметра	*seconds*: указывает интервал повторной передачи LSU. Измеряется в секундах. Значение варьируется от 0 до 65 535. Этот интервал должен быть больше, чем задержка передачи пакетов данных между двумя соседями туда и обратно
Командный режим	Режим настройки интерфейса
Руководство по использованию	После того, как маршрутизатор завершит отправку пакета LSU, этот пакет все еще сохраняется в очереди буфера передачи. Если подтверждение от соседа не получено в течение времени, определенного командой **ip ospf retransmit-interval**, маршрутизатор повторно передает пакет LSU. Задержку повторной передачи можно установить на большее значение на последовательной линии связи или виртуальном канале, чтобы предотвратить ненужную повторную передачу. Задержка повторной передачи LSU виртуального канала определяется параметром **retransmit-interval** в команде **area virtual-link**

Настройка времени генерации LSA

Команда	**timers throttle lsa all** *delay-time hold-time max-wait-time*
Описание параметра	*delay-time*: указывает минимальную задержку для генерации LSA. Первый LSA в базе данных всегда генерируется мгновенно. Значение варьируется от 0 до 600 000. Единица измерения — мс. *hold-time*: указывает минимальный интервал между первым обновлением LSA и вторым обновлением LSA. Значение варьируется от 1 до 600 000. Единица измерения — мс. *max-wait-time*: указывает максимальный интервал между двумя обновлениями LSA, когда LSA обновляется непрерывно. Этот интервал также используется для определения того, обновляется ли LSA постоянно. Значение варьируется от 1 до 600 000. Единица измерения — мс
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Если при изменении канала возникают высокие требования к конвергенции, вы можете установить время задержки **delay-time** на меньшее значение. Вы также можете соответствующим образом увеличить значения предыдущих параметров, чтобы уменьшить загрузку ЦП. При настройке этой команды значение **hold-time** не может быть меньше значения **delay-time**, а значение **max-wait-time** не может быть меньше значения **hold-time**

Настройка времени обновления группы LSA

Команда	**timers pacinglsa-group** *seconds*
Описание параметра	*seconds*: указывает интервал pacing группы LSA. Значение варьируется от 10 до 1800. Измеряется в секундах
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	У каждого LSA есть время жизни (возраст LSA). Когда возраст LSA достигает 1800 секунд, необходимо обновление, чтобы предотвратить очистку LSA, поскольку их возраст достигает максимума. Если обновление LSA и вычисление устаревания выполняются для каждого LSA, устройство будет потреблять много ресурсов ЦП. Чтобы эффективно использовать ресурсы ЦП, вы можете обновлять LSA по группам на устройстве. Интервал группового обновления называется интервалом pacing группы. Операция обновления группы заключается

	в организации LSA, сгенерированных в пределах интервала pacing группы, в группу и обновлении группы в целом. Если общее количество LSA не меняется, больший интервал pacing группы указывает на то, что после тайм-аута необходимо обработать больше LSA. Чтобы поддерживать стабильность ЦП, количество процессов LSA при каждом тайм-ауте не может быть слишком большим. Если количество LSA велико, рекомендуется уменьшить интервал pacing группы. Например, если в базе данных имеется 1000 LSA, вы можете уменьшить интервал pacing; если имеется от 40 до 100 LSA, интервал pacing можно установить на 10–20 минут

Настройка интервала обновления группы LSA

Команда	**timers pacing lsa-transmit** *transmit-time transmit-count*
Описание параметра	*transmit-time*: указывает интервал передачи группы LSA. Значение варьируется от 10 до 1000. Единица измерения — мс. *transmit-count*: указывает количество пакетов LS-UPD в группе. Значение варьируется от 1 до 200
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Если количество LSA велико и нагрузка на устройство в среде велика, правильная настройка *transmit-time* и *transmit-count* может ограничить количество пакетов LS-UPD, рассылаемых по сети. Если загрузка ЦП невелика и нагрузка на полосу пропускания сети невелика, уменьшение значений *transmit-time* и *transmit-count* может ускорить конвергенцию среды

Настройка задержки повторного приема LSA

Команда	**timers lsa arrival** *arrival-time*
Описание параметра	*arrival-time*: указывает задержку, после которой будет получен тот же LSA. Значение варьируется от 0 до 600 000. Единица измерения — мс
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Никакие действия не выполняются, если тот же LSA получен в течение указанного времени

Настройка задержки расчета межобластного маршрута

Команда	**timers throttle route inter-area** *ia-delay*
Описание параметра	*ia-delay*: указывает задержку расчета маршрута между областями. Единица измерения — мс. Значение варьируется от 0 до 600 000
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Эту задержку нельзя изменить, если к времени конвергенции сети предъявляются строгие требования

Настройка задержки вычисления внешнего маршрута

Команда	**timers throttle route ase** *ase-delay*
Описание параметра	*ase-delay*: указывает задержку расчета внешнего маршрута. Единица измерения — мс. Значение варьируется от 0 до 600 000
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Эту задержку нельзя изменить, если к времени конвергенции сети предъявляются строгие требования

Настройка задержки вычисления SPF

Команда	**timers throttle spf** *spf-delay spf-holdtime spf-max-waittime*
Описание параметра	*spf-delay*: указывает задержку вычисления SPF. Единица измерения — мс. Значение варьируется от 1 до 600 000. При обнаружении топологического изменения процесс маршрутизации OSPF запускает вычисление SPF по крайней мере после истечения задержки *spf-delay*. *spf-holdtime*: указывает минимальный интервал между двумя вычислениями SPF. Единица измерения — мс. Значение варьируется от 1 до 600 000. *spf-max-waittime*: указывает максимальный интервал между двумя вычислениями SPF. Единица измерения — мс. Значение варьируется от 1 до 600 000. *number*: указывает метрику суммарного маршрута
Командный режим	Режим конфигурации процесса маршрутизации OSPF

Руководство по использованию	*spf-delay* указывает минимальное время между возникновением топологического изменения и началом расчета SPF. *spf-holdtime* указывает минимальный интервал между первым вычислением SPF и вторым вычислением SPF. После этого интервал между двумя вычислениями SPF должен быть как минимум в два раза больше предыдущего интервала. Когда интервал достигает *spf-max-waittime*, интервал не может снова увеличиться. Если интервал между двумя вычислениями SPF уже превышает требуемое минимальное значение, интервал вычисляется, начиная с *spf-holdtime*. Вы можете установить *spf-delay* и *spf-holdtime* на меньшие значения, чтобы ускорить сходимость топологии, и установите для *spf-max-waittime* большее значение, чтобы уменьшить вычисление SPF. Гибкие настройки могут быть использованы в зависимости от стабильности топологии сети. По сравнению с командой **timers spf**, эта команда поддерживает более гибкие настройки для ускорения скорости сходимости вычислений SPF и дальнейшего снижения системных ресурсов, потребляемых вычислением SPF, когда топология постоянно меняется. Поэтому для настройки рекомендуется использовать команду **timers throttle spf**. Значение *spf-holdtime* не может быть меньше значения *spf-delay*; в противном случае для *spf-holdtime* будет автоматически установлено значение *spf-delay*. Значение *spf-max-waittime* не может быть меньше значения *spf-holdtime*; в противном случае для *spf-max-waittime* будет автоматически установлено значение *spf-holdtime*. Конфигурации **timers throttle spf** и **timers spf** взаимно перезаписываются. Когда обе команды **timers throttle spf** и **timers spf** не настроены, значения для **timers throttle spf** по умолчанию преобладают

4.4.20.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующих примерах конфигурации предполагается, что основные функции OSPF настроены. Подробную информацию об основных функциях OSPF см. в разделе Настройка основных функций OSPF.

Настройка интервала Hello и интервала dead

Сценарий:

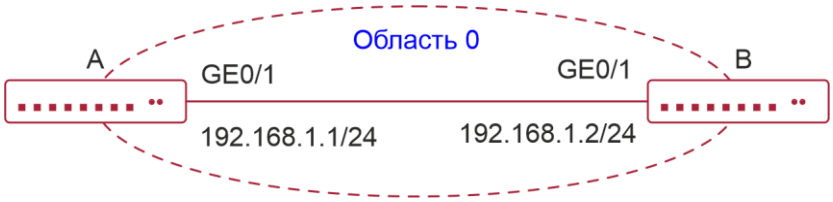


Рисунок 4-29.

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. (пропущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (пропущено) • Настройте интервал приветствия и dead-интервал на всех маршрутизаторах
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip ospf hello-interval 15 A(config-if-GigabitEthernet 0/1)# ip ospf dead-interval 50
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip ospf hello-interval 15 A(config-if-GigabitEthernet 0/1)# ip ospf dead-interval 50
Проверка	Проверьте параметры интерфейса на маршрутизаторе A. Убедитесь, что интервал Hello составляет 10 с, а интервал dead — 50 с
A	A# show ip ospf interface GigabitEthernet 0/1 is up, line protocol is up Internet Address 192.168.1.1/24, Ifindex 2, Area 0.0.0.0, MTU 1500 Matching network config: 192.168.1.0/24 Process ID 1, Router ID 192.168.1.2, Network Type POINTOMULTIPOINT, Cost: 1 Transmit Delay is 1 sec, State Point-To-Point Timer intervals configured, Hello 15, Dead 50, Wait 40, Retransmit 5 Hello due in 00:00:02 Neighbor Count is 1, Adjacent neighbor count is 0 Crypt Sequence Number is 4787 Hello received 465 sent 466, DD received 8 sent 8 LS-Req received 2 sent 2, LS-Upd received 8 sent 21 LS-Ack received 14 sent 7, Discarded 3

4.4.20.7. Распространенные ошибки

Настроенное время dead соседа короче интервала Hello.

4.5. Мониторинг

4.5.1.1. Очистка

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

Описание	Команда
Очищает и сбрасывает процесс OSPF	**clear ip ospf** [*process-id*] **process**

4.5.1.2. Отображение

Описание	Команда
Отображает конфигурации процесса OSPF	**show ip ospf** [*process-id*]
Отображает внутреннюю таблицу маршрутизации OSPF, включая маршруты к ABR и ASBR	**show ip ospf**[*process-id*] **border-routers**
Отображает информацию о OSPF LSDB	**show ip ospf** [*process-id area-id*] **database** [{ **asbr-summary** | **external** | **network** | **nssa-external** | **opaque-area** | **opaque-as** | **opaque-link** | **router** | **summary** }][{ **adv-router** *ip-address*| **self-originate** } |*link-state-id* | **brief**][**database-summary** | **max-age** | **detail**]
Отображает интерфейсы с поддержкой OSPF	**show ip ospf** [*process-id*] **interface** [*interface-type interface-number* | **brief**]
Отображает список соседей OSPF	**show ip ospf** [*process-id*] **neighbor** [**detail**] [*interface-type interface-number*] [*neighbor-id*]
Отображает таблицу маршрутизации OSPF	**show ip ospf** [*process-id*] **route**[**count**]
Отображает количество вычислений SPT в области OSPF	**show ip ospf** [*process-id*] **spf**

Описание	Команда
Отображает суммарный маршрут перераспределенных маршрутов OSPF	**show ip ospf**[*process-id*] **summary-address**
Отображает информацию о топологии сети OSPF	**show ip ospf** [*process-id*[*area-id*]] **topology**[**adv-router** *adv-router-id* [*router-id*] | **self-originate**[*router-id*]]
Отображает виртуальные каналы OSPF	**show ip ospf** [*process-id*] **virtual-links** [*ip-address*]

4.5.1.3. Отладка

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

Описание	Команда
Отладка событий OSPF	**debug ip ospf events [abr|asbr|lsa|nssa|os|restart| router|slink| vlink]**
Отладка интерфейсов OSPF	**debug ip ospf ifsm [events|status|timers]**
Отладка соседей OSPF	**debug ip ospf nfsm [events | status | timers]**
Отладка OSPF NSM	**debug ip ospf nsm [interface | redistribute | route]**
Отладка LSA OSPF	**debug ip ospf lsa [flooding | generate | install | maxage | refresh]**
Отладка пакетов OSPF	**debug ip ospf packet [dd|detail|hello|ls-ack|ls-request|ls-update|recv|send]**
Отладка маршрутов OSPF	**debug ip ospf route [ase | ia | install | spf | time]**

5. НАСТРОЙКА OSPFV3

5.1. Обзор

Open Shortest Path First (OSPF) — это протокол внутреннего шлюза (IGP), который используется в автономной системе (AS), чтобы позволить маршрутизаторам получать маршрут к удаленной сети.

ПРИМЕЧАНИЕ: OSPF версии 2 (OSPFv2) применимо к IPv4 и OSPF версии 3 (OSPFv3) применимо к IPv6. Механизм работы протокола и большинство конфигураций одинаковы.

OSPF имеет следующие характеристики:

- Широкая сфера применения: OSPF применим к более крупной сети, поддерживающей сотни маршрутизаторов.
- Быстрая конвергенция: при изменении топологии сети между маршрутизаторами можно быстро отправлять уведомления для обновления маршрутов.
- Отсутствие самозацикливания (self-loop): между маршрутизаторами синхронизируется только информация о состоянии канала. Каждый маршрутизатор самостоятельно вычисляет маршруты, поэтому самозацикливания не возникает.
- Разделение областей: большой домен маршрутизации делится на несколько небольших областей для экономии системных ресурсов и пропускной способности сети, а также обеспечения стабильности и надежности маршрутов.
- Классификация маршрутов: маршруты подразделяются на несколько типов для обеспечения гибкого управления.
- Эквивалентные маршруты: OSPF поддерживает эквивалентные маршруты.
- Аутентификация: OSPF поддерживает аутентификацию пакетов для обеспечения безопасности взаимодействия протоколов.
- Multicast-передача: пакеты протокола отправляются с использованием multicast-адреса, чтобы избежать взаимодействия с посторонними объектами и сэкономить системные ресурсы.

ПРИМЕЧАНИЕ: в этой главе термин «маршрутизатор» относится к любому сетевому устройству, поддерживающему функцию маршрутизации. Этими сетевыми устройствами могут быть коммутаторы L3, маршрутизаторы или фаерволы.

ПРИМЕЧАНИЕ: если не указано иное, «OSPF» в следующих описаниях относится к OSPFv3.

5.1.1.1. Протоколы и стандарты

RFC2740	В этом документе описаны изменения OSPF для поддержки версии 6 интернет-протокола (IPv6)
draft-ietf-ospf-ospfv3-graceful-restart	В этом документе описывается плавный перезапуск OSPFv3. Плавный перезапуск OSPFv3 идентичен OSPFv2, за исключением различий, описанных в этом документе. Эти различия включают формат отсрочки (grace) объявлений о состоянии канала (LSA) и другие соображения

RFC2740	В этом документе описаны изменения OSPF для поддержки версии 6 интернет-протокола (IPv6)
draft-ietf-ospf-ospfv3-mib-11	В этом документе определяется часть базы управляющей информации (MIB) для использования с протоколами управления сетью в сетях Интернет на базе IPv6. В частности, он определяет объекты для управления протоколом маршрутизации Open Shortest Path First для IPv6

5.2. Приложения

Приложение	Описание
Внутридоменное взаимодействие	OSPF работает внутри AS, которая разделена на несколько областей
Междоменное взаимодействие	Несколько AS связаны между собой. OSPF работает внутри каждой AS, а BGP работает между AS

5.2.1. Внутридоменное взаимодействие

5.2.1.1. Сценарий

OSPF работает внутри AS. Если количество маршрутизаторов превышает 40, рекомендуется разделить AS на несколько областей. Как правило, устройства высокого класса, обладающие надежной производительностью и высокой скоростью обработки, развертываются в магистральной области, а устройства низкого или среднего уровня с относительно низкой производительностью могут быть развернуты в обычной области. Все обычные области должны быть подключены к магистральной области. Рекомендуется настроить обычную область, расположенную в тупике, как тупиковую область. Как показано на Рисунке 5-1, сеть разделена на четыре области. Связь между этими областями должна идти через магистраль, т.е. область 0.

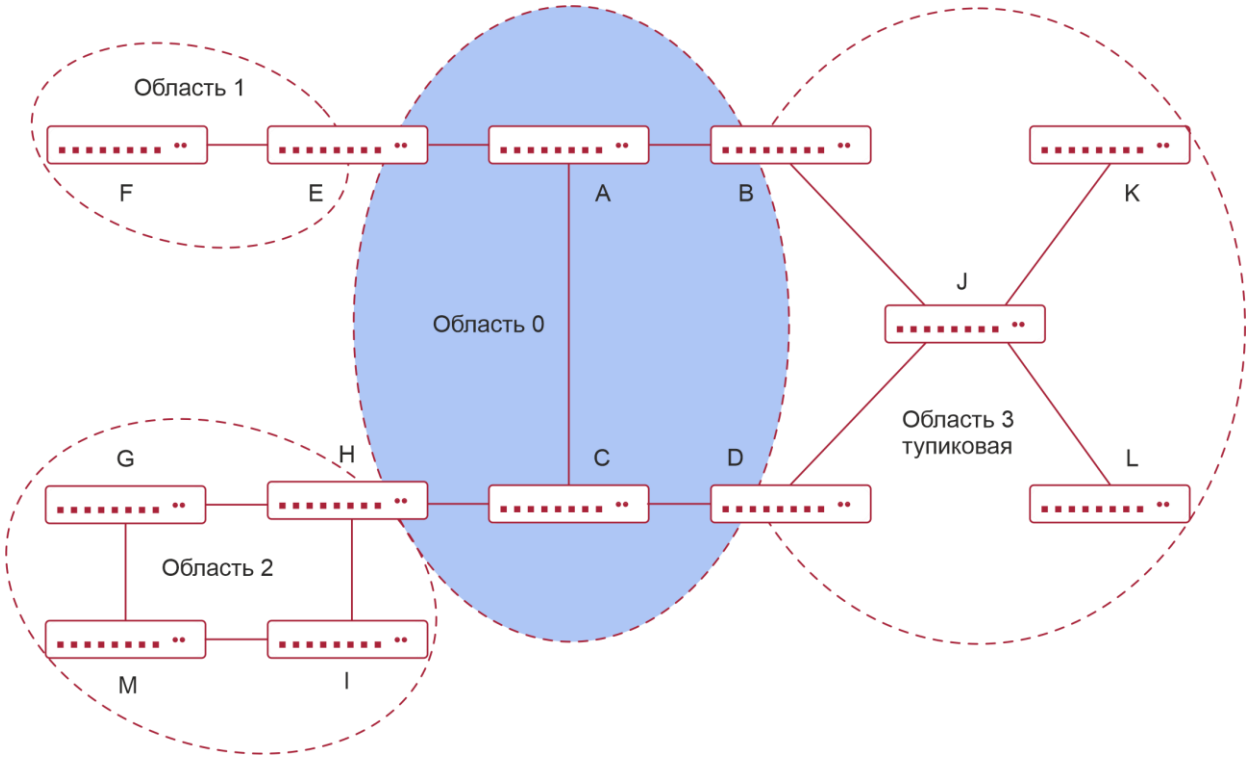


Рисунок 5-1. Разделение областей OSPF

A, B, C, D, E и H расположены в магистральной области и являются магистральными маршрутизаторами.

Область 3 настроена как тупиковая область.

5.2.1.2. Развертывание

OSPF работает на всех маршрутизаторах в пределах AS для реализации unicast-маршрутизации.

5.2.2. Междоменное взаимодействие

5.2.2.1. Сценарий

Несколько AS связаны между собой. OSPF работает внутри каждой AS, а BGP работает между AS. Обычно OSPF и BGP изучают информацию о маршрутизации друг у друга.

Как показано на Рисунке 5-2, unicast-маршрутизация реализована в AS 100 и AS 200 использует OSPF, а между двумя AS использует BGP.

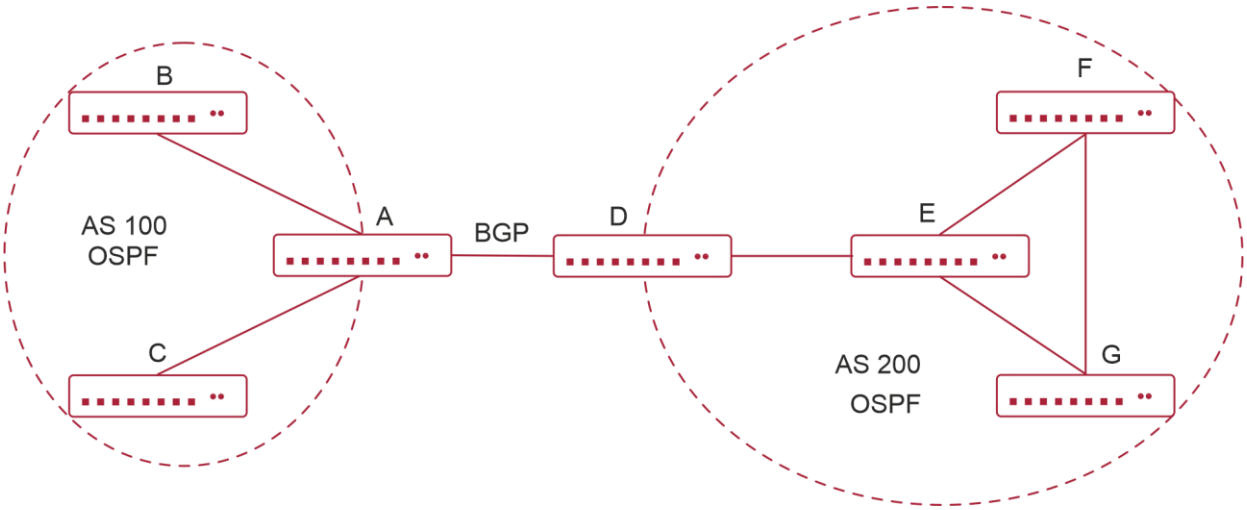


Рисунок 5-2. Взаимодействие между OSPF и BGP

OSPF и BGP работают одновременно на маршрутизаторах A и D.

5.2.2.2. Развертывание

- OSPF работает в AS 100 и AS 200 для реализации unicast-маршрутизации.
- BGP работает между двумя AS для реализации unicast-маршрутизации.

5.3. Функции

5.3.1. Базовые определения

Домен маршрутизации

Все маршрутизаторы в AS должны быть связаны между собой и использовать один и тот же протокол маршрутизации. Поэтому AS также называют доменом маршрутизации.

AS, на которой запущено OSPF, также называется доменом маршрутизации OSPF или сокращенно доменом OSPF.

Процесс OSPF

OSPF поддерживает несколько экземпляров, и каждый экземпляр соответствует процессу OSPF.

На маршрутизаторе можно запустить один или несколько процессов OSPF. Каждый процесс OSPF запускает OSPF независимо, и процессы взаимно изолированы.

Заголовок пакета OSPF содержит поле идентификатора экземпляра, и несколько экземпляров OSPF могут работать одновременно по одному каналу. Идентификатор процесса действителен только на локальном устройстве.

Идентификатор маршрутизатора

Идентификатор маршрутизатора однозначно идентифицирует маршрутизатор в домене OSPF. Идентификаторы любых двух маршрутизаторов не могут быть одинаковыми.

Если на маршрутизаторе существует несколько процессов OSPF, каждый процесс OSPF использует один идентификатор маршрутизатора. Идентификаторы маршрутизаторов любых двух процессов OSPF не могут быть одинаковыми.

Область

OSPF поддерживает несколько областей. Домен OSPF разделен на несколько областей, чтобы облегчить вычислительную нагрузку в крупномасштабной сети.

Область представляет собой логическую группу маршрутизаторов, каждая группа идентифицируется идентификатором области. Границей между областями является маршрутизатор. Маршрутизатор может принадлежать одной или нескольким областям. Один сегмент сети (канал) может принадлежать только одной области, либо каждый интерфейс с поддержкой OSPF должен принадлежать определенной области.

Область 0 — это магистральная область, а остальные области — обычные области. Обычные области должны быть напрямую подключены к магистральной области.

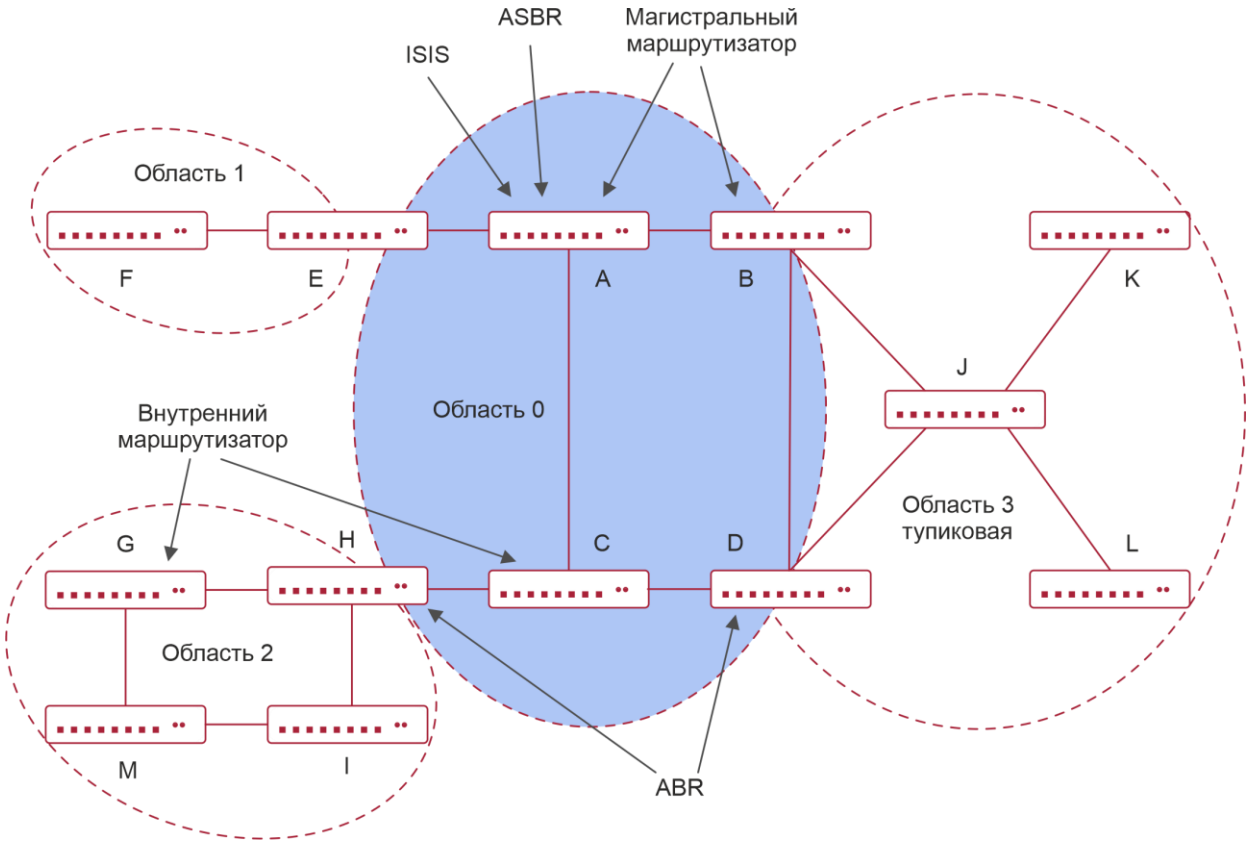


Рисунок 5-3. Разделение областей OSPF

OSPF-маршрутизатор

Следующие типы маршрутизаторов определены в OSPF и на них возложены различные обязанности:

Внутренний маршрутизатор (Internal router)

Все интерфейсы интервального маршрутизатора принадлежат одной области OSPF. Как показано на Рисунке 5-3, A, C, F, G, I, M, J, K и L — внутренние маршрутизаторы.

Пограничный маршрутизатор области (ABR)

ABR используется для соединения магистральной области с нормальной областью. ABR принадлежит двум или более областям, причем одна из областей должна быть магистральной. Как показано на Рисунке 5-3, B, D, E и H представляют собой ABR.

Магистральный маршрутизатор

Магистральный маршрутизатор имеет по крайней мере один интерфейс, принадлежащий магистральной области. Все ABR и все маршрутизаторы в области 0 являются магистральными маршрутизаторами. Как показано на Рисунке 5-3, A, B, C, D, E и H — магистральные маршрутизаторы.

Граничный маршрутизатор AS (ASBR)

ASBR используется для обмена информацией о маршрутизации с другими AS. ASBR не обязательно расположен на границе AS. Это может быть маршрутизатор внутри области или ABR. Как показано на Рисунке 5-3, A представляет собой ASBR.

Виртуальный канал

OSPF поддерживает виртуальные каналы. Виртуальный канал — это логический канал, принадлежащий магистральной области. Он используется для решения таких проблем, как прерывистая магистральная область или невозможность прямого подключения нормальной области к магистральной области в физической сети. Виртуальный канал поддерживает прохождение только одной нормальной области, и эта область называется транзитной областью. Маршрутизаторы на обоих концах виртуального канала являются ABR.

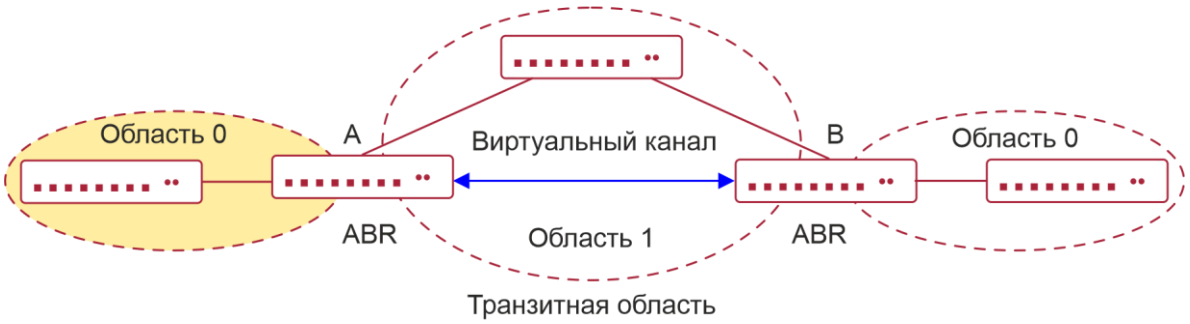


Рисунок 5-4. Прерывистая магистральная область в физической сети

Как показано на Рисунке 5-4, между A и B устанавливается виртуальный канал для соединения двух отдельных частей Области 0. Область 1 — транзитная область, а A и B — ABR Области 1.

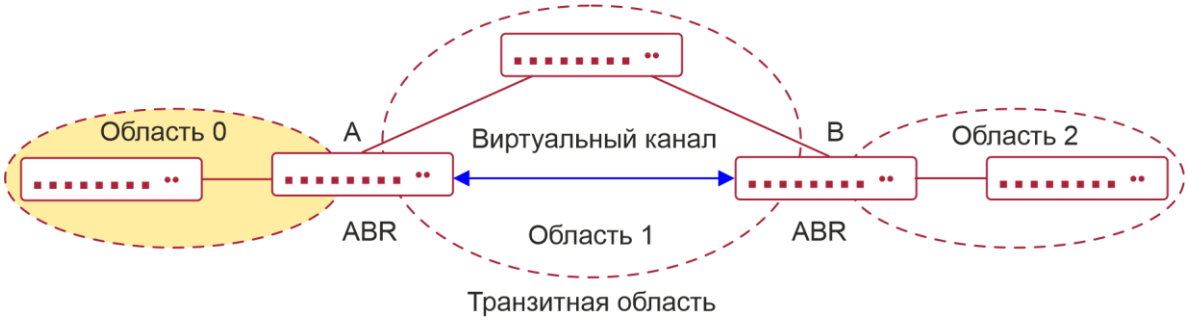


Рисунок 5-5. Невозможность прямого подключения обычной области к магистральной области физической сети.

Как показано на Рисунке 5-5 между A и B устанавливается виртуальное соединение для расширения области 0 до B, чтобы область 0 могла быть напрямую соединена с областью 2 на B. Область 1 является транзитной областью, A — ABR области 1, а B — ABR Области 0 и Области 2.

LSA

OSPF описывает информацию о маршрутизации посредством объявления состояния канала (LSA).

Тип LSA	Описание
Маршрутизатор-LSA (Тип 1) (Router-LSA)	Этот LSA создается каждым маршрутизатором. Он описывает состояние канала и стоимость маршрутизатора и объявляется только в пределах области, где находится исходный маршрутизатор
Сеть-LSA (Тип 2) (Network-LSA)	Этот LSA создается назначенным маршрутизатором (DR). Он описывает состояние текущего канала и объявляется только в пределах области, где расположен DR
Межобластной префикс-LSA (Тип 3) (Inter-Area-PrefixLSA)	Этот LSA создан ABR. Он описывает маршрут в другую область и объявляется в областях, за исключением полностью тупиковых областей или областей Not-So-Stubby Area (NSSA)
Межобластной маршрутизатор-LSA (Тип 4) (Inter-Area-RouterLSA)	Этот LSA создан ABR. Он описывает маршрут к ASBR и объявляется в областях, кроме областей, где расположен ASBR
AS-внешний-LSA (Тип 5) (AS-external-LSA)	Этот LSA создан ABR. Он описывает маршрут к месту назначения за пределами AS и объявляется во всех областях, кроме тупиковых областей и областей NSSA

Тип LSA	Описание
NSSA LSA (Тип 7)	Этот LSA создан ABR. Он описывает маршрут к месту назначения за пределами AS и объявляется только в областях NSSA
Канал-LSA (Тип 8) (Link-LSA)	Этот LSA создается каждым маршрутизатором. Он описывает локальный адрес канала и адрес префикса IPv6 для каждого канала, а также предоставляет параметр канала, который будет установлен в Network-LSA. Он объявляется только по текущему каналу
Внутриобластной префикс-LSA (Тип 9) (Intra-Area-Prefix-LSA)	Каждый маршрутизатор или DR генерирует один или несколько Intra-Area-Prefix-LSA, которые объявляются в области, к которой принадлежит маршрутизатор или DR. Intra-Area-Prefix-LSA, сгенерированный маршрутизатором, описывает адрес префикса IPv6, связанный с Route-LSA. Intra-Area-Prefix-LSA, сгенерированный DR, описывает адрес префикса IPv6, связанный с Network-LSA

ПРИМЕЧАНИЕ: тупиковые области, области NSSA, полностью тупиковые области и полностью NSSA области представляют собой особые формы обычных областей и помогают снизить нагрузку на маршрутизаторы и повысить надежность маршрутов OSPF.

Пакет OSPF

В следующей таблице перечислены пакеты протоколов, используемые OSPF. Эти пакеты OSPF инкапсулируются в IP-пакеты и передаются в multicast- или unicast-режиме.

Тип пакета	Описание
Hello	Пакеты Hello периодически отправляются для обнаружения и поддержания отношений соседства OSPF
Описание базы данных (DD)	Пакеты DD содержат краткую информацию о локальной базе данных состояния каналов (LSDB) и используются для синхронизации LSDB между соседями OSPF
Запрос состояния канала (LSR)	Пакеты LSR используются для запроса необходимых LSA от соседей. Пакеты LSR отправляются только после успешного обмена пакетами DD между соседями OSPF
Обновление состояния канала (LSU)	Пакеты LSU используются для отправки требуемых LSA peer-ам

Тип пакета	Описание
Подтверждение состояния канала (LSAck)	Пакеты LSAck используются для подтверждения полученных LSA

5.3.2. Обзор

Особенность	Описание
Протоколы маршрутизации по состоянию канала	Запустите OSPF на маршрутизаторе, чтобы получить маршруты к различным пунктам назначения в сети
Управление маршрутами OSPF	Правильно планируйте или оптимизируйте маршруты OSPF с помощью ручной настройки для реализации управления маршрутами OSPF
Повышенная безопасность и надежность	Используйте такие функции, как аутентификация и корреляция BFD, для повышения безопасности, стабильности и надежности OSPF
Функции управления сетью	Используйте такие функции, как MIB и Syslog, для облегчения управления OSPF

5.3.3. Протоколы маршрутизации по состоянию канала

OSPF — это тип протоколов маршрутизации по состоянию канала. Процесс его работы следующий:

Обнаружение соседей → Двусторонняя связь

Между соседними маршрутизаторами устанавливаются отношения соседства OSPF, и поддерживается двусторонняя связь.

Синхронизация базы данных → Полное смежность

Маршрутизатор использует LSA для объявления всех состояний своего канала. Между соседями происходит обмен LSA, а база данных состояний каналов (LSDB) синхронизируется для достижения полной смежности.

Вычисление «дерева» кратчайшего пути (SPT) → Формирование таблицы маршрутизации

Маршрутизатор вычисляет кратчайший путь к каждой сети назначения на основе LSDB и формирует таблицу маршрутизации OSPF.

5.3.3.1. Принцип работы

Обнаружение соседей → Двусторонняя связь

Маршрутизаторы отправляют пакеты Hello через все интерфейсы с поддержкой OSPF (или виртуальные каналы). Если два маршрутизатора могут обмениваться пакетами Hello и параметры, передаваемые в пакетах Hello, могут быть успешно согласованы, два маршрутизатора становятся соседями. Маршрутизаторы, являющиеся взаимно соседями, находят свои собственные идентификаторы маршрутизаторов из пакетов Hello, отправленных от соседей, и устанавливается двусторонняя связь.

Пакет Hello включает в себя, помимо прочего, следующую информацию:

- Идентификатор исходного маршрутизатора
- Идентификатор области исходного интерфейса маршрутизатора (или виртуального канала)
- Идентификатор экземпляра исходного интерфейса маршрутизатора (или виртуального канала)
- Идентификатор интерфейса исходного интерфейса маршрутизатора (или виртуального канала)
- Приоритет исходного интерфейса маршрутизатора (используется для выбора DR/BDR)
- Интервал Hello исходного интерфейса маршрутизатора (или виртуального канала)
- Интервал dead соседа исходного интерфейса маршрутизатора (или виртуального канала)
- IP-адреса DR и резервного назначенного маршрутизатора Backup Designated Router (BDR)
- Идентификатор маршрутизатора соседа исходного маршрутизатора

Синхронизация базы данных → Полная смежность

После установки двусторонней связи между соседними маршрутизаторами пакеты DD, LSR, LSU и LSAck используются для обмена LSA и настройки смежности. Краткий процесс выглядит следующим образом:

- Маршрутизатор генерирует LSA для описания всех состояний каналов на маршрутизаторе.
- LSA обменивается между соседями. Когда маршрутизатор получает LSA от своего соседа, он копирует LSA и сохраняет копию в локальной базе данных LSDB, а затем объявляет LSA другим соседям.
- Когда маршрутизатор и его соседи получают один и тот же LSDB, достигается полная смежность.

ПРИМЕЧАНИЕ: работа OSPF будет незаметна без изменений в стоимости канала или добавления или удаления сети. Если происходят какие-либо изменения, измененные состояния каналов объявляются для быстрой синхронизации LSDB.

SPT-вычисление → Формирование таблицы маршрутизации

После получения полной LSDB от маршрутизатора запускается алгоритм Dijkstra для генерации SPT от локального маршрутизатора к каждой сети назначения. SPT записывает сети назначения, адреса следующего hop-а и стоимость. OSPF генерирует таблицу маршрутизации на основе SPT.

Если произойдут изменения в стоимости каналов, добавлении или удалении сети, LSDB будет обновлена. Маршрутизатор снова запускает алгоритм Dijkstra, генерирует новый SPT и обновляет таблицу маршрутизации.

ПРИМЕЧАНИЕ: алгоритм Dijkstra используется для поиска кратчайшего пути от вершины к другим вершинам во взвешенном ориентированном графе.

Типы сетей OSPF

Маршрутизатору не обязательно необходимо обмениваться LSA с каждым соседом и настраивать смежность с каждым соседом. Чтобы повысить эффективность, OSPF классифицирует сети, использующие различные протоколы канального уровня, на пять типов, чтобы обмен LSA осуществлялся разными способами для установления смежности:

Broadcast

- Соседи обнаруживаются,DR и BDR избираются.
- DR (или BDR) обменивается LSA со всеми другими маршрутизаторами для настройки смежности. За исключением DR и BDR, все остальные маршрутизаторы не обмениваются LSA друг с другом, и смежность не настроена.
- Ethernet и оптоволоконный распределенный интерфейс данных (FDDI) по умолчанию относятся к типу broadcast-сети.

Non-broadcast multiple access (NBMA)

- Соседи настраиваются вручную и выбираются DR и BDR.
- DR (или BDR) обменивается LSA со всеми другими маршрутизаторами для настройки смежности. За исключением DR и BDR, все остальные маршрутизаторы не обмениваются LSA друг с другом, и смежность не настроена.
- X.25, Frame Relay и ATM по умолчанию принадлежат сетям NBMA.

Точка-точка (P2P)

- Соседи обнаруживаются автоматически, а DR или BDR не выбираются.
- LSA обмениваются между маршрутизаторами на обоих концах канала и устанавливается смежность.
- PPP, HDLC и LAPB по умолчанию относятся к типу сети P2P.

Точка-многоточка (P2MP)

- Соседи обнаруживаются автоматически, а DR или BDR не выбираются.
- Между любыми двумя маршрутизаторами происходит обмен LSA и устанавливается смежность.
- Сети без какого-либо протокола канального уровня по умолчанию относятся к типу сети P2MP.

P2MP broadcast

- Соседи настраиваются вручную, а DR или BDR не выбираются.
- Между любыми двумя маршрутизаторами происходит обмен LSA и устанавливается смежность.
- Сети без какого-либо протокола канального уровня по умолчанию относятся к типу сети P2MP.

Типы маршрутов OSPF

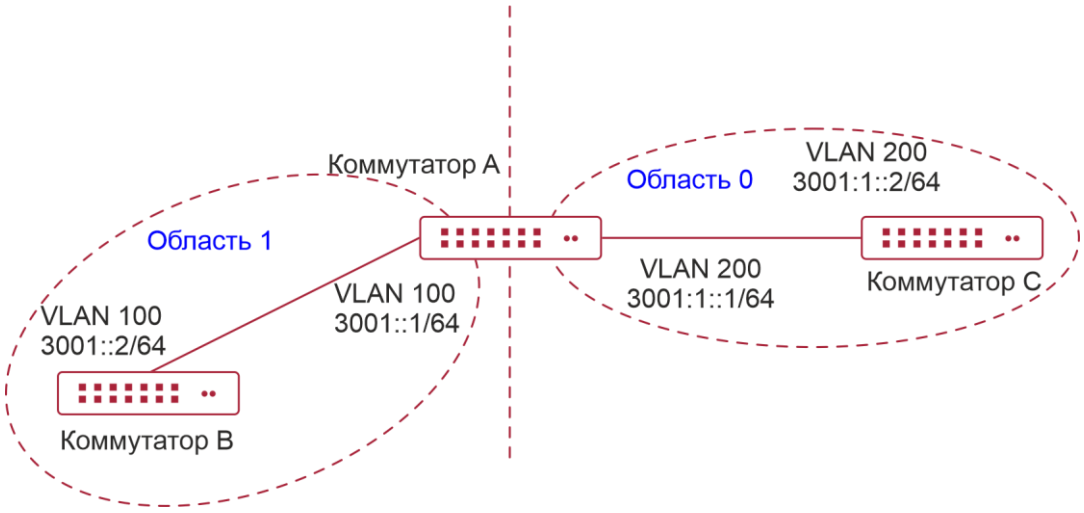


Рисунок 5-6.

Отобразите маршруты OSPF (отмечены красным) в таблице маршрутизации маршрутизатора C.

```
C#show ipv6 route ospf
IPv6 routing table name is Default(0) global scope - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra area, OI - OSPF inter area, OE1 - OSPF external type 1, OE2 - OSPF external type 2
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       [*] - NOT in hardware forwarding table
L      ::1/128 via Loopback, local host
OI     3001::/64 [110/2] via FE80::21A:A9FF:FE15:4CB9, VLAN 200
C      3001:1::/64 via VLAN 200, directly connected
L      3001:1::2/128 via VLAN 200, local host
L      FE80::/10 via ::1, Null0
C      FE80::/64 via VLAN 200, directly connected
L      FE80::21A:A9FF:FE01:FB1F/128 via VLAN 200, local host
```

Перед каждым маршрутом OSPF отображается метка, указывающая тип маршрута. Существует шесть типов маршрутов OSPF:

O: внутриобластной маршрут

Этот тип маршрута описывает, как добраться до сети назначения в локальной области. Стоимость этого типа маршрута равна стоимости маршрута от локального маршрутизатора до сети назначения.

OI: межобластной маршрут

Этот тип маршрута описывает, как добраться до сети назначения в другой области. Стоимость этого типа маршрута равна стоимости маршрута от локального маршрутизатора до сети назначения.

OE1: внешний маршрут типа 1

Этот тип маршрута описывает, как добраться до сети назначения за пределами AS. Стоимость этого типа маршрута равна стоимости маршрута от локального маршрутизатора до ASBR плюс стоимость маршрута от ASBR до сети назначения. Этот тип маршрута не существует на маршрутизаторах в тупиковой области или области NSSA.

OE2: внешний маршрут типа 2

Этот тип маршрута описывает, как добраться до сети назначения за пределами AS. Стоимость этого типа маршрута равна стоимости маршрута от ASBR до сети назначения. Этот тип маршрута не существует на маршрутизаторах в тупиковой области или области NSSA.

ON1: внешний маршрут типа 1 области NSSA

Этот тип маршрута описывает, как добраться до сети назначения за пределами AS через ASBR в области NSSA. Стоимость этого типа маршрута равна стоимости маршрута от локального маршрутизатора до ASBR плюс стоимость маршрута от ASBR до сети назначения. Этот тип маршрута существует только на маршрутизаторах в области NSSA.

ON2: внешний маршрут типа 2 области NSSA

Этот тип маршрута описывает, как добраться до сети назначения за пределами AS через ASBR в области NSSA. Стоимость этого типа маршрута равна стоимости маршрута от ASBR до сети назначения. Этот тип маршрута существует только на маршрутизаторах в области NSSA.

ПРИМЕЧАНИЕ: надежность маршрутов OE2 и ON2 низкая. OSPF считает, что стоимость маршрута от ASBR до пункта назначения за пределами AS намного превышает стоимость маршрута к ASBR внутри AS. Таким образом, при вычислении стоимости маршрута учитывается только стоимость маршрута от ASBR до пункта назначения за пределами AS.

5.3.3.2. Сопутствующая конфигурация

Включение OSPF

OSPF отключен по умолчанию.

Запустите команду **ipv6 router ospf** 1, чтобы создать процесс OSPF на маршрутизаторе.

Запустите команду **ipv6 ospfarea**, чтобы включить OSPF на интерфейсе, и укажите идентификатор области.

Запустите команду **area virtual-link**, чтобы создать виртуальный канал на маршрутизаторе. Виртуальный канал можно рассматривать как логический интерфейс.

Идентификатор маршрутизатора

По умолчанию процесс OSPF выбирает наибольший адрес IPv4 среди адресов IPv4 всех loopback-интерфейсов в качестве идентификатора маршрутизатора. Если loopback-интерфейсы, настроенные с адресами IPv4, недоступны, процесс OSPF выбирает самый большой адрес IPv4 среди адресов IPv4 всех физических портов в качестве идентификатора маршрутизатора.

Альтернативно вы можете запустить команду **router-id**, чтобы вручную указать идентификатор маршрутизатора.

Параметры управления протоколом

Запустите команду **ipv6 ospf hello-interval**, чтобы изменить интервал Hello на интерфейсе. Значение по умолчанию — 10 с (или 30 с для сетей NBMA).

Запустите команду **ipv6 ospf dead-interval**, чтобы изменить dead-интервал соседа на интерфейсе. Значение по умолчанию в четыре раза превышает интервал Hello.

Используйте параметр **poll-interval** в команде **ipv6 ospf neighbor**, чтобы изменить интервал опроса соседей на интерфейсе NBMA. Значение по умолчанию — 120 с.

Запустите команду **ipv6 ospf transmit-delay**, чтобы изменить задержку передачи пакетов LSU на интерфейсе. Значение по умолчанию — 1 с.

Запустите команду **ipv6 ospf retransmit-interval**, чтобы изменить интервал повторной передачи пакетов LSU на интерфейсе. Значение по умолчанию — 5 с.

Используйте параметр **hello-interval** в команде **area virtual-link**, чтобы изменить интервал Hello для виртуального канала. Значение по умолчанию — 10 с.

Используйте параметр **dead-interval** в команде **area virtual-link**, чтобы изменить dead-интервал соседа в виртуальном канале. Значение по умолчанию в четыре раза превышает интервал Hello.

Используйте параметр **transmit-delay** в команде **area virtual-link**, чтобы изменить задержку передачи пакетов LSU по виртуальному каналу. Значение по умолчанию — 1 с.

Используйте параметр **retransmit-interval** в команде **area virtual-link**, чтобы изменить интервал повторной передачи пакетов LSU по виртуальному каналу. Значение по умолчанию — 5 с.

Запустите команду **timers throttle lsa all**, чтобы изменить параметры алгоритма экспоненциальной задержки, генерирующего LSA. Значения этих параметров по умолчанию: 0 мс, 5000 мс и 5000 мс.

Запустите команду **timers pacing lsa-group**, чтобы изменить интервал обновления группы LSA. Значение по умолчанию — 30 с.

Запустите команду **timers pacing lsa-transmit**, чтобы изменить интервал отправки пакетов LS-UPD и количество отправленных пакетов LS-UPD. Значения по умолчанию: 40 мс и 1.

Запустите команду **timers lsa arrival**, чтобы изменить задержку, после которой будет получен тот же LSA. Значение по умолчанию — 1000 мс.

Запустите команду **timers throttle spf**, чтобы изменить задержку вычислений SPT, минимальный интервал между двумя вычислениями SPT и максимальный интервал между двумя вычислениями SPT. Значения по умолчанию: 1000 мс, 5000 мс и 10 000 мс.

Типы сетей OSPF

По умолчанию Ethernet и FDDI относятся к broadcast-типу, X.25, Frame Relay и ATM относятся к типу NBMA, а PPP, HDLC и LAPB относятся к типу P2P.

Запустите команду **ipv6 ospf network**, чтобы вручную указать тип сети интерфейса.

Запустите команду **ipv6 ospf neighbor**, чтобы вручную указать соседа. Для non-broadcast типов NBMA и P2MP необходимо вручную указать соседей.

Запустите команду **ipv6 ospf priority**, чтобы настроить приоритеты интерфейсов, которые используются для выбора DR/BDR. Выбор DR/BDR необходим для типов broadcast и NBMA. В выборах побеждает маршрутизатор с наивысшим приоритетом, а маршрутизатор с приоритетом 0 в выборах не участвует. Значение по умолчанию — 1.

5.3.4. Управление маршрутами OSPF

Правильно планируйте или оптимизируйте маршруты OSPF с помощью ручной настройки для реализации управления маршрутами OSPF.

5.3.4.1. Принцип работы

(Полностью) Тупиковая область и (Полностью) Область NSSA

Области (полностью) тупиковые и (полностью) NSSA помогают снизить нагрузку на взаимодействие протоколов и размер таблицы маршрутизации.

- Если соответствующая область настроена как (полностью) тупиковая область или область NSSA, можно избежать объявления большого количества LSA типа 5 и типа 3 внутри этой области.

Область	LSA типа 1 и типа 2	LSA типа 3	LSA типа 4	LSA типа 5	LSA типа 7
Не (полностью) тупиковая область и область NSSA	Допускается	Допускается	Допускается	Допускается	Не допус-кается
Тупиковая область	Допускается	Разрешено (содержит один маршрут по умолчанию)	Не допускается	Не допускается	Не допус-кается
Полностью тупиковая область	Допускается	Разрешен только один маршрут по умолчанию	Не допускается	Не допускается	Не допус-кается
Область NSSA	Допускается	Разрешено (содержит один маршрут по умолчанию)	Допускается	Не допускается	Допус-кается
Полностью область NSSA	Допускается	Разрешен только один маршрут по умолчанию	Допускается	Не допускается	Допус-кается

ПРИМЕЧАНИЕ: ABR использует LSA типа 3 для объявления маршрута по умолчанию к (полностью) тупиковой области или области NSSA.

ПРИМЕЧАНИЕ: ABR преобразует LSA типа 7 в области NSSA в LSA типа 5 и объявляет LSA типа 5 в магистральной области.

- Если область соответствующим образом настроена как (полностью) тупиковая область или область NSSA, большое количество маршрутов OE1, OE2 и OI не будет добавлено в таблицу маршрутизации маршрутизатора в этой области.

Область	Маршруты, доступные в таблице маршрутизации маршрутизатора внутри области
Не (полностью) тупиковая область и область NSSA	O: маршрут к сети назначения в локальной области. OI: маршрут к сети назначения в другой области. OE1 или OE2: маршрут или маршрут по умолчанию к целевому сегменту сети за пределами AS (через любой ASBR в AS)
Тупиковая область	O: маршрут к сети назначения в локальной области. OI: маршрут или маршрут по умолчанию к сети назначения в другой области
Полностью тупиковая область	O: маршрут к сети назначения в локальной области. OI: маршрут по умолчанию
Область NSSA	O: маршрут к сети назначения в локальной области. OI: маршрут или маршрут по умолчанию к сети назначения в другой области. ON1 или ON2: маршрут или маршрут по умолчанию к целевому сегменту сети за пределами AS (через ASBR в локальной области)
Полностью область NSSA	O: маршрут к сети назначения в локальной области. OI: маршрут по умолчанию ON1 или ON2: маршрут или маршрут по умолчанию к целевому сегменту сети за пределами AS (через ASBR в локальной области)

Перераспределение маршрутов

Перераспределение маршрутов — это процесс введения маршрутов других протоколов маршрутизации, маршрутов других процессов OSPF, статических маршрутов и прямых маршрутов, существующих на устройстве, в процесс OSPF, чтобы эти маршруты можно было объявлять соседям с использованием LSA типов 5 и 7. Маршрут по умолчанию не может быть введен во время перераспределения маршрута.

Перераспределение маршрутов часто используется для взаимодействия между AS. Вы можете настроить перераспределение маршрутов в ASBR для объявления маршрутов за пределами AS внутрь AS или маршрутов внутри AS за пределы AS.

Введение маршрута по умолчанию

Настроив команду в ASBR, вы можете ввести маршрут по умолчанию для процесса OSPF, чтобы этот маршрут можно было объявлять соседям с помощью LSA типа 5 и типа 7.

Введение маршрута по умолчанию часто используется для взаимодействия между AS. Один маршрут по умолчанию используется для замены всех маршрутов за пределами AS.

Суммирование маршрутов

Суммирование маршрутов — это процесс объединения информации о маршрутах с одним и тем же префиксом в один маршрут и объявления суммированного маршрута (замена большого количества отдельных маршрутов) соседям. Суммирование маршрутов помогает снизить нагрузку на взаимодействие протоколов и размер таблицы маршрутизации.

По умолчанию ABR объявляет информацию о маршрутизации между областями с помощью LSA типа 3 в сегменте сети и объявляет информацию о перераспределенной маршрутизации с помощью LSA типа 5 и 7. Если существуют непрерывные сегменты сети, рекомендуется настроить суммирование маршрутов.

Фильтрация маршрутов

OSPF поддерживает фильтрацию маршрутов для обеспечения безопасности и облегчения контроля при изучении, обмене или использовании информации о маршрутизации.

С помощью команд конфигурации вы можете настроить фильтрацию маршрутов для следующих элементов:

- Интерфейс: интерфейсу запрещено отправлять информацию о маршрутизации (любые LSA) или обмениваться информацией о маршрутизации (любые LSA) с соседями.
- Информация о маршрутизации за пределами AS: только та информация о маршрутизации, которая соответствует условиям фильтрации, может быть перераспределена в процесс OSPF (LSA типа 5 и типа 7).
- LSA, полученные маршрутизатором. В таблице маршрутизации OSPF могут объявляться только те маршруты, которые рассчитываются на основе LSA, соответствующих условиям фильтрации.

Стоимость маршрута

Если в сети существуют резервные каналы или устройства, может существовать несколько путей от локального устройства к сети назначения. OSPF выбирает путь с минимальной общей стоимостью для формирования маршрута OSPF. Общая стоимость пути равна сумме стоимостей отдельных каналов на этом пути. Общую стоимость пути можно минимизировать путем изменения стоимости отдельных каналов на этом пути. Таким образом, OSPF выбирает этот путь для формирования маршрута.

Используя команды конфигурации, вы можете изменить следующие затраты на соединение:

- Стоимость перехода от интерфейса к напрямую подключенному сегменту сети и стоимость от интерфейса к соседу
- Стоимость перехода от ABR к сегменту сети по умолчанию
- Стоимость перехода от ASBR к сегменту внешней сети и стоимость от ASBR к сегменту сети по умолчанию

ПРИМЕЧАНИЕ: и стоимость, и метрика указывают стоимость и не отличаются друг от друга.

Административное расстояние OSPF

Административное расстояние (AD) оценивает надежность маршрута. Его значение представляет собой целое число от 0 до 255. Меньшее значение AD указывает на то, что

маршрут заслуживает большего доверия. Если к одному и тому же пункту назначения существует несколько маршрутов, маршрут предпочтительно выбирает маршрут с меньшим значением AD. Маршрут с большим значением AD становится плавающим маршрутом, то есть резервным маршрутом оптимального маршрута.

По умолчанию маршрут, исходящий из одного источника, соответствует значению AD. Значение AD является местным понятием. Изменение значения AD влияет на выбор маршрута только на текущем маршрутизаторе.

Источник маршрута	AD по умолчанию
Сеть с прямым подключением	0
Статический маршрут	1
EBGP-маршрут	20
Маршрут OSPF	110
Маршрут IS-IS	115
RIP-маршрут	120
IBGP-маршрут	200
Недоступный маршрут	255

5.3.4.2. Сопутствующая конфигурация

Тупиковая область/область NSSA

По умолчанию тупиковая область или область NSSA не настроены.

Запустите команду **area stub**, чтобы настроить указанную область как тупиковую.

Запустите команду **area nssa**, чтобы настроить указанную область как область NSSA.

ПРИМЕЧАНИЕ: магистральную область нельзя настроить как тупиковую или область NSSA.

ПРИМЕЧАНИЕ: транзитную область (с проходящими виртуальными каналами) нельзя настроить как тупиковую область или область NSSA.

ПРИМЕЧАНИЕ: область, содержащая ASBR, не может быть настроена как тупиковая область.

Перераспределение маршрутов и введение маршрута по умолчанию

По умолчанию маршруты не перераспределяются и маршрут по умолчанию не вводится.

Запустите команду **redistribute**, чтобы настроить перераспределение маршрутов.

Запустите команду **default-information originate**, чтобы ввести маршрут по умолчанию.

После настройки перераспределения маршрутов и введения маршрута по умолчанию маршрутизатор автоматически становится ASBR.

Суммирование маршрутов

По умолчанию маршруты не суммируются. Если настроено суммирование маршрутов, автоматически будет добавлен отброшенный маршрут.

Запустите команду **area range**, чтобы суммировать маршруты (LSA типа 3), распределенные между областями на ABR.

Запустите команду **summary-prefix**, чтобы суммировать перераспределенные маршруты (LSA типа 5 и типа 7) на ASBR.

Фильтрация маршрутов

По умолчанию маршруты не фильтруются.

Запустите команду **passive-interface**, чтобы настроить пассивный интерфейс. Информацией о маршрутизации (любые LSA) нельзя обмениваться на пассивном интерфейсе.

Используйте параметр **route-map** в команде **redistribute** или используйте команду **distribute-list out** для фильтрации внешней информации о маршрутизации AS на ASBR. Только та информация о маршрутизации, которая соответствует условиям фильтрации, может быть перераспределена в процесс OSPF (LSA типа 5).

Запустите команду **distribute-list in**, чтобы отфильтровать LSA, полученные маршрутизатором. В таблице маршрутизации OSPF могут объявляться только те маршруты, которые рассчитываются на основе LSA, соответствующих условиям фильтрации.

Стоимость маршрута

- Стоимость от интерфейса до сегмента сети с прямым подключением (стоимость на интерфейсе). Значением по умолчанию является автоматическая стоимость. Автоматическая стоимость = эталонная полоса пропускания/пропускная способность интерфейса. Запустите команду **auto-cost reference-bandwidth**, чтобы установить эталонную полосу пропускания для автоматической стоимости. Значение по умолчанию — 100 Мбит/с. Запустите команду **ipv6 ospf cost**, чтобы вручную установить стоимость интерфейса. Приоритет конфигурации этого элемента выше, чем у автоматической стоимости.
- Стоимость от интерфейса до указанного соседа (то есть стоимость от локального устройства до указанного соседа). Значением по умолчанию является автоматическая стоимость. Используйте параметр **cost** в команде **ipv6 ospf neighbor**, чтобы изменить стоимость от интерфейса до указанного сосед. Приоритет конфигурации этого пункта выше, чем стоимость интерфейса. Этот элемент конфигурации применим только к интерфейсам типа P2MP.
- Стоимость от ABR до сегмента сети по умолчанию (то есть стоимость маршрута по умолчанию, который автоматически объявляется ABR до тупиковой области). Значение по умолчанию — 1. Запустите команду **area default-cost**, чтобы изменить стоимость маршрута по умолчанию, который ABR автоматически объявляет тупиковым областям или NSSA.
- Стоимость от ASBR до сегмента внешней сети (то есть метрика внешнего маршрута). По умолчанию метрика перераспределяемого маршрута BGP равна 1, метрика других типов перераспределяемых маршрутов равна 20, а тип маршрута — Внешний Тип. 2. Запустите команду **default-metric**, чтобы изменить метрику по умолчанию внешнего маршрута. Используйте параметры **metric**, **metric-type** и **route-map** в команде **redistribute**, чтобы изменить метрику и тип маршрута внешнего маршрута.

- Стоимость от ASBR до сегмента сети по умолчанию (то есть метрика маршрута по умолчанию, введенная вручную). По умолчанию метрика равна 1, а тип маршрута — Внешний Тип 2. Используйте параметры **metric**, **metric-type** и **route-map** в команде **default-information originate**, чтобы изменить метрику и тип маршрута маршрута по умолчанию, введенного вручную.
- Используйте параметры **metric** и **metric-type** в **default-information originate** в , команде **area nssa**, чтобы изменить метрику и тип маршрута по умолчанию, который вручную вводится в область NSSA.

Административное расстояние OSPF

По умолчанию OSPF AD равен 110.

Запустите команду **distance**, чтобы установить AD маршрута OSPF.

5.3.5. Повышенная безопасность и надежность

Используйте такие функции, как аутентификация и корреляция BFD, для повышения безопасности, стабильности и надежности OSPF.

5.3.5.1. Принцип работы

Аутентификация

OSPFv3 использует механизм аутентификации, то есть заголовок аутентификации IP (AH) и полезную нагрузку безопасности IP-инкапсуляции (ESP), предоставляемую IPv6, для предотвращения несанкционированного доступа маршрутизаторов к сети и хостов, которые подделывают пакеты OSPF для участия в маршрутизации OSPF. Пакеты OSPF, полученные на интерфейсе OSPF (или на обоих концах виртуального канала), аутентифицируются. Если аутентификация не удалась, пакеты отбрасываются и смежность не может быть установлена.

Включение аутентификации позволяет избежать изучения неаутентифицированных или недействительных маршрутов, тем самым предотвращая объявление действительных маршрутов неаутентифицированным устройствам. В сети broadcast-типа аутентификация также предотвращает превращение неаутентифицированных устройств в назначенные устройства, обеспечивая стабильность системы маршрутизации и защиту системы маршрутизации от вторжений.

Проверка MTU

При получении пакета DD OSPF проверяет, совпадает ли MTU соседнего интерфейса с MTU локального интерфейса. Если MTU интерфейса, указанного в полученном пакете DD, больше, чем MTU интерфейса, который получает пакет, то смежность настроить невозможно. Отключение проверки MTU позволяет избежать этой проблемы.

Двустороннее обслуживание

Маршрутизаторы OSPF периодически отправляют друг другу пакеты Hello для поддержания смежности. В большой сети может быть отправлено или получено множество пакетов, занимающих слишком много процессора и памяти. В результате некоторые пакеты задерживаются или отбрасываются. Если время обработки пакетов Hello превышает dead-интервал, смежность будет нарушена.

Если включена функция двустороннего обслуживания, в дополнение к пакетам Hello для поддержания двусторонней связи между соседями могут также использоваться пакеты DD, LSU, LSR и LSAck, что делает смежность более стабильной.

Ограничение одновременного взаимодействия с соседями

Когда маршрутизатор одновременно обменивается данными с несколькими соседями, это может повлиять на его производительность. При максимальном количестве соседей, которые одновременно инициируют или принимают взаимодействие с процессом OSPF, маршрутизатор может взаимодействовать с соседями пакетно, что обеспечивает пересылку данных и другие ключевые сервисы.

GR

Технология разделения управления и пересылки широко используется среди маршрутизаторов. В относительно стабильной топологии сети, когда маршрутизатор с поддержкой GR перезапускается на control plane, пересылка данных может продолжаться на forwarding plane. Кроме того, действия (такие как изменение смежности и вычисление маршрута), выполняемые на control plane, не влияют на функции forwarding plane. Таким образом, можно избежать прерывания обслуживания, вызванного изменением маршрута, что повышает надежность всей сети.

В настоящее время функция GR используется только во время переключения активный/резервный режим и обновления системы.

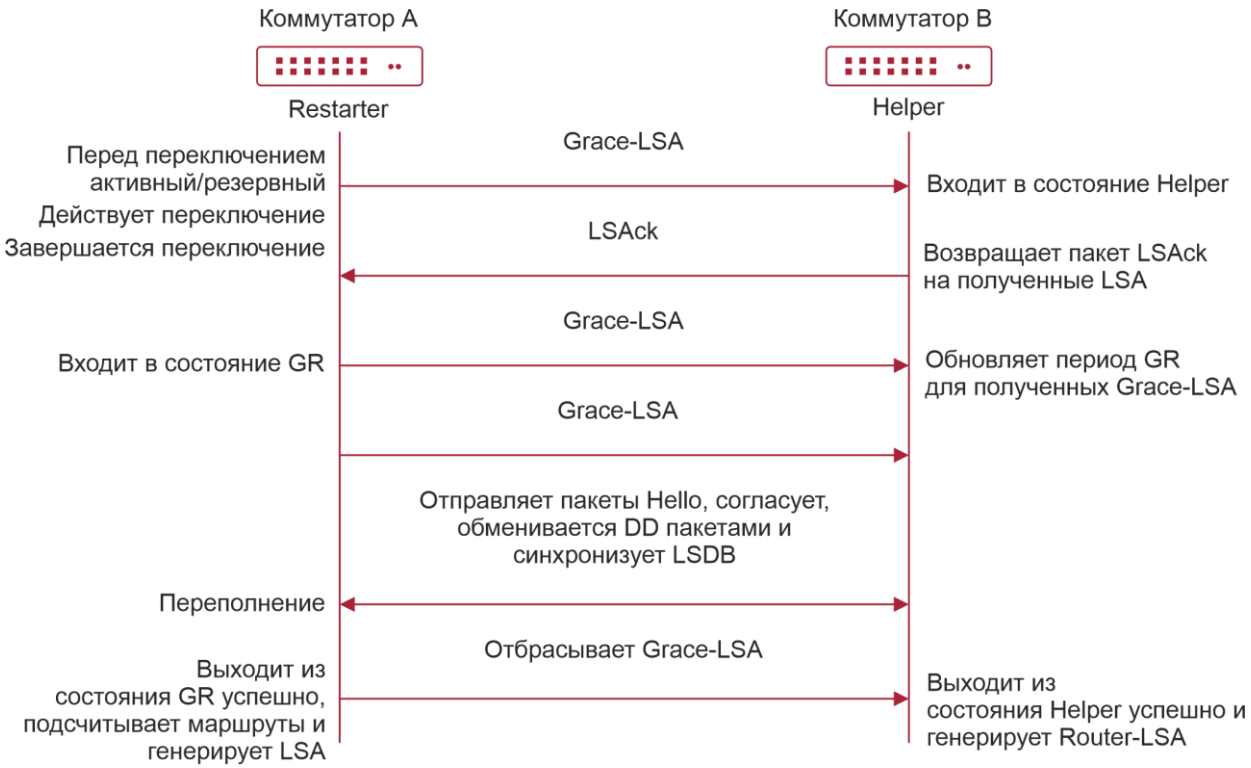


Рисунок 5-7. Обычный процесс GR OSPF

- Процесс GR требует сотрудничества между restarter-ом и helper-ом. Restarter — это маршрутизатор, на котором происходит GR. Helper является соседом restarter-а.
- При входе в процесс GR или выходе из него restarter отправляет Grace-LSA соседу, уведомляя соседа о необходимости войти в состояние helper-а или выйти из него.

- Когда смежность между restarter-ом и helper-ом достигает состояния Full, маршрутизатор может успешно выйти из процесса GR.

Корреляция Fast Hello и BFD

После возникновения сбоя канала проходит некоторое время (около 40 с), прежде чем OSPF сможет обнаружить отключение соседа. Затем OSPF объявляет информацию и повторно вычисляет SPT. В этот период трафик прерывается.

- После включения функции Fast Hello (то есть интервал dead соседа установлен на 1 с) OSPF может обнаружить отключение соседа в течение 1 с, если канал неисправен. Это значительно ускоряет сходимость маршрутов и предотвращает прерывание трафика.
- BFD используется для проверки связи между устройствами. Неисправность канала может быть обнаружена всего за 150 мс. После того как OSPF коррелирует с BFD, OSPF может обнаружить отключение соседа всего за 150 мс, если канал неисправен. Это значительно ускоряет сходимость маршрутов и предотвращает прерывание трафика.

5.3.5.2. Сопутствующая конфигурация

Аутентификация пакетов OSPF

По умолчанию аутентификация отключена.

- Запустите команду **area authentication**, чтобы включить аутентификацию во всей области, чтобы функция аутентификации вступила в силу на всех интерфейсах в этой области. Если аутентификация включена в области 0, функция также действует на виртуальный канал.
- Запустите команду **area authentication**, чтобы включить шифрование и аутентификацию во всей области, чтобы функции шифрования и аутентификации вступили в силу на всех интерфейсах в этой области. Если шифрование и аутентификация включены в области 0, эти функции также действуют на виртуальном канале.
- Запустите команду **ipv6 ospf authentication**, чтобы включить аутентификацию на интерфейсе. Эта конфигурация имеет приоритет над конфигурацией на основе области.
- Запустите команду **ipv6 ospf encryption**, чтобы включить шифрование и аутентификацию на интерфейсе. Эта конфигурация имеет приоритет над конфигурацией на основе области.
- Используйте параметр **authentication** в команде **area virtual-link**, чтобы включить аутентификацию на обоих концах виртуального канала. Эта конфигурация имеет приоритет над конфигурацией на основе области.
- Используйте параметр **encryption** в команде **area virtual-link**, чтобы включить шифрование и аутентификацию на обоих концах виртуального канала. Эта конфигурация имеет приоритет над конфигурацией на основе области.

Проверка MTU

По умолчанию проверка MTU отключена.

Запустите команду **ipv6 ospf mtu-ignore**, чтобы отключить проверку MTU на интерфейсе.

Двустороннее обслуживание

По умолчанию двустороннее обслуживание включено.

Запустите команду **two-way-maintain**, чтобы включить двустороннее обслуживание.

Ограничение одновременного взаимодействия с соседями

Запустите команду **max-concurrent-dd**, чтобы изменить максимальное количество соседей, одновременно взаимодействующих с текущим процессом OSPF. Значение по умолчанию — 5.

Запустите команду **ipv6 router ospf max-concurrent-dd**, чтобы изменить максимальное количество соседей, которые одновременно взаимодействуют со всеми процессами OSPF на маршрутизаторе. Значение по умолчанию — 10.

GR

По умолчанию функция restarter-a отключена, а функция helper-a включена.

Запустите команду **GR**, чтобы настроить функцию restarter-a.

Запустите команду **graceful-restart helper**, чтобы настроить функцию helper-a.

Fast Hello

По умолчанию интервал dead соседа на интерфейсе составляет 40 с.

Запустите команду **ipv6 ospf dead-interval minimal hello-multiplier**, чтобы включить функцию Fast Hello на интерфейсе, то есть dead-интервал соседа равен 1 с.

Корреляция OSPF с BFD

По умолчанию OSPF не коррелирует с BFD.

Запустите команду **bfd interval min_rx multiplier**, чтобы установить параметры BFD.

Запустите команду **bfd all-interfaces**, чтобы сопоставить OSPF с BFD на всех интерфейсах.

Запустите команду **ipv6 ospf bfd**, чтобы сопоставить OSPF с BFD на текущем интерфейсе.

5.3.6. Функции управления сетью

Используйте такие функции, как MIB и Syslog, для облегчения управления OSPF.

5.3.6.1. Принцип работы

MIB

MIB — это набор информации о состоянии устройства, поддерживаемый устройством. Вы можете использовать программу управления для просмотра и настройки узла MIB.

На маршрутизаторе можно одновременно запустить несколько процессов OSPF, но MIB OSPF можно связать только с одним процессом OSPF.

Trap

Сообщение Trap — это уведомление, генерируемое, когда система обнаруживает неисправность. Это сообщение содержит соответствующую информацию о неисправности.

Если функция Trap включена, маршрутизатор может заранее отправлять сообщения Trap на устройство управления сетью.

Syslog (системный журнал)

Syslog записывает операции (например, настройку команд), выполняемые пользователями на маршрутизаторах, а также определенные события (например, сбои сетевого подключения).

Если системному журналу разрешено записывать изменения смежности, сетевой администратор может просматривать журналы, чтобы узнать весь процесс настройки и поддержки смежности OSPF.

5.3.6.2. Сопутствующая конфигурация

MIB

По умолчанию MIB привязан к процессу OSPF с наименьшим идентификатором процесса.

Запустите команду **enable mib-binding**, чтобы связать MIB с текущим процессом OSPF.

Trap

По умолчанию все функции Trap отключены, и устройству не разрешено отправлять Trap OSPF.

Запустите команду **snmp-server enable traps ospf**, чтобы разрешить устройству отправлять Trap OSPF.

Запустите команду **enable traps**, чтобы включить указанную функцию Trap для процесса OSPF.

Syslog (системный журнал)

По умолчанию системному журналу разрешено записывать изменения смежности.

Запустите команду **log-adj-changes**, чтобы системный журнал мог записывать изменения смежности.

5.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций OSPF	(Обязательный) Используется для создания домена маршрутизации OSPF	
	ipv6 router ospf	Создает процесс OSPF
	router-id	Настраивает идентификатор маршрутизатора
	ipv6 ospf area	Включает OSPF на интерфейсе и указывает идентификатор области
	area virtual-link	Создает виртуальный канал
Установка типа сети	(Опционально) Конфигурации являются обязательными, если физическая сеть представляет собой сеть X.25, Frame Relay или ATM	
	ipv6 ospf network	Определяет тип сети
	ipv6 ospf neighbor	Указывает соседа
	ipv6 ospf priority	Настраивает приоритет DR

Конфигурация	Описание и команда	
Настройка перераспределения маршрутов и маршрута по умолчанию	(Опционально) Эти конфигурации рекомендуются, если домен маршрутизации OSPF подключен к внешней сети	
	redistribute	Настраивает перераспределение маршрутов
	default-information originate	Представляет маршрут по умолчанию
Настройка тупиковой области и области NSSA	(Опционально) Используется для уменьшения взаимодействия информации о маршрутизации и размера таблицы маршрутизации, а также для повышения стабильности маршрутов	
	area stub	Настраивает тупиковую область
	area nssa	Настраивает область NSSA
Настройка суммирования маршрутов	(Опционально) Используется для уменьшения взаимодействия информации о маршрутизации и размера таблицы маршрутизации, а также для повышения стабильности маршрутов	
	area range	Суммирует маршруты, объявляемые между областями
	summary-prefix	Суммирует маршруты, которые вводятся посредством перераспределения
Настройка фильтрации маршрутов	(Опционально) Используется для ручного управления взаимодействием информации о маршрутизации и фильтрации доступных маршрутов OSPF	
	passive-interface	Настраивает пассивный интерфейс
	distribute-list out	Фильтрует маршруты, введенные в результате перераспределения

Конфигурация	Описание и команда	
	distribute-list in	Фильтры получили LSA
Изменение стоимости маршрута и AD	(Опционально) Используется для ручного управления кратчайшим маршрутом, вычисленным OSPF, и определения предпочтительности выбора маршрута OSPF	
	auto-costreference-bandwidth	Изменяет эталонную полосу пропускания автоматической стоимости
	ipv6 ospf cost	Изменяет стоимость в исходящем направлении интерфейса
Изменение стоимости маршрута и AD	**area default-cost**	Изменяет стоимость маршрута по умолчанию в тупиковой области/области NSSA
	default-metric	Изменяет метрику по умолчанию перераспределенного маршрута
	distance	Изменяет OSPF AD
Включение аутентификации	(Опционально) Используется для предотвращения участия в процессе протокола OSPF маршрутизаторов, осуществляющих незаконный доступ к сети, и узлов, подделывающих пакеты OSPF	
	area authentication	Включает аутентификацию и устанавливает режим аутентификации в области
	area encryption	Включает шифрование и аутентификацию и устанавливает режим аутентификации в области
	ipv6 ospf authentication	Включает аутентификацию и устанавливает режим аутентификации на интерфейсе

Конфигурация	Описание и команда	
	ipv6 ospf encryption	Включает шифрование и аутентификацию и устанавливает режим аутентификации на интерфейсе
Изменение максимального количества одновременных соседей	(Опционально) Используется для предотвращения проблемы ухудшения производительности, вызванной чрезмерным потреблением ресурсов ЦП	
	max-concurrent-dd	Изменяет максимальное количество одновременных соседей в текущем процессе OSPF
	ipv6 router ospf max-concurrent-dd	Изменяет максимальное количество одновременных соседей во всех процессах OSPF
Отключение проверки MTU	(Опционально) Используется для предотвращения проблемы, связанной с невозможностью настройки смежности из-за несоответствия MTU на соседнем интерфейсе	
	ipv6 ospf mtu-ignore	Отключает проверку MTU на интерфейсе
Включение двустороннего обслуживания	(Опционально) Используется для предотвращения прекращения смежности из-за задержки или потери пакетов Hello	
	two-way-maintain	Обеспечивает двустороннее обслуживание
Включение GR	(Опционально) Используется для сохранения пересылки маршрутизации OSPF во время перезапуска или переключения между активным и резервным процессами OSPF, чтобы предотвратить прерывание трафика	
	graceful-restart	Включает функцию restarter-a
	graceful-restart helper	Включает функцию helper-a

Конфигурация	Описание и команда	
Включение Fast Hello	(Опционально) Используется для быстрого обнаружения отключения соседа и предотвращения прерывания трафика в случае неисправности канала	
	ipv6 ospf dead-interval minimal hello-multiplier	Включение функции Fast Hello на интерфейсе
Корреляция OSPF с BFD	(Опционально) Используется для быстрого обнаружения отключения соседа и предотвращения прерывания трафика в случае неисправности канала	
	bfd all-interfaces	Сопоставляет OSPF с BFD на всех интерфейсах
	ipv6 ospf bfd	Сопоставляет OSPF с BFD на текущем интерфейсе
Настройка функций управления сетью	(Опционально) Конфигурации позволяют пользователям использовать программное обеспечение управления сетью SNMP для управления OSPF	
	enable mib-binding	Привяжите MIB к процессу OSPF
	enable traps	Включает функцию Trap процесса OSPF
	log-adj-changes	Позволяет системным журналам записывать изменения в статус смежности
Изменение параметров управления протоколом	(Опционально) Рекомендуется не изменять параметры управления протоколом без необходимости	
	ipv6 ospf hello-interval	Изменяет интервал Hello на интерфейсе
	ipv6 ospf dead-interval	Изменяет интервал отключения соседей на интерфейсе
	ipv6 ospf transmit-delay	Изменяет задержку передачи пакетов LSU на интерфейсе

Конфигурация	Описание и команда	
	ipv6 ospf retransmit-interval	Изменяет интервал повторной передачи пакетов LSU на интерфейсе
	timers throttle lsa all	Изменяет параметры алгоритма экспоненциальной отсрочки, генерирующего LSA
	Timers pacing lsa-group	Изменяет интервал обновления группы LSA
	timers pacing lsa-transmit	Изменяет интервал отправки пакетов LS-UPD
Изменение параметров управления протоколом	**timers lsa arrival**	Изменяет задержку, после которой принимается тот же LSA
	timers throttle spf	Изменяет таймер вычислений SPT
	timers throttle route inter-area	Изменяет задержку расчета маршрута между областями
	timers throttle route ase	Изменяет задержку расчета маршрута между областями

5.4.1. Настройка основных функций OSPF

5.4.1.1. Эффект конфигурации

Настройте домен маршрутизации OSPF в сети, чтобы предоставить пользователям в сети сервис unicast-маршрутизации IPv6.

5.4.1.2. Примечания

- Убедитесь, что функция маршрутизации IPv6 включена, то есть **ipv6 routing** не отключена; в противном случае OSPF невозможно будет включить.
- IPv6 должен быть включен на интерфейсе.
- Настоятельно рекомендуется вручную настроить идентификатор маршрутизатора.

5.4.1.3. Шаги настройки

Создание процесса OSPF

- Обязательный.
- Конфигурация обязательна для каждого маршрутизатора.

Настройка идентификатора маршрутизатора

- (Опционально) Настоятельно рекомендуется вручную настроить идентификатор маршрутизатора.
- Если идентификатор маршрутизатора не настроен, OSPF выбирает IP-адрес интерфейса. Если IP-адрес не настроен ни для одного интерфейса или настроенные IP-адреса использовались другими экземплярами OSPF, необходимо вручную настроить идентификатор маршрутизатора.

Включение OSPF на интерфейсе и указание идентификатора области

- Обязательный.
- Конфигурация обязательна для каждого маршрутизатора.

5.4.1.4. Проверка

- Запустите команду **show ipv6 route ospf**, чтобы убедиться, что записи таблицы маршрутизации OSPF загружены правильно.
- Запустите команду **ping**, чтобы убедиться, что сервис unicast-рассылки IPv6 настроен правильно.

5.4.1.5. Связанные команды

Создание процесса OSPF

Команда	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]
Описание параметра	*process-id*: указывает идентификатор процесса OSPFv3. Если идентификатор процесса не указан, включается процесс 1. *vrf-name*: указывает маршрутизацию VPN и пересылку (VRF), к которой принадлежит процесс OSPFv3
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После включения процесса OSPFv3 устройство входит в режим настройки процесса маршрутизации

Настройка идентификатора маршрутизатора

Команда	**router-id** *router-id*
Описание параметра	*router-id*: указывает идентификатор устройства, который выражается в IPv4-адресе
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Каждое устройство, на котором работает OSPFv3, должно быть идентифицировано с помощью идентификатора маршрутизатора. Вы можете настроить любой IPv4-адрес в качестве идентификатора

	маршрутизатора устройства и обеспечить уникальность идентификатора маршрутизатора в AS. Если на одном устройстве выполняются несколько процессов OSPFv3, идентификатор маршрутизатора каждого процесса также должен быть уникальным. После изменения идентификатора маршрутизатора OSPF выполняет большую часть внутренней обработки. Поэтому рекомендуется не менять идентификатор маршрутизатора без необходимости. При попытке изменить идентификатор маршрутизатора отображается запрос на подтверждение изменения. После включения процесса OSPFv3 рекомендуется указать идентификатор маршрутизатора перед настройкой других параметров процесса

Включение OSPF на интерфейсе и указание идентификатора области

Команда	**ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*]
Описание параметра	*process-id*: указывает идентификатор процесса OSPFv3. Значение варьируется от 1 до 65 535. **area** *area-id*: указывает идентификатор области OSPFv3, в которой участвует интерфейс. Это может быть целое число или префикс IPv4. **instance** *instance-id*: указывает идентификатор указанного процесса OSPFv3 интерфейса. Значение варьируется от 0 до 255
Командный режим	Режим настройки интерфейса
Руководство по использованию	Запустите эту команду в режиме настройки интерфейса, чтобы разрешить интерфейсу участвовать в OSPFv3, а затем запустите команду **ipv6 router ospf**, чтобы настроить процесс OSPFv3. После настройки процесса OSPFv3 интерфейс автоматически будет участвовать в соответствующем процессе. Запустите команду **no ipv6 ospf area**, чтобы указанный интерфейс больше не участвовал в процессе маршрутизации OSPFv3. Запустите команду **no ipv6 router ospf**, чтобы все интерфейсы больше не участвовали в процессе маршрутизации OSPFv3. Смежность можно настроить только между устройствами с одинаковым *instance-id*. После настройки этой команды вся информация о префиксах интерфейса будет участвовать в процессе OSPFv3

Создание виртуального канала

Команда	**area** *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**dead-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**instance** *instance-id*] [**authentication ipsec spi** *spi*[**md5**|**sha1**] [**0**|**7**] *key*] [**encryption ipsec spi** *spi* **esp null** [**md5**|**sha1**] [**0**|**7**] **key**]
Описание параметра	*area-id*: указывает идентификатор области, где находится виртуальный канал. Это может быть целое число или префикс IPv4. *router-id*: указывает идентификатор маршрутизатора соседа, подключенного к виртуальному каналу. **dead-interval** *seconds*: указывает время, в течение которого локальный интерфейс виртуального канала обнаруживает сбой соседа. Измеряется в секундах. Значение варьируется от 1 до 65 535. **hello-interval** *seconds*: указывает время отправки пакета Hello на локальный интерфейс виртуального канала. Измеряется в секундах. Значение варьируется от 1 до 65 535. **retransmit-interval** *seconds*: указывает интервал, с которым LSA повторно передается на локальный интерфейс виртуального канала. Измеряется в секундах. Значение варьируется от 1 до 65 535. **transmit-delay** *seconds*: указывает задержку, после которой LSA отправляется на локальный интерфейс виртуального канала. Измеряется в секундах. Значение варьируется от 1 до 65 535. **instance** *instance-id*: указывает идентификатор экземпляра, соответствующего виртуальному каналу. Значение находится в диапазоне от 0 до 255. Виртуальное соединение невозможно установить между устройствами с разными идентификаторами экземпляров. *spi*: указывает индекс параметра безопасности (SPI). Значение варьируется от 256 до 4 294 967 295. **md5**: включает аутентификацию Message Digit 5 (MD5). **sha1**: включает аутентификацию по алгоритму безопасного хеширования 1 (SHA1). **0**: указывает, что ключ отображается в виде обычного текста. **7**: указывает, что ключ отображается в зашифрованном виде. *key*: указывает ключ аутентификации. **null**: указывает, что режим шифрования не используется
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	В AS OSPFv3 все области должны быть подключены к магистральной области, чтобы правильно изучить информацию о маршрутизации всей AS OSPFv3. Если область не может быть напрямую подключена к

	магистральной области, для подключения этой области к магистральной области можно использовать виртуальный канал. Область, в которой находится виртуальный канал, не может быть тупиковой областью или областью NSSA. На обоих концах соседей, между которыми настроен виртуальный канал, настройки hello-interval, dead-interval и instance должны быть согласованными; в противном случае смежность не может быть настроена должным образом

5.4.1.6. Пример конфигурации

Сценарий:

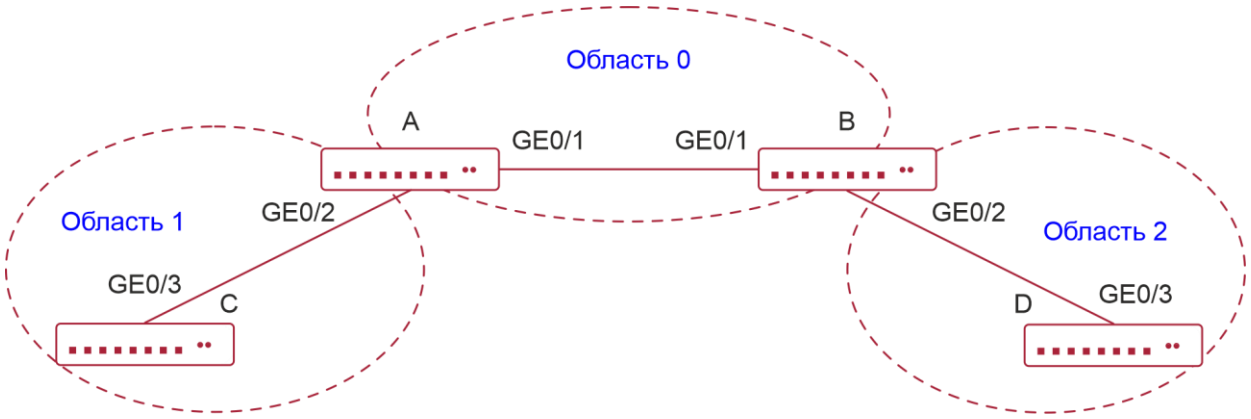


Рисунок 5-8.

IP-адреса интерфейса следующие:

A: GE 0/1 2001:1::1/64 GE 0/2 2001:2::1/64

B: GE 0/1 2001:1::2/64 GE 0/2 2001:3::1/64

C: GE 0/3 2001:2::2/64

D: GE 0/3 2001:3::2/64

Шаги настройки	• Настройте IP-адреса интерфейсов на всех маршрутизаторах. • Включите функцию unicast-маршрутизации IPv4 на всех маршрутизаторах. (Эта функция включена по умолчанию.) • Настройте экземпляры OSPF и идентификаторы маршрутизаторов на всех маршрутизаторах. • Включите OSPF на интерфейсах, настроенных на всех маршрутизаторах
A	A#configure terminal A(config)#interface GigabitEthernet 0/1

	A(config-if-GigabitEthernet 0/1)#ipv6 enable A(config-if-GigabitEthernet 0/1)#ipv6 address 2001:1::1/64 A(config-if-GigabitEthernet 0/1)#ipv6 ospf 1 area 0 A(config-if-GigabitEthernet 0/1)#exit A(config)#interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#ipv6 enable A(config-if-GigabitEthernet 0/2)#ipv6 address 2001:2::1/64 A(config-if-GigabitEthernet 0/2)#ipv6 ospf 1 area 1 A(config-if-GigabitEthernet 0/2)#exit A(config)#ipv6 router ospf 1 A(config-router)#router-id1.1.1.1
B	B#configure terminal B(config)#interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ipv6 enable B(config-if-GigabitEthernet 0/1)#ipv6 address 2001:1::2/64 B(config-if-GigabitEthernet 0/1)#ipv6 ospf 1 area 0 B(config-if-GigabitEthernet 0/1)#exit B(config)#interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)#ipv6 enable B(config-if-GigabitEthernet 0/2)#ipv6 address 2001:3::1/64 B(config-if-GigabitEthernet 0/2)#ipv6 ospf 1 area 2 B(config-if-GigabitEthernet 0/2)#exit B(config)#ipv6 router ospf 1 B(config-router)#router-id2.2.2.2
C	C#configure terminal C(config)#interface GigabitEthernet 0/3 C(config-if-GigabitEthernet 0/3)#ipv6 enable C(config-if-GigabitEthernet 0/3)#ipv6 address 2001:2::2/64 C(config-if-GigabitEthernet 0/3)#ipv6 ospf 1 area 1 C(config-if-GigabitEthernet 0/3)#exit C(config)#ipv6 router ospf 1 C(config-router)#router-id3.3.3.3
D	D#configure terminal

	D(config)#interface GigabitEthernet 0/3 D(config-if-GigabitEthernet 0/3)#ipv6 enable D(config-if-GigabitEthernet 0/3)#ipv6 address 2001:4::2/64 D(config-if-GigabitEthernet 0/3)#ipv6 ospf 1 area 2 D(config-if-GigabitEthernet 0/3)#exit D(config)#ipv6 router ospf 1 D(config-router)#router-id4.4.4.4
Проверка	• Убедитесь, что соседи OSPF указаны правильно на всех маршрутизаторах. • Убедитесь, что таблица маршрутизации правильно загружена на всех маршрутизаторах. • Убедитесь, что 2001:2::2/64 может быть успешно проверен на маршрутизаторе D
A	A#show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.2 1 Full/BDR 00:00:30 0 GigabitEthernet 0/1 3.3.3.31 Full/BDR 00:00:35 0 GigabitEthernet 0/2 A#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O IA2001:3::/64 [110/20] via FE80::2D0:F8FF:FE22:4524, GigabitEthernet 0/1
B	B# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 1.1.1.11 Full/DR 00:00:30 0 GigabitEthernet 0/1

	4.4.4.41 Full/BDR 00:00:35 0 GigabitEthernet 0/2 B#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter areawww.qtech.ru O IA2001:2::/64 [110/20] via FE80::2D0:F8FF:FE22:4536, GigabitEthernet 0/1
C	C# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 1.1.1.11 Full/DR 00:00:30 0 GigabitEthernet 0/3 C#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O IA2001:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4537, GigabitEthernet 0/3 O IA2001:3::/64 [110/3] via FE80::2D0:F8FF:FE22:4537, GigabitEthernet 0/3
D	D# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.2 1 Full/DR 00:00:30 0 GigabitEthernet 0/3 D#show ipv6 route ospf

	IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2www.qtech.ru IA - Inter area O IA2001:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/3 O IA2001:2::/64 [110/3] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/3 D# D#ping 2001:2::2 Sending 5, 100-byte ICMP Echoes to 2001:2::2, timeout is 2 seconds: < press Ctrl+C to break > !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 5/9/14 ms

5.4.1.7. Распространенные ошибки

- IPv6 отключен на интерфейсе.
- OSPF невозможно включить, поскольку функция unicast-маршрутизации IPv6 отключена.
- Идентификаторы областей, включенные на соседних интерфейсах, несовместимы.
- Один и тот же идентификатор маршрутизатора настроен на нескольких маршрутизаторах, что приводит к конфликту идентификаторов маршрутизатора.

5.4.2. Установка типа сети

5.4.2.1. Эффект конфигурации

Если физическая сеть является X.25, Frame Relay или ATM, OSPF также может работать для предоставления сервиса unicast-маршрутизации IPv6.

5.4.2.2. Примечания

- Необходимо настроить основные функции OSPF.
- Broadcast-сеть отправляет multicast-пакеты OSPF, автоматически обнаруживает соседей и выбирает DR и BDR.
- Сеть P2P отправляет multicast-пакеты OSPF и автоматически обнаруживает соседей.
- Сеть NBMA отправляет unicast-пакеты OSPF. Соседей необходимо указать вручную и выбрать DR и BDR.

- Сеть P2MP (без параметра **non-broadcast**) отправляет multicast-пакеты OSPF. Соседи обнаруживаются автоматически.
- Сеть P2MP (с параметром **non-broadcast**) отправляет unicast-пакеты OSPF. Соседей необходимо указывать вручную.

5.4.2.3. Шаги настройки

Настройка типа сети интерфейса

- Опционально.
- Выполните эту настройку на маршрутизаторах на обоих концах канала.

Настройка соседа

- (Необязат Опционально ельно) Если тип сети интерфейса установлен на NBMA или P2MP (с параметром **non-broadcast**), необходимо настроить соседей.
- Соседи настраиваются на маршрутизаторах на обоих концах сети NBMA или P2MP (с параметром **non-broadcast**).

Настройка приоритета интерфейса

- (Опционально) Необходимо настроить приоритет интерфейса, если маршрутизатор должен быть указан как DR или если маршрутизатор не может быть указан как DR.
- Настройте приоритет интерфейса на маршрутизаторе, который должен быть указан как DR или не может быть указан как DR.

5.4.2.4. Проверка

Запустите команду **show ipv6 ospf interface**, чтобы убедиться, что тип сети каждого интерфейса указан правильно.

5.4.2.5. Связанные команды

Настройка типа сети интерфейса

Команда	**ipv6 ospf network** {**broadcast** | **non-broadcast** |**point-to-point** | **point-to-multipoint** [**non-broadcast**]}[**instance** *instance-id*]
Описание параметра	**broadcast**: указывает тип сети broadcast. **non-broadcast**: указывает тип сети non-broadcast. **point-to-multipoint**: указывает тип сети «точка-многоточка» (P2MP). **point-to-multipoint non-broadcast**: указывает тип сети non-broadcast P2MP. **point-to-point**: указывает тип сети «точка-точка» (P2P). **instance** *instance-id*: указывает идентификатор указанного процесса OSPFv3 интерфейса. Значение варьируется от 0 до 255
Командный режим	Режим настройки интерфейса

Руководство по использованию	Вы можете настроить тип сети интерфейса на основе фактического типа канала и топологии

Настройка соседа

Команда	**ipv6 ospf neighbor** *ipv6-address*{ [**cost** *cost*] | [**poll-interval** *seconds* | **priority** *value*] }[**instance** *instance-id*]
Описание параметра	*ip-address*: указывает адрес соединения интерфейса соседа. **cost** *cost*: указывает стоимость, требуемую от сети P2MP для каждого соседа. Стоимость не определена по умолчанию. Используется стоимость, настроенная на интерфейсе. Значение варьируется от 1 до 65 535. Эту опцию поддерживает только сеть P2MP. **poll-interval** *seconds*: указывает интервал опроса соседей. Измеряется в секундах. Значение варьируется от 1 до 2 147 483 647. Эту опцию поддерживает только non-broadcast-сеть (NBMA). **priority** *value*: указывает значение приоритета соседа non-broadcast-сети. Значение находится в диапазоне от 0 до 255. Эту опцию поддерживает только non-broadcast-сеть (NBMA). **instance** *instance-id*: указывает идентификатор указанного процесса OSPFv3 интерфейса. Значение варьируется от 0 до 255
Командный режим	Режим настройки интерфейса
Руководство по использованию	Вы можете настроить параметры соседа в зависимости от фактического типа сети

Настройка приоритета интерфейса

Команда	**ipv6 ospf priority** *number-value*[**instance** *instance-id*]
Описание параметра	*number-value*: указывает приоритет интерфейса. Значение варьируется от 0 до 255. **instance** *instance-id*: указывает идентификатор указанного процесса OSPFv3 интерфейса. Значение варьируется от 0 до 255
Командный режим	Режим настройки интерфейса
Руководство по использованию	В broadcast-сети необходимо выбрать DR или BDR. Во время выбора DR/BDR устройство с более высоким приоритетом будет преимущественно выбрано как DR или BDR. Если приоритет одинаков, устройство с большим идентификатором маршрутизатора будет предпочтительно выбрано в качестве DR или BDR.

	Устройство с приоритетом 0 не участвует в выборе DR/BDR

5.4.2.6. Пример конфигурации

Настройка типа сети интерфейса

Сценарий:

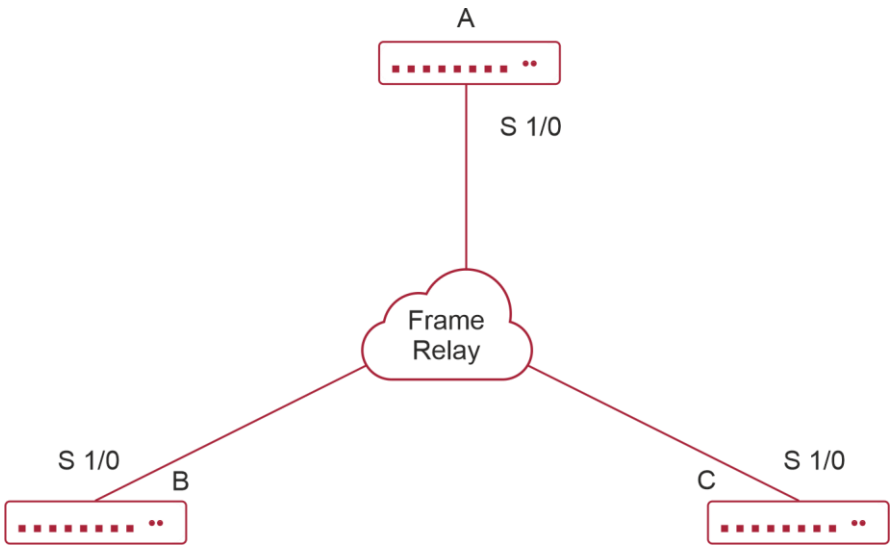


Рисунок 5-9.

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. • Настройте базовые функции OSPF на всех маршрутизаторах. • Установите тип сети интерфейса P2MP на всех маршрутизаторах
A	A#configure terminal A(config)# interface Serial1/0 A(config-Serial1/0)# encapsulation frame-relay A(config-Serial1/0)# ipv6 ospf network point-to-multipoint
B	B#configure terminal B(config)# interface Serial1/0 B(config-Serial1/0)# encapsulation frame-relay B(config-Serial1/0)# ipv6 ospf network point-to-multipoint
C	C#configure terminal C(config)# interface Serial1/0 C(config-Serial1/0)# encapsulation frame-relay

	C(config-Serial1/0)# ipv6 ospf network point-to-multipoint
Проверка	Убедитесь, что тип сети интерфейса — P2MP
A	A#show ipv6 ospf interface Serial1/0 Serial1/0 is up, line protocol is up Interface ID 2 IPv6 Prefixes fe80::2d0:f8ff:fe22:3346/64 (Link-Local Address) OSPFv3 Process (1), Area 0.0.0.1, Instance ID 0 Router ID 192.168.22.30,Network Type POINTOMULTIPOINT, Cost: 1 Transmit Delay is 1 sec, State Point-To-Point, Priority 1 Timer interval configured, Hello 30, Dead 120, Wait 40, Retransmit 10 Hello due in 00:00:06 Neighbor Count is 1, Adjacent neighbor count is 1 Hello received 40 sent 40, DD received 17 sent 9 LS-Req received 1 sent 3, LS-Upd received 6 sent 5 LS-Ack received 3 sent 4, Discarded 1

5.4.2.7. Распространенные ошибки

- Типы сетей, настроенные на интерфейсах на двух концах, несовместимы, что приводит к ненормальному изучению маршрута.
- Тип сети установлен NBMA или P2MP (non-broadcast), но соседи не указаны.

5.4.3. Настройка перераспределения маршрутов и маршрута по умолчанию

5.4.3.1. Эффект конфигурации

- Внедрите unicast-маршруты для других доменов AS в домен OSPF, чтобы предоставить сервис unicast-маршрутизации в другие домены AS для пользователей в домене OSPF.
- В домене OSPF внедрите маршрут по умолчанию в другой домен AS, чтобы сервис unicast-маршрутизации в другой домен AS мог быть предоставлен пользователям в домене OSPF.

5.4.3.2. Примечания

Необходимо настроить основные функции OSPF.

5.4.3.3. Шаги настройки

Настройка внешнего перераспределения маршрутов

- (Опционально) Эта конфигурация является обязательной, если в ASBR необходимо ввести внешние маршруты домена OSPF.
- Выполните эту настройку на ASBR.

Создание маршрута по умолчанию

- (Опционально) Выполните эту настройку, если маршрут по умолчанию должен быть введен в ASBR, чтобы другие маршрутизаторы в домене OSPF по умолчанию получали доступ к другим доменам AS через этот ASBR.
- Выполните эту настройку на ASBR.

5.4.3.4. Проверка

- На маршрутизаторе внутри домена OSPF запустите команду **show ipv6 route ospf**, чтобы убедиться, что загружены unicast-маршруты к другим доменам AS.
- На маршрутизаторе внутри домена OSPF выполните команду **show ipv6 route ospf**, чтобы убедиться, что маршрут по умолчанию к ASBR загружен.
- Запустите команду **ping**, чтобы убедиться, что сервис unicast-рассылки IPv6 другим доменам AS работает правильно.

5.4.3.5. Связанные команды

Настройка перераспределения маршрутов

Команда	**redistribute** {**bgp** | **connected** |**isis**[*area-tag*] |**ospf** *process-id*| **rip** | **static**}[{**level-1** | **level-1-2** | **level-2**} | **match** {**internal** | **external** [**1**|**2**] | **nssa-external** [**1** | **2**]} | **metric** *metric-value*|**metric-type** {**1**|**2**} | **route-map** *route-map-name* |**tag** *tag-value*]
Описание параметра	**bgp**: указывает на перераспределение из BGP. **connected**: указывает на перераспределение с прямых маршрутов. **isis**[*area-tag*]: указывает на перераспределение из IS-IS. **area-tag** указывает экземпляр IS-IS. **ospf** *process-id*: указывает на перераспределение из OSPF. **process-id** указывает экземпляр OSPF. Значение варьируется от 1 до 65 535. **rip**: указывает на перераспределение из RIP. **static**: указывает на перераспределение со статических маршрутов. **level-1** | **level-1-2** | **level-2**: используется только при перераспределении маршрутов IS-IS. Перераспределяются только маршруты указанного уровня. По умолчанию перераспределять можно только маршруты IS-IS Level-2. **match**: используется только при перераспределении маршрутов OSPF. Перераспределяются только маршруты, соответствующие указанным критериям. По умолчанию все маршруты OSPF могут быть перераспределены.

	metric *metric-value*: указывает метрику внешнего LSA OSPF. *metric-value* указывает размер метрики. Значение варьируется от 0 до 16 777 214. **metric-type** {**1**|**2**}: указывает тип внешнего маршрута, который может быть E-1 или E-2. **route-map** *route-map-name*: устанавливает правила фильтрации перераспределения. **tag** *tag-value*: указывает значение тега маршрута, который перераспределяется в домен маршрутизации OSPF. Значение варьируется от 0 до 4 294 967 295
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Когда устройство поддерживает несколько протоколов маршрутизации, взаимодействие между протоколами очень важно. Для одновременного запуска нескольких протоколов маршрутизации устройство должно иметь возможность перераспределять информацию о маршрутизации одного протокола на другой протокол. Это относится ко всем протоколам маршрутизации. При перераспределении маршрутов IS-IS, **level-1**, **level-2** или **level-1-2** можно настроить так, чтобы указать, что маршруты IS-IS указанных уровней будут перераспределены. По умолчанию перераспределяются маршруты IS-IS Level-2. Во время перераспределения маршрутов OSPFv3 можно настроить **match**, указывающее, что будут перераспределены маршруты OSPFv3 указанного подтипа. По умолчанию перераспределяются все типы маршрутов OSPFv3. Для параметра **level**, настроенного во время перераспределения маршрутов IS-IS, и параметра **match**, настроенного во время перераспределения маршрутов OSPFv3, маршруты сопоставляются с картой маршрутов только в том случае, если подтип маршрутов правильный. Во время настройки перераспределения маршрутов, правила **match** используются, настроенные в режиме конфигурации карты маршрутов на основе исходной информации о маршрутах. Приоритеты **tag**, **metric** и **metric-type** в конфигурации перераспределения маршрутов ниже приоритета правил **set**, настроенных в режиме конфигурации карты маршрутов. Значение **set metric** связанных карт маршрутов должно находиться в диапазоне от 0 до 16 777 214. Если значение превышает этот диапазон, маршруты ввести невозможно. Правила конфигурации для формы **no** команды **redistribute** следующие: 1. Если некоторые параметры указаны в форме **no** команды, значения этих параметров по умолчанию будут восстановлены.

	2. Если в форме **no** команды не указан ни один параметр, вся команда будет удалена. Например, если настроено **redistribute isis 112 level-2**, команда **no redistribute isis 112 level-2** восстанавливает только значение по умолчанию **level-2**. Поскольку уровень 2 сам по себе является значением параметра по умолчанию, сохраненная конфигурация по-прежнему **redistribute isis 112 level-2** после выполнения предыдущей формы команды **no**. Чтобы удалить всю команду, вам нужно запустить команду **no redistribute isis 112**

Представление маршрута по умолчанию

Команда	**default-information originate** [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map*]
Описание параметра	**always**: позволяет OSPF генерировать маршрут по умолчанию независимо от того, имеет ли локальный маршрутизатор маршрут по умолчанию. **metric** *metric*: указывает начальную метрику маршрута по умолчанию. Значение варьируется от 0 до 16 777 214. По умолчанию метрика маршрута по умолчанию равна 1. **metric-type** *type*: указывает тип маршрута по умолчанию. Внешние маршруты OSPF подразделяются на два типа: Тип 1: метрика зависит от маршрутизатора; Тип 2: метрика одинакова для всех маршрутизаторов. Внешние маршруты типа 1 более надежны, чем внешние маршруты типа 2. **route-map** *map*: указывает связанное имя карты маршрутов. По умолчанию карта маршрутов не связана
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	При выполнении команды **redistribute** или **default-information** маршрутизатор с поддержкой OSPFv3 автоматически становится ASBR. Однако ASBR не генерирует и не объявляет автоматически маршрут по умолчанию для всех маршрутизаторов в домене маршрутизации OSPF. Чтобы ASBR генерировал маршрут по умолчанию, настройте команду **default-information originate**. Если указано **always**, процесс OSPFv3 объявляет соседям внешний маршрут по умолчанию независимо от того, существует ли маршрут по умолчанию в базовой (core) таблице маршрутизации. Однако этот маршрут по умолчанию не отображается на локальном маршрутизаторе. Чтобы убедиться, что маршрут по умолчанию создан, запустите команду **show ipv6 ospf database**, чтобы отобразить базу данных состояния каналов OSPFv3. На соседе OSPFv3 вы можете

	запустить команду **show ipv6 route ospf**, чтобы увидеть маршрут по умолчанию. Метрику внешнего маршрута по умолчанию можно определить только в команде **default-information originate**, а не в команде **default-metric**. OSPFv3 имеет два типа внешних маршрутов. Метрика внешнего маршрута типа 1 изменится, но метрика внешнего маршрута типа 2 останется неизменной. Если два параллельных пути к одной и той же сети назначения имеют одинаковую метрику маршрута, приоритет маршрута типа 1 выше, чем приоритет маршрута типа 2. Таким образом, команда **show ipv6 route ospf** отображает только маршрут типа 1. Маршрутизатор в тупиковой области не может генерировать внешний маршрут по умолчанию

5.4.3.6. Пример конфигурации

Настройка перераспределения маршрутов

Сценарий:

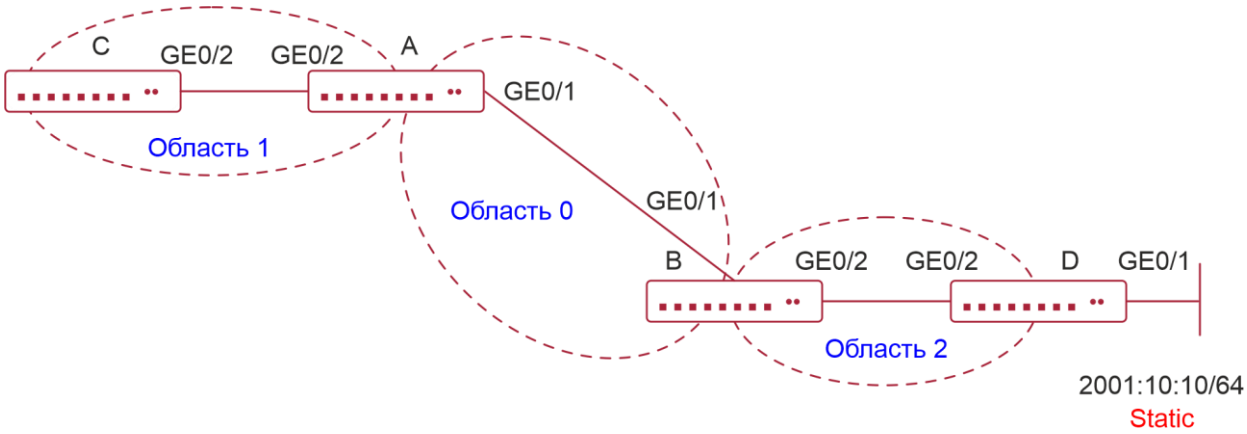


Рисунок 5-10.

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. • Настройте базовые функции OSPF на всех маршрутизаторах. • Введите внешний статический маршрут к маршрутизатору D
D	D#configure terminal D(config)#ipv6 router ospf 1 D(config-router)# redistribute static

Проверка	• На маршрутизаторе D запустите команду **show ipv6ospf database external brief**, чтобы убедиться, что создан LSA, соответствующий внешнему маршруту. • На маршрутизаторе C выполните команду **show ipv6 route ospf**, чтобы убедиться, что внешний статический маршрут введен
D	D#show ipv6 ospf database external OSPFv3 Router with ID (4.4.4.4) (Process 1) AS-external-LSA LS age: 7 LS Type: AS-External-LSA Link State ID: 0.0.0.6 Advertising Router: 4.4.4.4 LS Seq Number: 0x80000001 Checksum: 0x9C1F Length: 36 Metric Type: 2 (Larger than any link state path) Metric: 20 Prefix: 2001:10:10::/64 Prefix Options: 0 (-|-|-|-)
C	C#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O E2 2001:10:10::/64 [110/20] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/2

Настройка маршрута по умолчанию

Сценарий:

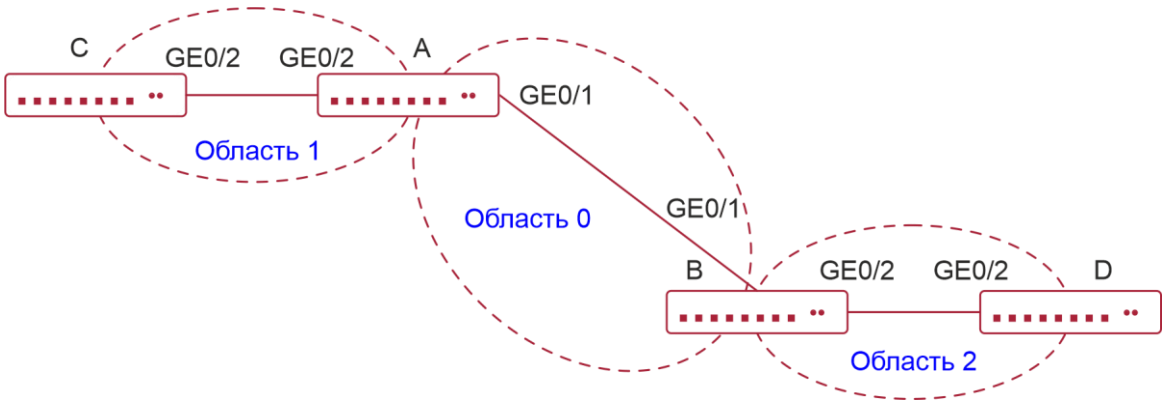


Рисунок 5-11.

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. • Настройте базовые функции OSPF на всех маршрутизаторах. • Настройте маршрут по умолчанию на маршрутизаторе D
D	D#configure terminal D(config)#ipv6 router ospf 1 D(config-router)#default-information originate always
Проверка	• На маршрутизаторе D запустите команду **show ipv6ospf database external brief**, чтобы убедиться, что создан LSA, соответствующий маршруту по умолчанию. • На маршрутизаторе C запустите команду **show ipv6 route ospf**, чтобы убедиться, что существует маршрут по умолчанию OSPF
D	D#show ipv6 ospf database external OSPFv3 Router with ID (4.4.4.4) (Process 1) AS-external-LSA LS age: 3 LS Type: AS-External-LSA Link State ID: 0.0.0.7 Advertising Router: 4.4.4.4 LS Seq Number: 0x80000001 Checksum: 0x1839 Length: 32

	Metric Type: 2 (Larger than any link state path) Metric: 1 Prefix: ::/0 Prefix Options: 0 (-|-|-|-) External Route Tag: 1
C	C#show ipv6route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O E2::/0 [110/20] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/2

5.4.3.7. Распространенные ошибки

- Петля маршрутизации формируется из-за того, что команда **default-information originate always** настроена на нескольких маршрутизаторах.
- Маршруты ввести невозможно, поскольку на маршрутизаторе в тупиковой области настроено перераспределение маршрутов.

5.4.4. Настройка тупиковой области и области NSSA

5.4.4.1. Эффект конфигурации

Настройте область, расположенную в тупике, как тупиковую область, чтобы уменьшить взаимодействие информации о маршрутизации и размера таблицы маршрутизации, а также повысить стабильность маршрутов.

5.4.4.2. Примечания

- Необходимо настроить основные функции OSPF.
- Магистральную или транзитную области нельзя настроить как тупиковую область или область NSSA.
- Маршрутизатор в тупиковой области не может вводить внешние маршруты, но маршрутизатор в области NSSA может вводить внешние маршруты.

5.4.4.3. Шаги настройки

Настройка тупиковой области

- (Опционально) Выполните эту настройку, если хотите уменьшить размер таблицы маршрутизации на маршрутизаторах в этой области.
- Выполните эту настройку на всех маршрутизаторах в одной области.

Настройка области NSSA

- (Опционально) Выполните эту настройку, если вы хотите уменьшить размер таблицы маршрутизации на маршрутизаторах в области и ввести в эту область внешние маршруты OSPF.
- Область должна быть настроена как область NSSA на всех маршрутизаторах в этой области.

5.4.4.4. Проверка

Проверка тупиковой области

На маршрутизаторе в тупиковой области выполните команду **show ipv6 route**, чтобы убедиться, что маршрутизатор не загружен какими-либо внешними маршрутами.

Проверка области NSSA

- На маршрутизаторе в области NSSA выполните команду **show ipv6 ospf database**, чтобы убедиться, что введенный внешний маршрут генерирует LSA типа 7.
- На маршрутизаторе в магистральной области выполните команду **show ipv6 route**, чтобы убедиться, что маршрутизатор загружен внешними маршрутами, введенными из области NSSA.

5.4.4.5. Связанные команды

Настройка тупиковой области

Команда	**area** *area-id* **stub** [**no-summary**]
Описание параметра	*area-id*: указывает идентификатор тупиковой области. Значение может быть целым числом или префиксом IPv4. **no-summary**: эта опция действительна только для ABR в тупиковой области. Если указана эта опция, ABR объявляет только один LSA типа 3, указывающий маршрут по умолчанию к тупиковой области, и не объявляет другие LSA типа 3
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Область, расположенная на тупике сети, может быть настроена как тупиковая область. Вы должны запустить команду **area stub** на всех маршрутизаторах в тупиковой области. Устройства в тупиковой области не могут изучать внешние маршруты (LSA типа 5) AS. На практике внешние маршруты занимают большую часть базы данных состояния каналов. Таким образом, устройства в тупиковой области могут изучить лишь небольшой объем информации о маршрутизации,

	что снижает объем системных ресурсов, необходимых для запуска протокола OSPFv3. По умолчанию ABR в тупиковой области генерирует LSA типа 3, указывающий на ошибку по умолчанию, и объявляет LSA в тупиковой области. Таким образом, устройства в тупиковой области могут получить доступ к устройствам за пределами AS. Чтобы настроить полностью тупиковую область, добавьте ключевое слово **no-summary** при запуске команды **area stub** на ABR

Настройка области NSSA

Команда	**area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate**[**metric** *value*] [**metric-type** *type*]] [**no-summary**] [**translator** [**stability-interval** *seconds* | **always**]] [**translate type7 suppress-fa**]
Описание параметра	*area-id*: указывает идентификатор области NSSA. **no-redistribution**: выберите эту опцию, если маршрутизатор является NSSA ABR и вы хотите использовать только команду **redistribute** для внесения информации о маршрутизации в общую область, а не в область NSSA. **default-information-originate**: указывает, что LSA типа 7 по умолчанию создается и вводится в область NSSA. Этот параметр действует только для NSSA ABR или ASBR. **metric** *value*: указывает метрику созданного LSA по умолчанию. Значение находится в диапазоне от 0 до 16 777 214. Значение по умолчанию — 1. **metric-type** *type*: указывает тип маршрута созданного LSA по умолчанию. Значения включают **1** и **2**. **1** представляет N-1, а **2** представляет N-2. Значение по умолчанию — 2. **no-summary**: запрещает ABR в области NSSA отправлять суммарные LSA (LSA типа 3). **translator**: указывает, что NSSA ABR является транслятором. **stability-interval** *seconds*: указывает интервал стабильности после того, как NSSA ABR переключается с транслятора на не транслятор. Измеряется в секундах. Значение по умолчанию — 40. Значение находится в диапазоне от 0 до 2 147 483 647. **always**: указывает, что текущий ABR NSSA всегда действует как транслятор. Значение по умолчанию — резервный транслятор. **translate type7 suppress-fa**: указывает, что LSA типа 5 не несет адрес пересылки (FA), когда LSA типа 7 преобразуется в LSA типа 5
Командный режим	Режим конфигурации процесса маршрутизации OSPF

Руководство по использованию	Параметр **default-information-originate** используется для создания LSA типа 7 по умолчанию. Этот параметр имеет разные функции в ABR и ASBR в области NSSA. В ABR создается маршрут по умолчанию LSA типа 7 независимо от того, существует ли маршрут по умолчанию в таблице маршрутизации. В ASBR (не ABR) маршрут по умолчанию LSA типа 7 генерируется только в том случае, если маршрут по умолчанию существует в таблице маршрутизации. Если в ASBR настроен параметр **no-redistribution**, другие внешние маршруты, введенные OSPF с помощью команды **redistribute**, не могут быть объявлены в области NSSA. Этот параметр обычно используется, когда маршрутизатор в области NSSA действует и как ASBR, и как ABR. Это предотвращает попадание внешней информации о маршрутизации в область NSSA. Чтобы еще больше сократить количество LSA, отправляемых в область NSSA, вы можете настроить параметр **no-summary** в ABR, чтобы запретить ABR отправлять суммарные LSA (LSA типа 3) в область NSSA. **area default-cost** используется на ABR или ASBR, подключенном к области NSSA. Эта команда настраивает стоимость маршрута по умолчанию, отправляемого из ABR/ASBR в область NSSA. По умолчанию стоимость маршрута по умолчанию, отправленного в область NSSA, равна 1. Если область NSSA имеет два или более ABR, ABR с наибольшим идентификатором маршрутизатора выбирается по умолчанию в качестве транслятора для преобразования LSA типа 7 в LSA типа 5. Если текущим устройством всегда является транслятор ABR для преобразования LSA типа 7 в LSA типа 5, используйте параметр **translator always**. Если роль транслятора текущего устройства заменяется другим ABR, возможность преобразования сохраняется в течение времени, указанного с помощью **stability-interval**. Если маршрутизатор снова не станет транслятором в течение **stability-interval**, LSA, преобразованные из типа 7 в тип 5, будут удалены из AS после истечения **stability-interval**. Чтобы предотвратить петлю маршрутизации, LSA, преобразованные из типа 7 в тип 5, будут удалены из AS сразу после того, как текущее устройство потеряет роль транслятора, даже если **stability-interval** не истечет. В одной и той же области NSSA рекомендуется настраивать **translator always** только на одном ABR

5.4.4.6. Пример конфигурации

Настройка тупиковой области

Сценарий:

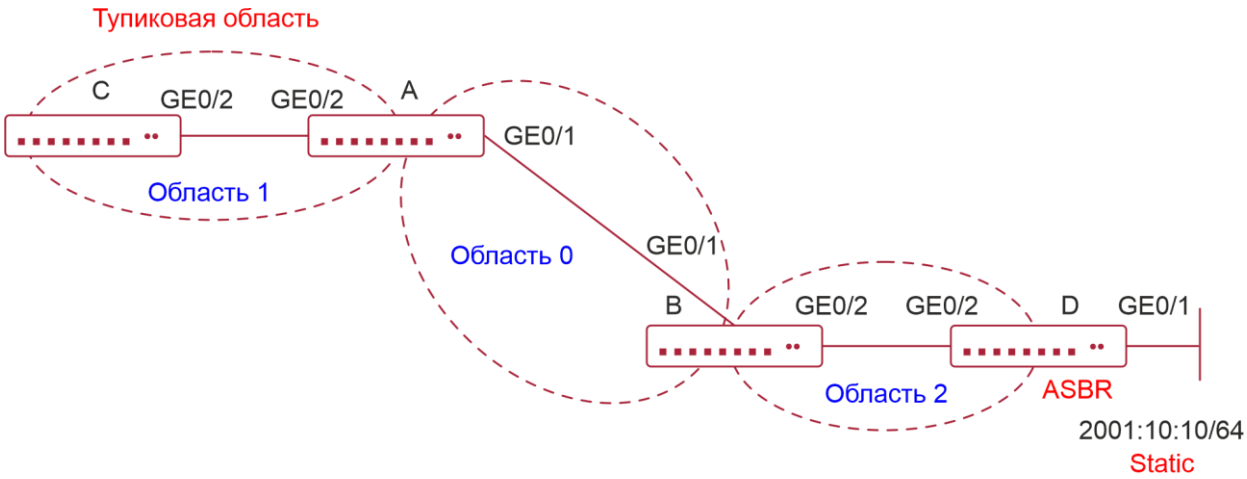


Рисунок 5-12.

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. (Опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • Введите внешний статический маршрут к маршрутизатору D. • Настройте область 1 как тупиковую область на маршрутизаторе A и маршрутизаторе C
D	D#configure terminal D(config)#ipv6 router ospf 1 D(config-router)#redistribute static
A	A# configure terminal A(config)#ipv6 router ospf 1 A(config-router)#area 1 stub no-summary
C	C#configure terminal C(config)#ipv6 router ospf 1 C(config-router)#area 1 stub
Проверка	На маршрутизаторе C выполните команду **show ipv6 route ospf**, чтобы отобразить таблицу маршрутизации. Убедитесь, что существует только

	один межобластной маршрут по умолчанию и не введен внешний статический маршрут от маршрутизатора D
C	C#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O IA::/0 [110/3] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/2

Настройка области NSSA

Сценарий:

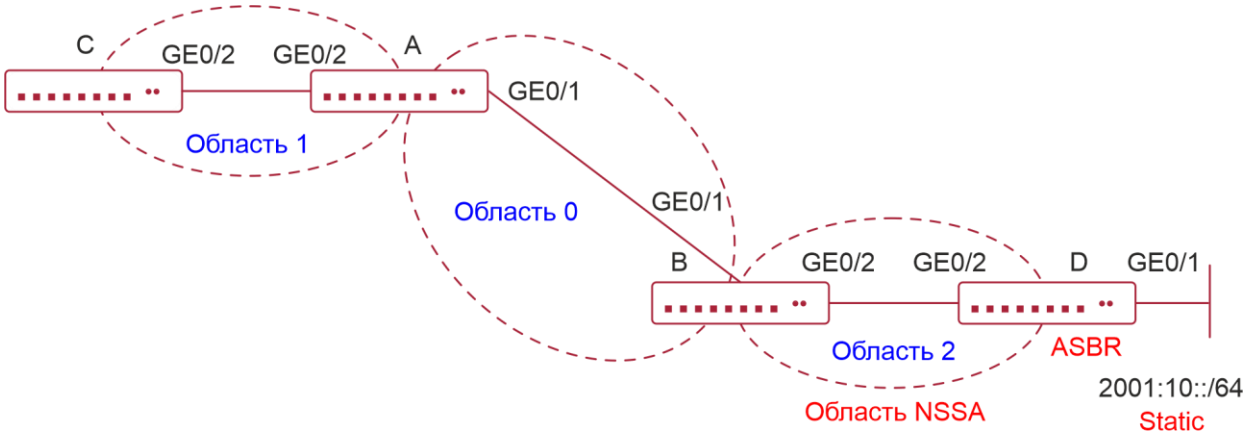


Рисунок 5-13.

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. (Опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • Введите внешний статический маршрут к маршрутизатору D. • Настройте область 1 как область NSSA на маршрутизаторах B и D
D	D#configure terminal

	D(config)#ipv6 router ospf 1 D(config-router)#area 1 nssa D(config-router)#redistribute static
B	B#configure terminal B(config)#ipv6 router ospf 1 B(config-router)#area 1 nssa
Проверка	• На маршрутизаторе D запустите команду **show ipv6 ospf database**, чтобы отобразить информацию о базе данных, и убедитесь, что генерируются LSA типа 7. • На маршрутизаторе A выполните команду **show ipv6 route ospf**, чтобы отобразить таблицу маршрутизации, и убедитесь, что внешний статический маршрут введен маршрутизатором D
D	D#show ipv6 ospf database nssa-external OSPFv3 Router with ID (1.1.1.1) (Process 1) NSSA-external-LSA (Area 0.0.0.1) LS age: 1196 LS Type: NSSA-external-LSA Link State ID: 0.0.0.3 Advertising Router: 1.1.1.1 LS Seq Number: 0x80000004 Checksum: 0x1F25 Length: 52 Metric Type: 2 (Larger than any link state path) Metric: 20 Prefix: 2001:10::/64 Prefix Options: 8 (P|-|-|-) Forwarding Address: 4000::1
A	A#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

	IA - Inter area O N2 2001:10::/64 [110/20] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1

5.4.4.7. Распространенные ошибки

- Конфигурации типа области несовместимы на маршрутизаторах в одной и той же области.
- Внешние маршруты ввести невозможно, так как на маршрутизаторе в тупиковой области настроено перераспределение маршрутов.

5.4.5. Настройка суммирования маршрутов

5.4.5.1. Эффект конфигурации

- Суммируйте маршруты, чтобы уменьшить взаимодействие информации о маршрутизации и размера таблицы маршрутизации, а также повысить стабильность маршрутов.
- Экранируйте или фильтруйте маршруты.

5.4.5.2. Примечания

- Необходимо настроить основные функции OSPF.
- Диапазон адресов суммарного маршрута может превышать фактический диапазон сети в таблице маршрутизации. Если данные отправляются в сеть за пределами диапазона суммирования, может образоваться петля маршрутизации и нагрузка на обработку маршрутизатора может увеличиться. Чтобы предотвратить эти проблемы, необходимо добавить отброшенный маршрут в таблицу маршрутизации или экранировать или фильтровать маршруты.

5.4.5.3. Шаги конфигурации

Настройка суммирования межобластных маршрутов

- (Опционально) Выполните эту настройку, если необходимо суммировать маршруты области OSPF.
- Если не требуется иное, выполните эту настройку на ABR в области, где расположены суммируемые маршруты.

Настройка суммирования внешних маршрутов

- (Опционально) Выполните эту настройку, если необходимо суммировать маршруты, внешние по отношению к домену OSPF.
- Если не требуется иное, выполните эту настройку на ASBR, в который вводятся маршруты, которые необходимо суммировать.

5.4.5.4. Проверка

Запустите команду **show ipv6 route ospf**, чтобы убедиться, что отдельные маршруты не существуют и существует только суммарный маршрут.

5.4.5.5. Связанные команды

Настройка суммирования межобластных маршрутов

Команда	**area** *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise**|**not-advertise**]
Описание параметра	*area-id*: указывает идентификатор области OSPF, в которую следует внедрить суммарный маршрут. Значение может быть целым числом или префиксом IPv4. *ipv6-prefix*/*prefix-length*: указывает диапазон IP-адресов, подлежащих суммированию. **advertise**|**not-advertise**: указывает, следует ли объявлять суммарный маршрут
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Эта команда действует только на ABR и используется для объединения нескольких маршрутов в области в маршрут и объявления этого маршрута другим областям. Объединение маршрутной информации происходит только на границе области. Маршрутизаторы внутри области могут изучать конкретную информацию о маршрутизации, тогда как маршрутизаторы в других областях могут изучать только один суммарный маршрут. Кроме того, вы можете настроить объявление или не объявление, чтобы определить, следует ли объявлять суммарный маршрут для защиты и фильтрации маршрутов. По умолчанию объявляется суммарный маршрут. Вы можете использовать параметр **cost**, чтобы задать метрику суммарного маршрута. Вы можете настроить команды суммирования маршрутов для нескольких областей. Это упрощает маршруты во всем домене маршрутизации OSPF и повышает производительность сетевой пересылки, особенно для сетей большого размера. Когда несколько команд суммирования маршрутов настроены и имеют взаимосвязь друг с другом, диапазон областей, подлежащих суммированию, определяется на основе принципа максимального соответствия

Настройка суммирования внешних маршрутов

Команда	**summary-prefix** *ipv6-prefix*/*prefix-length* [**not-advertise** | **tag** *number*]
Описание параметра	*ipv6-prefix*/*prefix-length*: указывает диапазон IP-адресов, подлежащих суммированию. **not-advertise**: указывает, что суммарный маршрут не объявляется. Если этот параметр не указан, объявляется суммарный маршрут.

	tag *number*: указывает значение тега маршрута, который перераспределяется в домен маршрутизации OSPFv3. Значение варьируется от 0 до 4 294 967 295
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Когда маршруты перераспределяются из других процессов маршрутизации и вводятся в процесс маршрутизации OSPFv3, каждый маршрут объявляется маршрутизаторам OSPFv3 с использованием внешнего LSA. Если внедренные маршруты представляют собой непрерывное адресное пространство, ABR может объявлять только один суммарный маршрут, чтобы значительно уменьшить размер таблицы маршрутизации. **area range** суммирует маршруты между областями OSPFv3, тогда как **summary-prefix** суммирует внешние маршруты домена маршрутизации OSPFv3. При настройке на трансляторе NSSA ABR **summary-prefix** суммирует перераспределенные маршруты и маршруты, полученные на основе LSA, преобразованных из типа 7 в тип 5. При настройке на ASBR (не трансляторе NSSA ABR) **summary-prefix** суммирует только перераспределенные маршруты

5.4.5.6. Пример конфигурации

Сценарий:

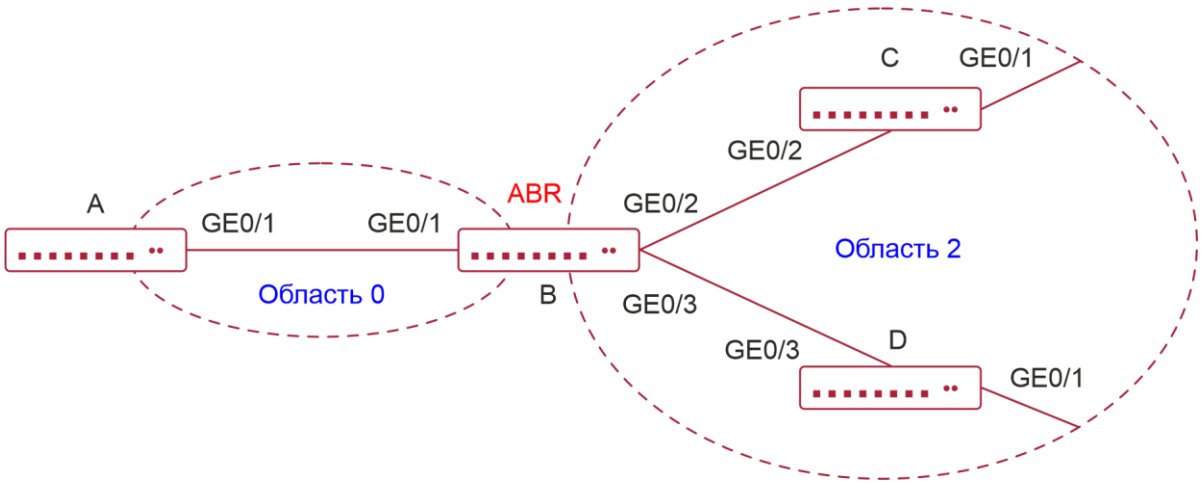


Рисунок 5-14.

IPv6-адреса интерфейса следующие:

B: GE0/2 2001:16:2::1/64 GE0/3 2001:16:3::1/64

C: GE0/2 2001:16:2::2/64 GE0/1 2001:16:4::2/64

D: GE0/3 2001:16:3::2/64 GE0/1 2001:16:5::1/64

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. (Опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • Суммируйте маршруты области 2 на маршрутизаторе B
B	B#configure terminal B(config)#ipv6 router ospf 1 B(config-router)#area 2 range 2001:16::/64
Проверка	На маршрутизаторе A проверьте таблицу маршрутизации и убедитесь, что запись 2001:16::/64 создана и другие маршруты не существуют
A	A#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O IA 2001:16::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1

5.4.5.7. Распространенные ошибки

Суммирование маршрутов между областями невозможно реализовать, поскольку команда **area range** настроена на устройстве, не поддерживающем ABR.

5.4.6. Настройка фильтрации маршрутов

5.4.6.1. Эффект конфигурации

Маршруты, не соответствующие условиям фильтрации, не могут быть загружены в таблицу маршрутизации или объявлены соседям. Пользователи сети не могут получить доступ к указанной сети назначения.

5.4.6.2. Примечания

- Необходимо настроить основные функции OSPF.
- Фильтрация маршрутов с помощью команды **distribute-list in** влияет на пересылку локальных маршрутов, но не влияет на вычисление маршрутов на основе LSA. Таким образом, если на ABR настроена фильтрация маршрутов, LSA типа 3 по-прежнему будут генерироваться и объявляться в других областях, поскольку маршруты по-прежнему можно рассчитывать на основе LSA. В результате

генерируются маршруты black-hole. В этом случае вы можете запустить команду **area filter-list** или **area range** (содержащую параметр **not-advertise**) на ABR, чтобы предотвратить создание маршрутов black-hole.

5.4.6.3. Шаги настройки

Настройка фильтрации межобластных маршрутов

- (Опционально) Эту конфигурацию рекомендуется использовать, если пользователям необходимо ограничить доступ к сети в определенной области OSPF.
- Если не требуется иное, выполните эту настройку на ABR в области, где расположены отфильтрованные маршруты.

Настройка фильтрации перераспределенных маршрутов

- (Опционально) Выполните эту настройку, если необходимо фильтровать внешние маршруты, введенные ASBR.
- Если не требуется иное, выполните эту настройку на ASBR, к которому введены фильтруемые маршруты.

Настройка фильтрации изученных маршрутов

- (Опционально) Выполните эту настройку, если пользователям необходимо ограничить доступ к указанной целевой сети.
- Если не требуется иное, выполните эту настройку на маршрутизаторе, требующем фильтрации маршрутов.

5.4.6.4. Проверка

- Запустите команду **show ipv6 route**, чтобы убедиться, что маршрутизатор не загружен отфильтрованными маршрутами.
- Запустите команду **ping**, чтобы убедиться, что указанная сеть назначения недоступна.

5.4.6.5. Связанные команды

Настройка пассивного интерфейса

Команда	**passive-interface** {**default** | *interface-type interface-number* }
Описание параметра	*interface-type interface-number*: указывает интерфейс, который следует настроить как пассивный интерфейс. **default**: указывает, что все интерфейсы будут настроены как пассивные интерфейсы
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Когда интерфейс настроен как пассивный интерфейс, он больше не отправляет и не получает пакеты Hello. Эта команда действует только на интерфейсе с поддержкой OSPFv3, а не на виртуальном канале

Настройка фильтрации перераспределенных маршрутов

Команда	**distribute-list**{*name* | **prefix-list** *prefix-list-name*}**out**[**bgp** | **connected** |**isis**[*area-tag*]| **ospf** *process-id*| **rip** | **static**]
Описание параметра	*name*: использует ACL для фильтрации. **prefix-list** *prefix-list-name*: использует список префиксов для фильтрации. **bgp** | **connected** |**isis**[*area-tag*]| **ospf** *process-id*| **rip** | **static**: указывает источник маршрутов, подлежащих фильтрации
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	**distribute-list out** похож на **redistribute route-map** и используется для фильтрации маршрутов, перераспределяемых из других протоколов в OSPFv3. Сама команда **distribute-list out** не перераспределяет маршруты и обычно используется вместе с командой **redistribute**. ACL и правила фильтрации списка префиксов в конфигурации являются взаимоисключающими. То есть, если ACL используется для фильтрации маршрутов, поступающих из определенного источника, список префиксов нельзя настроить для фильтрации одних и тех же маршрутов

Настройка фильтрации изученных маршрутов

Команда	**distribute-list**{*name* | **prefix-list** *prefix-list-name*}**in** [*interface-type interface-number*]
Описание параметра	*name*: использует ACL для фильтрации. **prefix-list** *prefix-list-name*: использует список префиксов для фильтрации. *interface-type interface-number*: указывает интерфейс, для которого фильтруются маршруты LSA
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Фильтруйте маршруты, вычисляемые на основе полученных LSA. Пересылаться могут только маршруты, соответствующие условиям фильтрации. Команда не влияет на LSDB или таблицы маршрутизации соседей. ACL и правила фильтрации списка префиксов в конфигурации являются взаимоисключающими. То есть, если ACL используется для фильтрации маршрутов на указанном интерфейсе, список префиксов нельзя настроить для фильтрации маршрутов на том же интерфейсе. Фильтрация маршрутов с помощью команды **distribute-list in** влияет на пересылку локальных маршрутов, но не влияет на вычисление

	маршрутов на основе LSA. Таким образом, если на ABR настроена фильтрация маршрутов, LSA типа 3 по-прежнему будут генерироваться и объявляться в других областях, поскольку маршруты по-прежнему можно рассчитывать на основе LSA. В результате генерируются маршруты black-hole. В этом случае вы можете запустить команду **area range** (содержащую параметр **not-advertise**) на ABR, чтобы предотвратить создание маршрутов black-hole

5.4.6.6. Пример конфигурации

Сценарий:

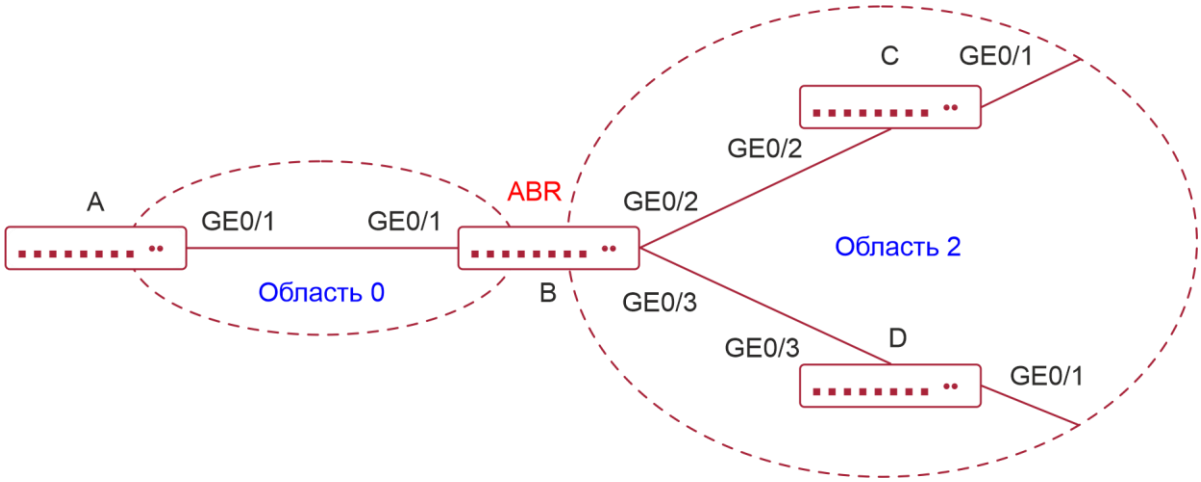


Рисунок 5-15.

IPv6-адреса интерфейса следующие:

B: GE0/2 2001:16:2::1/64 GE0/3 2001:16:3::1/64

C: GE0/2 2001:16:2::2/64 GE0/1 2001:16:4::2/64

D: GE0/3 2001:16:3::2/64 GE0/1 2001:16:5::1/64

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. (Опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • На маршрутизаторе A настройте фильтрацию маршрутов
A	A#configure terminal A(config)#ipv6 access-list test A (config-ipv6-acl)#permit ipv6 2001:16:5::/64 any A(config)#ipv6 router ospf 1 A(config-router)#distribute-list test in GigabitEthernet0/1

Проверка	На маршрутизаторе A проверьте таблицу маршрутизации. Убедитесь, что загружена только запись 2001:16:5::/64
A	A#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O IA 2001:16:5::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1

5.4.6.7. Распространенные ошибки

Фильтрация маршрутов с помощью команды **distribute-list in** влияет на пересылку локальных маршрутов, но не влияет на вычисление маршрутов на основе LSA. Таким образом, если на ABR настроена фильтрация маршрутов, LSA типа 3 по-прежнему будут генерироваться и объявляться в других областях, поскольку маршруты по-прежнему можно рассчитывать на основе LSA. В результате генерируются маршруты black-hole.

5.4.7. Изменение стоимости маршрута и AD

5.4.7.1. Эффект конфигурации

- Измените маршруты OSPF так, чтобы трафик проходил через указанные узлы или обходил указанные узлы.
- Измените последовательность выбора маршрутов маршрутизатором, чтобы изменить приоритеты маршрутов OSPF.

5.4.7.2. Примечания

- Необходимо настроить основные функции OSPF.
- Если вы запустите команду **ipv6 ospf cost** для настройки стоимости интерфейса, настроенная стоимость автоматически перезапишет стоимость, рассчитанную на основе автоматической стоимости.

5.4.7.3. Шаги настройки

Настройка эталонной полоса пропускания

- Опционально.
- Маршрутизатор подключен к линиям связи с разной полосой пропускания. Эту конфигурацию рекомендуется использовать, если вы хотите преимущественно выбрать линию связи с большей полосой пропускания.

Настройка стоимости интерфейса

- Опционально.
- Маршрутизатор подключен по нескольким линиям связи. Эту конфигурацию рекомендуется использовать, если вы хотите вручную указать приоритетную линию связи.

Настройка метрики по умолчанию для перераспределения

- Опционально.
- Эта конфигурация является обязательной, если стоимость внешних маршрутов домена OSPF должна быть указана при введении внешних маршрутов в ASBR.

Настройка максимальной метрики

- Опционально.
- Маршрутизатор может работать нестабильно во время процесса перезапуска или в течение определенного периода времени после перезапуска маршрутизатора, и пользователи не хотят пересылать данные через этот маршрутизатор. В этом случае рекомендуется использовать данную конфигурацию.

Настройка AD

- Опционально.
- Выполните эту настройку, если вы хотите изменить приоритеты маршрутов OSPF на маршрутизаторе, который использует несколько протоколов unicast-маршрутизации.

5.4.7.4. Проверка

- Запустите команду **show ipv6 ospf interface**, чтобы убедиться в правильности стоимости интерфейсов.
- Запустите команду **show ipv6 route**, чтобы убедиться, что стоимость внешних маршрутов, введенных ASBR, верна.
- Перезагрузите маршрутизатор. В течение заданного периода времени данные не пересылаются через перезапущенный маршрутизатор.

5.4.7.5. Связанные команды

Настройка эталонной полосы пропускания

Команда	**auto-cost reference-bandwidth** *ref-bw*
Описание параметра	*ref-bw*: указывает эталонную полосу пропускания. Единица измерения — Мбит/с. Значение варьируется от 1 до 4 294 967
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Вы можете запустить команду **ipv6 ospf cost** в режиме настройки интерфейса, чтобы указать стоимость интерфейса. Приоритет этой стоимости выше, чем у метрики, вычисляемой на основе эталонной полосы пропускания

Настройка стоимости интерфейса

Команда	**ipv6 ospf cost** *cost*[**instance** *instance-id*]
Описание параметра	*cost*: указывает стоимость интерфейса OSPF. Значение варьируется от 0 до 65 535. **instance** *instance-id*: указывает идентификатор указанного процесса OSPFv3 интерфейса. Значение варьируется от 0 до 255
Командный режим	Режим настройки интерфейса
Руководство по использованию	По умолчанию стоимость интерфейса OSPFv3 равна 100 Мбит/с/Bandwidth, где Bandwidth — это полоса пропускания интерфейса, настраиваемая командой **bandwidth** в режиме настройки интерфейса. Стоимость интерфейсов OSPF по нескольким типовым линиям связи следующая: Последовательная линия 64 кбит/с: стоимость — 1562. Линия E1: стоимость — 48. 10M Ethernet: стоимость — 10. 100M Ethernet: стоимость — 1. Если вы запустите команду **ipv6 ospf cost** для настройки стоимости интерфейса, настроенная стоимость автоматически перезапишет стоимость, рассчитанную на основе автоматической стоимости

Настройка стоимости маршрута по умолчанию в тупиковой области/области NSSA

Команда	**area** *area-id* **default-cost** *cost*
Описание параметра	*area-id*: указывает идентификатор тупиковой области/области NSSA. *cost*: указывает стоимость суммарного маршрута по умолчанию, введенного в тупиковую область/область NSSA. Значение находится в диапазоне от 0 до 16 777 215
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Эта команда действует только на ABR в тупиковой области/области NSSA

Настройка метрики по умолчанию для перераспределения

Команда	**default-metric** *metric*
Описание параметра	*metric*: указывает метрику по умолчанию для перераспределенного маршрута OSPF. Значение варьируется от 1 до 16 777 214
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Команда **default-metric** должна использоваться вместе с командой **redistribute** для изменения исходных метрик всех перераспределяемых маршрутов. Команда **default-metric** не действует на внешние маршруты, которые вводятся в домен маршрутизации OSPF командой **default-information originate**. Метрика по умолчанию перераспределенного прямого маршрута всегда равна 20

Настройка AD

Команда	**distance** { *distance* | **ospf**{ [**intra-area** *distance*] [**inter-area** *distance*] [**external** *distance*]} }
Описание параметра	*distance*: указывает AD маршрута. Значение варьируется от 1 до 255. **intra-area** *distance*: указывает AD внутриобластного маршрута. Значение варьируется от 1 до 255. **inter-area** *distance*: указывает AD межобластного маршрута. Значение варьируется от 1 до 255. **external** *distance*: указывает AD внешнего маршрута. Значение варьируется от 1 до 255
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Используйте эту команду, чтобы указать разные AD для разных типов маршрутов OSPF. AD позволяет различным протоколам маршрутизации сравнивать приоритеты маршрутов. Меньший AD указывает на более высокий приоритет маршрута. Приоритеты маршрутов, генерируемых различными процессами OSPFv3, необходимо сравнивать на основе AD. Если для AD записи маршрута установлено значение 255, запись маршрута не заслуживает доверия и не участвует в пересылке пакетов

5.4.7.6. Пример конфигурации

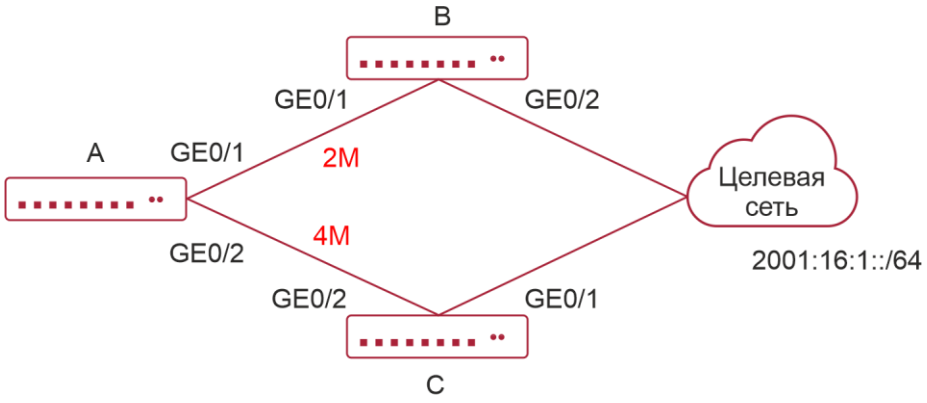


Рисунок 5-16.

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. (Опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (пропущено) • На маршрутизаторе A настройте стоимость каждого интерфейса
A	A#configure terminal A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ipv6 ospf cost 10 A(config)#interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#ipv6 ospf cost 20
Проверка	На маршрутизаторе A проверьте таблицу маршрутизации. Следующий hop оптимального пути к 2001:16:1::/64 — это маршрутизатор B
A	A#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O E2 2001:16:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1

5.4.7.7. Распространенные ошибки

Если в команде **ipv6 ospf cost** стоимость интерфейса установлена равной 0, может возникнуть ошибка расчета маршрута. Например, получается петля маршрутизации.

5.4.8. Включение аутентификации

5.4.8.1. Эффект конфигурации

Все маршрутизаторы, подключенные к сети OSPF, должны пройти аутентификацию, чтобы обеспечить стабильность OSPF и защитить OSPF от вторжений.

5.4.8.2. Примечания

- Необходимо настроить основные функции OSPF.
- Если для области настроена аутентификация, конфигурация вступает в силу на всех интерфейсах, принадлежащих этой области.
- Если аутентификация настроена как для интерфейса, так и для области, к которой принадлежит интерфейс, конфигурация интерфейса вступает в силу преимущественно.

5.4.8.3. Шаги настройки

Настройка аутентификации

- Опционально.
- Выполните эту настройку, если маршрутизатор получает доступ к сети, требующей аутентификации.

Настройка шифрования

- Опционально.
- Выполните эту настройку, если маршрутизатор получает доступ к сети, требующей шифрования.

Настройка аутентификации виртуального канала

- Опционально.
- Выполните эту настройку, если маршрутизатор получает доступ к сети, требующей аутентификации.

Настройка шифрования виртуального канала

- Опционально.
- Выполните эту настройку, если маршрутизатор получает доступ к сети, требующей шифрования.

5.4.8.4. Проверка

- Если маршрутизаторы настроены с разными ключами аутентификации, запустите команду **show ipv6 ospf neighbor**, чтобы убедиться в отсутствии соседа OSPF.
- Если маршрутизаторы настроены с одним и тем же ключом аутентификации, запустите команду **show ipv6 ospf neighbor**, чтобы проверить наличие соседей OSPF.

5.4.8.5. Связанные команды

Настройка аутентификации на основе области

Команда	**area** *area-id* **authentication ipsec spi** *spi*[**md5**|**sha1**] [**0** | **7**] *key*
Описание параметра	*area-id*: указывает идентификатор области. Значение может быть целым числом или префиксом IPv4. *spi*: указывает SPI. Значение варьируется от 256 до 4 294 967 295. **md5**: включает аутентификацию MD5. **sha1**: включает аутентификацию SHA1. **0**: указывает, что ключ отображается в виде обычного текста. **7**: указывает, что ключ отображается в зашифрованном тексте. *key*: указывает ключ аутентификации
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Поддерживается три типа аутентификации: • Нет аутентификации • аутентификация MD5 • аутентификация SHA1 Настройка аутентификации на основе области для OSPFv3 действует на все интерфейсы (кроме виртуальных каналов) в области, но конфигурация аутентификации на основе интерфейса имеет приоритет над конфигурацией на основе области

Настройка шифрования и аутентификации на основе области

Команда	**area** *area-id* **encryption ipsec spi** *spi* **esp**[**null**|[**des** | **3des**][**0** | **7**] *des-key*][**md5**|**sha1**] [**0**|**7**] *key*
Описание параметра	*area-id*: указывает идентификатор области. Значение может быть целым числом или префиксом IPv4. *spi*: указывает SPI. Значение варьируется от 256 до 4 294 967 295. **null**: указывает, что режим шифрования не используется. **des**: указывает, что используется режим стандарта шифрования данных (DES). **3des**: указывает, что используется режим Triple DES (3DES). *des-key*: указывает ключ шифрования. **md5**: включает аутентификацию MD5. **sha1**: включает аутентификацию SHA1. **0**: указывает, что ключ отображается в виде обычного текста.

	7: указывает, что ключ отображается в зашифрованном виде. *key*: указывает ключ аутентификации
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Поддерживается два режима шифрования и два режима аутентификации. Два режима шифрования следующие: • DES • 3DES Два режима аутентификации следующие: • MD5 • SHA1 Настройка шифрования и аутентификации на основе области для OSPFv3 действует на все интерфейсы (кроме виртуальных каналов) в этой области, но конфигурация шифрования и аутентификации на основе интерфейса имеет приоритет над конфигурацией на основе области

Настройка аутентификации на основе интерфейса

Команда	**ipv6 ospf authentication**[**null** | **ipsec spi** *spi*[**md5**|**sha1**] [**0**|**7**]*key*][**instance** *instance-id*]
Описание параметра	*area-id*: указывает идентификатор области. Значение может быть целым числом или префиксом IPv4. *spi*: указывает SPI. Значение варьируется от 256 до 4 294 967 295. **md5**: включает аутентификацию MD5. **sha1**: включает аутентификацию SHA1. **0**: указывает, что ключ отображается в виде обычного текста. **7**: указывает, что ключ отображается в зашифрованном тексте. *key*: указывает ключ аутентификации. **instance** *instance-id*: указывает идентификатор указанного процесса OSPFv3 интерфейса. Значение варьируется от 0 до 255
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Поддерживается три типа аутентификации: • Нет аутентификации • аутентификация MD5

	• аутентификация SHA1 Параметры аутентификации OSPFv3, настроенные на взаимосвязанных интерфейсах, должны быть согласованными

Настройка шифрования и аутентификации на основе интерфейса

Команда	**ipv6 ospf encryption ipsec spi** *spi* **esp**[**null**|[**des** | **3des**][**0** | **7**] *des-key*][**md5**|**sha1**] [**0**|**7**] *key*[**instance** *instance-id*]
Описание параметра	*spi*: указывает SPI. Значение варьируется от 256 до 4 294 967 295. **null**: указывает, что режим шифрования не используется. **des**: указывает, что используется режим DES. **3des**: указывает, что используется режим 3DES. *des-key*: указывает ключ шифрования. **md5**: включает аутентификацию MD5. **sha1**: включает аутентификацию SHA1. **0**: указывает, что ключ отображается в виде обычного текста. **7**: указывает, что ключ отображается в зашифрованном виде. *key*: указывает ключ аутентификации. **instance** *instance-id*: указывает идентификатор указанного процесса OSPFv3 интерфейса. Значение варьируется от 0 до 255
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Поддерживается два режима шифрования и два режима аутентификации. Два режима шифрования следующие: • DES • 3DES Два режима аутентификации следующие: • MD5 • SHA1 Параметры шифрования и аутентификации OSPFv3, настроенные на локальном интерфейсе, должны соответствовать параметрам, настроенным на взаимосвязанных интерфейсах

5.4.8.6. Пример конфигурации

Сценарий:



Рисунок 5-17.

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. (Опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (пропущено) • Настройте аутентификацию MD5 для интерфейсов всех маршрутизаторов
A	A#configure terminal A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ipv6 ospf authentication ipsec spi 256 md5 01234567890123456789012345678912
B	B# configure terminal B(config)#interface GigabitEthernet 0/3 B(config-if-GigabitEthernet 0/3)#ipv6 ospf authentication ipsec spi 256 md5 01234567890123456789012345678912
Проверка	На маршрутизаторе A и маршрутизаторе B убедитесь, что статус соседа OSPF правильный
A	A# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.2 1 Full/DR 00:00:38 0 GigabitEthernet 0/1
B	B# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface

	1.1.1.1	1	Full/BDR	00:00:38	0	GigabitEthernet 0/1

5.4.8.7. Распространенные ошибки

- Настроенные режимы аутентификации несовместимы.
- Настроенные ключи аутентификации несовместимы.

5.4.9. Изменение максимального количества одновременных соседей

5.4.9.1. Эффект конфигурации

Управляйте максимальным количеством одновременных соседей в процессе OSPF, чтобы снизить нагрузку на устройство.

5.4.9.2. Примечания

Необходимо настроить основные функции OSPF.

5.4.9.3. Шаги настройки

Настройка максимального количества одновременных соседей в процессе OSPF

- (Опционально) Эту конфигурацию рекомендуется использовать, если вы хотите быстрее настроить смежность OSPF, когда маршрутизатор подключен к множеству других маршрутизаторов.
- Выполните эту настройку на главном маршрутизаторе.

5.4.9.4. Проверка

Запустите команду **show ipv6 ospf neighbor**, чтобы отобразить количество соседей, одновременно взаимодействующих с процессом OSPF.

5.4.9.5. Связанные команды

Настройка максимального количества одновременных соседей в текущем процессе

Команда	**max-concurrent-dd** *number*
Описание параметра	*number*: указывает максимальное количество соседей, одновременно взаимодействующих с процессом OSPF. Значение варьируется от 1 до 65 535
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Если на производительность маршрутизатора влияет обмен данными с несколькими соседями, вы можете настроить эту команду, чтобы ограничить максимальное количество соседей, с которыми каждый процесс OSPF может одновременно инициировать или принимать взаимодействие

Настройка максимального количества одновременных соседей для всех процессов

Команда	**Ipv6 router ospf max-concurrent-dd** *number*
Описание параметра	*number*: указывает максимальное количество соседей, одновременно взаимодействующих с процессом OSPF. Значение варьируется от 1 до 65 535
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если производительность маршрутизатора снижается из-за того, что маршрутизатор обменивается данными с несколькими соседями, вы можете настроить эту команду, чтобы ограничить максимальное количество соседей, с которыми все процессы OSPF могут одновременно инициировать или принимать взаимодействие

5.4.9.6. Пример конфигурации

Сценарий:

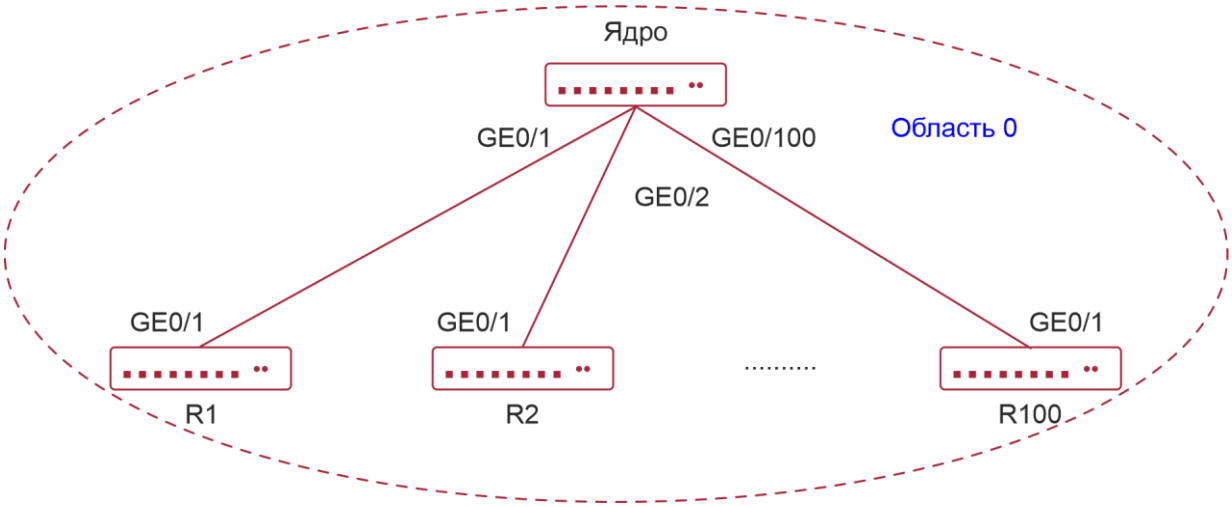


Рисунок 5-18.

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. (Опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • На маршрутизаторе Core установите максимальное количество одновременных соседей равным 4
Core	`Core# configure terminal`

	Core(config)# ipv6 router ospf max-concurrent-dd 4
Проверка	На маршрутизаторе Core проверьте состояние соседа и убедитесь, что не более восьми соседей одновременно взаимодействуют с процессом OSPF

5.4.10. Отключение проверки MTU

5.4.10.1. Эффект конфигурации

Сервис unicast-маршрутизации может предоставляться, даже если MTU интерфейсов соседних маршрутизаторов различны.

5.4.10.2. Примечания

Необходимо настроить основные функции OSPF.

5.4.10.3. Шаги настройки

Отключение проверки MTU

- (Опционально) Проверка MTU отключена по умолчанию. Рекомендуется сохранить конфигурацию по умолчанию.
- Выполните эту настройку на двух маршрутизаторах с разными MTU интерфейса.

5.4.10.4. Проверка

Смежность можно настроить между маршрутизаторами с разными MTU.

5.4.10.5. Связанные команды

Отключение проверки MTU

Команда	**Ipv6 ospf mtu-ignore**
Командный режим	Режим настройки интерфейса
Руководство по использованию	При получении пакета описания базы данных OSPF проверяет, совпадает ли MTU интерфейса соседа с MTU его собственного интерфейса. Если MTU интерфейса, указанный в полученном пакете описания базы данных, больше, чем MTU локального интерфейса, установить смежность невозможно. Чтобы решить эту проблему, вы можете отключить проверку MTU

5.4.10.6. Пример конфигурации

Сценарий:



Рисунок 5-19.

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. (Опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • Настройте разные MTU для интерфейсов на двух маршрутизаторах. • Отключите проверку MTU на всех роутерах. (По умолчанию функция отключения проверки MTU включена.)
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ipv6 mtu 1400 A(config-if-GigabitEthernet 0/1)#ipv6 ospf mtu-ignore
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ipv6 mtu 1600 B(config-if-GigabitEthernet 0/1)# ipv6 ospf mtu-ignore
Проверка	На маршрутизаторе A проверьте правильность информации о соседе OSPF
A	A# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.2 1 Full/DR 00:00:38 0 GigabitEthernet 0/1

5.4.11. Включение двустороннего обслуживания

5.4.11.1. Эффект конфигурации

Пакеты, отличные от Hello, также могут использоваться для поддержания смежности.

5.4.11.2. Примечания

Необходимо настроить основные функции OSPF.

5.4.11.3. Шаги настройки

Включение двустороннего обслуживания

- (Опционально) Эта функция включена по умолчанию. Рекомендуется сохранить конфигурацию по умолчанию.
- Выполните эту настройку на всех маршрутизаторах.

5.4.11.4. Проверка

Пакеты, отличные от Hello, также могут использоваться для поддержания смежности.

5.4.11.5. Связанные команды

Включение двустороннего обслуживания

Команда	**two-way-maintain**
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	В большой сети может быть отправлено или получено множество пакетов, занимающих слишком много процессора и памяти. В результате некоторые пакеты задерживаются или отбрасываются. Если время обработки пакетов Hello превышает dead-интервал, смежность будет нарушена из-за тайм-аута. Если включена функция двустороннего обслуживания, в дополнение к пакетам Hello также могут передаваться пакеты DD, LSU, LSR и LSAck для поддержания двусторонней связи между соседями, когда в сети существует большое количество пакетов. Это предотвращает прекращение смежности, вызванное задержкой или отклонением пакетов Hello

5.4.11.6. Пример конфигурации

Сценарий:



Рисунок 5-20.

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. (Опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (пропущено) • На маршрутизаторе A включите функцию двустороннего обслуживания. (Эта функция включена по умолчанию.)
A	A# configure terminal A(config)# ipv6 routerospf 1 A(config-router)#two-way-maintain
Проверка	При настройке смежности маршрутизатор A проверяет dead-интервал соседа и обновляет dead-интервал, не дожидаясь, пока маршрутизатор B отправит пакет Hello
A	A# show ipv6 ospfneighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.2 1 Full/DR 00:00:38 0 GigabitEthernet 0/1

5.4.12. Корреляция OSPF с BFD

5.4.12.1. Эффект конфигурации

Если канал неисправен, OSPF может быстро обнаружить сбой маршрута. Эта конфигурация помогает сократить время прерывания трафика.

5.4.12.2. Примечания

- Необходимо настроить основные функции OSPF.
- Параметры BFD должны быть настроены для интерфейса заранее.
- Если BFD настроен как для процесса, так и для интерфейса, конфигурация на основе интерфейса вступает в силу преимущественно.

5.4.12.3. Шаги настройки

Корреляция OSPF с BFD

- (Опционально) Выполните эту настройку, если хотите ускорить конвергенцию сети OSPF.
- Выполните эту настройку на маршрутизаторах на обоих концах канала.

5.4.12.4. Проверка

Запустите команду **show bfd neighbor**, чтобы убедиться, что соседи BFD в порядке.

5.4.12.5. Связанные команды

Корреляция интерфейса OSPF с BFD

Команда	**Ipv6 ospf bfd** [**disable**]
Описание параметра	**disable**: отключает BFD для обнаружения каналов на указанном интерфейсе с поддержкой OSPF
Командный режим	Режим настройки интерфейса
Руководство по использованию	Конфигурация на основе интерфейса имеет приоритет над командой **bfd all-interfaces**, используемой в режиме конфигурации процесса. В зависимости от реальной среды вы можете запустить команду **ipv6 ospf bfd**, чтобы включить BFD на указанном интерфейсе для обнаружения каналов, или запустить команду **bfd all-interfaces** в режиме конфигурации процесса OSPF, чтобы включить BFD на всех интерфейсах процесса OSPF, или запустите команду **ipv6 ospf bfd disable**, чтобы отключить BFD на указанном интерфейсе

Корреляция процесса OSPF с BFD

Команда	**bfd all-interfaces**
Командный режим	Режим конфигурации процесса OSPF
Руководство по использованию	OSPF динамически обнаруживает соседей с помощью пакетов Hello. После того, как OSPF включит функцию BFD, будет настроен сеанс BFD для достижения полной смежности и использования механизма BFD для определения статуса соседа. Как только с помощью BFD обнаруживается сбой соседа, OSPF немедленно выполняет конвергенцию сети. Вы также можете запустить команду **ipv6 ospf bfd [disable]** в режиме конфигурации интерфейса, чтобы включить или отключить функцию BFD на указанном интерфейсе, и эта конфигурация имеет приоритет над командой **bfd all-interfaces**, используемой в режиме конфигурации процесса OSPF

5.4.12.6. Пример конфигурации

Сценарий:

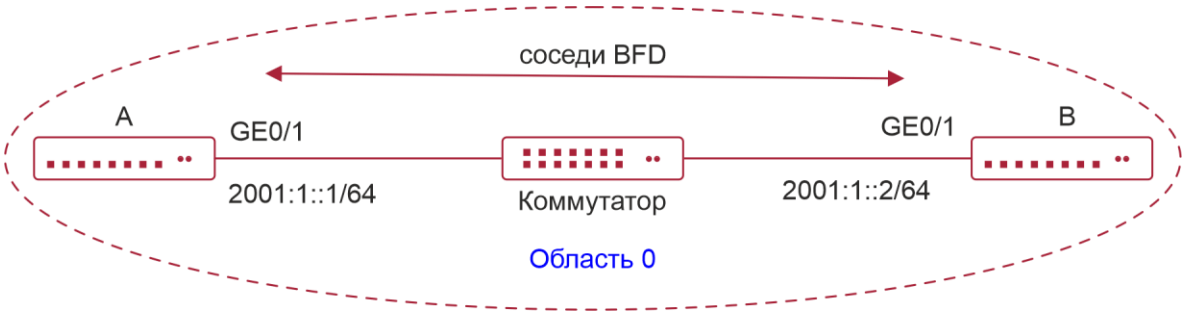


Рисунок 5-21.

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. (Опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (пропущено) • Настройте параметры BFD для интерфейсов всех маршрутизаторов. • Сопоставьте OSPF с BFD на всех маршрутизаторах
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet0/1)#bfd interval 200 min_rx 200 multiplier 5 A(config)# ipv6 router ospf 1 A(config-router)#bfd all-interfaces
B	B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 2/1)#bfd interval 200 min_rx 200 multiplier 5 B(config)# ipv6 router ospf 1 B(config-router)#bfd all-interfaces
Проверка	• На маршрутизаторе A и маршрутизаторе B убедитесь, что состояние BFD — «Включено» (Up). • Отключите маршрутизатор B от коммутатора. На маршрутизаторе A убедитесь, что сосед отключен во время BFD, а соответствующий маршрут OSPF удален
A	A# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State BFD State Dead Time Instance ID Interface

	2.2.2.2 1 Full/BDR Up 00:00:35 0 GigabitEthernet 0/1
B	B# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State BFD State Dead Time Instance ID Interface 1.1.1.1 1 Full/DR Up 00:00:35 0 GigabitEthernet 0/1

5.4.13. Включение GR

5.4.13.1. Эффект конфигурации

- Когда распределенный маршрут переключает сервисы с активной платы на резервную, пересылка трафика продолжается и не прерывается.
- При перезапуске процесса OSPF пересылка данных продолжается и не прерывается.

5.4.13.2. Примечания

- Необходимо настроить основные функции OSPF.
- Соседний маршрутизатор должен поддерживать функцию GR helper.
- Период отсрочки не может быть короче времени dead соседнего маршрутизатора.

5.4.13.3. Шаги настройки

Настройка функции GR OSPF

- (Опционально) Эта функция включена по умолчанию. Рекомендуется сохранить конфигурацию по умолчанию.
- Выполните эту настройку на маршрутизаторах, где срабатывает переключение горячего резерва или перезапускается процесс OSPF.

Настройка функции OSPF GR Helper

- (Опционально) Эта функция включена по умолчанию. Рекомендуется сохранить конфигурацию по умолчанию.
- Выполните эту настройку на маршрутизаторе, если срабатывает переключение на горячий резерв или процесс OSPF перезапускается на соседе этого маршрутизатора.

5.4.13.4. Проверка

- Когда распределенный маршрутизатор переключает сервисы с активной платы на резервную, пересылка данных продолжается и трафик не прерывается.
- При перезапуске процесса OSPF пересылка данных продолжается, а трафик не прерывается.

5.4.13.5. Связанные команды

Настройка функции GR OSPF

Команда	**graceful-restart** [**grace-period** *grace-period*|**inconsistent-lsa-checking**]
Описание параметра	**grace-period** *grace-period*: указывает период отсрочки, который представляет собой максимальное время от возникновения сбоя OSPF до завершения GR OSPF. Значение периода отсрочки варьируется от 1 до 1800 секунд. Значение по умолчанию — 120 с. **inconsistent-lsa-checking**: включает обнаружение топологических изменений. Если обнаружено какое-либо топологическое изменение, OSPF завершает процесс GR для завершения конвергенции. После включения GR обнаружение топологических изменений включается по умолчанию
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Функция GR настроена на основе процесса OSPF. Вы можете настроить разные параметры для разных процессов OSPF в зависимости от реальных условий. Эта команда используется для настройки возможности GR restarter-а устройства. Период отсрочки — это максимальное время всего процесса GR, в течение которого состояние канала перестраивается таким образом, чтобы восстанавливалось исходное состояние процесса OSPF. По истечении периода отсрочки OSPF выходит из состояния GR и выполняет общие операции OSPF. Запустите команду **graceful-restart**, чтобы установить период отсрочки равным 120 с. Команда **graceful-restart grace-period** позволяет вам явно изменить период отсрочки. Предпосылкой успешного выполнения GR и бесперебойной пересылки является стабильность топологии. Если топология меняется, OSPF быстро сходится, не дожидаясь дальнейшего выполнения GR, что позволяет избежать длительной пересылки black-hole. • Отключение обнаружения топологии: если OSPF не может сходиться вовремя при изменении топологии во время процесса горячего резерва, через долгое время может возникнуть пересылка black-hole. • Включение обнаружения топологии: пересылка может быть прервана, когда обнаружение топологии включено, но время прерывания намного короче, чем когда обнаружение топологии отключено. В большинстве случаев рекомендуется включить определение топологии. В особых сценариях обнаружение топологии можно отключить, если топология изменится после процесса горячего резерва, но можно гарантировать, что пересылка black-hole не

	появится в течение длительного времени. Это может минимизировать время прерывания пересылки во время процесса горячего резерва. Если функция Fast Hello включена, функцию GR включить невозможно

Настройка функции OSPF GR Helper

Команда	**graceful-restart helper** { **disable** |**strict-lsa-checking** | **internal-lsa-checking**}
Описание параметра	**disable**: запрещает устройству выступать в качестве GR helper-а для другого устройства. **strict-lsa-checking**: указывает, что изменения в LSA от типа 1 до типа 5 и типа 7 будут проверяться в течение периода, в течение которого устройство действует как GR helper для определения изменений в сети. Если сеть изменится, устройство перестанет выступать в роли GR helper-а. **internal-lsa-checking**: указывает, что изменения в LSA от типа 1 до типа 3 будут проверяться в течение периода, в течение которого устройство действует как GR helper для определения изменений в сети. Если сеть изменится, устройство перестанет выступать в роли GR helper-а
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Эта команда используется для настройки возможности GR helper-а маршрутизатора. Когда соседний маршрутизатор реализует GR, он отправляет Grace-LSA для уведомления всех соседних маршрутизаторов. Если функция GR helper включена на локальном маршрутизаторе, локальный маршрутизатор становится GR helper-ом при получении Grace-LSA и помогает соседу завершить GR. Опция **disable** указывает, что GR helper не предоставляется ни для одного устройства, реализующего GR. После того как устройство становится GR helper-ом, изменения в сети по умолчанию не обнаруживаются. Если в сети происходят какие-либо изменения, топология сети сходится после завершения GR. Если вы хотите, чтобы изменения в сети могли быть быстро обнаружены во время процесса GR, вы можете настроить **strict-lsa-checking** для проверки LSA типов от 1 до 5 и типа 7, которые указывают сетевую информацию, или **internal-lsa-checking** для проверки LSA типов от 1 до 3, указывающие внутренние маршруты домена AS. Если масштаб сети велик, рекомендуется отключить параметры проверки LSA (**strict-lsa-checking** и **internal-lsa-checking**), поскольку изменения в региональной сети могут привести к прекращению работы GR и, как следствие, к снижению конвергенции всей сети

5.4.13.6. Пример конфигурации

Сценарий:

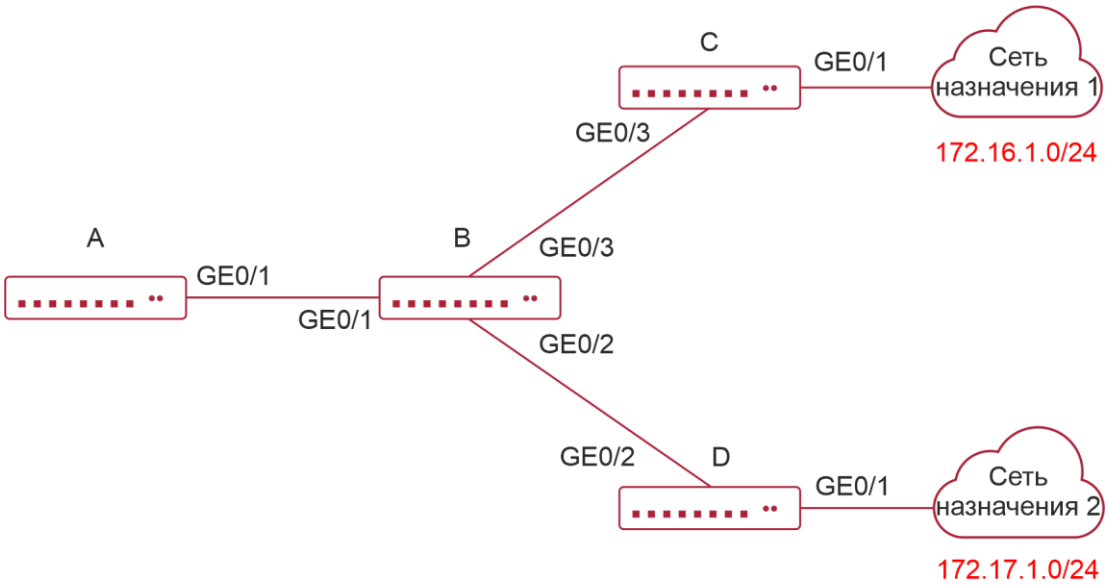


Рисунок 5-22.

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. (пропущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (пропущено) • На маршрутизаторах A, C и D включите функцию GR helper. (Эта функция включена по умолчанию.) • На маршрутизаторе B включите функцию GR
B	B# configure terminal B(config)# ipv6 router ospf1 B(config-router)# graceful-restart
Проверка	• Запустите переключение на горячий резерв на маршрутизаторе B и убедитесь, что таблицы маршрутизации сети назначения 1 и 2 остаются неизменными на маршрутизаторе A во время переключения. • Запустите переключение на горячий резерв на маршрутизаторе B, пропингуйте сеть назначения 1 от маршрутизатора A и убедитесь, что пересылка трафика не прерывается во время переключения

5.4.13.7. Распространенные ошибки

Пересылка трафика прерывается во время процесса GR, поскольку настроенный период отсрочки короче, чем время dead соседнего маршрутизатора.

5.4.14. Настройка функций управления сетью

5.4.14.1. Эффект конфигурации

Используйте программное обеспечение управления сетью для управления параметрами OSPF и мониторинга рабочего состояния OSPF.

5.4.14.2. Примечания

- Необходимо настроить основные функции OSPF.
- Перед включением функции OSPF MIB необходимо включить функцию MIB сервера SNMP.
- Перед включением функции Trap OSPF необходимо включить функцию Trap SNMP-сервера.
- Перед выводом журналов OSPF необходимо включить функцию ведения журнала на устройстве.

5.4.14.3. Шаги настройки

Связывание MIB с процессом OSPF

- (Опционально) Эта конфигурация необходима, если вы хотите использовать программное обеспечение управления сетью для управления параметрами указанного процесса OSPF.
- Выполните эту настройку на всех маршрутизаторах.

Включение функции Trap

- (Опционально) Эта конфигурация необходима, если вы хотите использовать программное обеспечение управления сетью для мониторинга рабочего состояния OSPF.
- Выполните эту настройку на всех маршрутизаторах.

Настройка функции ведения журналов

- (Опционально) Эта функция включена по умолчанию. Рекомендуется сохранить конфигурацию по умолчанию. Если вы хотите уменьшить вывод журнала, отключите эту функцию.
- Выполните эту настройку на всех маршрутизаторах.

5.4.14.4. Проверка

- Используйте программное обеспечение управления сетью для управления параметрами OSPF.
- Используйте программное обеспечение управления сетью для мониторинга рабочего состояния OSPF.

5.4.14.5. Связанные команды

Связывание MIB с процессом OSPF

Команда	**enable mib-binding**
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	MIB OSPFv2 не содержит информации о процессе OSPFv3. Таким образом, вы можете выполнять операции только над одним процессом OSPFv2 через SNMP. По умолчанию MIB OSPFv3 привязан к процессу OSPFv3 с наименьшим идентификатором процесса, и все пользовательские операции применяются к этому процессу. Если вы хотите выполнять операции с указанным процессом OSPFv3 через SNMP, запустите эту команду, чтобы связать MIB с процессом

Включение функции Trap

Команда	**enable traps**[**error** [**IfConfigError**| **IfRxBadPacket** | **VirtIfConfigError** | **VirtIfRxBadPacket**] | **state-change**[**IfStateChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **VirtIfStateChange** | **VirtNbrStateChange** | **RestartStatusChange** | **NbrRestartHelperStatusChange** | **VirtNbrRestartHelperStatusChange**]]
Описание параметра	**IfConfigError**: указывает на то, что произошла ошибка конфигурации параметров интерфейса. **IfRxBadPacket**: указывает, что интерфейс получил неверный пакет. **VirtIfConfigError**: указывает на то, что произошла ошибка конфигурации параметров виртуального интерфейса. **VirtIfRxBadPacket**: указывает, что виртуальный интерфейс получил неверный пакет. **IfStateChange**: указывает на изменение состояния интерфейса. **NbrStateChange**: указывает на изменение состояния соседа. **NssaTranslatorStatusChange**: указывает на изменения состояния NSSA. **VirtIfStateChange**: указывает на изменение состояния виртуального интерфейса. **VirtNbrStateChange**: указывает на изменение состояния виртуального соседа. **RestartStatusChange**: указывает на изменение состояния GR локального устройства. **NbrRestartHelperStatusChange**: указывает на изменение состояния процесса GR соседа.

	VirtNbrRestartHelperStatusChange: указывает на изменение состояния GR виртуального соседа
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Функция, настроенная этой командой, ограничена командой **snmp-server**. Вы можете настроить **snmp-server enable traps ospf**, а затем включить команду **enable traps**, прежде чем соответствующие Trap OSPF смогут быть правильно отправлены. Эта команда не ограничена MIB, связанным с процессом. Функцию Trap можно включить одновременно для разных процессов

Настройка функции ведения журналов

Команда	**log-adj-changes**[**detail**]
Описание параметра	**detail**: записывает всю информацию об изменении статуса
Командный режим	Режим конфигурации процесса маршрутизации OSPF

5.4.14.6. Пример конфигурации

Сценарий:



Рисунок 5-23.

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. (Опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (опущено) • Свяжите MIB с процессом OSPF на маршрутизаторе A. • Включите функцию Trap на маршрутизаторе A
A	A# configure terminal A(config)#snmp-server host 192.168.2.2 traps version 2c public A(config)#snmp-server community public rw

	A(config)#snmp-server enable traps A(config)# A(config)# ipv6 routerospf 10 A(config-router)# enable mib-binding A(config-router)# enable traps
Проверка	Используйте инструмент MIB для чтения и установки параметров OSPF, а также отображения рабочего состояния OSPF

5.4.15. Изменение параметров управления протоколом

5.4.15.1. Эффект конфигурации

Измените параметры управления протоколом, чтобы изменить статус работы протокола.

5.4.15.2. Примечания

- Необходимо настроить основные функции OSPF.
- Время dead соседа не может быть короче интервала Hello.

5.4.15.3. Шаги настройки

Настройка интервала Hello

- (Опционально) Рекомендуется сохранить конфигурацию по умолчанию.
- Выполните эту настройку на маршрутизаторах на обоих концах канала.

Настройка интервала dead

- (Опционально) Рекомендуется сохранить конфигурацию по умолчанию. Эту конфигурацию можно изменить, если вы хотите ускорить конвергенцию OSPF при сбое канала.
- Выполните эту настройку на маршрутизаторах на обоих концах канала.

Настройка интервала повторной передачи LSU

(Опционально) Рекомендуется изменить эту конфигурацию, если в пользовательской среде существует много маршрутов и перегрузка сети серьезна.

Настройка времени генерации LSA

(Опционально) Рекомендуется сохранить конфигурацию по умолчанию.

Настройка времени обновления группы LSA

- (Опционально) Рекомендуется сохранить конфигурацию по умолчанию. Эту конфигурацию можно настроить, если в пользовательской среде существует много маршрутов.
- Выполните эту настройку на ASBR или ABR.

Настройка задержки повторного приема LSA

(Опционально) Рекомендуется сохранить конфигурацию по умолчанию.

Настройка задержки вычисления SPF

(Опционально) Эту конфигурацию можно изменить, если часто происходит flapping сети.

Настройка задержки расчета межобластного маршрута

- (Опционально) Рекомендуется сохранить конфигурацию по умолчанию.
- Выполните эту настройку на всех маршрутизаторах.

5.4.15.4. Проверка

Запустите команды **show ipv6 ospf** и **show ipv6 ospf neighbor**, чтобы отобразить рабочие параметры и состояние протокола.

5.4.15.5. Связанные команды

Настройка интервала Hello

Команда	**ipv6 ospf hello-interval** *seconds*
Описание параметра	*seconds*: указывает интервал, с которым OSPF отправляет пакет Hello. Измеряется в секундах. Значение варьируется от 1 до 65 535
Командный режим	Режим настройки интерфейса
Руководство по использованию	Интервал Hello содержится в пакете Hello. Более короткий интервал Hello указывает на то, что OSPF может быстрее обнаруживать топологические изменения, но сетевой трафик увеличивается. Интервал Hello должен быть одинаковым на всех маршрутизаторах в одном сегменте сети. Если вы хотите вручную изменить интервал dead соседа, убедитесь, что интервал dead соседа длиннее интервала Hello

Настройка интервала dead

Команда	**ipv6 ospf dead-interval** *seconds*
Описание параметра	*seconds*: указывает время, когда сосед объявлен потерянным. Измеряется в секундах. Значение варьируется от 2 до 65 535
Командный режим	Режим настройки интерфейса
Руководство по использованию	Dead-интервал OSPF содержится в пакете Hello. Если OSPF не получает пакет Hello от соседа в течение интервала dead, он объявляет соседа недействительным и удаляет эту запись соседа из списка соседей. По умолчанию dead-интервал в четыре раза превышает интервал Hello. Если интервал Hello изменяется, dead-интервал изменяется автоматически. При использовании этой команды для изменения интервала dead вручную обратите внимание на следующие проблемы: 1. Dead-интервал не может быть короче интервала Hello.

	2. Dead-интервал должен быть одинаковым на всех маршрутизаторах в одном сегменте сети

Настройка задержки передачи LSU

Команда	**ipv6 ospf transmit-delay** *seconds*
Описание параметра	*seconds*: указывает задержку передачи LSU на интерфейсе OSPF. Измеряется в секундах. Значение варьируется от 0 до 65 535
Командный режим	Режим настройки интерфейса
Руководство по использованию	Перед передачей пакета LSU поля Age во всех LSA в этом пакете будут увеличиваться в зависимости от величины, указанной командой **ip ospf transmit-delay**. Учитывая задержку передачи и задержку line propagation на интерфейсе, необходимо установить задержку передачи LSU на большее значение для низкоскоростной линии связи или интерфейса. Задержка передачи LSU виртуального канала определяется параметром **transmit-delay** в команде **area virtual-link**. Если значение поля Age LSA достигает 3600, пакет будет передан повторно или будет запрошена повторная передача. Если LSA не будет обновлено вовремя, LSA с истекшим сроком действия будет удалено из LSDB

Настройка интервала повторной передачи LSU

Команда	**ipv6 ospf retransmit-interval** seconds
Описание параметра	*seconds*: указывает интервал повторной передачи LSU. Измеряется в секундах. Значение варьируется от 0 до 65 535. Этот интервал должен быть больше, чем задержка передачи пакетов данных между двумя соседями
Командный режим	Режим настройки интерфейса
Руководство по использованию	После того, как маршрутизатор завершит отправку пакета LSU, этот пакет все еще сохраняется в очереди буфера передачи. Если подтверждение от соседа не получено в течение времени, определенного командой **ip ospf retransmit-interval**, маршрутизатор повторно передает пакет LSU. Задержку повторной передачи можно установить на большее значение на последовательной линии связи или виртуальном канале, чтобы предотвратить ненужную повторную передачу. Задержка повторной передачи LSU виртуального канала определяется параметром **retransmit-interval** в команде **area virtual-link**

Настройка времени генерации LSA

Команда	**timers throttle lsa all** *delay-time hold-time max-wait-time*
Описание параметра	*delay-time*: указывает минимальную задержку для генерации LSA. Первый LSA в базе данных всегда генерируется мгновенно. Значение варьируется от 0 до 600 000. Единица измерения — мс. *hold-time*: указывает минимальный интервал между первым обновлением LSA и вторым обновлением LSA. Значение варьируется от 1 до 600 000. Единица измерения — мс. *max-wait-time*: указывает максимальный интервал между двумя обновлениями LSA, когда LSA обновляется непрерывно. Этот интервал также используется для определения того, обновляется ли LSA постоянно. Значение варьируется от 1 до 600 000. Единица измерения — мс
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Если при изменении канала возникают высокие требования к конвергенции, вы можете установить *delay-time* на меньшее значение. Вы также можете соответствующим образом увеличить значения предыдущих параметров, чтобы уменьшить загрузку ЦП. При настройке этой команды значение *hold-time* не может быть меньше значения *delay-time*, а значение *max-wait-time* не может быть меньше значения *hold-time*

Настройка времени обновления группы LSA

Команда	**timers pacing lsa-group** *seconds*
Описание параметра	*seconds*: указывает интервал pacing группы LSA. Значение варьируется от 10 до 1800. Измеряется в секундах
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	У каждого LSA есть время жизни (возраст LSA). Когда возраст LSA достигает 1800 секунд, необходимо обновление, чтобы предотвратить очистку LSA, поскольку их возраст достигает максимума. Если обновление LSA и вычисление устаревания выполняются для каждого LSA, устройство будет потреблять много ресурсов ЦП. Чтобы эффективно использовать ресурсы ЦП, вы можете обновить LSA по группам на устройстве. Интервал группового обновления называется интервалом pacing группы. Операция обновления группы заключается в организации LSA, сгенерированных в пределах интервала pacing группы, в группу и обновлении группы в целом.

	Если общее количество LSA не меняется, больший интервал pacing группы указывает на то, что после тайм-аута необходимо обработать больше LSA. Чтобы поддерживать стабильность ЦП, количество процессов LSA при каждом тайм-ауте не может быть слишком большим. Если количество LSA велико, рекомендуется уменьшить интервал pacing группы. Например, если в базе данных имеется 1000 LSA, вы можете уменьшить интервал pacing; если имеется от 40 до 100 LSA, интервал pacing можно установить на 10–20 минут

Настройка интервала обновления группы LSA

Команда	**timers pacing lsa-transmit** *transmit-time transmit-count*
Описание параметра	*transmit-time*: указывает интервал передачи группы LSA. Значение варьируется от 10 до 600 000. Единица измерения — мс. *transmit-count*: указывает количество пакетов LS-UPD в группе. Значение варьируется от 1 до 200
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Если количество LSA велико и нагрузка на устройство в среде велика, правильная настройка *transmit-time* и *transmit-count* может ограничить количество пакетов LS-UPD, рассылаемых по сети. Если загрузка ЦП невелика и нагрузка на полосу пропускания сети невелика, уменьшение значения *transmit-time* и увеличение значения *transmit-count* может ускорить конвергенцию среды

Настройка задержки повторного приема LSA

Команда	**timers lsa arrival** *arrival-time*
Описание параметра	*arrival-time*: указывает задержку, после которой будет получен тот же LSA. Значение варьируется от 0 до 600 000. Единица измерения — мс
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Никакая обработка не выполняется, если тот же LSA получен в течение указанного времени

Настройка задержки вычисления SPF

Команда	**timers throttle spf** *spf-delay spf-holdtime spf-max-waittime*
Описание параметра	*spf-delay*: указывает задержку вычисления SPF. Единица измерения — мс. Значение варьируется от 1 до 600 000. При обнаружении

	топологического изменения процесс маршрутизации OSPF запускает вычисление SPF по крайней мере после истечения *spf-delay*. *spf-holdtime*: указывает минимальный интервал между двумя вычислениями SPF. Единица измерения — мс. Значение варьируется от 1 до 600 000. *spf-max-waittime*: указывает максимальный интервал между двумя вычислениями SPF. Единица измерения — мс. Значение варьируется от 1 до 600 000. *number*: указывает метрику суммарного маршрута
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	*spf-delay* указывает минимальное время между возникновением топологического изменения и началом расчета SPF. *spf-holdtime* указывает минимальный интервал между первым вычислением SPF и вторым вычислением SPF. После этого интервал между двумя вычислениями SPF должен быть как минимум в два раза больше предыдущего интервала. Когда интервал достигает *spf-max-waittime*, интервал не может снова увеличиться. Если интервал между двумя вычислениями SPF уже превышает требуемое минимальное значение, интервал вычисляется, начиная с *spf-holdtime*. Вы можете установить *spf-delay* и *spf-holdtime* на меньшие значения, чтобы ускорить сходимость топологии, и установите для *spf-max-waittime* большее значение, чтобы уменьшить вычисление SPF. Гибкие настройки могут быть использованы в зависимости от стабильности топологии сети. По сравнению с командой **timers spf**, эта команда поддерживает более гибкие настройки для ускорения скорости сходимости вычислений SPF и дальнейшего снижения системных ресурсов, потребляемых вычислением SPF, когда топология постоянно меняется. Поэтому для настройки рекомендуется использовать команду **timers throttle spf**. 1. Значение *spf-holdtime* не может быть меньше значения *spf-delay*; в противном случае для *spf-holdtime* будет автоматически установлено значение *spf-delay*. 2. Значение *spf-max-waittime* не может быть меньше значения *spf-holdtime*; в противном случае для *spf-max-waittime* будет автоматически установлено значение *spf-holdtime*. 3. Конфигурации **timers throttle spf** и **timers spf** взаимно перезаписываются. 4. Если оба **timers throttle spf** и **timers spf** не настроены, значения таймеров **timers throttle spf** по умолчанию имеют преимущественную силу

Настройка задержек вычислений межобластных и внешних маршрутов

Команда	**timers throttle route**{**inter-area** *ia-delay*|**ase** *ase-delay*}
Описание параметра	**inter-area** *ia-delay*: указывает задержку расчета маршрута между областями. Единица измерения — мс. Значение варьируется от 0 до 600 000. **ase** *ase-delay*: указывает задержку расчета внешнего маршрута. Единица измерения — мс. Значение варьируется от 0 до 600 000
Командный режим	Режим конфигурации процесса маршрутизации OSPF
Руководство по использованию	Если предъявляются строгие требования ко времени конвергенции сети, используйте значение по умолчанию. Если в сети существует множество межобластных или внешних маршрутов и сеть нестабильна, отрегулируйте задержки и оптимизируйте вычисление маршрутов, чтобы снизить нагрузку на устройство

5.4.15.6. Пример конфигурации

Настройка интервала Hello и интервала dead

Сценарий:



Рисунок 5-24.

Шаги настройки	• Включите IPv6 на интерфейсах всех маршрутизаторов. (Опущено) • Настройте базовые функции OSPF на всех маршрутизаторах. (пропущено) • Настройте интервал Hello и dead-интервал на всех маршрутизаторах
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ipv6 ospf hello-interval 15 A(config-if-GigabitEthernet 0/1)# ipv6 ospf dead-interval 50

B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ipv6 ospf hello-interval 15 A(config-if-GigabitEthernet 0/1)# ipv6 ospf dead-interval 50
Проверка	• Проверьте параметры интерфейса на маршрутизаторах A и B. Убедитесь, что интервал Hello составляет 10 с, а интервал dead — 50 с. • На маршрутизаторах A и B проверьте правильность информации о соседе OSPF
A	A# show ipv6 ospf interface GigabitEthernet 0/1 is up, line protocol is up Interface ID 2 IPv6 Prefixes fe80::2d0:f8ff:fe22:3346/64 (Link-Local Address) OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0 Router ID 1.1.1.1,Network Type BROADCAST, Cost: 1 Transmit Delay is 1 sec, State DR, Priority 1 Timer interval configured, Hello 15, Dead 50, Wait 40, Retransmit 10 Hello due in 00:00:06 Neighbor Count is 1, Adjacent neighbor count is 1 Hello received 40 sent 40, DD received 17 sent 9 LS-Req received 1 sent 3, LS-Upd received 6 sent 5 LS-Ack received 3 sent 4, Discarded 1 A# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.21 Full/BDR 00:00:30 0 GigabitEthernet 0/1
B	B# show ipv6 ospf interface GigabitEthernet 0/1 is up, line protocol is up Interface ID 2 IPv6 Prefixes fe80::2d0:f8ff:fe22:3446/64 (Link-Local Address) OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0

	Router ID 2.2.2.2,Network Type BROADCAST, Cost: 1 Transmit Delay is 1 sec, State BDR, Priority 1 Timer interval configured, Hello 15, Dead 50, Wait 40, Retransmit 10 Hello due in 00:00:06 Neighbor Count is 1, Adjacent neighbor count is 1 Hello received 40 sent 40, DD received 17 sent 9 LS-Req received 1 sent 3, LS-Upd received 6 sent 5 LS-Ack received 3 sent 4, Discarded 1 B# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 1.1.1.11 Full/DR 00:00:38 0 GigabitEthernet 0/1

5.4.15.7. Распространенные ошибки

Настроенное время dead соседа короче интервала Hello.

5.5. Мониторинг

5.5.1. Очистка

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

Описание	Команда
Очищает и сбрасывает процесс OSPF	**clear ipv6 ospf** [*process-id*]**process**

5.5.2. Отображение

Описание	Команда
Отображает конфигурации процесса OSPF	**show ipv6 ospf** [*process-id*]
Отображает информацию о OSPF LSDB	**show ipv6 ospf**[*process- id*] **database**[*lsa-type* [**adv-router** *router-id*]]

Описание	Команда
Отображает интерфейсы с поддержкой OSPF	**show ipv6 ospf** [*process-id*] **interface** [*interface-type interface number* | **brief**]
Отображает список соседей OSPF	**show ipv6 ospf**[*process- id*] **neighbor**[*interface-type interface number*[**detail**]| *neighbor-id* |**detail**]
Отображает таблицу маршрутизации OSPF	**show ipv6 ospf** [*process-id*] **route**[**count**]
Отображает суммарный маршрут перераспределенных маршрутов OSPF	**show ipv6 ospf** [*process-id*] **summary-prefix**
Отображает информацию о топологии сети OSPF	**show ipv6 ospf** [*process- id*] **topology** [**area** *area-id*]
Отображает виртуальные каналы OSPF	**show ipv6 ospf** [*process-id*] **virtual-links**

5.5.3. Отладка

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

Описание	Команда
Отладка событий OSPF	**debug ipv6 ospf events** [**abr**|**asbr**|**os**|**router**| **vlink**]
Отладка интерфейсов OSPF	**debug ipv6 ospf ifsm** [**events**|**status**|**timers**]
Отладка соседей OSPF	**debug ipv6 ospf nfsm** [**events** | **status** | **timers**]
Отладка OSPF NSM	**debug ipv6 ospf nsm** [**interface** | **redistribute** | **route**]
Отладка LSA OSPF	**debug ipv6 ospf lsa** [**flooding** | **generate** | **install** | **maxage** | **refresh**]
Отладка пакетов OSPF	**debug ipv6 ospf packet** [**dd**|**detail**|**hello**|**ls-ack**|**ls-request**|**lsupdate**|**recv**|**send**]
Отладка маршрутов OSPF	**debug ipv6 ospf route** [**ase** | **ia** | **install** | **spf** | **time**]

6. НАСТРОЙКА IS-IS

6.1. Обзор

Intermediate System to Intermediate System (IS-IS) — это расширяемый, надежный и простой в использовании Interior Gateway Protocol (IGP) для выбора маршрута, применимый к сети с двойной средой IP-ISO CLNS (ISO CLNS — сокращение от Международной организации по стандартизации сетевого сервиса без установления соединения).

IS-IS имеет общие характеристики протокола состояния канала. Он отправляет пакеты Hello для обнаружения и поддержания отношений между соседями, а также отправляет блоки данных протокола состояния канала (LSP) соседям, чтобы объявить о своем состоянии канала. IS-IS поддерживает маршрутизацию Level-1 и маршрутизацию Level-2. Все устройства на одном уровне поддерживают одну и ту же базу данных состояния каналов (LSDB), в которой хранятся LSP, сгенерированные устройствами для уведомления друг друга о топологии сети уровня. Каждое устройство использует алгоритм Dijkstra Shortest Path First (SPF) для расчета наилучшего маршрута, выбора пути и быстрой сходимости.

6.1.1. Протоколы и стандарты

- RFC1142: протокол внутридоменной маршрутизации OSI IS-IS.
- RFC1195: использование OSI IS-IS для маршрутизации в TCP/IP и двойных средах.
- RFC3786: увеличение числа фрагментов PDU состояния канала промежуточной системы (LSP) до уровня промежуточной системы (IS-IS), превышающее предел в 256.
- RFC3373: трехстороннее подтверждение связи между промежуточными системами (IS-IS) по принципу «точка-точка».
- RFC3358: дополнительные контрольные суммы в промежуточной системе (IS-IS).
- RFC3784: расширения между промежуточными системами (IS-IS) для Traffic Engineering (TE).
- RFC2763: механизм динамического обмена именами хостов для IS-IS.
- RFC6119(draft-ietf-isis-ipv6-te-00): управление трафиком IPv6 в IS-IS.
- RFC 2966: распространение префиксов по всему домену с помощью двухуровневого IS-IS.

6.2. Приложения

Приложение	Описание
Планарная топология	Планарная топология применима к небольшой сети. На начальном этапе построения крупномасштабной сети основные устройства развертываются для формирования области на основе планарной топологии
Иерархическая топология	Иерархическая топология применима к крупномасштабной сети с частым flapping-ом каналов

6.2.1. Планарная топология

6.2.1.1. Сценарий

Планарная топология формируется устройствами, находящимися в одной области.

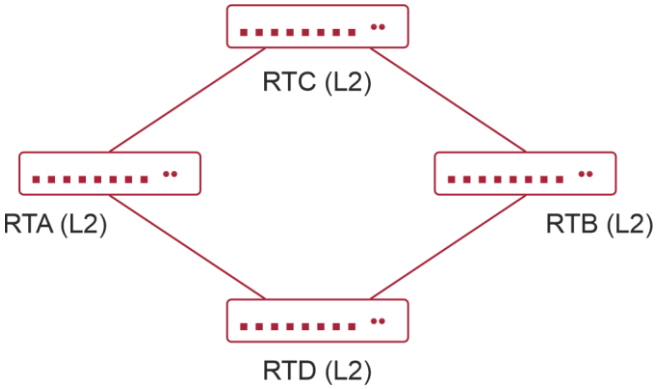


Рисунок 6-1. Планарная топология

6.2.1.2. Развертывание

Чтобы облегчить будущее расширение и снизить нагрузку на устройства, настройте устройства в планарной топологии как устройства Level-2.

6.2.2. Иерархическая топология

6.2.2.1. Сценарий

Иерархическая топология делит сеть на уровень ядра, уровень конвергенции и уровень доступа. См. Рисунок 6-2.

- Обобщение маршрутов на уровне конвергенции облегчается планированием адресов.
- При наличии первичных и вторичных маршрутов устройства на уровне конвергенции передают маршруты Level-2 в области Level-1.

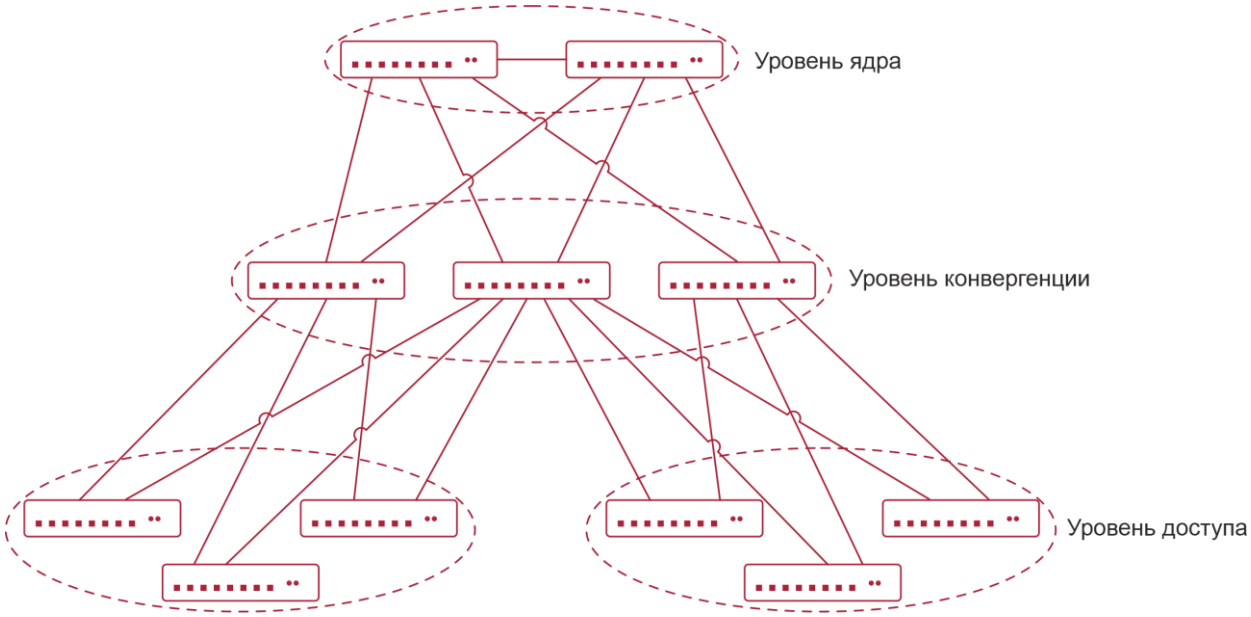


Рисунок 6-2. Иерархическая топология

ПРИМЕЧАНИЕ: устройства на уровне ядра должны быть подключены последовательно.

6.2.2.2. Развертывание

- Спроектируйте топологию сети, начиная с уровня ядра.
- Настройте устройства на уровне ядра как устройства Level-2.
- Настройте устройства на уровне конвергенции как устройства Level-1/Level-2.
- Настройте устройства на уровне доступа как устройства Level-1.

6.3. Функции

6.3.1. Базовые определения

Конечная система (ES)

ES — это устройство, не являющееся маршрутизатором, например хост.

Промежуточная система (IS)

IS — это маршрутизатор, который является основным устройством, используемым для передачи информации о маршрутизации и создания маршрутов в IS-IS.

Протокол обмена маршрутизацией между конечной системой и промежуточной системой (ES-IS)

ES-IS — это протокол, используемый для связи между ES и IS в рамках взаимодействия открытых систем (OSI) для динамического обнаружения соседских отношений Level-2.

Домен

Набор IS в одном домене маршрутизации (RD) использует один и тот же протокол маршрутизации для обмена информацией о маршрутизации.

Область

RD можно разделить на несколько областей.

Полный серийный номер PDU (CSNP)

CSNP отправляются назначенной промежуточной системой (DIS) каждые 10 секунд для синхронизации состояний каналов в broadcast-сети.

PDU частичного порядкового номера (PSNP)

PSNP передаются по каналу «точка-точка» (P2P) для подтверждения LSP или запроса LSP в broadcast-сети.

Сетевой протокол без установления соединения (CLNP)

CLNP — это протокол OSI, используемый для передачи данных и сообщений об ошибках на сетевом уровне. Он аналогичен протоколу IP.

Сетевой сервис без установления соединения (CLNS)

CLNS представляет собой тип ненадежного соединения и не требует настройки схемы перед передачей данных.

Назначенная промежуточная система (DIS)

Подобно маршрутизатору DIS (DR) в режиме Open Shortest Path First (OSPF), DIS распространяет LSP на другие машины в локальной сети (LAN). Отношения соседства устанавливаются не только между DIS и другими машинами, но также и между этими машинами. Этой характеристикой не обладает OSPF.

Пакет Hello

Пакеты Hello используются для установления и поддержания отношений соседства.

LSP

LSP описывают состояния каналов, аналогично объявлению состояния канала (LSA) в OSPF, но первые не зависят от информации TCP/IP. LSP подразделяются на LSP Level-1 и LSP Level-2, в зависимости от различных типов маршрутов.

Селектор сети (NSEL)

NSEL (иногда называемый SEL) определяет целевой сервис протокола сетевого уровня. Он аналогичен порту TCP/UDP для сервиса верхнего уровня в протоколе IP. В IS-IS SEL обычно имеет значение 00, чтобы указать устройство.

Точка доступа к сетевым сервисам (NSAP)

NSAP — это полный адрес CLNS, включая адрес OSI и процессы высокого уровня. Он состоит из идентификатора области, идентификатора системы и SEL. Если для SEL установлено значение 00, NSAP представляет собой заголовок сетевого объекта (NET), аналогичный IP-адресу и номеру протокола.

Точка подключения подсети (SNPA)

SNPA обеспечивает физические соединения и сервисы сетевого уровня. Он аналогичен MAC-адресу, используемому в протоколе IP, идентификатору соединения канала передачи данных (DLCI), используемому Frame Relay (FR), или управлению каналом передачи данных высокого уровня (HDLC) в глобальной сети (WAN).

Маршрут Level-1

Маршрут Level-1 — это внутриобластной маршрут, который получает соответствующую информацию только внутри этой области. Чтобы добраться до других областей, вам

необходимо сохранить на Level-1 маршрут по умолчанию, предназначенный для ближайшего Level-2.

Маршрут Level-2

Маршрут Level-2 представляет собой межобластной магистральный маршрут. Level-1 и Level-2 не могут быть соединены напрямую.

Маршрут Level-1/Level-2

Маршрут Level-1/Level-2 — это пограничный маршрут, соединяющий маршрут Level-1 и маршрут Level-2. Он поддерживает две базы данных для маршрутов Level-1 и Level-2 соответственно. Он похож на пограничный маршрутизатор области (ABR) в OSPF.

Псевдоузел

Псевдоузел идентифицирует broadcast-подсеть (LAN) и позволяет broadcast-среде работать как виртуальное устройство, интерфейсом которого является маршрут. Отношения маршрут-псевдоузел управляются DIS.

Название сетевого объекта (NET)

NET является частью адреса OSI и описывает идентификатор области и идентификатор системы, но не определяет NSEL, который содержится в NSAP указанной системы.

Circuit

Circuit — это термин, связанный с интерфейсом, используемый в IS-IS. В то время как NSAP и NET обозначают целые устройства, Circuit указывает на интерфейс. Идентификатор Circuit P2P-интерфейса имеет длину один байт. Например, идентификатор Circuit HDLC — 0x00. В broadcast-сети (например, локальной сети) идентификатор Circuit имеет длину семь байт, включая идентификатор системы, например 1921.6800.0001.01.

ПРИМЕЧАНИЕ: подробную информацию о терминах, связанных с IS-IS, см. в ISO 10589 и RFC1195.

6.4. Обзор

Особенность	Описание
Иерархия сети IS-IS	Сеть IS-IS делится на уровень 1 и уровень 2. Узлы, на которых устройства обмениваются информацией в одной области, образуют один Уровень (Level-1)
Режим кодирования адреса IS-IS	Адрес IS-IS называется NET и состоит из идентификатора области, идентификатора системы и идентификатора NSAP
Типы пакетов IS-IS	Существует три типа пакетов IS-IS: LSP, пакет Hello IS-IS (IIH PDU) и пакет серийного номера (SNP), классифицированные на CSNP и PSNP
Выборы DIS	DIS моделирует множественные каналы доступа в качестве псевдоузла и генерирует LSP для псевдоузла. Псевдоузел устанавливает связь с каждым устройством в локальной сети и запрещает прямую связь между устройствами

Особенность	Описание
Поддерживаемые IS-IS типы TLV	IS-IS поддерживает 21 тип Type-Length-Value (TLV)
Расширение фрагмента LSP	IS-IS рассылает LSP для объявления состояний каналов. Размер LSP ограничен размером максимального блока передачи (MTU) канала. Когда объем объявляемого контента превышает один LSP, IS-IS создаст фрагменты LSP для переноса новой информации о состоянии канала
IS-IS VRF	Маршрутизация и пересылка VPN (VRF) в основном используется для локальной маршрутизации и разделения пакетов. Это позволяет избежать конфликта маршрутов, вызванного использованием одного и того же префикса несколькими VPN
IS-IS MTR	Мультитопологическая маршрутизация (MTR) в основном используется для расчета unicast-маршрутов IPv4 и IPv6 в IS-IS на основе различных топологий

6.4.1. Иерархия сети IS-IS

Сеть IS-IS делится на уровень 1 и уровень 2. Узлы, на которых устройства обмениваются информацией в одной области, образуют один Уровень (Level-1).

6.4.1.1. Принцип работы

Все устройства в области знают топологию сети и обмениваются данными внутри этой области. Устройство Level-1/Level-2 — это пограничное устройство, принадлежащее разным областям и обеспечивающее соединения между областями. Области соединены устройствами Level-2. Пограничные устройства в различных регионах образуют магистральную сеть Level-2 для межобластного обмена данными.

Устройства Level-1 интересуются только топологией локальной области, включая все узлы в локальной области и устройства следующего hop-а, предназначенные для этих узлов. Устройства Level-1 получают доступ к другим областям через устройства Level-2 и пересылают пакеты из целевой сети за пределами локальной области на ближайшее устройство Level-2.

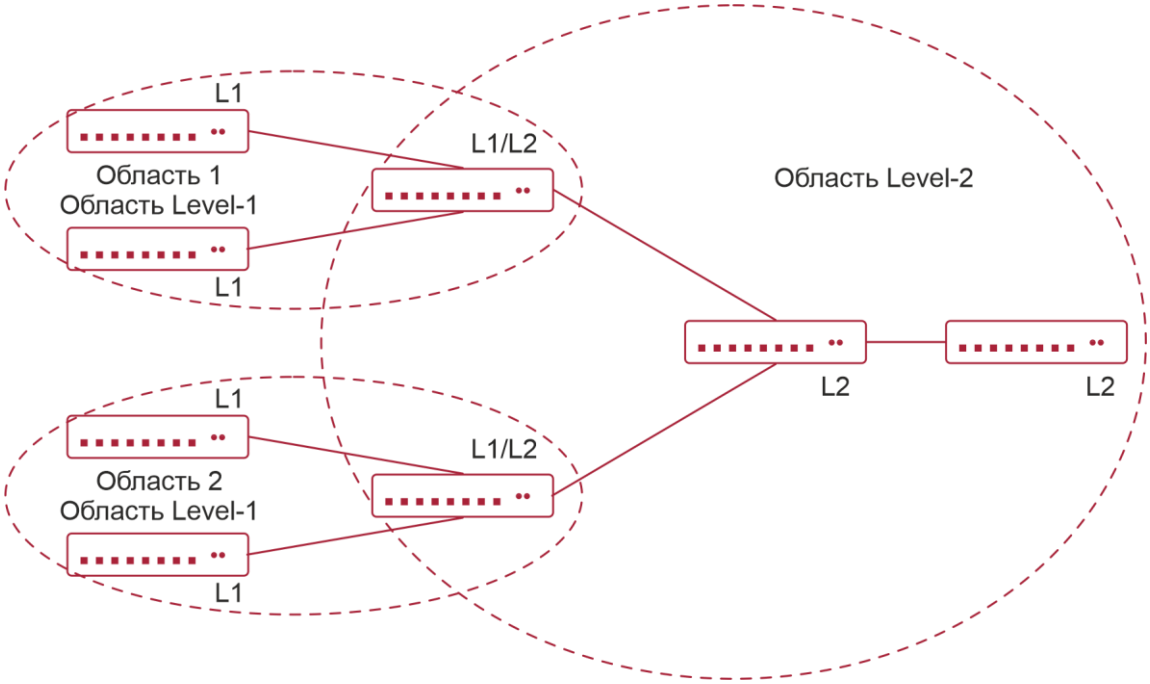


Рисунок 6-3. Топология сети IS-IS

6.4.1.2. Сопутствующая конфигурация

Настройка типа circuit интерфейса IS-IS

По умолчанию **circuit-type** установлен на Level-1/Level-2.

Запустите команду **isis circuit-type**, чтобы изменить уровень интерфейса.

Если для **circuit-type** установлено значение Level-1 или Level-2-only, IS-IS будет отправлять PDU только соответствующего уровня.

Указание уровня IS-IS

По умолчанию для **is-type** установлено значение Level-1/Level-2, если ни один экземпляр IS-IS не работает на Level-2 (включая Level-1/Level-2). **is-type** устанавливается на Level-1, если существуют экземпляры IS-IS, работающие на Level-2 (включая Level-1/Level-2).

Запустите команду **is-type**, чтобы указать уровень, на котором будет работать IS-IS.

Изменение значения **is-type** включит или отключит маршруты определенного Уровня. Устройство может иметь только один экземпляр, работающий на Level-2 (включая Level-1/Level-2).

6.4.2. Режим кодирования адреса IS-IS

Адрес IS-IS называется NET и состоит из идентификатора области, идентификатора системы и идентификатора NSAP длиной от восьми до 20 байт.

6.4.2.1. Принцип работы

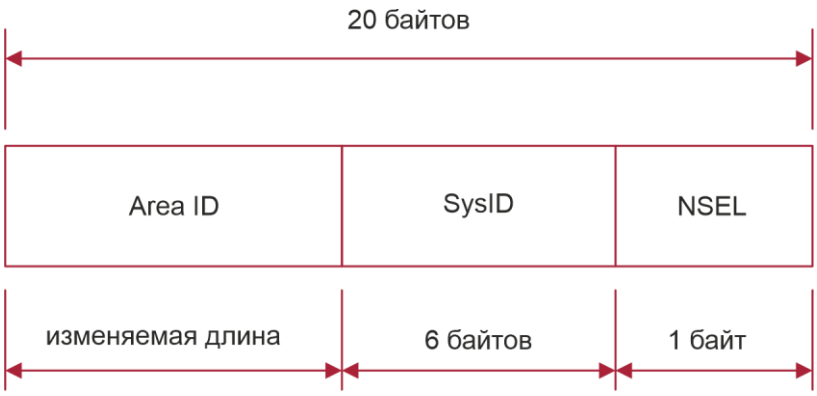


Рисунок 6-4. NET-формат адреса

- Идентификатор области идентифицирует длину RD в области и фиксируется относительно RD. Он варьируется от одного до 13 байт.
- Идентификатор системы уникален в автономной системе (AS).
- NSAP — это сетевой селектор, который иногда называют SEL. В IS-IS SEL обычно имеет значение 00, чтобы указать устройство.

6.4.2.2. Сопутствующая конфигурация

Настройка NET-адреса в IS-IS

По умолчанию в IS-IS не настроен NET-адрес.

Запустите команду **net**, чтобы настроить NET-адрес в IS-IS.

Команда настраивает идентификатор области и идентификатор системы в IS-IS. Разные NET-адреса должны иметь один и тот же системный идентификатор.

6.4.3. Типы пакетов IS-IS

Существует три типа пакетов IS-IS:

- LSP
- IIH PDU
- SNP (классифицируется на CSNP и PSNP)

6.4.3.1. Принцип работы

Существует три типа пакетов IS-IS:

- LSP

LSP используются для передачи записей о состоянии канала внутри области и подразделяются на LSP Level-1 и LSP Level-2. LSP заполняются только до соответствующего уровня.

- IIH PDU

IIH PDU используются для поддержания отношений соседства. Они содержат MAC-адреса multicast-рассылки, используемые для определения того, используют ли другие системы IS-IS.

- SNP (классифицируется на CSNP и PSNP)

CSNP используются для синхронизации LSDB. По умолчанию DIS отправляет CSNP каждые 10 секунд в broadcast-сети. В сети P2P CSNP отправляется только после установления соседских отношений.

PSNP также используются для синхронизации LSDB.

6.4.3.2. Сопутствующая конфигурация

Настройка интервала LSP на интерфейсе IS-IS

По умолчанию интервал LSP составляет 33 мс. Если уровень не указан, интервал вступает в силу для LSP Level-1 и Level-2.

Запустите команду **isis lsp-interval**, чтобы настроить интервал LSP на интерфейсе IS-IS в секундах.

Команда изменяет интервал LSP.

Настройка максимального количества LSP PDU, отправляемых интерфейсом IS-IS одновременно

Значение по умолчанию — 5. Если конкретный уровень не указан, уровень по умолчанию устанавливается на **level-1-2**, то есть конфигурация максимального количества вступает в силу одновременно на Level-1 и Level-2.

Запустите команду **isis lsp-flood**, чтобы установить количество LSP PDU, отправляемых интерфейсом IS-IS одновременно.

Эту команду можно использовать для изменения максимального количества LSP PDU, отправляемых интерфейсом одновременно.

Настройка интервала приема дубликатов пакетов LSP

По умолчанию данная команда не настроена и функция установки интервала приема LSP-пакетов не поддерживается. Если конкретный уровень не указан, уровень по умолчанию устанавливается на **level-1-2**, то есть конфигурация интервала вступает в силу одновременно на Level-1 и Level-2.

Запустите команду **min-lsp-arrival**, чтобы установить интервал для получения дубликатов LSP-пакетов.

Во время flapping-а сети пакеты LSP часто дублируются, и порядковый номер пакета LSP постоянно увеличивается. Если устройство обрабатывает дубликаты пакетов LSP, потребляется больше системных ресурсов. Таким образом, установка интервала получения дубликатов LSP-пакетов может разгрузить устройство.

Настройка интервала пакетов Hello на интерфейсе IS-IS

По умолчанию интервал пакетов Hello составляет 10 секунд для Level-1 и Level-2.

Запустите команду **isis hello-interval**, чтобы настроить интервал пакетов Hello на интерфейсе IS-IS в секундах.

Команда изменяет интервал пакетов Hello. DIS отправляет пакеты Hello с частотой в три раза большей, чем устройства, не относящиеся к DIS, в broadcast-сети. Если IS выбран в качестве DIS на интерфейсе, по умолчанию интерфейс отправляет пакет Hello каждые 3,3 секунды.

Настройка минимального интервала PSNP

По умолчанию минимальный интервал PSNP не настроен, а для PSNP Level-1 и Level-2 действует интервал по умолчанию равный 2 с.

Запустите команду **isis psnp-interval**, чтобы настроить минимальный интервал PSNP в секундах.

PSNP в основном используются для запроса LSP, которые отсутствуют локально, или для ответа на полученные LSP (в сети P2P). Интервал PSNP должен быть минимизирован. Если существует множество LSP и производительность устройства низкая, вы можете увеличить интервал PSNP и интервал повторной передачи LSP, чтобы снизить нагрузку на устройство.

Настройка интервала broadcast CSNP на интерфейсе IS-IS

По умолчанию CSNP отправляются с интервалом в 10 секунд в broadcast-сети. В сети P2P CSNP не отправляются. При настройке нового интервала CSNP без указания Level-1 или Level-2 этот интервал вступает в силу для CSNP Level-1 и Level-2.

Запустите команду **isis csnp-interval**, чтобы указать интервал broadcast-рассылки CSNP на интерфейсе IS-IS в секундах.

Команда изменяет интервал CSNP. По умолчанию DIS отправляет CSNP каждые 10 секунд в broadcast-сети. В сети P2P CSNP отправляется только после установления соседских отношений. Интерфейс, настроенный **mesh-groups**, можно настроить на периодическую отправку CSNP. CSNP не отправляются, если интервал CSNP установлен на 0.

6.4.4. Выборы DIS

DIS — это назначенное устройство в broadcast-сети, работающее как DR в OSPF.

Псевдоузел генерируется DIS и устанавливает связь с каждым устройством в локальной сети.

6.4.4.1. Принцип работы

DIS моделирует множественные каналы доступа в качестве псевдоузла и генерирует LSP для псевдоузла. Псевдоузел устанавливает связь с каждым устройством в локальной сети и запрещает прямую связь между устройствами. Broadcast-подсеть и non-broadcast-сеть множественного доступа (NBMA) считаются внешними псевдоузлами. Устройства, не поддерживающие DIS, сообщают о своих состояниях канала DIS в той же сети, а DIS поддерживает состояния каналов, сообщаемые всеми IS в сети. Подобно выбору DR в OSPF, DIS выбирается для уменьшения ненужных отношений соседства и обмена информацией о маршрутах.

Выборы DIS в IS-IS являются упреждающими. Результатом выборов можно управлять вручную посредством настройки приоритета интерфейса. Устройство с более высоким приоритетом интерфейса с большей вероятностью будет выбрано в качестве DIS.

6.4.4.2. Сопутствующая конфигурация

Настройка приоритета выбора DIS в локальной сети (LAN)

По умолчанию приоритет 64 действует для Level-1 и Level-2.

Запустите команду **isis priority**, чтобы настроить приоритет выбора DIS в локальной сети.

Команда изменяет приоритет пакетов Hello в локальной сети. Устройство с более низким приоритетом с меньшей вероятностью будет выбрано в качестве DIS.

Команда недействительна на сетевом интерфейсе P2P. Команда **no isis priority** с параметрами или без них восстанавливает приоритет до значения по умолчанию. Чтобы изменить настроенный приоритет, запустите команду **isis priority** с указанным

приоритетом, чтобы перезаписать существующую конфигурацию, или вы можете сначала восстановить приоритет до значения по умолчанию, а затем настроить новый приоритет.

6.4.5. Поддерживаемые IS-IS типы TLV

IS-IS поддерживает 26 типов TLV.

6.4.5.1. Принцип работы

В следующей таблице перечислены типы TLV, поддерживаемые IS-IS:

TLV-код	Описание
Код = 1	Идентификатор области
Код = 2	Приоритет IS-соседа
Код = 3	ES-сосед
Код = 6	MAC-адрес IS-соседа
Код = 8	Поле заполнения
Код = 9	Сущность LSP
Код = 10	Поле подтверждения
Код = 14	Размер исходного LSP-буфера
Код = 22	Расширенная доступность IS
Код = 128	Информация о внутренней доступности IP
Код = 129	Поддерживаемый протокол
Код = 130	Информация о внешней доступности IP
Код = 131	Информация о протоколе междоменной маршрутизации
Код = 132	IP-адрес интерфейса
Код = 133	Информация о проверке
Код = 135	TLV расширенной доступности IP
Код = 137	Динамическое имя хоста

TLV-код	Описание
Код = 211	Плавный перезапуск (GR)
Код = 222	Мультитопологическая (MT) доступность IS
Код = 229	MT TLV
Код = 211	GR
Код=232	IPv6-интерфейс
Код = 235	TLV доступности IPv4 MT IP
Код =236	TLV доступности IPv6 IP
Код = 237	TLV доступности IPv6 MT IP
Код = 240	TLV трехстороннего рукопожатия P2P

6.4.5.2. Сопутствующая конфигурация

Настройка протокола обнаружения соседей, передаваемого в пакетах Hello

По умолчанию обнаружение соседей включено.

Запустите команду **adjacency-check**, чтобы настроить протокол обнаружения соседей, передаваемый в пакетах Hello.

6.4.6. Расширение фрагмента LSP

IS-IS рассылает LSP для объявления состояний каналов. Размер LSP ограничен размером MTU канала. Когда объем объявляемого контента превышает один LSP, IS-IS создаст фрагменты LSP для переноса новой информации о состоянии канала. Согласно стандартам ISO, фрагмент LSP идентифицируется однобайтовым номером LSP. Устройство IS-IS может генерировать до 256 фрагментов LSP.

6.4.6.1. Принцип работы

256 фрагментов LSP недостаточно в любой из следующих ситуаций:

1. Новые приложения (например, управление трафиком [TE]) расширяют новый TLV или Sub-TLV.
2. Сеть постоянно расширяется.
3. Объявляются маршруты с пониженной степенью детализации или другие маршруты перераспределяются в IS-IS.

После того, как фрагменты LSP будут израсходованы, новая информация о маршрутизации и информация о соседях будут отброшены, что приведет к сетевым исключениям, таким как black hole или петли маршрутизации. Фрагменты LSP должны быть

расширены, чтобы нести больше информации о состоянии канала, обеспечивая тем самым нормальную работу сети.

Вы можете настроить дополнительный системный идентификатор и включить расширение фрагмента, чтобы позволить IS-IS объявлять больше информации о состоянии канала в расширенных фрагментах LSP. Каждую виртуальную систему можно рассматривать как виртуальное устройство, которое устанавливает отношения соседства (со значением пути, равным 0) с исходной системой. Расширенные LSP публикуются соседом исходной системы, то есть виртуальной системой.

Следующие термины связаны с расширением фрагмента:

Обычный системный идентификатор

Идентификатор системы, определенный ISO, используется для установления отношений соседства и изучения маршрутов. Далее он определяется как обычный системный идентификатор, чтобы отличать его от дополнительного системного идентификатора, введенного в расширение фрагмента.

Дополнительный системный идентификатор

Дополнительный системный идентификатор настраивается администратором для создания расширенных LSP. Дополнительный системный идентификатор применяет правила использования обычного системного идентификатора (например, дополнительный системный идентификатор должен быть уникальным во всей области), за исключением того, что дополнительный системный идентификатор не передается в пакетах Hello для установления отношений соседства.

Исходная система

Исходная система — это устройство с поддержкой IS-IS, которое сопоставляет виртуальную систему, идентифицируемую дополнительным идентификатором системы.

Виртуальная система (Виртуальная IS)

Виртуальная система идентифицируется дополнительным идентификатором системы и используется для создания расширенных LSP. Концепция виртуальной системы предложена RFC для отличия от концепции исходной системы. Каждая виртуальная система может генерировать до 256 фрагментов LSP. Администратор может настроить несколько дополнительных идентификаторов системы (виртуальных систем) для создания дополнительных фрагментов LSP.

Исходный LSP

Исходный LSP — это LSP, системный идентификатор которого, содержащийся в LSP ID, является обычным системным идентификатором. Исходные LSP генерируются исходной системой.

Расширенный LSP

Расширенный LSP — это LSP, системный идентификатор которого, содержащийся в LSP ID, является дополнительным системным идентификатором. Расширенные LSP генерируются виртуальной системой.

6.4.6.2. Сопутствующая конфигурация

Включение расширения фрагмента

По умолчанию расширение фрагмента отключено. Если вы не укажете уровень при включении расширения фрагмента, оно вступит в силу для LSP Level-1 и Level-2.

Запустите команду **lsp-fragments-extend**, чтобы включить расширение фрагмента.

Имеется до 256 фрагментов LSP. Когда фрагменты израсходованы, последующая информация о состоянии канала, включая информацию о соседях и информацию об IP-маршруте, будет отброшена, что приведет к сетевому исключению. Чтобы решить эту проблему, включите расширение фрагмента на указанном уровне и настройте дополнительный идентификатор системы с помощью команды **virtual-system**.

6.4.7. IS-IS VRF

VRF в основном используется для локальной маршрутизации и разделения пакетов. Это позволяет избежать конфликта маршрутов, вызванного использованием одного и того же префикса несколькими VPN. IPv4 VPN и IPv6 VPN сочетают в себе преимущества Multiprotocol Label Switching (MPLS) с точки зрения качества обслуживания (QoS) и обеспечения безопасности и являются основными решениями для соединения географически разных филиалов предприятия или отраслевого пользователя.

6.4.7.1. Принцип работы

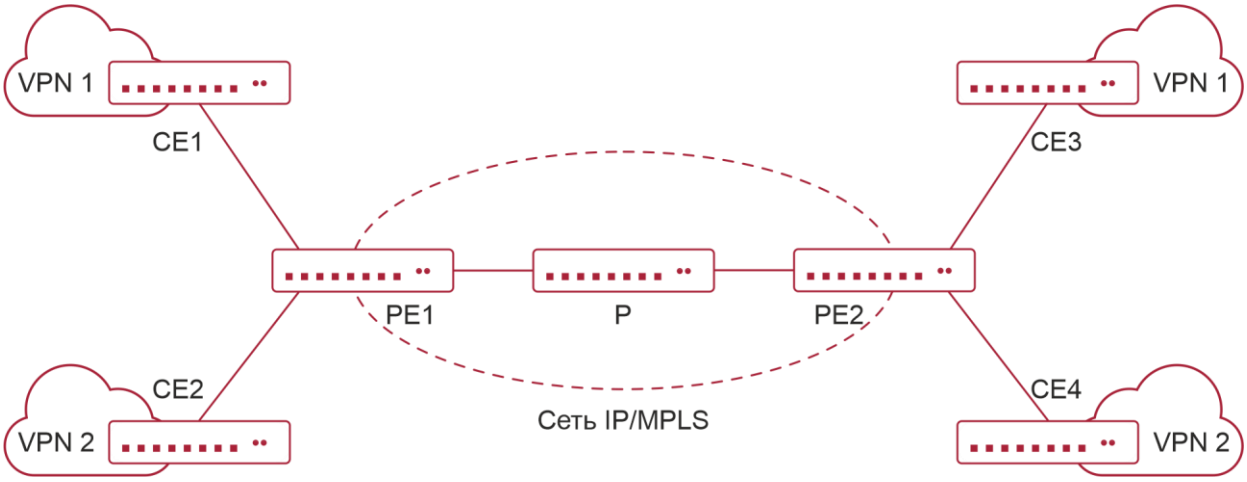


Рисунок 6-5. Разделение различных VPN с помощью таблиц VRF, настроенных на устройствах Provider Edge (PE)

На Рисунке 6-5 существуют следующие требования к конфигурации: Настройте два сайта (CE1 и CE3) в VPN1 для доступа друг к другу и два сайта (CE2 и CE4) в VPN2 для доступа друг к другу, а также запретите доступ между сайтами в VPN1 и VPN2, поскольку VPN1 и VPN2 принадлежат разным клиентам или отделам и могут иметь одинаковые IP-адреса.

Пограничные устройства клиента (CE) подключают сеть клиента к PE для обмена информацией о маршрутизации VPN с PE, то есть объявляют локальные маршруты PE и изучают удаленные маршруты от PE.

Каждый PE изучает маршруты от напрямую подключенных CE и обменивается полученными маршрутами VPN с другим PE через протокол пограничного шлюза (BGP). PE предоставляют доступ к сервису VPN.

Устройство поставщика (P) в сети поставщика сервисов (SP) не подключено напрямую к CE. Устройству P требуется только возможность пересылки MPLS, и оно не поддерживает информацию VPN.

Протокол IS-IS, работающий между PE и CE, требует возможности VRF для разделения информации маршрутизации между VPN1 и VPN2. То есть IS-IS изучает маршруты только через VRF.

6.4.7.2. Сопутствующая конфигурация

Связывание экземпляра IS-IS с таблицей VRF

По умолчанию экземпляр IS-IS не привязан ни к одной таблице VRF.

Запустите команду **VRF**, чтобы связать экземпляр IS-IS с таблицей VRF.

Обратите внимание на следующие ограничения или соглашения для операции привязки:

- Экземпляры IS-IS, связанные с одной и той же таблицей VRF, отличной от стандартной, должны быть настроены с разными системными идентификаторами. Экземпляры IS-IS, связанные с разными таблицами VRF, можно настроить с одним и тем же системным идентификатором.
- Один экземпляр IS-IS может быть связан только с одной таблицей VRF, но одна таблица VRF может быть связана с несколькими экземплярами IS-IS.
- При изменении таблицы VRF, привязанной к экземпляру IS-IS, все интерфейсы IS-IS, связанные с этим экземпляром, будут удалены. То есть конфигурация интерфейса **ip** (или **ipv6**) **router isis** [*tag*] и конфигурация перераспределения в режиме процесса маршрутизации будут удалены.

6.4.8. IS-IS MTR

IS-IS MTR — это расширенная функция, используемая для разделения расчета unicast-маршрута IPv4 и расчета unicast-маршрута IPv6 на основе топологий. Он соответствует спецификации расширения IS-IS MT, определенной в RFC 5120. В IIH PDU и LSP введены новые типы TLV для передачи информации о топологии unicast-рассылки IPv6. Одну физическую сеть можно разделить на логическую топологию unicast-рассылки IPv4 и логическую топологию unicast-рассылки IPv6. Две топологии выполняют расчет SPF отдельно и поддерживают независимые таблицы unicast-маршрутизации IPv4 и IPv6 соответственно. Таким образом, трафик сервиса unicast-рассылки IPv4 и трафик сервиса unicast-рассылки IPv6 пересылаются по разным путям. Метод IS-IS MTR помогает пользователям развертывать сети unicast-рассылки IPv6 без ограничений на согласованность информации о топологии unicast-рассылки IPv4 и IPv6.

IS-IS MTR является производным от IS-IS MT, который используется для разделения unicast-топологий IPv4 и IPv6, unicast- и multicast-топологий, а также топологий, использующих различные стеки протоколов (например, IPv4 и Pv6). IS-IS MTR разделяет топологии unicast-рассылки IPv4 и IPv6 на основе IS-IS MT.

6.4.8.1. Принцип работы

На Рисунке 6-6 показано типичное сетевое приложение. Существуют следующие требования к реализации: Разверните топологию unicast-рассылки IPv6 в инкрементальном режиме и обновите некоторые устройства для поддержки стеков двойных протоколов IPv4 и IPv6, оставив при этом другие устройства с поддержкой IPv4 без изменений.

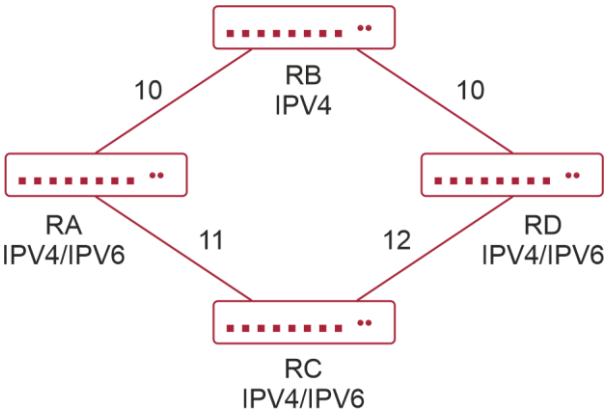


Рисунок 6-6. Физическая топология для гибридного развертывания IPv4-IPv6

На Рисунке 6-6 каждый канал помечается числом, указывающим ее метрику. RB поддерживает только стек протоколов IPv4, тогда как другие устройства поддерживают двойные стеки протоколов IPv4 и IPv6.

Сетевое ограничение согласованности между топологиями unicast-рассылки IPv4 и IPv6 должно быть отменено, чтобы сохранить использование RB; в противном случае RB не сможет установить отношения соседства с RA или RD, что вызовет новые проблемы.

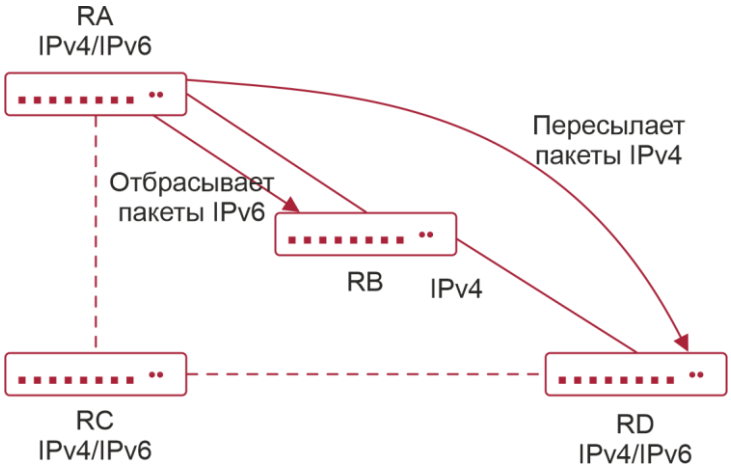


Рисунок 6-7. Гибридная топология IPv4-IPv6

На Рисунке 6-7 без поддержки IS-IS MTR вычисления SPF, выполняемые RA, RB, RC и RD, учитывают только одну гибридную топологию. Рассчитанный кратчайший путь — RA -> RB -> RD, при этом накладные расходы равны 20. RB будет отбрасывать пакеты IPv6, поскольку он не поддерживает IPv6.

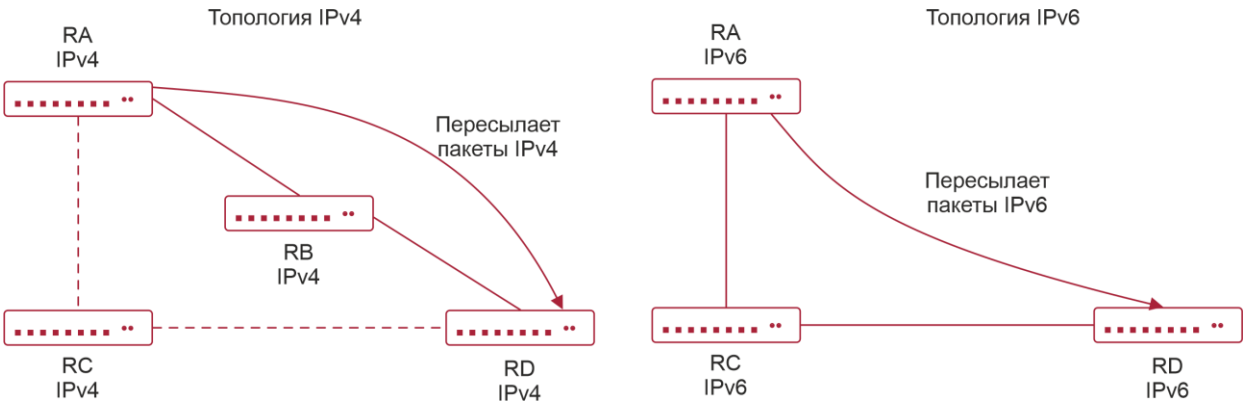


Рисунок 6-8. Разделение топологий IPv4 и IPv6

На Рисунке 6-8 метод IS-IS MTR используется для разделения топологий unicast-рассылки IPv4 и IPv6. RA, RB, RC и RD устанавливают отношения соседства на основе топологии unicast-рассылки IPv4 и топологии unicast-рассылки IPv6 соответственно. В левой части показана топология IPv4, образованная маршрутизаторами с поддержкой IPv4. Рассчитанный кратчайший путь IPv4 — RA -> RB -> RC, который реализует пересылку пакетов IPv4. В правой части показана топология IPv6, образованная маршрутизаторами с поддержкой IPv6. Рассчитанный кратчайший путь IPv6 — RA -> RC -> RD, который реализует пересылку пакетов IPv6.

Необходимо развернуть IS-IS MTR, чтобы избежать маршрутизации black hole, когда некоторые устройства поддерживают только один протокол. IS-IS MTR не требуется, если все устройства поддерживают двойные стеки протоколов IPv4 и IPv6.

- Развертывание новой сети: IS-IS MTR не требуется, если устройства поддерживают только стек протоколов IPv4. Для устройств, поддерживающих только стек протоколов IPv6, или устройств, поддерживающих стек протоколов IPv4 и IPv6, включите режим MT для IS-IS MTR. Рекомендуется не включать мультитопологический переход (MTT); в противном случае могут возникнуть петли.
- Реконструкция существующей сети с устройствами, поддерживающими только один стек протоколов: последовательно включите режим MTT IS-IS MTR на устройствах, поддерживающих двойные стеки протоколов IPv4 и IPv6 (начиная с устройства, ближайшего к устройству, поддерживающему только один стек протоколов в топология сети). После включения режима MTT на всех новых устройствах последовательно переключайте режим MTT в режим MT на этих устройствах (начиная с устройства, наиболее удаленного от устройства, поддерживающего только один стек протоколов в топологии сети).

6.4.8.2. Сопутствующая конфигурация

Включение MTR для экземпляров IS-IS

По умолчанию экземпляры IS-IS не поддерживают MTR.

Запустите команду **multi-topology**, чтобы настроить IS-IS для поддержки топологий unicast-рассылки IPv6. После этого unicast-маршруты IPv4 и IPv6 в IS-IS будут рассчитываться на основе разных топологий.

Обратите внимание на следующие ограничения и соглашения при использовании команды **multi-topology**:

1. Прежде чем запускать команду, установите **metric-style** в значение **Wide** или **Transition**.
2. Функция MTR будет отключена, если для **metric-style** установлено значение **Narrow** или только один уровень настроен для поддержки режима **Wide** или **Transition**.

6.4.9. Сосед IS-IS

Следующие условия должны быть выполнены для того, чтобы два устройства маршрутизации установили отношения соседства, когда IS-IS MTR не настроен:

- Адреса интерфейсов на обоих устройствах маршрутизации находятся в одном сегменте сети.
- Уровни интерфейса на обоих устройствах маршрутизации совпадают.
- Устройства маршрутизации аутентифицируются друг другом.
- Устройства маршрутизации поддерживают тот же протокол.

Следующие условия должны быть выполнены, чтобы устройства маршрутизации могли установить отношения соседства при настройке IS-IS MTR:

- Адреса интерфейсов обоих устройств маршрутизации находятся в одних и тех же сегментах сети.
- Уровни интерфейса на обоих устройствах маршрутизации совпадают.
- Устройства маршрутизации аутентифицируются друг другом.
- Устройства маршрутизации имеют по крайней мере один согласованный идентификатор MT при настройке каналов P2P.
- Нет никаких ограничений на идентификаторы MT, которые поддерживают устройства маршрутизации при настройке каналов локальной сети.

6.5. Конфигурация

Конфигурация	Описание и команда	
Включение IS-IS	(Обязательный) Используется для включения IS-IS на определенных интерфейсах. Вам необходимо заранее создать процесс маршрутизации IS-IS	
	router isis [*tag*]	Запускает процесс маршрутизации IS-IS. *tag* указывает имя процесса
	net *area Address.SystemId.00*	Настраивает NET-адрес в IS-IS
	ip router isis [*tag*]	Включает IS-IS на интерфейсе. *tag* указывает имя процесса маршрутизации IS-IS

Конфигурация	Описание и команда	
Настройка пакетов Hello IS-IS	(Опционально) Используется для настройки времени удержания (holdtime) пакета IS-IS Hello	
	isis hello-interval { *interval* | **minimal** } [**level-1** | **level-2**]	Настраивает интервал пакетов Hello на интерфейсе. Диапазон значений: от 1 до 65 535 в секундах
	isis hello-multiplier *multiplier-number* [**level-1** | **level-2**]	Настраивает множитель времени holdtime пакета Hello на интерфейсе IS-IS. Диапазон значений от 2 до 100. Значение по умолчанию — 3
Настройка IS-IS LSP	(Опционально) Используется для выполнения связанной со временем настройки LSP, для определения, следует ли игнорировать ошибки контрольной суммы LSP, а также для включения/выключения расширения фрагмента LSP	
	isis lsp-interval *interval* [**level-1** | **level-2**]	Настраивает минимальный интервал LSP на интерфейсе. Диапазон значений: от 1 до 4 294 967 295 в миллисекундах
	isis lsp-flood *lsp-number* [**level-1** | **level-2**]	Указывает максимальное количество пакетов LSP, отправляемых интерфейсом IS-IS одновременно. Диапазон значений: от 1 до 1000. Значение по умолчанию — 5
	isis retransmit-interval *interval* [**level-1** | **level-2**]	Настраивает интервал повторной передачи LSP по каналам P2P на интерфейсе. Диапазон значений: от 0 до 65 535 в секундах

Конфигурация	Описание и команда	
Настройка IS-IS LSP	**lsp-gen-interval** [**level-1** | **level-2**] *maximum-interval* [*initial-interval hold-interval*]	Настраивает цикл генерации LSP. *maximum-interval*: указывает максимальный интервал для генерации двух последовательных пакетов LSP. Диапазон значений: от 1 до 65 535 (в секундах). Значение по умолчанию — 5. *initial-interval*: указывает время ожидания для первой генерации пакета LSP. Диапазон значений: от 0 до 60 000 (в миллисекундах). Значение по умолчанию — 50. *hold-interval*: указывает минимальный интервал для генерации пакета LSP во второй раз. Диапазон значений: от 10 до 60 000 (в миллисекундах). Значение по умолчанию — 200
	ignore-lsp-errors	Настраивается для игнорирования ошибок контрольной суммы LSP
	lsp-fragments-extend [**level-1** | **level-2**] [**compatible rfc3786**]	Включает расширение фрагмента
	virtual-system *system-id*	Настраивает дополнительный идентификатор системы
Настройка SNP IS-IS	(Опционально) Используется для настройки интервала broadcast CSNP	
	isis csnp-interval *interval* [**level-1** | **level-2**]	Настраивает интервал CSNP на интерфейсе. Диапазон значений: от 0 до 65 535 в секундах. Значение по умолчанию — 10 с. CSNP не отправляются, если интервал CSNP установлен на 0

Конфигурация	Описание и команда	
Настройка типа уровня IS-IS	(Опционально) Используется для настройки типа системы или типа схемы интерфейса в IS-IS	
	is-type { **level-1** | **level-1-2** | **level-2-only** }	Настраивает тип системы
	isis circuit-type { **level-1** | **level-1-2** | **level-2-only** [**external**] }	Настраивает тип circuit интерфейса
Настройка аутентификации IS-IS	(Опционально) Используется для настройки аутентификации интерфейса, аутентификации области и аутентификации RD	
	isis password [**0** | **7**] *password* [**send-only**] [**level-1** | **level-2**]	Настраивает пароль для аутентификации открытого текста пакетов Hello на интерфейсе. Если включен параметр **send-only**, пароль аутентификации используется только для аутентификации отправленных пакетов Hello. Полученные пакеты Hello не аутентифицируются. Если уровень не указан, настроенная аутентификация и пароль вступают в силу для всех уровней. Эта команда не вступает в силу, если выполняется команда **isis authentication mode**. Обе команды используются для настройки аутентификации интерфейса IS-IS, но команда **isis password** имеет более низкий приоритет. Прежде чем запускать команду **isis password**, удалите конфигурацию команды **isis authentication mode**

Конфигурация	Описание и команда	
Настройка аутентификации IS-IS	**isis authentication mode** { **text** | **md5** } [**level-1** | **level-2**]	Указывает аутентификацию в виде открытого текста или MD5. Если уровень (Level) не указан, режим аутентификации вступает в силу для всех уровней. Если вы используете эту команду после **isis password** *password* [**level-1** | **level-2**], то предыдущая конфигурация команды будет перезаписана. Обе команды используются для настройки аутентификации интерфейса IS-IS, но команда **isis authentication mode** имеет более высокий приоритет
	isis authentication key-chain *name-of-chain* [**level-1** | **level-2**]	Настраивает пароль для аутентификации интерфейса. Если уровень не указан, настроенная цепочка ключей вступает в силу для всех уровней. Эту команду необходимо использовать с командой **isis authentication mode** для настройки аутентификации интерфейса IS-IS
	isis authentication send-only [**level-1** | **level-2**]	(Опционально) Указывает, что аутентификация интерфейса выполняется только для отправленных пакетов. Полученные пакеты не аутентифицируются. Если уровень не указан, режим аутентификации **send-only** вступает в силу для всех уровней. Эта команда используется, чтобы избежать flapping-а сети, вызванной временным сбоем аутентификации, когда настроена аутентификация

Конфигурация	Описание и команда	
		IS-IS. Прежде чем развернуть аутентификацию IS-IS во всей сети, запустите команды **isis authentication mode** { **text** | **md5** } [**level-1** | **level-2**] и **isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**] на каждом устройстве. После этого запустите команду **no isis authentication send-only**, чтобы восстановить аутентификацию полученных пакетов. Это обеспечивает плавное развертывание аутентификации и позволяет избежать flapping-а сети
Настройка аутентификации IS-IS	**area-password** [**0** | **7**] *password* [**send-only**]	Настраивает пароль для аутентификации области в виде открытого текста (Level-1). Если включен параметр **send-only**, пароль аутентификации используется только для аутентификации отправленных пакетов. Полученные пакеты не аутентифицируются. Эта команда не вступает в силу, если выполняется команда **authentication mode**. Обе команды используются для настройки аутентификации области IS-IS, но **команда area-password** имеет более низкий приоритет. Прежде чем запускать команду **area-password**, удалите конфигурацию команды **authentication mode**
	authentication mode { **text** | **md5** } **level-1**	Указывает режим аутентификации области IS-IS. Если вы используете эту команду после выполнения команды **area-password** *password*, предыдущая

Конфигурация	Описание и команда	
		конфигурация команды будет перезаписана. Обе команды используются для настройки аутентификации области IS-IS, но команда **authentication mode** имеет более высокий приоритет
Настройка аутентификации IS-IS	**authentication key-chain** *name-of-chain* **level-1**	Настраивает цепочку ключей для аутентификации области IS-IS. Эту команду необходимо использовать с командой **authentication mode** для настройки аутентификации области IS-IS
	authentication send-only level-1	(Опционально) Указывает, что аутентификация области IS-IS выполняется только для отправленных пакетов. Полученные пакеты не аутентифицируются. Эта команда используется, чтобы избежать flapping-а сети, вызванной временным сбоем аутентификации, когда настроена аутентификация IS-IS. Прежде чем развернуть аутентификацию IS-IS во всей области, запустите команды **authentication mode** { **text** | **md5** } **level-1** и **authentication key-chain** *name-of-chain* **level-1** на каждом устройстве. После этого запустите команду **no authentication send-only**, чтобы восстановить аутентификацию полученных пакетов. Это обеспечивает плавное развертывание аутентификации и позволяет избежать flapping-а сети

Конфигурация	Описание и команда	
	domain-password [**0** | **7**] *password* [**send-only**]	Настраивает пароль для аутентификации в виде открытого текста RD (Level-2). Если включен параметр **send-only**, пароль аутентификации используется только для аутентификации отправленных пакетов. Полученные пакеты не аутентифицируются. Эта команда не вступает в силу, если выполняется команда **authentication mode**. Обе команды используются для настройки аутентификации IS-IS RD, но команда **domain-password** имеет более низкий приоритет. Прежде чем запускать команду **domain-password**, удалите конфигурацию команды **authentication mode**
Настройка аутентификации IS-IS	**authentication mode** { **text** | **md5** } **level-2**	Указывает режим аутентификации IS-IS RD. Если вы используете эту команду после выполнения команды **domain-password** *password*, предыдущая конфигурация команды будет перезаписана. Обе команды используются для настройки аутентификации IS-IS RD, но команда **authentication mode** имеет более высокий приоритет
	authentication key-chain *name-of-chain* **level-2**	Настраивает пароль для аутентификации IS-IS RD. Эту команду необходимо использовать с командой **authentication mode** для настройки аутентификации IS-IS RD

Конфигурация	Описание и команда	
Настройка аутентификации IS-IS	**authentication send-only level-2**	(Опционально) Указывает, что аунтетификация IS-IS RD выполняется только для отправленных пакетов. Полученные пакеты не аутентифицируются. Эта команда используется, чтобы избежать flapping-а сети, вызванной временным сбоем аутентификации, когда настроена аутентификация IS-IS. Прежде чем развернуть аутентификацию IS-IS на всем RD, запустите команды **authentication mode** { **text** | **md5** } **level-2** и **authentication key-chain** *name-of-chain* **level-2** на каждом устройстве. После этого запустите команду **no authentication send-only**, чтобы восстановить аутентификацию полученных пакетов. Это обеспечивает плавное развертывание аутентификации и позволяет избежать flapping-а сети
Настройка IS-IS GR	(Необязательный) Используется для включения IS-IS GR	
	graceful-restart	Включает возможность GR Restart на устройстве, которое работает в качестве Restarter-а. По умолчанию возможность GR Restart включена
	graceful-restart grace-period *seconds*	(Опционально) Настраивает время IS-IS GR на устройстве, которое работает в качестве Restarter-а. Значение по умолчанию — 300 с
	no graceful-restart helper disable	Включает функцию GR Help IS-IS на устройстве, которое работает в качестве Helper-а. По умолчанию функция GR Help включена

Конфигурация	Описание и команда	
Настройка IS-IS NSR	(Опционально) Используется для включения IS-IS NSR	
	nsr	Включает IS-IS NSR. По умолчанию он отключен
Настройка поддержки BFD для IS-IS	(Опционально) Используется для включения поддержки BFD для IS-IS	
	bfd all-interfaces [**anti-congestion**]	Включает поддержку BFD для IS-IS на всех интерфейсах
	isis bfd [**disable** | **anti-congestion**]	Включает или отключает поддержку BFD для IS-IS на текущем интерфейсе
Установка бита перегрузки IS-IS	(Опционально) Используется для установки бита перегрузки в LSP	
	set-overload-bit [**on-startup** { *seconds* | **wait-for-bgp** [*bgpseconds*] }] [**suppress** { [**interlevel**] [**external**] }] [**level-1** | **level-2**]	Устанавливает бит перегрузки
Настройка IS-IS VRF	(Опционально) Используется для привязки экземпляра IS-IS к таблице VRF	
	vrf *vrf-name*	Связывает экземпляр IS-IS с таблицей VRF
Настройка IS-IS MTR	(Опционально) Используется для расчета unicast-маршрутов IPv4 и IPv6 в IS-IS на основе различных топологий	
	multi-topology [**transition**]	Настраивает IS-IS для поддержки топологий unicast-рассылки IPv6

Конфигурация	Описание и команда	
Настройка SNMP для IS-IS	(Опционально) Используется, чтобы позволить программному обеспечению SNMP выполнять операции с базой информации управления (MIB) на экземплярах IS-IS	
	enable mib-binding	Выполняет операции MIB на экземпляре, связанном с тегом 1
	configure terminal	Вход в режим глобальной конфигурации
	snmp-server enable traps isis	Включает Trap IS-IS глобально
	snmp-server host { *host-addr* | **ipv6** *ipv6-addr* } [**vrf** *vrfname*] [**traps**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*]	Настраивает хост SNMP в режиме глобальной конфигурации для получения сообщений Trap IS-IS
	router isis	Вход в режим настройки процесса маршрутизации IS-IS
Настройка SNMP для IS-IS	**enable traps all**	Разрешает отправку всех сообщений Trap IS-IS на хост с IP-адресом 10.1.1.1
Настройка двустороннего обслуживания IS-IS	Опционально	
	two-way-maintain	Обеспечивает двустороннее обслуживание IS-IS
Настройка других параметров IS-IS	Опционально	
	maximum-paths *maximum*	Настраивает максимальное количество путей IS-IS IPv4/IPv6 с равной стоимостью
	lsp-length *receive size*	Настраивает максимальную длину, разрешенную для полученных LSP

Конфигурация	Описание и команда	
Настройка других параметров IS-IS	**lsp-length originate** *size* [**level-1** | **level-2**]	Настраивает максимальную длину, разрешенную для отправленных LSP
	passive-interface [**default**] { *interface-type interface-number* }	Настраивает пассивный интерфейс
	bandwidth-reference *value*	Настраивает ссылку на полосу пропускания для IS-IS для автоматического расчета метрики канала
	interfaces-protocol-compatible	Настраивает поле TLV протокола IS-IS для заполнения на основе протоколов, поддерживаемых интерфейсом
	is-name *name*	Настраивает имя экземпляра
	isis metric *metric* [**level-1** | **level-2**]	Настраивает метрику интерфейса, которая действительна только в том случае, если для параметра **metric-style** установлено значение **Narrow**
	isis wide-metric *metric* [**level-1** | **level-2**]	Настраивает значение широкой метрики интерфейса, которое допустимо только в том случае, если для параметра **metric-style** установлено значение **Wide**
	isis passive	Настраивает пассивный интерфейс
	isis priority *value* [**level-1** | **level-2**]	Настраивает приоритет выбора DIS на интерфейсе

Конфигурация	Описание и команда	
Настройка других параметров IS-IS	**default-information originate** [**route-map** *map-name*]	Создает маршрут по умолчанию Level-2, который будет объявляться через LSP. Если команда включает опцию **route-map**, маршрут по умолчанию генерируется только в том случае, если критерии в **route-map** выполняются
	summary-address ip-*address net-mask* [**level-1** | **level-2** | **level-1-2**] [**metric** *number*]	Настраивает суммарный маршрут IPv4
	summary-prefix *ipv6-prefix/prefix-length* [**level-1** | **level-2** | **level-1-2**]	Настраивает суммарный маршрут IPv6
	ignore-lsp-errors	Настраивается для игнорирования ошибок контрольной суммы LSP
	log-adjacency-changes	Активирует ведение журналов изменений отношений соседства IS-IS
	redistribute	Настраивает перераспределение маршрутов

6.5.1. Включение IS-IS

6.5.1.1. Эффект конфигурации

- Прежде чем запускать IS-IS, создайте процесс маршрутизации IS-IS в режиме глобальной конфигурации. Вы можете установить параметр **tag** после команды **router isis**, чтобы назвать процесс. Вы можете добавлять разные теги для настройки различных процессов маршрутизации IS-IS. Настройка параметра **tag** не является обязательной.
- Идентификатор системы однозначно идентифицирует IS в AS маршрутизации; поэтому системный идентификатор должен быть уникальным в пределах AS. В IS-IS каждая область может содержать один или несколько идентификаторов области. Обычно вам нужно настроить только один идентификатор области. Вы можете настроить несколько идентификаторов областей для разделения областей. Если IS настроена с несколькими идентификаторами областей, идентификаторы системы должны быть одинаковыми.

- После добавления интерфейса в указанный процесс маршрутизации IS-IS этот интерфейс установит отношения соседства.

6.5.1.2. Примечания

- Устройства Level-1 в области должны быть настроены с одинаковым идентификатором области.
- Базовая (core) таблица маршрутизации не различает записи маршрутизации, созданные различными процессами маршрутизации IS-IS.
- IP-адреса интерфейсов, подключенных между соседями, должны находиться в одном сегменте сети.
- Если два IP-адреса находятся в разных сегментах сети, отношения соседства не могут быть установлены.
- Если вам нужно добавить интерфейс к указанному процессу маршрутизации IS-IS, установите параметр **tag** после команды **ip router isis**, чтобы указать имя процесса.
- Если вы запустите команду **no ip routing** в режиме глобальной конфигурации, IS-IS отключит маршрутизацию IPv4 на всех интерфейсах. То есть команда **no ip router isis** [*tag*] автоматически выполняется на всех интерфейсах. Остальные настройки IS-IS остаются неизменными.
- По умолчанию защита ЦП на устройствах включена. Для пакетов, сопоставленных с групповыми адресами назначения (AllISSystems, AllL1ISSystems и AllL2ISSystems) в IS-IS, существует ограничение по умолчанию (например, 400 пакетов в секунду) на количество пакетов, отправляемых в ЦП. Если устройство имеет много отношений соседства или отправляет пакеты Hello через короткие интервалы времени, пакеты IS-IS, которые получает устройство, могут превысить предел по умолчанию, вызывая частый flapping отношений соседства. Чтобы решить проблему, вы можете использовать команду защиты ЦП в режиме глобальной конфигурации, чтобы увеличить предел.

6.5.1.3. Шаги настройки

Запуск процесса маршрутизации IS-IS

- Обязательный.
- Выполните эту настройку в режиме глобальной конфигурации на каждом устройстве, если не указано иное.

Настройка NET-адреса в IS-IS

- Обязательный.
- Выполните эту настройку в режиме настройки процесса маршрутизации IS-IS на каждом устройстве, если не указано иное.

Включение IS-IS на интерфейсах

- Обязательный.
- Выполните эту настройку в режиме настройки интерфейса на каждом устройстве, если не указано иное.

6.5.1.4. Проверка

- Проверьте, отправляют ли устройства пакеты Hello.
- Проверьте, устанавливают ли устройства отношения соседства.

- Проверьте, обмениваются ли устройства LSP.

6.5.1.5. Связанные команды

Запуск процесса маршрутизации IS-IS

Команда	**router isis** [*tag*]
Описание параметра	*tag*: указывает имя экземпляра IS-IS
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду для инициализации экземпляра IS-IS и входа в режим настройки процесса маршрутизации IS-IS. Экземпляр IS-IS начнет работать после настройки NET-адреса. Если вы установили параметр *tag* при запуске процесса маршрутизации IS-IS, вам необходимо добавить параметр *tag* при закрытии процесса маршрутизации IS-IS. По умолчанию защита ЦП на устройствах включена. Для пакетов, сопоставленных с групповыми адресами назначения (AllISSystems, AllL1ISSystems и AllL2ISSystems) в IS-IS, существует ограничение по умолчанию (например, 400 пакетов в секунду) на количество пакетов, отправляемых в ЦП. Если устройство имеет много отношений соседства или отправляет пакеты Hello через короткие интервалы времени, пакеты IS-IS, которые получает устройство, могут превысить предел по умолчанию, вызывая частый flapping отношений соседства. Чтобы решить проблему, вы можете использовать команду защиты ЦП в режиме глобальной конфигурации, чтобы увеличить предел

Настройка NET-адреса в IS-IS

Команда	**net** *net-address*
Описание параметра	*net-address*: NET-адрес имеет формат XX.XXXX.YYYY.YYYY.YYYY.00. XX.XXXX указывает идентификатор области, а YYYY.YYYY.YYYY указывает идентификатор системы
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Используйте эту команду для настройки идентификатора области и идентификатора системы в IS-IS. Разные NET-адреса должны иметь один и тот же системный идентификатор

Включение IS-IS на интерфейсе

Команда	**ip router isis** [*tag*]
Описание параметра	*tag*: указывает имя экземпляра IS-IS
Командный режим	Режим настройки интерфейса
Руководство по использованию	Используйте эту команду, чтобы включить интерфейс для участия в маршрутизации IS-IS IPv4. Используйте форму **no** этой команды, чтобы отключить процесс маршрутизации IS-IS на интерфейсе. Если вы запустите команду **no ip routing** в режиме глобальной конфигурации, IS-IS отключит маршрутизацию IPv4 на всех интерфейсах. То есть команда **no ip router isis** [*tag*] автоматически выполняется на всех интерфейсах. Остальные настройки IS-IS остаются неизменными

6.5.1.6. Пример конфигурации

Установление отношений соседства на канале IS-IS P2P

Сценарий: Маршрутизатор A и маршрутизатор B подключены в режиме P2P.

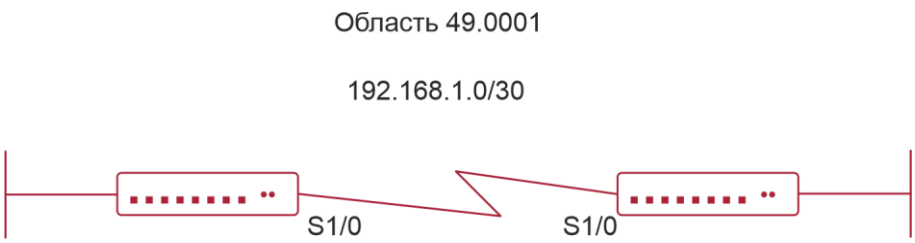


Рисунок 6-9. Топология канала P2P

Шаги настройки	• Настройте IS-IS. • Настройте интерфейсы сети Wide Area Network (WAN)
A	A(config)# router isis A(config-router)# net 49.0001.0000.0000.0001.00 A(config)# interface Serial 1/0 A(config-if)# ip address 192.168.1.1 255.255.255.252 A(config-if)# ip router isis
B	B(config)# router isis

	B(config-router)# net 49.0001.0000.0000.0002.00 B(config)# interface Serial 1/0 B(config-if)# ip address 192.168.1.2 255.255.255.252 B(config-if)# ip router isis
Проверка	• Включите отправку пакетов Hello с интерфейса 192.168.1.1 на маршрутизаторе A на интерфейс 192.168.1.2 на маршрутизаторе B. • Установите отношения соседства IS-IS между маршрутизаторами A и B, при этом состояние соседа будет Up. • Проверьте LSP на маршрутизаторе A и маршрутизаторе B. Должны существовать системные идентификаторы 0000.0000.0001 и 0000.0000.0002
A	A# show isis neighbors A# show isis database detail
B	B# show isis neighbors

Установление соседских отношений по broadcast-каналу IS-IS

Сценарий: Маршрутизатор A, маршрутизатор B и маршрутизатор C соединены между собой через Ethernet.

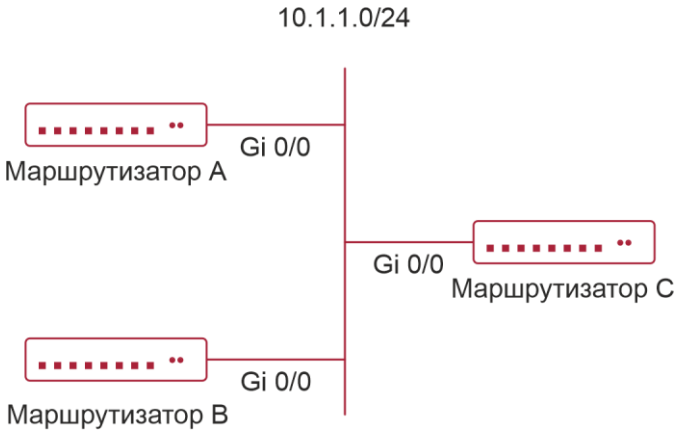


Рисунок 6-10. Топология broadcast-канала IS-IS

Шаги настройки	• Настройте IS-IS. • Настройте интерфейсы Ethernet
A	A(config)# router isis A(config-router)# net 49.0001.0000.0000.0001.00 A(config)# interface GigabitEthernet 0/0

	A(config-if)# ip address 10.1.1.1 255.255.255.0 A(config-if)# ip router isis
B	B(config)# router isis B(config-router)# net 49.0001.0000.0000.0002.00 B(config)# interface GigabitEthernet 0/0 B(config-if)# ip address 10.1.1.2 255.255.255.0 B(config-if)# ip router isis
C	C(config)# router isis C(config-router)# net 49.0001.0000.0000.0003.00 C(config)# interface GigabitEthernet 0/0 C(config-if)# ip address 10.1.1.3 255.255.255.0 C(config-if)# ip router isis
Проверка	Включите отправку пакетов Hello с интерфейса 10.1.1.1 на маршрутизаторе A на интерфейс 10.1.1.2 на маршрутизаторе B и интерфейс 10.1.1.3 на маршрутизаторе C. • Установите отношения соседства IS-IS между маршрутизатором A и маршрутизатором B, а также между маршрутизатором A и маршрутизатором C, при этом состояние соседа будет Up. • Проверьте LSP на маршрутизаторе A, маршрутизаторе B и маршрутизаторе C. Должны существовать системные идентификаторы 0000.0000.0001, 0000.0000.0002 и 0000.0000.0003
A	A# show isis neighbors A# show isis database detail
B	B# show isis neighbors
C	C# show isis neighbors

Выполнение простой настройки IS-ISv6

Сценарий: Маршрутизатор A и маршрутизатор B соединены через Ethernet.

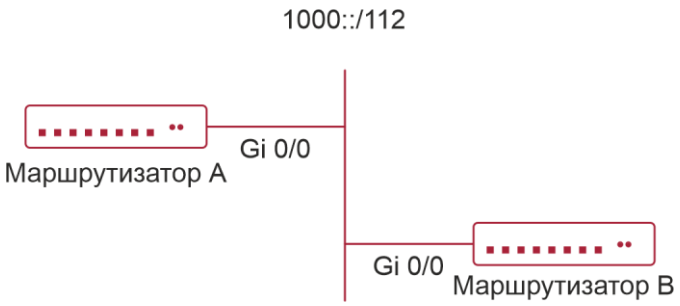


Рисунок 6-11. Топология broadcast-канала IS-ISv6

Шаги настройки	• Настройте IS-IS. • Настройте интерфейсы Ethernet
A	A(config)# router isis A(config-router)# net 49.0001.0000.0000.0001.00 A(config)# interface GigabitEthernet 0/0 A(config-if)# ipv6 address 1000 ::1/112 A(config-if)# ipv6 router isis
B	B(config)# router isis B(config-router)# net 49.0001.0000.0000.0002.00 B(config)# interface GigabitEthernet 0/0 B(config-if)# ipv6 address 1000 ::2/112 B(config-if)# ipv6 router isis
Проверка	Включите отправку пакетов Hello с интерфейса 1000::1 на маршрутизаторе A на интерфейс 1000::2 на маршрутизаторе B. Установите отношения соседства IS-IS между маршрутизаторами A и B, при этом состояние соседа будет Up. Проверьте LSP на маршрутизаторе A и маршрутизаторе B. Должны существовать системные идентификаторы 0000.0000.0001 и 0000.0000.0002
A	A# show isis neighbors A# show isis database detail
B	B# show isis neighbors

6.5.1.7. Распространенные ошибки

- IP-адреса интерфейсов, подключенных между соседями, не находятся в одном сегменте сети.
- Команда **ip router isis** не выполняется на интерфейсах.
- NET-адрес не настроен или на Level-1 существуют разные NET-адреса.
- **max-area-addresses** с обеих сторон настроен по-разному.
- **metric-style** с обеих сторон настроен по-разному.
- Уровни интерфейса с обеих сторон разные. Одна сторона — это Level-1, а другая — Level-2.
- Одна сторона настроена на режим P2P, тогда как другая сторона настроена на broadcast-режим.
- На одной стороне включена аутентификация, а на другой — нет.

6.5.2. Настройка пакетов Hello IS-IS

6.5.2.1. Эффект конфигурации

- Настройте интервал пакетов Hello на интерфейсе. Диапазон значений: от 1 до 65 535 в секундах.
- Настройте множитель времени удержания (holdtime) пакета Hello на интерфейсе IS-IS.

6.5.2.2. Примечания

- Вы можете изменить время удержания пакета Hello, используя команду **isis hello-multiplier**, команду **isis hello-interval** или обе команды.
- По умолчанию защита ЦП на устройствах включена. Для пакетов, сопоставленных с групповыми адресами назначения (AllISSystems, AllL1ISSystems и AllL2ISSystems) в IS-IS, существует ограничение по умолчанию (например, 400 пакетов в секунду) на количество пакетов, отправляемых в ЦП. Если устройство имеет много отношений соседства или отправляет пакеты Hello с короткими интервалами, пакеты IS-IS, которые получает устройство, могут превышать предел по умолчанию, вызывая частый flapping отношений соседства. Чтобы решить проблему, вы можете использовать команду защиты процессора в глобальном режиме для увеличения предела.

6.5.2.3. Шаги настройки

Настройка интервала пакетов Hello на интерфейсе

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **isis hello-interval** в режиме настройки интерфейса на нужном устройстве, если не указано иное.

Настройка множителя времени удержания пакета Hello на интерфейсе

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **isis hello-multiplier** в режиме настройки интерфейса на нужном устройстве, если не указано иное.

6.5.2.4. Проверка

- Включите маршрутизатор A для отправки пакетов Hello на маршрутизатор B и маршрутизатор C, а также захватывайте пакеты для проверки интервала передачи пакетов.
- Выключите маршрутизатор B или маршрутизатор C. По истечении времени удержания (holdtime) проверьте, недействительны ли соответствующие отношения соседства на маршрутизаторе A.

6.5.2.5. Связанные команды

Настройка интервала пакетов Hello на интерфейсе

Команда	**isis hello-interval** { *interval* | **minimal** } [**level-1** | **level-2**]
Описание параметра	*interval*: указывает интервал передачи пакетов Hello. Диапазон значений: от 1 до 65 535 в секундах. Значение по умолчанию — 10. **minimal**: указывает минимальное значение времени удержания, равное 1. **level-1**: применяет настройку к пакетам Hello Level-1. **level-2**: применяет настройку к пакетам Hello Level-2
Командный режим	Режим настройки интерфейса
Руководство по использованию	Используйте эту команду для изменения интервала передачи пакетов Hello. Интервал по умолчанию составляет 10 секунд. DIS отправляет пакеты Hello с частотой в три раза большей, чем устройства, не относящиеся к DIS, в broadcast-сети. Если IS выбран в качестве DIS на интерфейсе, по умолчанию интерфейс отправляет пакет Hello каждые 3,3 секунды. Если используется ключевое слово **minimal**, время удержания пакета Hello устанавливается равным 1. Интервал пакета Hello будет рассчитываться на основе множителя времени удержания. Если множитель времени удержания установлен на 4 и выполняется команда **isis hello-interval minimal**, интервал пакета Hello равен 1 с, разделенному на 4. Множитель времени удержания пакета Hello по умолчанию на интерфейсе IS-IS равен 3. Время удержания равно множителю времени удержания, умноженному на интервал пакета. Если используется ключевое слово **minimal**, время удержания устанавливается равным 1. Интервал пакета равен 1, разделенному на множитель времени удержания. Если множитель времени удержания установлен на 4 и выполняется команда **isis hello-interval minimal**, интервал пакета равен 1, разделенному на 4 с, что составляет 250 мс

Настройка множителя времени удержания пакета Hello на интерфейсе

Команда	**isis hello-multiplier** *multiplier-number* [**level-1** | **level-2**]
Описание параметра	*multiplier-number*: указывает множитель времени удержания пакета Hello. Диапазон значений: от 2 до 100. Значение по умолчанию — 3
Командный режим	Режим настройки интерфейса
Руководство по использованию	Время удержания пакета Hello равно интервалу пакета Hello, умноженному на множитель времени удержания

6.5.2.6. Пример конфигурации

Настройка интервала пакетов Hello и времени удержания на интерфейсе IS-IS

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте интервал пакетов Hello на интерфейсе IS-IS. • Настройте множитель времени удержания пакета Hello на интерфейсе IS-IS
	A(config)# interface GigabitEthernet 0/0 A(config-if)# isis hello-interval 5 A(config-if)# isis hello-multiplier 5
Проверка	• Включите маршрутизатор A для отправки пакетов Hello на маршрутизатор B и маршрутизатор C, а также захватывайте пакеты для проверки интервала передачи пакетов. • Выключите маршрутизатор B или маршрутизатор C. По истечении времени удержания проверьте, недействительны ли соответствующие отношения соседства на маршрутизаторе A
	A# show isis neighbor

6.5.3. Настройка IS-IS LSP

6.5.3.1. Эффект конфигурации

- **isis lsp-interval**: настраивает интервал LSP на интерфейсе IS-IS.
- **isis lsp-flood**: устанавливает количество LSP PDU, отправляемых интерфейсом IS-IS одновременно.
- **lsp-gen-interval**: настраивает минимальный интервал генерации LSP. Интервал генерации LSP — это интервал между временем генерации LSP новой версии и временем генерации LSP старой версии.

- **isis retransmit-interval**: если устройство на одном конце P2P-канала отправляет пакет LSP и устройство не получает ответа в течение определенного периода времени, оно определяет, что пакет LSP потерян или отброшен из-за ошибки. Устройство повторно отправит пакет LSP.
- **lsp-gen-interval**: указывает экспоненциальный алгоритм отсрочки генерации пакетов LSP. Любое обновление связанной информации, формирующей пакет LSP, приводит к генерации пакета LSP. Во время flapping-а сети часто генерируются пакеты LSP, что увеличивает потребление системных ресурсов. Соответствующее значение можно установить, выполнив команду **lsp-gen-interval**. Таким образом, пакеты LSP генерируются и объявляются вовремя, когда сеть стабильна. Когда сеть становится нестабильной, по мере продолжения flapping-а генерируется меньше пакетов LSP, что снижает потребление устройств.
- **lsp-refresh-interval**: все текущие LSP периодически передаются повторно, чтобы позволить каждому узлу сети поддерживать последние LSP. Период повторной передачи называется интервалом обновления LSP, целью которого является обновление и синхронизация LSP во всей области.
- **max-lsp-lifetime**: LSP содержит поле, указывающее время жизни. Когда устройство генерирует LSP, в поле устанавливается максимальное время жизни LSP. После того, как LSP получен устройством peer, его время жизни со временем будет уменьшаться. Устройство peer заменит старый LSP на вновь полученный. Если устройство не получает нового LSP до тех пор, пока время жизни существующего LSP не уменьшится до 0, существующий LSP по-прежнему будет храниться в LSDB еще 60 секунд. Если в течение этого периода устройство по-прежнему не получит нового LSP, существующий LSP будет удален из LSDB. Этот механизм обновляет и синхронизирует LSP во всей области.
- **min-lsp-arrival**: во время flapping-а сети пакеты LSP часто дублируются, а порядковый номер пакета LSP постоянно увеличивается. В результате устройство продолжает получать дубликаты пакетов LSP с разными порядковыми номерами. Если устройство обрабатывает дубликаты пакетов LSP, потребляется больше системных ресурсов. Соответствующее значение можно установить, выполнив команду **min-lsp-arrival**. Таким образом, LSP принимаются и обрабатываются вовремя, когда сеть стабильна. Когда сеть становится нестабильной, по мере продолжения flapping-а принимается и обрабатывается меньше повторяющихся пакетов LSP, что снижает потребление устройства.
- **ignore-lsp-errors:** после получения LSP локальный сосед IS-IS вычисляет свою контрольную сумму и сравнивает ее с контрольной суммой, содержащейся в LSP. По умолчанию, если две контрольные суммы несовместимы, LSP будет отброшен. Если вы запустите команду **ignore-lsp-errors**, чтобы настроить игнорирование ошибок контрольной суммы, LSP будет обрабатываться нормально, несмотря на несогласованность контрольной суммы.
- **lsp-fragments-extend**: включает расширение фрагмента LSP, которое используется для создания расширенного LSP, когда 256 фрагментов исходного LSP израсходованы.

6.5.3.2. Примечания

- Интервал обновления LSP должен быть меньше максимального времени жизни LSP.
- Максимальное время жизни LSP должно быть больше интервала обновления LSP.

- Значение **initial-interval** не может быть больше значения **maximum-interval**. В противном случае значение **initial-interval** будет использоваться как значение **maximum-interval**.
- Значение **hold-interval** не может быть больше значения **maximum-interval**. В противном случае значение **hold-interval** будет использоваться как значение **maximum-interval**.
- Значение **initial-interval** не может быть больше, чем значение **hold-interval**. В противном случае значение **initial-interval** будет использоваться как значение **hold-interval**.

6.5.3.3. Шаги настройки

Настройка минимального интервала LSP

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **isis lsp-interval** в режиме настройки интерфейса на нужном устройстве, если не указано иное.

Настройка максимального количества пакетов LSP, отправляемых одновременно

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **isis lsp-flood** в режиме настройки интерфейса на нужном устройстве, если не указано иное.

Настройка интервала повторной передачи LSP

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **isis retransmit-interval** в режиме конфигурации интерфейса на нужном устройстве, если не указано иное.

Настройка цикла генерации пакетов LSP

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **lsp-gen-interval** в режиме настройки интерфейса на нужном устройстве, если не указано иное.

Настройка интервала обновления LSP

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **lsp-refresh-interval** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Настройка времени жизни LSP

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **max-lsp-lifetime** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Настройка интервала приема повторяющихся пакетов LSP

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **min-lsp-arrival** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Настройка игнорирования ошибок контрольной суммы LSP

- Выполните эту настройку в соответствии с требованиями.

- Запустите команду **ignore-lsp-errors** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Настройка расширения фрагмента LSP

- Выполните эту настройку в соответствии с требованиями.
- Запустите команды **lsp-fragments-extend** и **virtual-system** в режиме конфигурации процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

6.5.3.4. Проверка

- Постоянно обновляйте LSP и фиксируйте LSP, чтобы проверять минимальный интервал LSP.
- Отключите соседние маршруты и захватите LSP, чтобы проверить интервал повторной передачи LSP.
- Захватите LSP, чтобы проверить интервал обновления.
- Проверьте время жизни LSP.
- Отправьте LSP с неправильной контрольной суммой и проверьте, отброшен ли LSP.
- Уменьшите значение команды **lsp-length originate**, добавьте информацию о маршрутизации и запишите LSP, чтобы проверить, генерируется ли более 256 фрагментов LSP.

6.5.3.5. Связанные команды

Настройка минимального интервала LSP

Команда	**isis lsp-interval** *interval* [**level-1** | **level-2**]
Описание параметра	*milliseconds*: указывает интервал LSP. Диапазон значений: от 1 до 4 294 967 295 в миллисекундах. **level-1**: применяет настройку только к LSP Level-1. **level-2**: применяет настройку только к LSP Level-2
Командный режим	Режим настройки интерфейса

Настройка максимального количества пакетов LSP, отправляемых одновременно

Команда	**isis lsp-flood** *lsp-number* [**level-1** | **level-2**]
Описание параметра	*lsp-number*: указывает максимальное количество пакетов LSP, отправленных интерфейсом IS-IS одновременно. Диапазон значений: от 1 до 1000. Значение по умолчанию — 5. **level-1**: применяет конфигурацию только для Level-1. **level-2**: применяет конфигурацию только для Level-2

Командный режим	Режим настройки интерфейса

Настройка цикла генерации пакетов LSP

Команда	**lsp-gen-interval** [**level-1** | **level-2**] *maximum-interval* [*initial-interval hold-interval*]
Описание параметра	**level-1:** применяет конфигурацию только для Level-1. **level-2:** применяет конфигурацию только для Level-2. *maximum-interval*: указывает максимальный интервал для генерации двух последовательных пакетов LSP. Диапазон значений: от 1 до 65 535 (в секундах). Значение по умолчанию — 5. *initial-interval*: указывает время ожидания для первой генерации пакета LSP. Диапазон значений: от 0 до 60 000 (в миллисекундах). Значение по умолчанию — 50. *hold-interval*: указывает минимальный интервал для генерации пакета LSP во второй раз. Диапазон значений: от 10 до 60 000 (в миллисекундах). Значение по умолчанию — 200
Режим конфигурации	Режим настройки процесса маршрутизации IS-IS
Руководство по использованию	Интервал генерации пакетов LSP относится к интервалу генерации двух разных пакетов LSP. Меньший интервал генерации указывает более быструю конвергенцию сети,что, однако, будет сопровождаться частым флудингом сети. Время ожидания для генерации пакета LSP в первый раз является начальным интервалом. Если сеть становится нестабильной, интервал восстановления пакета LSP изменяется на меньший, чем максимальный интервал, и интервал для генерации пакета LSP во второй раз становится интервалом ожидания. К этому интервалу будет добавлен соответствующий штраф: следующий интервал для регенерации пакета LSP удваивает предыдущий интервал для генерации того же пакета LSP, пока интервал регенерации не достигнет максимального значения интервала. Последующие пакеты LSP будут генерироваться с максимальным интервалом. Когда сеть становится стабильной, интервал восстановления пакета LSP становится больше максимального интервала, и время ожидания генерации пакета LSP восстанавливается до начального интервала. Изменения канала предъявляют высокие требования к конвергенции. Начальный интервал может быть установлен на небольшое значение. Предыдущие параметры также можно изменить на более высокие значения, чтобы снизить нагрузку на процессор.

	Значение **initial-interval** не может быть больше, чем **maximum-interval**. В противном случае значение **initial-interval** будет использоваться в качестве значения **maximum-interval**. Значение **hold-interval** не может быть больше, чем **maximum-interval**. В противном случае значение **hold-interval** будет использоваться в качестве значения **maximum-interval**. Значение **initial-interval** не может быть больше, чем **hold-interval**. В противном случае значение **initial-interval** будет использоваться в качестве значения **hold-interval**

Настройка интервала повторной передачи LSP

Команда	**isis retransmit-interval** *interval* [**level-1** | **level-2**]
Описание параметра	*seconds*: указывает интервал повторной передачи LSP. Диапазон значений: от 0 до 65 535 в секундах. **level-1**: применяет настройку только к LSP Level-1. **level-2**: применяет настройку только к LSP Level-2
Командный режим	Режим настройки интерфейса
Руководство по использованию	Используйте эту команду для настройки интервала повторной передачи LSP. В сети P2P, если после того, как устройство отправит LSP, устройство не получит ответа PSNP в течение времени, указанного этой командой, оно отправит LSP повторно. Если интервал повторной передачи установлен на 0, LSP не будет отправляться повторно

Настройка интервала обновления LSP

Команда	**lsp-refresh-interval** *interval*
Описание параметра	*interval*: указывает интервал обновления LSP. Диапазон значений: от 1 до 65 535 в секундах. Значение по умолчанию — 900
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	После того, как LSP остается стабильным в течение периода, указанного этой командой, он будет обновлен и обновлен перед публикацией. Интервал обновления LSP должен быть меньше максимального времени жизни LSP

Настройка времени жизни LSP

Команда	**max-lsp-lifetime** *value*
Описание параметра	*value*: указывает максимальное время, в течение которого LSP остаются активными. Диапазон значений: от 1 до 65 535 в секундах. Значение по умолчанию — 1200
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Максимальное время жизни LSP должно быть больше интервала обновления LSP

Настройка интервала приема повторяющихся пакетов LSP

Команда	**min-lsp-arrival** [**level-1** | **level-2**] *maximum-interval initial-interval hold-interval*
Описание параметра	**level-1**: применяет конфигурацию только для Level-1. **level-2**: применяет конфигурацию только для Level-2. *maximum-interval*: указывает максимальный интервал для получения двух повторяющихся пакетов LSP. Диапазон значений: от 1 до 120 (в секундах). *initial-interval*: указывает интервал для первого получения дублированного пакета LSP. Диапазон значений: от 0 до 60 000 (в миллисекундах). *old-interval*: указывает минимальный интервал для получения дублированного пакета LSP во второй раз. Диапазон значений: от 10 до 60 000 (в миллисекундах)
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Интервал получения дубликата LSP-пакета в первый раз — это начальный интервал. Когда интервал получения дубликатов пакетов LSP меньше максимального интервала, интервал получения дубликата LSP-пакета во второй раз становится интервалом удержания. Кроме того, к этому интервалу добавляется соответствующий штраф: следующий интервал получения дублированного пакета LSP удваивает предыдущий интервал получения того же пакета LSP, пока этот интервал не достигнет максимального интервала. Когда сеть станет стабильной, интервал получения дубликата LSP-пакета становится больше максимального интервала, и интервал получения дублированного LSP-пакета восстанавливается до начального интервала.

	Изменения канала предъявляют высокие требования к конвергенции. Начальный интервал может быть установлен на небольшое значение. Предыдущие параметры также можно изменить на более высокие значения, чтобы снизить нагрузку на процессор. Значение **initial-interval** не может быть больше, чем **maximum-interval**. В противном случае значение **initial-interval** будет использоваться в качестве значения **maximum-interval**. Значение **hold-interval** не может быть больше, чем **maximum-interval**. В противном случае значение **hold-interval** будет использоваться в качестве значения **maximum-interval**. Значение **initial-interval** не может быть больше, чем **hold-interval**. В противном случае значение **initial-interval** будет использоваться в качестве значения **hold-interval**

Настройка игнорирования ошибок контрольной суммы LSP

Команда	**ignore-lsp-errors**
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	После получения LSP локальный сосед IS-IS вычисляет свою контрольную сумму и сравнивает ее с контрольной суммой, содержащейся в LSP. По умолчанию, если две контрольные суммы несовместимы, LSP будет отброшен. Если вы запустите команду **ignore-lsp-errors**, чтобы настроить игнорирование ошибок контрольной суммы, LSP будет обрабатываться нормально, несмотря на несогласованность контрольной суммы

Настройка расширения фрагмента LSP

Команда	**lsp-fragments-extend** [**level-1** | **level-2**] [**compatible rfc3786**]
Описание параметра	**level-1**: применяет настройку только к LSP Level-1. **level-2**: применяет настройку только к LSP Level-2. **compatible**: указывает на совместимость с версией RFC расширенных LSP. **rfc3786**: расширяет старую версию LSP
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Используйте эту команду, чтобы включить расширение фрагмента LSP

Настройка дополнительного системного идентификатора

Команда	**virtual-system** *system-id*
Описание параметра	*system-id*: указывает дополнительный системный идентификатор (6 байт)
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Используйте эту команду для настройки дополнительного системного идентификатора процесса маршрутизации IS-IS, который используется расширенным LSP, созданным после использования 256 фрагментов исходного LSP. Чтобы включить расширение фрагмента, выполните команду **lsp-fragments-extend**

6.5.3.6. Пример конфигурации

Настройка минимального интервала LSP

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте минимальный интервал LSP
	A(config)# interface GigabitEthernet 0/1 A(config-if)# isis lsp-interval 100 level-2
Проверка	Запустите команду **show isis interface**, чтобы постоянно обновлять LSP и захватывать LSP для проверки минимального интервала LSP

Настройка максимального количества пакетов LSP, отправляемых одновременно

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте максимальное количество пакетов LSP, отправляемых одновременно
	A(config)# interface GigabitEthernet 0/1 A(config-if)# isis lsp-flood 10 level-2
Проверка	Запустите команду **show isis interface**, чтобы проверить максимальное количество LSP-пакетов, отправляемых одновременно

Настройка интервала повторной передачи LSP

Шаги настройки	• Настройте соседей IS-IS в режиме P2P. (опущено) • Настройте интервал повторной передачи LSP
	A(config)# interface serial 0/1 A(config-if)# isis retransmit-interval 10 level-2
Проверка	Отключите соседние маршруты и захватите LSP, чтобы проверить интервал повторной передачи LSP

Настройка цикла генерации пакетов LSP

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте цикл генерации пакетов LSP
	A(config)# router isis A(config-router)# lsp-gen-interval 5 50 100
Проверка	Генерируйте пакеты LSP часто, чтобы увидеть ,используется ли алгоритм экспоненциальной отсрочки

Настройка интервала обновления LSP

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте интервал обновления LSP
	A(config)# router isis A(config-router)# lsp-refresh-interval 600
Проверка	Захватите LSP для проверки интервала обновления

Настройка времени жизни LSP

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте время жизни LSP
	A(config)# router isis A(config-router)# max-lsp-lifetime 1500
Проверка	Проверьте время жизни LSP (поле **LSP Holdtime**)
	A# show isis database

Настройка интервала приема повторяющихся пакетов LSP

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте интервал получения дубликатов LSP-пакетов
	A(config)# router isis A(config-router)# min-lsp-arrival 10 100 200
Проверка	Проверьте поле **LSP Seq Num**, то есть статус принимающего LSP
	A# show isis database

Настройка игнорирования ошибок контрольной суммы LSP

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте игнорирование ошибок контрольной суммы LSP
	A(config)# router isis A(config-router)# ignore-lsp-errors
Проверка	Отправьте LSP с неправильной контрольной суммой и проверьте, отброшен ли LSP

Настройка расширения фрагмента LSP

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте расширение фрагмента LSP. • Настройте дополнительный системный идентификатор процесса маршрутизации IS-IS
	A(config)# router isis A(config-router)# lsp-fragments-extend A(config-router)# virtual-system 0000.0000.0034
Проверка	Уменьшите значение команды **lsp-length originate**, добавьте информацию о маршрутизации и запишите LSP, чтобы проверить, генерируется ли более 256 фрагментов LSP

6.5.4. Настройка SNP IS-IS

6.5.4.1. Эффект конфигурации

- CSNP периодически передаются DIS в broadcast-сети для синхронизации LSDB. В сети P2P CSNP отправляется только после установления соседских отношений. Интерфейс, настроенный на **mesh-groups**, можно настроить на периодическую отправку CSNP.

- Если вам необходимо установить **mesh-group** на интерфейсе IS-IS, запустите команду **isis csnp-interval**, чтобы настроить интервал CSNP, отличный от 0, и обеспечить полную синхронизацию LSP между соседями в сети. После этого CNSP будут периодически отправляться для синхронизации LSP.

6.5.4.2. Шаги настройки

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **isis csnp-interval** *interval* [**level-1** | **level-2**] в режиме настройки интерфейса на нужном устройстве, если не указано иное.

6.5.4.3. Проверка

Захватите CSNP в broadcast-сети, чтобы проверить интервал CSNP.

6.5.4.4. Связанные команды

Настройка фильтра регистрации источника

Команда	**isis csnp-interval** *interval* [**level-1** | **level-2**]
Описание параметра	*interval*: указывает интервал CSNP. Диапазон значений: от 0 до 65 535 в секундах. **level-1**: применяет настройку только к CSNP Level-1. **level-2**: применяет настройку только к CSNP Level-2
Командный режим	Режим настройки интерфейса
Руководство по использованию	Используйте эту команду для изменения интервала CSNP. По умолчанию DIS отправляет CSNP каждые 10 секунд в broadcast-сети. В сети P2P CSNP отправляется только после установления соседских отношений. Интерфейс, настроенный на **mesh-groups**, можно настроить на периодическую отправку CSNP. CSNP не отправляются, если интервал CSNP установлен на 0

6.5.4.5. Пример конфигурации

Настройка интервала Broadcast CSNP

Шаги настройки	• Настройте соседей IS-IS. (пропущено) • Настройте интервал broadcast CSNP
	A(config)# interface GigabitEthernet 0/1 A(config-if)# isis csnp-interval 20
Проверка	Перехватывайте пакеты, чтобы проверить интервал CSNP

6.5.5. Настройка типа уровня IS-IS

6.5.5.1. Эффект конфигурации

- IS-IS поддерживает двухуровневую систему для реализации управления маршрутизацией и расширяемого выбора маршрутов в большой сети. Каждый уровень заботится только о поддержании топологии соответствующей области.
- Вы можете запустить команду **is-type** в режиме конфигурации процесса маршрутизации IS-IS, чтобы настроить уровень IS-IS, или запустить команду **isis circuit-type** в режиме конфигурации интерфейса, чтобы настроить уровень IS-IS интерфейса. Уровни по умолчанию, заданные командами **is-type** и **isis circuit-type**, — это Level-1/Level-2. Если вы выполняете обе команды, интерфейс отправляет только PDU того же уровня, который указан в обеих командах.

6.5.5.2. Примечания

- Если Level-1 или Level-2-only настроен с использованием команды **circuit-type**, IS-IS будет отправлять PDU только соответствующего уровня.
- Если для интерфейса установлено значение **external**, он будет работать как интерфейс внешнего домена, и IS-IS не будет отправлять PDU соответствующего уровня.
- Устройство может иметь только один экземпляр, работающий на Level-2 (включая Level-1/Level-2).

6.5.5.3. Шаги настройки

Настройка типа системы

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **is-type** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Настройка типа circuit интерфейса

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **isis circuit-type** в режиме настройки интерфейса на нужном устройстве, если не указано иное.

6.5.5.4. Проверка

- Проверьте, обрабатываются ли только экземпляры Уровня (Level), заданные командой **is-type**, и создаются ли соседи соответствующего Уровня.
- Проверьте, отправляет ли интерфейс PDU только того же уровня, который указан командами **is-type** и **circuit-type**.

6.5.5.5. Связанные команды

Настройка типа системы

Команда	**is-type** { **level-1** | **level-1-2** | **level-2-only** }
Описание параметра	**level-1**: указывает, что IS-IS работает только на Level-1. **level-1-2**: указывает, что IS-IS работает на Level-1 и Level-2.

	level-2-only: указывает, что IS-IS работает только на Level-2
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Изменение значения **is-type** позволит включить или отключить маршруты соответствующего уровня

Настройка типа circuit интерфейса

Команда	**isis circuit-type** { **level-1** | **level-1-2** | **level-2-only** [**external**] }
Описание параметра	**level-1**: устанавливает отношения соседства Level-1. **level-1-2**: устанавливает отношения соседства Level-1/Level-2. **level-2-only**: устанавливает отношения соседства Level-2. **external**: использует интерфейс как интерфейс внешнего домена
Командный режим	Режим настройки интерфейса
Руководство по использованию	Если для типа circuit установлено значение Level-1 или Level-2-only, IS-IS будет отправлять PDU только соответствующего уровня. Если для типа системы установлено значение Level-1 или Level-2-only, IS-IS обрабатывает только экземпляры соответствующего уровня, а интерфейс отправляет только PDU того же уровня, указанного командами **is-type** и **circuit-type**. Если для интерфейса установлено значение **external**, интерфейс будет работать как интерфейс внешнего домена, и IS-IS не будет отправлять PDU соответствующего уровня

6.5.5.6. Пример конфигурации

Настройка уровней IS-IS

Требования к конфигурации: маршрутизатор A подключен к маршрутизатору B и маршрутизатору C последовательными каналами P2P. Маршрутизатор B и маршрутизатор C соединены через Ethernet, а маршрутизатор D и маршрутизатор E также соединены через Ethernet. На маршрутизаторе A настройте суммирование маршрутов области IS-IS. Обратите внимание, что суммирование маршрутов по области можно настроить только на пограничных устройствах.

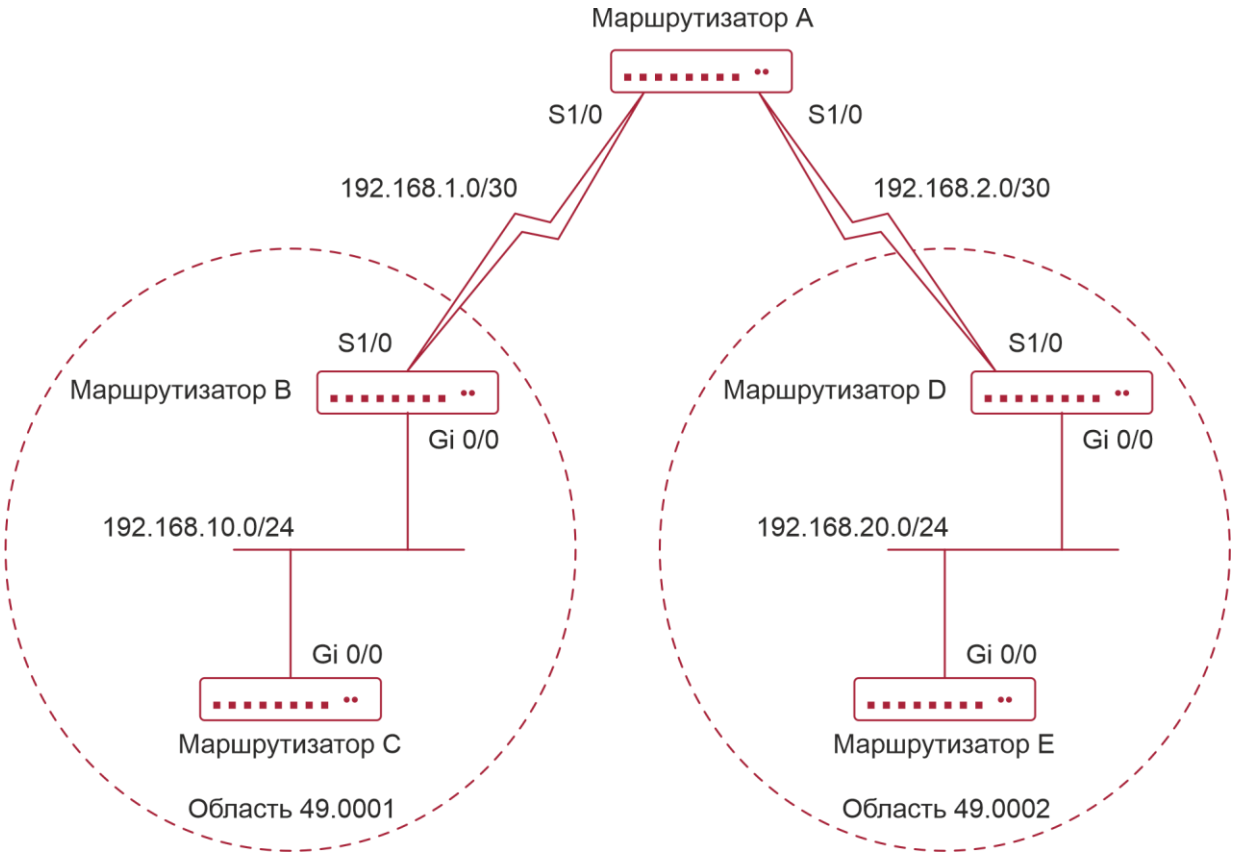


Рисунок 6-12. Конфигурация уровня IS-IS

Шаги настройки	• Настройте IS-IS. • Настройте интерфейсы Ethernet. • Настройте структуру уровня IS-IS
A	Настройте IS-IS. A(config)# router isis A(config-router)# net 50.0001.0000.0000.0001.00 A(config-router)# is-type level-2-only
	Настройте два последовательных порта. A(config)# interface Serial 1/0 A(config-if)# ip address 192.168.1.1 255.255.255.252 A(config-if)# ip router isis A(config)# interface Serial 1/1 A(config-if)# ip address 192.168.2.1 255.255.255.252

	A(config-if)# ip router isis
B	Настройте IS-IS
	B(config)# router isis B(config-router)# net 49.0001.0000.0000.0002.00
	Настройте интерфейс Ethernet
	B(config)# interface GigabitEthernet 0/0 B(config-if)# ip address 192.168.10.1 255.255.255.0 B(config-if)# ip router isis
	Настройте последовательный порт
	B(config)# interface Serial 1/0 B(config-if)# ip address 192.168.1.2 255.255.255.252 B(config-if)# ip router isis
C	Настройте IS-IS
	C(config)# router isis C(config-router)# net 49.0001.0000.0000.0003.00 C(config-router)# is-type level-1
	Настройте интерфейс Ethernet
	C(config)# interface GigabitEthernet 0/0 C(config-if)# ip address 192.168.10.2 255.255.255.0 C(config-if)# ip router isis
D	Настройте IS-IS
	D(config)# router isis D(config-router)# net 49.0002.0000.0000.0004.00
	Настройте интерфейс Ethernet
	D(config)# interface GigabitEthernet 0/0 D(config-if)# ip address 192.168.20.1 255.255.255.0

	D(config-if)# ip router isis
	Настройте последовательный порт
	D(config)# interface Serial 1/0 D(config-if)# ip address 192.168.2.2 255.255.255.252 D(config-if)# ip router isis
E	Настройте IS-IS
	E(config)# router isis E(config-router)# net 49.0002.0000.0000.0005.00 E(config-router)# is-type level-1
	Настройте интерфейс Ethernet
	E(config)# interface GigabitEthernet 0/0 E(config-if)# ip address 192.168.20.2 255.255.255.0 E(config-if)# ip router isis
Проверка	• Проверьте, нормально ли устанавливаются соседские отношения. • Захватывайте пакеты, чтобы проверить, отправляет ли маршрутизатор A только пакеты Level-2. • Перехватывайте пакеты, чтобы проверить, отправляют ли маршрутизаторы B и D только пакеты Level-1 и Level-2. • Перехватывайте пакеты, чтобы проверить, отправляют ли маршрутизаторы C и E только пакеты Level-1
A	A# show isis neighbors A# show isis database detail
B	B# show isis neighbors B# show isis database detail
C	C# show isis neighbors C# show isis database detail
D	D# show isis neighbors D# show isis database detail

E	E# show isis neighbors E# show isis database detail

6.5.6. Настройка аутентификации IS-IS

6.5.6.1. Эффект конфигурации

- Аутентификация интерфейса предназначена для установления и поддержания отношений соседства. Отношения соседства не могут быть установлены между двумя устройствами IS-IS с разными паролями аутентификации интерфейса. Это предотвращает подключение неавторизованных или неаутентифицированных устройств IS-IS к сети IS-IS, требующей аутентификации. Пароли аутентификации интерфейса инкапсулируются в пакеты Hello перед отправкой.
- Аутентификация области и аутентификация RD в IS-IS выполняются для проверки LSP, CSNP и PSNP, чтобы предотвратить внедрение несанкционированной или неаутентифицированной информации о маршрутизации в LSDB. Пароли аутентификации инкапсулируются в LSP, CSNP и PSNP перед отправкой.

6.5.6.2. Примечания

- Пароль аутентификации интерфейса инкапсулируется в пакет Hello перед отправкой интерфейсом. Когда интерфейс получает пакет Hello, он сверяет пароль в пакете с существующим.
- Пароли аутентификации области инкапсулированы в LSP Level-1, CSNP и PSNP. Когда интерфейс получает LSP, CSNP или PSNP, он сверяет пароль в пакете с существующим.
- Пароли аутентификации RD инкапсулированы в LSP Level-2, CSNP и PSNP. Когда интерфейс получает LSP, CSNP или PSNP, он сверяет пароль в пакете с существующим.

6.5.6.3. Шаги настройки

Настройка аутентификации интерфейса

- Выполните эту настройку в соответствии с требованиями.
- Настройте **isis password** в режиме настройки интерфейса на нужном устройстве, если не указано иное.

Настройка аутентификации области

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **area-password** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Настройка аутентификации RD

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **domain-password** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

6.5.6.4. Проверка

- Аутентификация открытого текста IS-IS обеспечивает лишь ограниченную безопасность, поскольку пароль, передаваемый через пакет, виден.
- Аутентификация IS-IS MD5 обеспечивает более высокий уровень безопасности, поскольку пароль, передаваемый через пакет, шифруется с использованием алгоритма MD5.

6.5.6.5. Связанные команды

Настройка пароля для аутентификации открытого текста пакетов Hello на интерфейсе

Команда	**isis password** [**0** | **7**] *password* [**send-only**] [**level-1** | **level-2**]
Описание параметра	**0**: указывает, что ключ отображается в виде открытого текста. **7**: указывает, что ключ отображается в зашифрованном виде. *password-string*: указывает строку пароля для аутентификации в виде открытого текста. Строка может содержать до 126 символов. **send-only**: указывает, что пароль аутентификации в виде открытого текста используется только для аутентификации отправленных пакетов. Полученные пакеты не аутентифицируются. **level-1**: применяет настройку к типу circuit Level-1. **level-2**: применяет настройку к типу circuit Level-2
Командный режим	Режим настройки интерфейса
Руководство по использованию	Используйте эту команду для настройки пароля для аутентификации пакетов Hello на интерфейсе. Используйте форму **no** этой команды, чтобы очистить пароль. Если уровень не указан, по умолчанию пароль вступает в силу для типов circuit Level-1 и Level-2. Эта команда не вступает в силу, если выполняется команда **isis authentication mode**. Вам необходимо сначала удалить предыдущую конфигурацию команды. Если вы включаете параметр **send-only** при удалении конфигурации команды **isis authentication mode**, отменяется только настройка параметра

Указание аутентификации интерфейса в виде открытого текста или MD5

Команда	**isis authentication mode** { **md5** | **text** } [**level-1** | **level-2**]
Описание параметра	**md5**: использует аутентификацию MD5. **text**: использует аутентификацию в виде открытого текста.

	level-1: применяет настройку к типу circuit Level-1. **level-2**: применяет настройку к типу circuit Level-2
Командный режим	Режим настройки интерфейса
Руководство по использованию	Используйте эту команду, чтобы указать режим аутентификации, прежде чем вы сможете активировать цепочку ключей, настроенную с помощью команды **isis authentication key-chain**. Если уровень не указан, режим аутентификации вступит в силу для типов circuit Level-1 и Level-2. Если вы используете команду **isis authentication mode** после выполнения команды **isis password** для настройки аутентификации в виде открытого текста, предыдущая конфигурация команды будет перезаписана. Команда **isis password** не вступает в силу, если выполняется команда **isis authentication mode**. Чтобы запустить команду **isis password**, сначала удалите конфигурацию команды **isis authentication mode**

Настройка пароля для аутентификации интерфейса

Команда	**isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**]
Описание параметра	*name-of-chain*: указывает название цепочки ключей. Максимальная длина — 255. **level-1**: указывает, что цепочка ключей аутентификации вступает в силу для Level-1. **level-2**: указывает, что цепочка ключей аутентификации вступает в силу для Level-2
Командный режим	Режим настройки интерфейса
Руководство по использованию	Аутентификация не выполняется, если с помощью команды **key chain** не настроена цепочка ключей. В дополнение к команде **key chain** вам также необходимо запустить команду **isis authentication mode**, чтобы аутентификация цепочки ключей IS-IS вступила в силу. Цепочка ключей применима для аутентификации по открытому тексту и аутентификации MD5. Какой режим аутентификации использовать, можно определить с помощью команды **isis authentication mode**. Для аутентификации в виде открытого текста строка ключей в цепочке ключей не может превышать 80 символов; в противном случае цепочка ключей будет недействительна.

	Одновременно можно использовать только один цепочку ключей. После того, как вы настроите новый цепочку ключей, она заменит исходную. Если уровень не указан, цепочка ключей вступает в силу для Level-1 и Level-2. Цепочка ключей применима к пакетам Hello. IS-IS отправит или получит пароли, принадлежащие цепочке ключей. Цепочка ключей может содержать несколько паролей. Для отправки пакета предпочтительно используется пароль с меньшим серийным номером. Когда пакет прибудет на устройство peer, устройство получит пакет, если пароль, передаваемый в пакете, соответствует паролю в цепочке ключей. Команды аутентификации (например, **authentication key-chain**), выполняемые в режиме конфигурации процесса маршрутизации IS-IS, предназначены для LSP и SNP. Они не действуют для интерфейсов IS-IS

(Опционально) Применение аутентификации интерфейса только к отправленным пакетам (полученные пакеты не аутентифицируются)

Команда	**isis authentication send-only** [**level-1** | **level-2**]
Описание параметра	**level-1**: устанавливает режим **send-only** для Level-1 на интерфейсе. **level-2**: устанавливает на интерфейсе режим **send-only** для Level-2
Командный режим	Режим настройки интерфейса
Руководство по использованию	Используйте эту команду, чтобы разрешить IS-IS устанавливать пароль аутентификации в пакете Hello, отправленном интерфейсом. Однако IS-IS не проверяет подлинность пакета Hello, полученного интерфейсом. Эту команду можно использовать перед развертыванием аутентификации интерфейса IS-IS на всех устройствах в сети или перед изменением пароля или режима аутентификации. После запуска команды **isis authentication send-only** устройства не будут аутентифицировать полученные пакеты Hello, чтобы избежать flapping-а сети при развертывании аутентификации интерфейса IS-IS. После развертывания аутентификации во всей сети запустите команду **no isis authentication send-only**, чтобы отменить настройку **send-only**. Команда **isis authentication send-only** применима к аутентификации по открытому тексту и аутентификации MD5. Вы можете запустить команду **isis authentication mode**, чтобы указать режим аутентификации для интерфейса IS-IS. Если уровень не указан, режим аутентификации вступит в силу для Level-1 и Level-2 на интерфейсе

Настройка пароля для аутентификации по открытому тексту области (Level-1)

Команда	**area-password** [**0** | **7**] *password* [**send-only**]
Описание параметра	**0**: указывает, что ключ отображается в виде открытого текста. **7**: указывает, что ключ отображается в зашифрованном виде. *password-string*: указывает строку пароля для аутентификации в виде открытого текста. Строка может содержать до 126 символов. **send-only**: указывает, что пароль аутентификации в виде открытого текста используется только для аутентификации отправленных пакетов Hello в областях Level-1. Полученные пакеты Hello не аутентифицируются
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Запустите эту команду, чтобы включить аутентификацию полученных LSP, CSNP и PSNP в областях Level-1 и включить аутентификационную информацию в эти пакеты перед их отправкой. Все устройства IS-IS в области должны быть настроены с использованием одного и того же пароля. Эта команда не вступает в силу, если выполняется команда **authentication mode**. Вам необходимо сначала удалить предыдущую конфигурацию команды. Чтобы удалить пароль, выполните команду **no area-password**. Если вы запустите команду **no area password send-only**, отменяется только настройка **send-only**. Если вы последовательно запускаете команды **area-password** *psw* **send-only** и **no area-password send-only**, конфигурация меняется на **area-password** *psw*

Настройка пароля для аутентификации открытого текста RD (Level-2)

Команда	**domain-password** [**0** | **7**] *password* [**send-only**]
Описание параметра	**0**: указывает, что ключ отображается в виде открытого текста. **7**: указывает, что ключ отображается в зашифрованном виде. *password-string*: указывает строку пароля для аутентификации в виде открытого текста. Строка может содержать до 126 символов. **send-only**: указывает, что пароль аутентификации в виде открытого текста используется только для аутентификации отправленных пакетов Hello в областях Level-1. Полученные пакеты Hello не аутентифицируются

Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Запустите эту команду, чтобы включить аутентификацию полученных LSP, CSNP и PSNP в доменах Level-2 и включить аутентификационную информацию в эти пакеты перед их отправкой. Все устройства IS-IS в домене Level-2 должны быть настроены с использованием одного и того же пароля. Эта команда не вступает в силу, если выполняется команда **authentication mode**. Вам необходимо сначала удалить предыдущую конфигурацию команды. Чтобы удалить пароль, выполните команду **no domain-password**. Если вы запустите команду **no domain-password send-only**, отменяется только настройка **send-only**. Если последовательно выполнить команды **domain-password** *psw* **send-only** и no **domain-password send-only**, конфигурация изменится на **domain-password** *psw*

Указание режима аутентификации IS-IS RD

Команда	**authentication mode** { **md5** | **text** } [**level-1** | **level-2**]
Описание параметра	**md5**: использует аутентификацию MD5. **text**: использует аутентификацию в виде открытого текста. **level-1**: указывает, что режим аутентификации вступает в силу для Level-1. **level-2**: указывает, что режим аутентификации вступает в силу для Level-2
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Используйте эту команду, чтобы указать режим аутентификации, прежде чем вы сможете сделать цепочку ключей, настроенную с помощью команды **authentication key-chain**, вступить в силу. Если уровень не указан, режим аутентификации вступит в силу для Level-1 и Level-2. Если вы используете команду **authentication mode** после выполнения команды **area-password** или **domain-password** для настройки аутентификации в виде открытого текста, предыдущая конфигурация команды будет перезаписана. Команда **area-password** или **domain-password** не вступает в силу, если выполняется команда **authentication mode**. Чтобы запустить команду **area-password** или **domain-password**, сначала удалите конфигурацию команды **authentication mode**

Указание цепочки ключей для аутентификации IS-IS

Команда	**authentication key-chain** *name-of-chain* [**level-1** | **level-2**]
Описание параметра	*name-of-chain*: указывает название цепочки ключей. Максимальная длина — 255. **level-1**: указывает, что цепочка ключей аутентификации вступает в силу для Level-1. **level-2**: указывает, что цепочка ключей аутентификации вступает в силу для Level-2
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Аутентификация не выполняется, если с помощью команды **key chain** не настроена цепочка ключей. В дополнение к команде **key chain** вам также необходимо запустить команду **authentication mode**, чтобы аутентификация цепочки ключей IS-IS вступила в силу. Цепочка ключей применима для аутентификации по открытому тексту и аутентификации MD5. Какой режим аутентификации использовать, можно определить с помощью команды **authentication mode**. Для аутентификации в виде открытого текста строка ключей в цепочке ключей не может превышать 80 символов; в противном случае цепочка ключей будет недействительна. Одновременно можно использовать только одну цепочку ключей. После того, как вы настроите новую цепочку ключей, она заменит исходную. Если уровень не указан, цепочка ключей вступает в силу для Level-1 и Level-2. Цепочка ключей применима к LSP, CSNP и PSNP. IS-IS отправит или получит пароли, принадлежащие цепочке ключей. Цепочка ключей может содержать несколько паролей. Для отправки пакета предпочтительно используется пароль с серийным номером. Когда пакет прибудет на устройство peer, устройство получит пакет, если пароль, передаваемый в пакете, соответствует паролю в цепочке ключей

Применение аутентификации IS-IS только к отправленным пакетам

Команда	**authentication send-only** [**level-1** | **level-2**]
Описание параметра	**level-1**: применяет настройку **send-only** к Level-1. **level-2**: применяет настройку **send-only** к Level-2

Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Используйте эту команду, чтобы разрешить IS-IS устанавливать пароль аутентификации в отправляемом пакете Hello. Однако IS-IS не аутентифицирует полученные пакеты Hello. Эту команду можно использовать перед развертыванием аутентификации IS-IS на всех устройствах в сети или перед изменением пароля или режима аутентификации. После запуска команды **authentication send-only** устройства не будут аутентифицировать полученные пакеты, чтобы избежать flapping-а сети при развертывании паролей аутентификации. После развертывания аутентификации во всей сети запустите команду **no isis authentication send-only**, чтобы отменить настройку **send-only**. Команда **authentication send-only** применима к аутентификации открытым текстом и аутентификации MD5. Вы можете запустить команду **authentication mode**, чтобы указать режим аутентификации. Если уровень не указан, режим аутентификации вступит в силу для Level-1 и Level-2

6.5.6.6. Пример конфигурации

Настройка аутентификации IS-IS

Требования к конфигурации: маршрутизатор A, маршрутизатор B и маршрутизатор C подключены через Ethernet и работают по протоколу IS-IS. Маршрутизатор A — это устройство Level-1, Маршрут B — устройство Level-1/Level-2, а Маршрутизатор C — устройство Level-2. Существуют следующие требования к конфигурации: примените аутентификацию открытого текста к пакетам Hello между маршрутизаторами A и B, а также к LSP и SNP Level-1. Примените аутентификацию MD5 к пакетам Hello между маршрутизаторами B и C, а также LSP и SNP Level-2.



Рисунок 6-13. Топология аутентификации IS-IS

Шаги настройки	• Настройте IS-IS. • Настройте интерфейсы Ethernet. • Настройте пароль для аутентификации IS-IS

A	Настройте IS-IS
	A(config)# router isis A(config-router)# net 49.0001.0000.0000.0001.00 A(config-router)# is-type level-1 A(config-router)# area-password aa
	Настройте интерфейс Ethernet. A(config)# interface GigabitEthernet 0/0 A(config-if)# ip address 192.168.20.1 255.255.255.0 A(config-if)# ip router isis A(config-if)# isis password cc
B	Настройте пароль для аутентификации IS-IS
	B(config)# key chain kc1 B(config-keychain)# key 1 B(config-keychain-key)# key-string aa B(config)# key chain kc2 B(config-keychain)# key 1 B(config-keychain-key)# key-string bb B(config)# key chain kc3 B(config-keychain)# key 1 B(config-keychain-key)# key-string cc
	Настройте IS-IS
	B(config)# router isis B(config-router)# net 49.0001.0000.0000.0002.00 B(config-router)# authentication mode text level-1 B(config-router)# authentication key-chain kc1 B(config-router)# authentication mode md5 level-2 B(config-router)# authentication key-chain kc2
	Настройте два интерфейса Ethernet
	B(config)# interface GigabitEthernet 0/0 B(config-if)# ip address 192.168.20.2 255.255.255.0

	B(config-if)# ip router isis B(config-if)# isis authentication mode text B(config-if)# isis authentication key-chain kc3 B(config)# interface GigabitEthernet 0/1 B(config-if)# ip address 192.168.30.2 255.255.255.0 B(config-if)# ip router isis B(config-if)# isis authentication mode md5 B(config-if)# isis authentication key-chain kc3
	Настройте пароль для аутентификации IS-IS
C	C(config)# key chain kc2 C(config-keychain)# key 1 C(config-keychain-key)# key-string bb C(config)# key chain kc3 C(config-keychain)# key 1 C(config-keychain-key)# key-string cc
	Настройте IS-IS
	C(config)# router isis C(config-router)# net 49.0002.0000.0000.0002.00 C(config-router)# is-type level-2 C(config-router)# authentication mode md5 level-2 C(config-router)# authentication key-chain kc2
	Настройте интерфейс Ethernet
	C(config)# interface GigabitEthernet 0/1 C(config-if)# ip address 192.168.30.3 255.255.255.0 C(config-if)# ip router isiswww.qtech.ru C(config-if)# isis authentication mode md5 C(config-if)# isis authentication key-chain kc3
Проверка	Проверьте, нормально ли устанавливаются соседские отношения
A	A# show isis neighbors A# show isis database detail

B	B# show isis neighbors
C	C# show isis neighbors

6.5.6.7. Распространенные ошибки

- Между соседями настраиваются разные пароли аутентификации.
- Между соседями настраиваются разные режимы аутентификации.

6.5.7. Настройка IS-IS GR

6.5.7.1. Эффект конфигурации

IS-IS GR помогает повысить надежность системы. На устройствах, которые отделяют control plane от forwarding plane, GR гарантирует, что пересылка данных не прерывается во время перезапуска протокола маршрутизации.

Рабочий механизм IS-IS GR

Для того чтобы GR был успешным, должны быть выполнены следующие два условия: (1) топология сети стабильна; (2) устройство может обеспечить бесперебойную пересылку после перезапуска IS-IS.

В процессе GR существуют две роли: Restarter и Helper. Соответственно, IS-IS GR делится на возможность IS-IS GR Restart и возможность IS-IS GR Help. Устройство с возможностью GR Restart может отправить запрос GR и выполнить GR. Устройство с функцией GR Help может получить запрос GR и помочь своему соседу с внедрением GR. Процесс GR запускается, когда Restarter отправляет запрос GR. После получения запроса GR соседнее устройство переходит в режим Help, чтобы помочь Restarter-у восстановить свою LSDB, сохраняя при этом отношения соседства с Restarter-ом. Основной механизм работы GR заключается в следующем:

Когда устройству IS-IS необходимо выполнить GR, оно инструктирует своего соседа поддерживать свои отношения с соседями, чтобы другие устройства в сети не могли обнаружить изменение топологических отношений, а сосед не пересчитывал маршрут и не обновлял свою таблицу пересылки. Устройство IS-IS синхронизирует и восстанавливает LSDB в состояние до GR с помощью соседа, чтобы гарантировать, что таблица маршрутизации и пересылки остается неизменной до и после реализации GR, а пересылка данных не прерывается.

В процессе GR Restarter выполняет следующие операции:

1. GR Restarter уведомляет GR Helper о том, что он будет перезапущен.

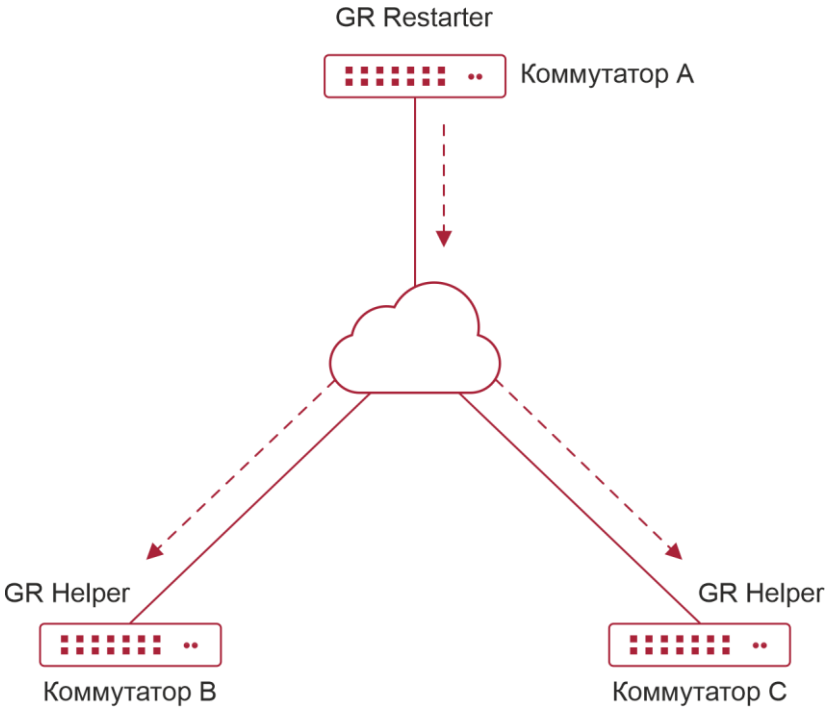


Рисунок 6-14. Уведомление о перезапуске (Restart) от GR Restarter

Коммутатор A является GR Restarter-ом, а коммутатор B и коммутатор C являются GR Helper-ами для коммутатора A. Коммутатор A отправляет запрос GR, инструктирующий всех своих соседей не удалять отношения соседства с коммутатором A при его перезапуске. После получения запроса GR соседи отправляют ответы GR на GR Restarter и будут поддерживать свои соседские отношения с GR Restarter в течение времени GR (заданного с помощью **GR grace-period**), уведомленного GR Restarter-ом.

2. GR Restarter перезапускается.

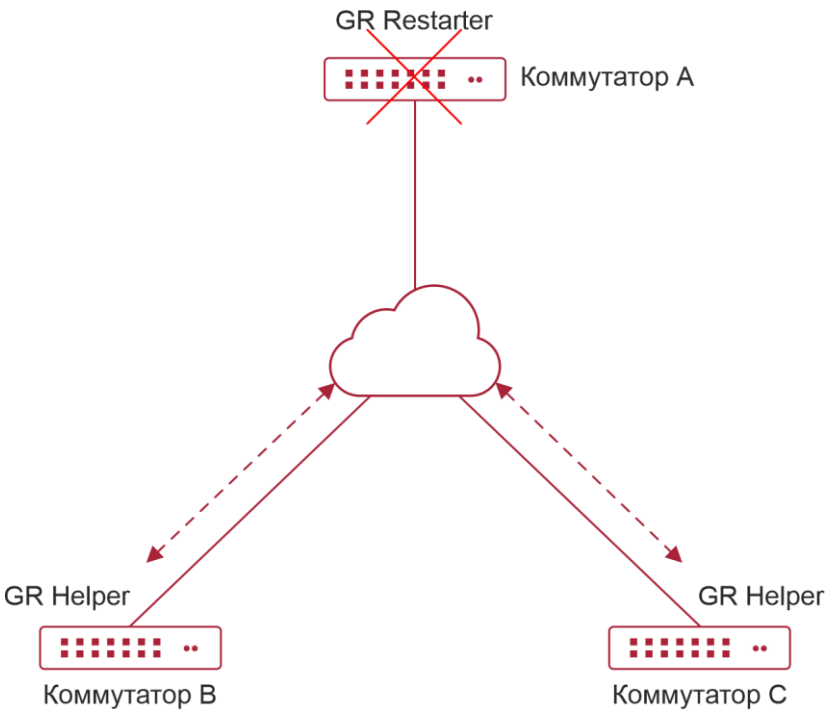


Рисунок 6-15. Перезапуск, выполняемый GR Restarter-ом

При перезапуске GR Restarter-а его интерфейс IS-IS переключается с состояния Down на Up. Поскольку GR Helper-ы знают, что GR Restarter находится в состоянии перезапуска IS-IS, они поддерживают отношения соседства с GR Restarter-ом в течение времени GR и сохраняют маршруты от GR Restarter-а.

3. GR Restarter синхронизирует информацию о топологии и маршрутизации от GR Helper-ов.

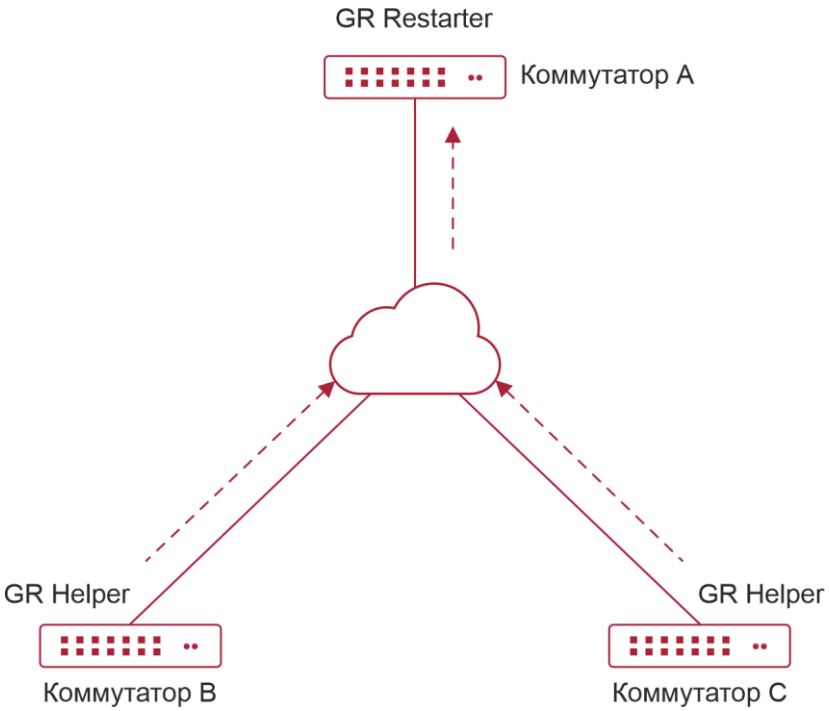


Рисунок 6-16. Синхронизация LSDB

После перезапуска IS-IS GR Restarter синхронизирует топологию или информацию о маршрутизации от GR Helper-ов и пересчитывает свою таблицу маршрутизации. Во время этого процесса любые изменения в таблице маршрутизации не обновляются в таблице пересылки.

4. GR завершается, когда GR Restarter завершает синхронизацию LSDB. Затем все устройства переходят в состояние взаимодействия IS-IS.

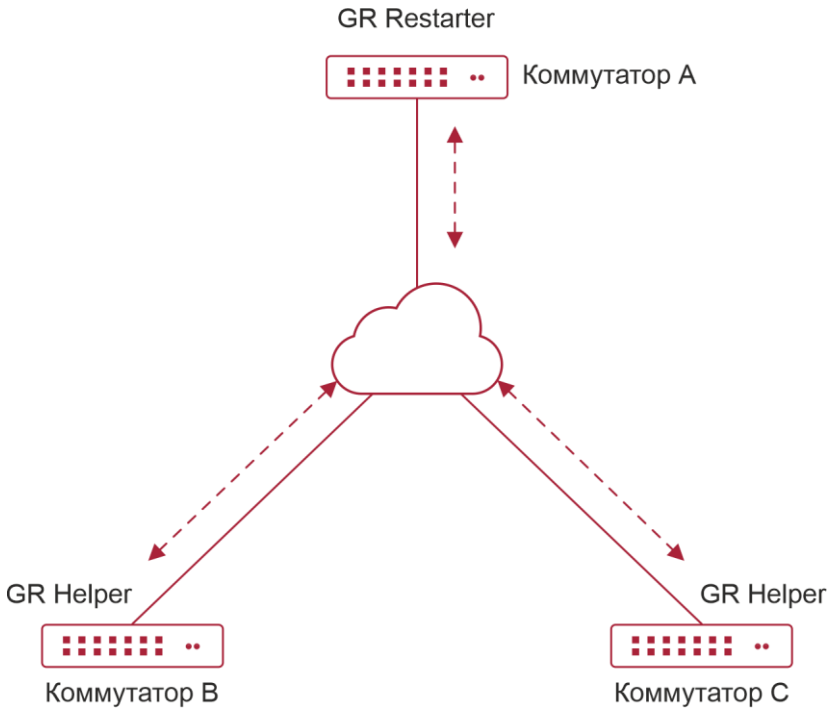


Рисунок 6-17. Завершение GR

После того как GR Restarter синхронизирует все необходимые данные, все устройства переходят в состояние взаимодействия IS-IS. Таблица маршрутизации GR Restarter обновляется до таблицы пересылки, а недействительные записи удаляются. Поскольку GR Restarter полностью восстанавливается в состояние перед перезапуском при стабильных условиях сети, его таблица маршрутизации и таблица пересылки остаются неизменными до и после GR.

6.5.7.2. Примечания

IS-IS GR реализован на основе RFC5306: Сигнализация перезапуска для IS-IS.

ПРИМЕЧАНИЕ: все продукты поддерживают функцию IS-IS GR Helper.

6.5.7.3. Шаги настройки

Включение возможности IS-IS GR Restart

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **graceful-restart** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Настройка максимального времени GR

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **graceful-restart grace-period** в режиме конфигурации процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Включение возможности IS-IS GR Help

- Выполните эту настройку в соответствии с требованиями.

- Запустите команду **graceful-restart helper** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

6.5.7.4. Проверка

Проверьте, остаются ли неизменными таблица маршрутизации и таблица пересылки до и после GR.

6.5.7.5. Связанные команды

Включение возможности IS-IS GR Restart

Команда	**graceful-restart**
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Используйте эту команду, чтобы включить возможность IS-IS GR Restart. Пока условия сети остаются неизменными, IS-IS может быть перезапущен и восстановлен в состояние, предшествующее перезапуску, без влияния на пересылку данных

Настройка максимального времени GR

Команда	**graceful-restart grace-period** *seconds*
Описание параметра	*seconds*: указывает время GR. Диапазон значений: от 1 до 65 535 с. Значение по умолчанию — 300 с
Командный режим	Режим конфигурации процесса маршрутизации IS-IS

Включение возможности IS-IS GR Help

Команда	**graceful-restart helper disable**
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Используйте команду **graceful-restart helper disable**, чтобы отключить возможность IS-IS GR Help. Команда позволяет IS-IS игнорировать запрос GR, отправленный устройством на перезапуск

6.5.8. Настройка IS-IS NSR

6.5.8.1. Эффект конфигурации

Непрерывная маршрутизация IS-IS (IS-IS NSR) помогает повысить надежность системы. Во время переключения между активным и резервным устройствами в распределенном

режиме или режиме виртуального коммутатора (VSU) трафик пользовательских данных продолжает передаваться без перерывов.

Рабочий механизм IS-IS NSR

NSR поддерживает соответствующую информацию IS-IS от master Supervisor Engine к slave Supervisor Engine распределенного устройства или от master-устройства к slave-устройству в режиме VSU, чтобы устройство могло автоматически восстанавливать состояние канала и регенерировать маршрут при переключении активный/резервный, не требуя помощи от соседей устройства во время восстановления.

6.5.8.2. Примечания

Для одного и того же процесса IS-IS разрешены либо NSP, либо GR, поскольку они являются эксклюзивными.

Переключение распределенных устройств и устройств VSU занимает некоторое время. Если продолжительность жизни соседа IS-IS меньше продолжительности переключения, отношения соседства IS-IS с соседним устройством удаляются, и сервисы прерываются во время переключения. Поэтому рекомендуется установить продолжительность жизни соседа IS-IS не меньше значения по умолчанию. Если включено Fast Hello, продолжительность жизни соседа IS-IS составляет менее 1 секунды, а время взаимодействия соседей IS-IS истекает во время переключения, что приводит к сбоям NSR. Поэтому рекомендуется отключать Fast Hello, когда включен NSR.

6.5.8.3. Шаги настройки

Настройка IS-IS NSR

- Опционально. IS-IS NSR отключен по умолчанию. Выполните эту настройку по мере необходимости.
- Настройте NSR в режиме настройки процесса маршрутизации IS-IS на необходимых устройствах, если не указано иное.

6.5.8.4. Проверка

Убедитесь, что трафик пользовательских данных пересылается без перебоев во время переключения устройств в режиме горячего резервирования в распределенном режиме или режиме VSU.

6.5.8.5. Связанные команды

Включение NSR

Команда	**nsr**
Режим конфигурации	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	NSR выполняет резервное копирование соответствующей информации IS-IS от master Supervisor Engine к slave Supervisor Engine распределенного устройства или от master-устройства к slave-устройству в режиме VSU, чтобы устройство могло автоматически восстановить состояние канала и повторно сгенерировать маршрут при переключении активный/резервный режим

	без необходимости помощи соседних устройств во время восстановления. Такая информация, как отношения соседства и состояние канала, должны резервироваться. Для одного и того же процесса IS-IS разрешены либо NSP, либо GR, поскольку они являются эксклюзивными
	Переключение распределенных устройств и устройств VSU занимает некоторое время. Если продолжительность жизни соседа IS-IS меньше продолжительности переключения, отношения соседства IS-IS с соседним устройством удаляются, и сервисы прерываются во время переключения. Поэтому рекомендуется установить продолжительность жизни соседа IS-IS не меньше значения по умолчанию. Если включено Fast Hello, продолжительность активности соседа IS-IS составляет менее 1 секунды, а время взаимодействия соседей IS-IS истекает во время переключения, что приводит к сбоям NSR. Поэтому рекомендуется отключать Fast Hello, когда включен NSR. По умолчанию, если DIS является устройством QTECH, отношения соседства между соседним устройством и устройством QTECH поддерживаются не более 10 секунд (интерфейс DIS отправляет один пакет Hello каждые 3,3 секунды). Однако переключение устройств QTECH в активный/резервный режим занимает не менее 7 секунд. Если переключение происходит, когда интерфейс должен отправлять пакеты Hello, период повторного получения пакетов Hello соседним устройством может превышать 10 секунд, что приводит к отключению соседнего устройства. Чтобы избежать отключения соседа, когда NSR включен, увеличьте время поддержания отношений соседства с соседним устройством, которое должно отправлять пакеты Hello, на 10 секунд

6.5.9. Настройка поддержки BFD для IS-IS

6.5.9.1. Эффект конфигурации

IS-IS динамически обнаруживает соседей с помощью пакетов Hello. После того, как IS-IS включит функцию BFD, будет установлен сеанс BFD с соседом в состоянии Up. Механизм BFD используется для определения состояния соседа. Как только с помощью BFD обнаруживается сбой соседа, IS-IS немедленно выполняет конвергенцию сети. Время сходимости может быть уменьшено с 30 с до менее 1 с. По умолчанию пакеты IS-IS Hello в P2P-сети отправляются с интервалом 10 с, а время, необходимое для обнаружения сбоя соседа, в три раза превышает интервал пакета, то есть 30 с.

6.5.9.2. Примечания

- Прежде чем включать поддержку BFD для IS-IS, необходимо установить параметры сеанса BFD.
- Когда вы запускаете команду **bfd up-dampening** на интерфейсе с поддержкой BFD для IS-IS, вам необходимо запустить команду **bfd all-interfaces** с выбранной опцией [*anti-congestion*].

- При запуске команды **bfd all-interfaces** с выбранной опцией [*anti-congestion*] запустите команду **bfd up-dampening** на интерфейсе.
- IP-маршрутизация может привести к тому, что интерфейс соседа для настройки сеанса BFD будет несовместим с интерфейсом для исходящих пакетов BFD. В этом случае сеанс BFD невозможно настроить.
- Если интерфейс соседа для настройки сеанса BFD несовместим с интерфейсом для исходящих пакетов BFD, сеанс BFD невозможно настроить.

6.5.9.3. Шаги настройки

Включение поддержки BFD для IS-IS на всех интерфейсах

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **bfd all-interfaces** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Включение поддержки BFD для IS-IS на текущем интерфейсе

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **isis bfd** в режиме настройки интерфейса на нужном устройстве, если не указано иное.

6.5.9.4. Проверка

- Постройте топологию с двумя параллельными линиям связи. Обычно IS-IS выбирает одну линию связи в качестве master, а другую — в качестве резервной. Включите BFD на master-линии.
- Сделайте так, чтобы master-линия вышла из строя. Проверьте, выполняет ли IS-IS конвергенцию маршрутов на основе состояния мониторинга BFD и запускает резервную линию связи.

6.5.9.5. Связанные команды

Включение поддержки BFD для IS-IS на текущем интерфейсе

Команда	**bfd all-interfaces** [*anti-congestion*]
Описание параметра	*anti-congestion*: указывает опцию предотвращения перегрузки IS-IS BFD
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Вы можете включить или отключить BFD на интерфейсе IS-IS, используя любой из следующих двух методов: Способ 1. Запустите команду **bfd all-interfaces** в режиме конфигурации процесса маршрутизации IS-IS, чтобы включить BFD на всех интерфейсах IS-IS, а затем запустите команду **no bfd all-interfaces**, чтобы отключить BFD на всех интерфейсах IS-IS. Способ 2. Запустите команду **isis bfd** [**disable**] в режиме конфигурации интерфейса, чтобы включить BFD на указанном интерфейсе IS-IS, а

	затем запустите команду **isis bfd disable**, чтобы отключить BFD на интерфейсе

Включение поддержки BFD для IS-IS на текущем интерфейсе

Команда	**isis bfd** [*disable* | *anti-congestion*]
Описание параметра	*disable*: отключает поддержку BFD для IS-IS на текущем интерфейсе. *anti-congestion*: указывает опцию предотвращения перегрузки IS-IS BFD
Командный режим	Режим настройки интерфейса
Руководство по использованию	Вы можете включить или отключить BFD на интерфейсе IS-IS, используя любой из следующих двух методов: Способ 1. Запустите команду [**no**] **bfd all-interfaces** [**anti-congestion**] в режиме конфигурации процесса маршрутизации IS-IS, чтобы включить или отключить BFD на всех интерфейсах IS-IS. Способ 2: Запустите **isis bfd** [**disable** | **anti-congestion**] в режиме конфигурации интерфейса, чтобы включить или отключить BFD на указанном интерфейсе. Обычно BFD отправляет пакеты обнаружения с миллисекундными интервалами для определения состояния канала. Когда происходит исключение канала (например, отключенное соединение), BFD может быстро обнаружить его и дать указание IS-IS удалить отношения соседства и информацию о доступности соседа в LSP. Затем IS-IS пересчитывает и генерирует новый маршрут для обхода аномального канала, обеспечивая таким образом быструю конвергенцию. С появлением новых технологий, таких как мультисервисная транспортная платформа (MSTP), перегрузка каналов имеет тенденцию возникать в часы пик передачи данных. BFD быстро обнаруживает исключение канала и дает указание IS-IS удалить отношения соседства и информацию о доступности соседа в LSP. Переключение канала выполняется для обхода перегруженного канала. Пакет Hello для обнаружения соседей IS-IS отправляется каждые 10 с, а время его действия составляет 30 с. Пакет Hello по-прежнему может быть принят в обычном режиме, когда BFD обнаруживает исключение, и поэтому отношения соседства IS-IS быстро восстанавливаются, что приводит к восстановлению маршрута к перегруженному каналу. Затем BFD обнаруживает ненормальное соединение, и переключение канала выполняется снова. Этот процесс повторяется, что приводит к переключению маршрута между перегруженным каналом и другими каналами, вызывая повторяющийся flapping. Опция **anti-congestion** используется, чтобы избежать flapping-а маршрутизации в случае перегрузки канала. После настройки этой

	опции состояние соседа IS-IS по-прежнему сохраняется при возникновении перегрузки канала, но информация о доступности соседа в LSP удаляется. Маршрут переключается на нормальный канал. Когда перегруженный канал восстанавливается, информация о доступности соседей в LSP восстанавливается, и маршрут переключается обратно, что позволяет избежать flapping-а маршрута. При запуске команды **bfd all-interfaces** [*anti-congestion*] запустите команду **bfd up-dampening** на интерфейсе. Обе команды необходимо использовать вместе. Если вы запустите только одну команду, функция подавления flapping-а маршрута может не вступить в силу или могут возникнуть другие сетевые исключения

6.5.9.6. Пример конфигурации

Включение поддержки BFD для IS-IS на текущем интерфейсе

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Установите параметры сеанса BFD. (опущено) • Включите поддержку BFD для IS-IS на текущем интерфейсе
	A(config)# interface GigabitEthernet 0/1 A(config-if)# isis bfd
Проверка	Включите S1 (192.168.1.10) и S2 (192.168.2.10) для отправки пакетов G1 (229.1.1.1) и G2 (229.1.2.1). Добавьте пользователя в группы G1 и G2. • Проверьте multicast-пакет, который получает пользователь. Пользователь должен получать только пакет (S1, G1). • Убедитесь, что в таблице маршрутизации PIM-SM нет записей (S1, G2), (S2, G1) и (S2, G2)
	A# show bfd neighbors detail

6.5.9.7. Распространенные ошибки

Поддержка BFD для IS-IS не включена на соседях.

6.5.10. Установка бита перегрузки IS-IS

6.5.10.1. Эффект конфигурации

Бит перегрузки используется в следующих трех ситуациях:

- Перегрузка устройства

На локальном узле IS-IS возникают проблемы с перегрузкой, например нехватка памяти или полная загрузка ЦП; в результате его таблица маршрутизации содержит неполные маршруты или не содержит данных о пересылке ресурсов. Вы можете установить бит перегрузки в LSP, чтобы указать соседу не использовать локальный узел в качестве устройства пересылки.

Чтобы установить бит перегрузки, запустите команду **set-overload-bit** без ключевого слова **on-startup**. Бит перегрузки можно настроить или отменить вручную. Когда локальный узел IS-IS будет восстановлен, вручную отмените настройку команды; в противном случае узел всегда находится в состоянии перегрузки.

- Мгновенная black hole

В сценарии, описанном в RFC3277, скорость конвергенции IS-IS выше, чем скорость BGP; в результате после перезапуска узла IS-IS маршрут может стать мгновенно недоступным, что называется мгновенной black hole. Вы можете установить бит перегрузки в LSP, чтобы указать соседу не использовать локальный узел в качестве устройства пересылки, пока не истечет указанное время.

Чтобы установить бит перегрузки, запустите команду **set-overload-bit** с ключевым словом **on-startup**. Бит перегрузки может быть настроен или отменен автоматически узлом IS-IS в зависимости от конфигурации. Если выбрано ключевое слово **on-startup**, узел IS-IS автоматически переходит в мгновенное состояние black-hole после перезапуска. Когда отношения соседства установлены, узел IS-IS отправляет LSP с битом перегрузки, чтобы уведомить соседа о том, что локальный узел входит в состояние мгновенной black hole (или перегрузки), и дать указание соседу не использовать локальный узел в качестве пересылающего устройства. По истечении заданного времени узел IS-IS немедленно отправляет LSP с отмененным битом перегрузки, чтобы уведомить соседа о том, что локальный узел вышел из состояния мгновенной black hole (или перегрузки) и может работать как пересылающее устройство.

- Отключение реальной пересылки данных на локальном узле IS-IS

Если вам нужно подключить локальный узел IS-IS только к производственной сети для тестирования или для удовлетворения других функциональных требований, но не требуется, чтобы узел пересылал реальные данные в сети, вы можете установить бит перегрузки в LSP, чтобы дать указание соседу, что он не должен использовать локальный узел в качестве пересылающего устройства.

Чтобы установить бит перегрузки, запустите команду **set-overload-bit** без ключевого слова **on-startup**. Бит перегрузки можно настроить или отменить вручную. Вы можете установить ключевое слово **suppress** в зависимости от требований по ограничению информации о маршрутизации, передаваемой по LSP, в случае перегрузки. Например, можно запретить внутренние и внешние маршруты и объявлять только локальный прямой маршрут.

6.5.10.2. Примечания

На том же уровне конфигурация с ключевым словом **on-startup** является взаимоисключающей с конфигурацией без ключевого слова **on-startup**.

6.5.10.3. Шаги настройки

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **set-overload-bit** в режиме конфигурации процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

6.5.10.4. Проверка

Перехватывайте пакеты и проверяйте, что сосед не пересылает LSP от локального узла.

6.5.10.5. Связанные команды

Команда	**set-overload-bit** [**on-startup** { *seconds* | **wait-for-bgp** [*bgpseconds*] }] [**suppress** { [**interlevel**] [**external**] }] [**level-1** | **level-2**]
Описание параметра	**on-startup** *seconds*: указывает продолжительность, в течение которой узел IS-IS остается в состоянии перегрузки после перезапуска. Диапазон значений: от 5 до 86 400 с. **wait-for-bgp** *bgpseconds*: указывает продолжительность, в течение которой узел IS-IS автоматически входит и остается в состоянии ожидания конвергенции BGP после перезапуска. Значение варьируется от 5 до 86 400 в секундах. Значение по умолчанию — 600. **suppress**: указывает на то, что не следует объявлять внутренние маршруты (внутриобластные и межобластные маршруты) или внешние маршруты соседям, когда узел IS-IS находится в состоянии перегрузки. **interlevel**: указывает на то, что не следует объявлять внутриобластные и межобластные маршруты соседям, когда узел IS-IS находится в состоянии перегрузки. Он используется с ключевым словом **suppress**. **external**: указывает на то, что внешние маршруты не объявляются соседям, когда узел IS-IS находится в состоянии перегрузки. Он используется с ключевым словом **suppress**. **level-1**: отправляет LSP с битом перегрузки только соседям Level-1. **level-2**: отправляет LSP с битом перегрузки только соседям Level-2
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Используйте эту команду, чтобы заставить узел IS-IS установить бит перегрузки в невиртуальном LSP, чтобы дать указание своим соседям IS-IS не использовать локальный узел в качестве устройства пересылки. Если вы выберете ключевое слово **on-startup**, узел IS-IS автоматически перейдет в состояние перегрузки после перезапуска. Если вы не выберете ключевое слово **on-startup**, узел IS-IS перейдет в состояние перегрузки сразу после перезапуска

6.5.10.6. Пример конфигурации

Настройка бита перегрузки в случае мгновенной black hole

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Убедитесь, что узел IS-IS переходит в состояние мгновенной black hole сразу после перезапуска и остается в этом состоянии до истечения заданного времени (300 с), а узел IS-IS только объявляет своим соседям локальные прямые каналы в течение указанного времени

	A(config)# router isis A(config-router)#set-overload-bit on-startup 300 suppress interlevel external
Проверка	• Перехватывайте пакеты для проверки LSP. • Убедитесь, что узел IS-IS автоматически переходит в состояние мгновенной black hole после перезапуска. Как только отношения соседства установлены, узел IS-IS отправляет LSP с битом перегрузки. • По истечении заданного времени узел IS-IS немедленно отправляет LSP с отмененным битом перегрузки, чтобы уведомить своих соседей о том, что локальный узел вышел из состояния мгновенной black hole (или перегрузки)
	A# show isis neighbors

Отключение пересылки реальных данных на локальном узле IS-IS

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Подключите локальный узел IS-IS в качестве тестового устройства к производственной сети. Узлу не требуется пересылать реальные данные в сеть, чтобы избежать влияния на производство
	A(config)# router isis A(config-router)#set-overload-bit suppress interlevel external
Проверка	Перехватывайте пакеты для проверки LSP. Убедитесь, что LSP несут бит перегрузки и объявляют только локальные прямые маршруты
	A# show isis neighbors

6.5.11. Настройка IS-IS VRF

6.5.11.1. Эффект конфигурации

- Каждую таблицу VRF можно рассматривать как виртуальное устройство или выделенное PE-устройство.
- Виртуальное устройство содержит следующие элементы: независимую таблицу маршрутизации, а также независимое адресное пространство; набор интерфейсов, принадлежащих таблице VRF; набор протоколов маршрутизации, применимый только к таблице VRF.
- Каждое устройство может поддерживать одну или несколько таблиц VRF и таблицу маршрутизации общедоступной сети (также называемую глобальной таблицей маршрутизации). Несколько экземпляров VRF отделены друг от друга.

6.5.11.2. Примечания

- Обратите внимание на следующие ограничения или соглашения при связывании экземпляров IS-IS и таблиц VRF:
- Экземпляры IS-IS, связанные с одной и той же таблицей VRF, должны быть настроены с разными системными идентификаторами. Экземпляры IS-IS, связанные с разными таблицами VRF, можно настроить с одним и тем же системным идентификатором.
- Один экземпляр IS-IS может быть связан только с одной таблицей VRF, но одна таблица VRF может быть связана с несколькими экземплярами IS-IS.
- При изменении таблицы VRF, привязанной к экземпляру IS-IS, все интерфейсы IS-IS, связанные с этим экземпляром, будут удалены. То есть конфигурация интерфейса **ip router isis** [*tag*] и конфигурация перераспределения в режиме настройки процесса маршрутизации будут удалены.

6.5.11.3. Шаги настройки

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **vrf** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

6.5.11.4. Проверка

Проверьте, устанавливает ли локальное устройство отношения соседства с другими устройствами, указанными в таблице VRF.

6.5.11.5. Связанные команды

Настройка IS-IS VRF

Команда	**vrf** *vrf-name*
Описание параметра	*vrf-name*: указывает имя существующей таблицы VRF
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Прежде чем привязать экземпляр IS-IS к таблице VRF, убедитесь, что таблица VRF настроена. Если вам необходимо установить отношения соседства IS-ISv6, включите IPv6 и убедитесь, что привязываемая таблица является многопротокольной таблицей VRF. Обратите внимание на следующие ограничения или соглашения при связывании экземпляров IS-IS и таблиц VRF: • Экземпляры IS-IS, связанные с одной и той же таблицей VRF, отличной от таблицы по умолчанию, должны быть настроены с разными системными идентификаторами. Экземпляры IS-IS, связанные с разными таблицами VRF, можно настроить с одним и тем же системным идентификатором.

	• Один экземпляр IS-IS может быть связан только с одной таблицей VRF, но одна таблица VRF может быть связана с несколькими экземплярами IS-IS. • При изменении таблицы VRF, привязанной к экземпляру IS-IS, все интерфейсы IS-IS, связанные с этим экземпляром, будут удалены. То есть конфигурация интерфейса **ip** (или **ipv6) router isis** [*tag*] и конфигурация перераспределения в режиме настройки процесса маршрутизации будут удалены

6.5.11.6. Пример конфигурации

Настройка IS-IS VRF

Шаги настройки	Привяжите экземпляр IS-IS к таблице VRF. Добавьте интерфейсы в таблицу VRF и экземпляр IS-IS. (опущено)
	A(config)#vrf definition vrf_1 A(config-vrf)#address-family ipv4 A(config-vrf-af)#exit-address-family A(config)# router isis A(config-router)# vrf vrf_1
Проверка	Проверьте, устанавливает ли локальное устройство отношения соседства с другими устройствами, указанными в таблице VRF
	A# show isis neighbors

6.5.11.7. Распространенные ошибки

- Интерфейсы не добавляются в таблицу VRF.
- IP-адреса интерфейсов, подключенных между соседями, не находятся в одном сегменте сети.
- Команда **ip router isis** не выполняется на интерфейсах.
- NET-адрес не настроен или на Level-1 существуют разные NET-адреса.
- **max-area-addresses** с обеих сторон настроен по-разному.
- **metric-style** с обеих сторон настроен по-разному.
- Уровни интерфейса с обеих сторон разные. Одна сторона — это Level-1, а другая — Level-2.
- Одна сторона настроена на режим P2P, тогда как другая сторона настроена на broadcast-режим.
- На одной стороне включена аутентификация, а на другой — нет.

6.5.12. Настройка IS-IS MTR

6.5.12.1. Эффект конфигурации

Если команда **multi-topology** не выполняется, IPv4 и IPv6 используют одну физическую топологию IS-IS, также называемую топологию по умолчанию. Если команда **multi-topology** выполняется без параметра **transition**, устройства маршрутизации работают в режиме MT. IS-ISv4 работает в топологии по умолчанию, а IS-ISv6 работает в топологии unicast-рассылки IPv6. Если команда **multi-topology** выполняется с параметром **transition**, устройства маршрутизации работают в режиме MTT. IS-ISv6 работает в топологии по умолчанию и топологии unicast-рассылки IPv6. Эти три конфигурации являются взаимоисключающими. Устройства маршрутизации в режиме MTT могут передавать MT TLV или TLV топологии по умолчанию. Режим MTT применим для поэтапного развертывания, чтобы обеспечить плавную миграцию сети. Режим MTT может вызвать утечку маршрутов между топологией по умолчанию и топологией unicast-рассылки IPv6. Если режим MTT настроен неправильно, могут возникнуть сбои в сети, такие как black hole и петли маршрутизации.

6.5.12.2. Примечания

Обратите внимание на следующие ограничения и соглашения при настройке функции IS-IS MTR:

- Прежде чем запускать команду **multi-topology**, установите для **metric-style** значение **Wide** или **Transition**.
- Функция MTR будет отключена, если для **metric-style** установлено значение **Narrow** или только один уровень настроен для поддержки режима **Wide** или **Transition**.

6.5.12.3. Шаги настройки

- Выполните эту настройку в соответствии с требованиями.
- Настройте функцию MTR в режиме конфигурации семейства адресов IPv6 IS-IS на нужном устройстве, если не указано иное.

6.5.12.4. Проверка

Проверьте, устанавливает ли локальное устройство отношения соседства с другими устройствами.

6.5.12.5. Связанные команды

Настройка IS-IS MTR

Команда	**multi-topology** [*transition*]
Описание параметра	*transition*: настраивает режим MTT, который поддерживает плавный переход от гибридной топологии IPv4-IPv6 к раздельным топологиям IPv4 и IPv6
Командный режим	Режим конфигурации IS-IS семейства адресов IPv6

Руководство по использованию	Если команда **multi-topology** не выполняется, IPv4 и IPv6 используют одну физическую топологию IS-IS, также называемую топологию по умолчанию. Если команда **multi-topology** выполняется без параметра **transition**, устройства маршрутизации работают в режиме MT. IS-ISv4 работает в топологии по умолчанию, а IS-ISv6 работает в топологии unicast-рассылки IPv6. Если команда **multi-topology** выполняется с параметром **transition**, устройства маршрутизации работают в режиме MTT. IS-ISv6 работает в топологии по умолчанию и топологии unicast-рассылки IPv6. Эти три конфигурации являются взаимоисключающими. Устройства маршрутизации в режиме MTT могут передавать MT TLV или TLV топологии по умолчанию. Режим MTT применим для поэтапного развертывания, чтобы обеспечить плавную миграцию сети. Режим MTT может вызвать утечку маршрутов между топологией по умолчанию и топологией unicast-рассылки IPv6. Если режим MTT настроен неправильно, могут возникнуть сбои в сети, такие как black hole и петли маршрутизация. Прежде чем запускать команду, установите для **metric-style** значение **Wide** или **Transition**. Функция MTR будет отключена, если для **metric-style** установлено значение **Narrow** или только один уровень настроен для поддержки режима **Wide** или **Transition**

6.5.12.6. Пример конфигурации

Настройка IS-IS MTR

Требования к конфигурации: типичный сценарий применения MTR — сохранение устройств, поддерживающих только сервисы IPv4, в сети, где будет выполняться расширение сервиса IPv6.

На Рисунке 6-18 маршрутизатор 2 поддерживает только стек протоколов IPv4, но не поддерживает функцию MTR; следовательно, он может запускать только сервиса IPv4. Пропускную способность сети необходимо масштабировать для поддержки сервисов IPv6, чтобы удовлетворить требования к расширению сервисов. (Будут добавлены Маршрутизатор 1, Маршрутизатор 3 и Маршрутизатор 4, поддерживающие функцию MTR.) Устройство (Маршрутизатор 2), поддерживающее только один стек протоколов, необходимо заменить, чтобы обеспечить стабильность сети, в которой используются двойные стеки протоколов IPv4 и IPv6; в противном случае могут возникнуть black hole-ы маршрутизации IPv6.

Если вам необходимо сохранить маршрутизатор 2, вы можете настроить функцию MTR на маршрутизаторе 1, маршрутизаторе 3 и маршрутизаторе 4. Функция MTR позволяет маршрутизатору 2 продолжать работу сервисов IPv4 без помех для сервисов IPv4 и IPv6 на маршрутизаторе 1, маршрутизаторе 3 и маршрутизаторе 4. Функция MTR повышает гибкость сети, косвенно продлевает срок сервиса старых устройств и отвечает требованиям расширения сервисов, одновременно максимизируя ценность старых устройств.

Требования к конфигурации следующие:

- Сохраните маршрутизатор 2, который поддерживает только сервисы IPv4.
- Добавляйте устройства, поддерживающие двойную топологию IPv4 и IPv6, а также разделяйте расчет маршрута IPv4 и расчет маршрута IPv6 на основе разных топологий.

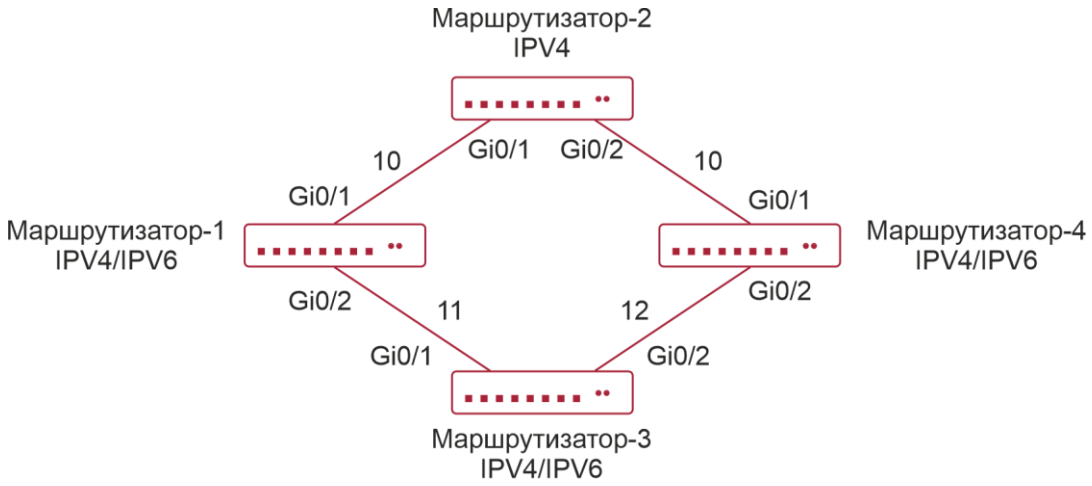


Рисунок 6-18. Топология IS-IS MTR

Маршру-тизатор 1	Настройте интерфейсы IS-IS и Ethernet
	Настройте IS-IS: QTECH(config)# router isis QTECH(config-router)# net 49.0001. 0000.0000.0001.00 QTECH(config-router)# is-type level-1 QTECH(config-router)# metric-style wide QTECH(config-router)# address-family ipv6 QTECH(config-router-af)# multi-topology Настройте Ethernet-интерфейсы: QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# ipv6 enable QTECH(config-if-GigabitEthernet 0/1)# ipv6 address 1002: : 1/112 QTECH(config-if-GigabitEthernet 0/1)# ipv6 router isis QTECH(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0 QTECH(config-if-GigabitEthernet 0/1)# ip router isis QTECH(config-if-GigabitEthernet 0/1)# interface gigabitEthernet 0/2 QTECH(config-if-GigabitEthernet 0/2)# ipv6 enable QTECH(config-if-GigabitEthernet 0/2)# ipv6 address 1003: : 1/112 QTECH(config-if-GigabitEthernet 0/2)# ipv6 router isis QTECH(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0 QTECH(config-if-GigabitEthernet 0/2)# ip router isis

	QTECH(config-if-GigabitEthernet 0/2)#isis wide-metric 11
Маршру-тизатор 2	Настройте интерфейсы IS-IS и Ethernet
	Настройте IS-IS: QTECH(config)# router isis QTECH(config-router)# net 49.0001. 0000.0000.0002.00 QTECH(config-router)# is-type level-1 QTECH(config-router)# metric-style wide QTECH(config-router)#address-family ipv6 QTECH(config-router-af)#no adjacency-check Настройте Ethernet-интерфейсы: QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0 QTECH(config-if-GigabitEthernet 0/1)# ip router isis QTECH(config-if-GigabitEthernet 0/1)# interface gigabitEthernet 0/2 QTECH(config-if-GigabitEthernet 0/2)# ip address 192.168.3.2 255.255.255.0 QTECH(config-if-GigabitEthernet 0/2)# ip router isis
Маршру-тизатор 3	Настройте интерфейсы IS-IS и Ethernet
	Настройте IS-IS: QTECH(config)# router isis QTECH(config-router)# net 49.0001. 0000.0000.0003.00 QTECH(config-router)# is-type level-1 QTECH(config-router)# metric-style wide QTECH(config-router)# address-family ipv6 QTECH(config-router-af)# multi-topology Настройте Ethernet-интерфейсы: QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# ipv6 enable QTECH(config-if-GigabitEthernet 0/1)# ipv6 address 3001: : 1/112 QTECH(config-if-GigabitEthernet 0/1)# ipv6 router isis QTECH(config-if-GigabitEthernet 0/1)# ip address 192.168.2.3 255.255.255.0 QTECH(config-if-GigabitEthernet 0/1)# ip router isis

	QTECH(config-if-GigabitEthernet 0/1)#isis wide-metric 11 QTECH(config-if-GigabitEthernet 0/1)# interface gigabitEthernet 0/2 QTECH(config-if-GigabitEthernet 0/2)# ipv6 enable QTECH(config-if-GigabitEthernet 0/2)# ipv6 address 3004: : 1/112 QTECH(config-if-GigabitEthernet 0/2)# ipv6 router isis QTECH(config-if-GigabitEthernet 0/2)# ip address 192.168.4.3 255.255.255.0 QTECH(config-if-GigabitEthernet 0/2)# ip router isis QTECH(config-if-GigabitEthernet 0/2)#isis wide-metric 12
Маршру-тизатор 4	Настройте интерфейсы IS-IS и Ethernet
	Настройте IS-IS: QTECH(config)# router isis QTECH(config-router)# net 49.0001.0000.0000.0004.00 QTECH(config-router)# is-type level-1 QTECH(config-router)# metric-style wide QTECH(config-router)# address-family ipv6 QTECH(config-router-af)# multi-topology Настройте Ethernet-интерфейсы: QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# ipv6 enable QTECH(config-if-GigabitEthernet 0/1)# ipv6 address 4002: : 1/112 QTECH(config-if-GigabitEthernet 0/1)# ipv6 router isis QTECH(config-if-GigabitEthernet 0/1)# ip address 192.168.3.4 255.255.255.0 QTECH(config-if-GigabitEthernet 0/1)# ip router isis QTECH(config-if-GigabitEthernet 0/1)# interface gigabitEthernet 0/2 QTECH(config-if-GigabitEthernet 0/2)# ipv6 enable QTECH(config-if-GigabitEthernet 0/2)# ipv6 address 4003: : 1/112 QTECH(config-if-GigabitEthernet 0/2)# ipv6 router isis QTECH(config-if-GigabitEthernet 0/2)# ip address 192.168.4.4 255.255.255.0 QTECH(config-if-GigabitEthernet 0/2)# ip router isis
Проверка	• Запустите команду **show** на маршрутизаторе 1, чтобы проверить, является ли следующий hop маршрута IPv4, предназначенный для маршрутизатора 4, маршрутизатором 2.

	• Запустите команду **show** на маршрутизаторе 1, чтобы проверить, является ли следующий hop маршрута IPv6, предназначенный для маршрутизатора 4, маршрутизатором 3
Проверка маршрута IPv4	QTECH#show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 192.168.1.0/24 is directly connected, GigabitEthernet 0/1 C 192.168.1.1/32 is local host. C 192.168.2.0/24 is directly connected, GigabitEthernet 0/2 C 192.168.2.1/32 is local host. i L1 192.168.3.0/24 [115/20] via 192.168.1.2, 00:13:14, GigabitEthernet 0/1 i L1 192.168.4.0/24 [115/23] via 192.168.2.3, 00:02:40, GigabitEthernet 0/2
Проверка маршрута IPv6	QTECH#show ipv6 route IPv6 routing table name is - Default - 16 entries Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary O - OSPF intra area, OI - OSPF inter area, OE1 - OSPF external type 1, OE2 – OSPF external type 2 ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2 L ::1/128 via Loopback, local host C 1002::/112 via GigabitEthernet 0/1, directly connected L 1002::1/128 via GigabitEthernet 0/1, local host C 1003::/112 via GigabitEthernet 0/2, directly connected L 1003::1/128 via GigabitEthernet 0/2, local host I1 3001::/112 [115/21] via FE80::C806:5FF:FEE8:38, GigabitEthernet 0/2 I1 3004::/112 [115/21] via FE80::C806:5FF:FEE8:38, GigabitEthernet 0/2 I1 4002::/112 [115/31] via FE80::C806:5FF:FEE8:38, GigabitEthernet 0/2 I1 4003::/112 [115/31] via FE80::C806:5FF:FEE8:38, GigabitEthernet 0/2 L FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/2, directly connected

	L FE80::1614:4BFF:FE12:ADFC/128 via GigabitEthernet 0/2, local host C FE80::/64 via GigabitEthernet 0/1, directly connected L FE80::1614:4BFF:FE12:ADFD/128 via GigabitEthernet 0/1, local host C FE80::/64 via Local 0, directly connected L FE80::1614:4BFF:FE12:ADFC/128 via Local 0, local host

6.5.12.7. Распространенные ошибки

- Для **metric-style** не установлено значение **Wide** или **Transition**.
- Типы протоколов, используемые двумя соседями, не совпадают; следовательно, отношения соседства не могут быть установлены.
- IP-адреса интерфейсов, подключенных между соседями, не находятся в одном сегменте сети.
- Команда **ip router isis** не выполняется на интерфейсах.
- NET-адрес не настроен или на Level-1 существуют разные NET-адреса.
- **max-area-addresses** с обеих сторон настроен по-разному.
- **metric-style** с обеих сторон настроен по-разному.
- Уровни интерфейса с обеих сторон разные. Одна сторона — это Level-1, а другая — Level-2.
- Одна сторона настроена на режим P2P, тогда как другая сторона настроена на broadcast-режим.
- На одной стороне включена аутентификация, а на другой — нет.

6.5.13. Настройка SNMP для IS-IS

6.5.13.1. Эффект конфигурации

По умолчанию программное обеспечение SNMP может выполнять операцию MIB на первом экземпляре IS-IS. Чтобы выполнить операцию MIB на других экземплярах, вам необходимо вручную указать эти экземпляры.

6.5.13.2. Примечания

По умолчанию программное обеспечение SNMP может выполнять операцию MIB на первом отображаемом экземпляре IS-IS.

6.5.13.3. Шаги настройки

Привязка экземпляров, на которых будет выполняться операция IS-IS MIB

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **enable mib-binding** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Глобальное включение Trap IS-IS

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **snmp-server enable traps isis** в режиме глобальной конфигурации на нужном устройстве, если не указано иное.

Глобальная настройка хоста SNMP

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **snmp-server host** в режиме глобальной конфигурации на нужном устройстве, если не указано иное.

Разрешение отправки всех сообщений Trap IS-IS на хост SNMP

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **enable traps all** в режиме конфигурации процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

6.5.13.4. Проверка

Используйте инструмент MIB для чтения и записи настроек IS-IS.

6.5.13.5. Связанные команды

Привязка экземпляров, на которых будет выполняться операция IS-IS MIB

Команда	**enable mib-binding**
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Новейшие стандарты предусматривают, что операция MIB может выполняться в одном экземпляре. По умолчанию операция MIB выполняется над первым отображаемым экземпляром IS-IS. Поскольку можно настроить несколько экземпляров IS-IS, администратор может использовать эту команду, чтобы указать экземпляры, на которых будет выполняться операция MIB

Глобальное включение Trap IS-IS

Команда	**snmp-server enable traps** [*isis*]
Описание параметра	*isis*: включает Trap события IS-IS
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эту команду необходимо использовать с командой **snmp-server host** в режиме глобальной конфигурации, чтобы можно было отправлять сообщения Trap

Глобальная настройка хоста SNMP

Команда	**snmp-server host** { *host-addr* | **ipv6** *ipv6-addr* } [**vrf** *vrfname*] [**traps**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*] [*notification-type*]
Описание параметра	*host-addr*: указывает адрес хоста SNMP. *ipv6-addr*: указывает IPv6-адрес хоста SNMP. *vrfname*: указывает имя таблицы VRF. **version**: указывает версию SNMP, для которой можно установить **V1**, **V2C** или **V3**. **auth** | **noauth** | **priv**: указывает уровень безопасности пользователей V3. *community-string*: указывает строку сообщества или имя пользователя (версия V3). *port-num*: указывает номер порта SNMP-хоста. *notification-type*: указывает тип активно отправляемых сообщений Trap, например snmp
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется вместе с командой **snmp-server enable traps** для активной отправки сообщений Trap в систему управления сетью (NMS). Вы можете настроить разные хосты SNMP для получения сообщений Trap. Хост поддерживает различные типы Trap, порты и таблицы VRF. Для того же хоста (с той же конфигурацией порта и конфигурацией VRF) последняя конфигурация объединяется с предыдущими конфигурациями. То есть, чтобы отправлять разные сообщения Trap на один и тот же хост, каждый раз настраивайте тип сообщений Trap. Эти конфигурации в итоге объединятся

Разрешение отправки сообщений Trap

Команда	**enable traps** { **all** | *traps set* }
Описание параметра	**all**: указывает все сообщения Trap. *traps set*: указывает тип сообщения Trap в любом наборе
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Пакеты IS-IS классифицируются на 18 типов сообщений Trap, которые сгруппированы в несколько наборов, каждый из которых содержит несколько типов сообщений Trap. Чтобы включить отправку сообщений Trap IS-IS, запустите команду **snmp-server enable traps isis** в режиме

	глобальной конфигурации и укажите хост-получатель и тип сообщений Trap, которые можно отправлять

6.5.13.6. Пример конфигурации

Настройка IS-IS SNMP

Шаги настройки	• Привяжите экземпляры, над которыми будет выполняться операция IS-IS MIB. • Выполните настройки, связанные с сообщениями Trap
	A(config)# router isis A(config-router)# enable mib-binding A# configure terminal A(config)#snmp-server enable traps isis A(config)#snmp-server host 10.1.1.1 traps version 2c public A(config)#router isis A(config-router)# enable traps all
Проверка	Запустите инструмент MIB, чтобы прочитать и записать настройки IS-IS
	A# show running-config

6.5.14. Настройка двустороннего обслуживания IS-IS

6.5.14.1. Эффект конфигурации

Включите двустороннее обслуживание IS-IS.

6.5.14.2. Примечания

- Необходимо настроить основные функции IS-IS.
- Отношения соседства успешно установлены.

6.5.14.3. Шаги настройки

Настройка двустороннего обслуживания IS-IS

- При необходимости настройте функцию двустороннего обслуживания.
- Запустите команду **two-way-maintain** в режиме настройки процесса маршрутизации IS-IS на необходимых устройствах, если не указано иное.

6.5.14.4. Проверка

- Запустите команду **show isis neighbor**, чтобы проверить время обновления соседа.
- Запустите команду **show isis protocol**, чтобы проверить, включена ли функция двустороннего обслуживания.

6.5.14.5. Связанные команды

Настройка двустороннего обслуживания IS-IS

Команда	**two-way-maintain**
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	В крупномасштабной сети отправляется и принимается большое количество пакетов, что занимает много ресурсов ЦП и памяти, что приводит к задержке или отклонению некоторых пакетов IS-IS. Если время, необходимое для обработки пакетов Hello, превышает время обслуживания отношений соседства, время обслуживания соответствующих отношений соседства истекает и удаляется. Когда включена функция двустороннего обслуживания, если в сети существует большое количество пакетов, пакеты LSP, пакеты CSNP и пакеты PSNP от соседа в дополнение к пакетам Hello также могут использоваться для поддержания двусторонней связи с соседом, предотвращая сбой соседа, вызванный задержкой или отбрасыванием пакетов Hello

6.5.14.6. Пример конфигурации

ПРИМЕЧАНИЕ: следующий пример реализован на основе базовых функций IS-IS. Подробную информацию об основных функциях IS-IS см. в предыдущем описании.

Настройка двустороннего обслуживания IS-IS

Сценарий:

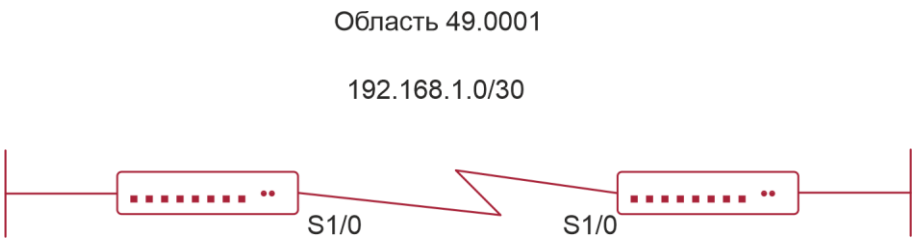


Рисунок 6-19.

Шаги настройки	• Настройте основные функции IS-IS на всех устройствах. • Отношения соседства успешно установлены
Проверка	Убедитесь, что соседний интерфейс IS-IS установлен на устройстве A. Проверьте состояние экземпляра IS-IS на устройстве A

6.5.15. Настройка других параметров IS-IS

6.5.15.1. Эффект конфигурации

- **maximum-paths**: настраивает максимальное количество путей равной стоимости IS-IS, которые можно установить в таблицу маршрутизации.
- **lsp-length receive**: настраивает максимальную длину, разрешенную для полученных LSP.
- **lsp-length originate**: настраивает максимальную длину, разрешенную для отправленных LSP.
- **passive-interface**: предотвращает получение и отправку пакетов IS-IS пассивными интерфейсами. То есть отношения соседства IS-IS не будут устанавливаться на пассивных интерфейсах. IP-адреса пассивных интерфейсов передаются через другие интерфейсы.
- **bandwidth-reference**: настраивает эталон полосы пропускания для IS-IS для автоматического расчета метрики канала. Если метрика настроена, она имеет преимущественную силу. Если метрика не настроена, метрика рассчитывается автоматически на основе настроенной эталонной полосы пропускания.
- **interface-protocol-compatible**: настраивает поле TLV протокола IS-IS для заполнения на основе протоколов, поддерживаемых интерфейсом.
- **is-name**: заменяет системный идентификатор экземпляра настроенным именем.
- **isis metric**: сохраняет метрику, которая используется при вычислении SPF, в TLV информации о доступности IP. Чем больше метрика, тем больше потребление маршрутизации интерфейсом и тем длиннее путь, полученный в результате расчета SPF.
- **isis passive**: запрещает интерфейсу отправлять или получать пакеты IS-IS, но соответствующий IP-адрес будет передаваться через другие интерфейсы.
- **isis priority**: в broadcast-сети IS-IS необходимо выбрать DIS среди всех устройств. DIS сгенерирует псевдоузел и связанные с ним LSP. Устройство с наивысшим приоритетом выбирается в качестве DIS. Вы можете настроить разные приоритеты для разных уровней.
- **default-information originate**: создает маршрут по умолчанию Level-2, который будет объявляться через LSP.
- **spf-interval**: настраивает алгоритм экспоненциальной задержки SPF.
- **summary-address** и **summary-prefix**: создает суммарный маршрут для представления группы маршрутов в таблице маршрутизации. Суммарный маршрут может включать в себя несколько маршрутов указанного уровня. Метрика интерфейса суммарного маршрута соответствует наименьшей метрике интерфейса среди всех маршрутов.
- **log-adjacency-changes**: включает вывод событий отношений соседства для ведения журнала изменений отношений соседства IS-IS.
- **redistribute**: перераспределяет другие маршруты на IS-IS; перераспределяет маршруты Level-1 на Level-2; перераспределяет маршруты Level-2 на Level-1.

6.5.15.2. Шаги настройки

Настройка максимального количества путей с одинаковой стоимостью

- Выполните эту настройку в соответствии с требованиями.

- Запустите команду **maximum-paths** в режиме конфигурации процесса маршрутизации IS-IS или режиме конфигурации семейства адресов IPv6 IS-IS на нужном устройстве, если не указано иное.

Настройка максимальной длины, разрешенной для полученных LSP

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **lsp-length receive** в режиме конфигурации процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Настройка максимальной длины, разрешенной для отправляемых LSP

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **lsp-length originate** в режиме конфигурации процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Настройка пассивного интерфейса

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **passive-interface** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Настройка эталонной полосы пропускания интерфейса IS-IS

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **bandwidth-reference** в режиме конфигурации процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Настройка поля TLV протокола IS-IS для заполнения на основе протоколов, поддерживаемых интерфейсом

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **interfaces-protocol-compatible** в режиме настройки процесса маршрутизации IS-IS на нужных устройствах, если не указано иное.

Настройка псевдонима экземпляра IS-IS

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **is-name** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Настройка метрики интерфейса IS-IS

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **isis metric** в режиме настройки интерфейса на нужном устройстве, если не указано иное.

Настройка интерфейса как пассивного интерфейса

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **isis passive** в режиме настройки интерфейса на нужном устройстве, если не указано иное.

Настройка приоритета DIS

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **isis priority** в режиме настройки интерфейса на нужном устройстве, если не указано иное.

Создание маршрута по умолчанию

- Выполните эту настройку в соответствии с требованиями.

- Запустите команду **default-information originate** в режиме конфигурации процесса маршрутизации IS-IS или режиме конфигурации семейства адресов IPv6 IS-IS на нужном устройстве, если не указано иное.

Настройка цикла расчета SPF

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **spf-interval** в режиме настройки интерфейса на нужном устройстве, если не указано иное.

Настройка суммарного маршрута

- Выполните эту настройку в соответствии с требованиями.
- Запустите команды **summary-address** и **summary-prefix** в режиме конфигурации процесса маршрутизации IS-IS или режиме конфигурации семейства адресов IPv6 IS-IS на нужном устройстве, если не указано иное.

Включение вывода событий отношений соседства

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **log-adjacency-changes** в режиме конфигурации процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

Настройка перераспределения маршрутов

- Выполните эту настройку в соответствии с требованиями.
- Запустите команду **redistribute** в режиме настройки процесса маршрутизации IS-IS на нужном устройстве, если не указано иное.

6.5.15.3. Проверка

- **maximum-paths**: проверьте, соответствует ли максимальное количество путей с одинаковой стоимостью, отображаемых в записях маршрутизации, конфигурации.
- **lsp-length receive**: захват пакетов для проверки длины LSP.
- **lsp-length originate**: захват пакетов для проверки длины LSP.
- **passive-interface**: захват пакетов, чтобы проверить, получает ли и отправляет ли интерфейс пакеты IS-IS.
- **bandwidth-reference**: проверьте метрику таблицы маршрутизации.
- **interfaces-protocol-compatible**: проверьте статус установления соседских отношений.
- **is-name**: проверьте детали базы данных IS-IS.
- **isis metric**: проверьте детали базы данных IS-IS.
- **isis priority**: проверьте, выбрано ли устройство с измененной настройкой приоритета в качестве DIS.
- **default-information originate**: проверьте, создан ли маршрут по умолчанию.
- **spf-interval**: проверьте, работает ли цикл расчета SPF.
- **summary-address** и **summary-prefix**: захват пакетов, чтобы проверить, объявляется ли через LSP суммарный маршрут вместо подробных (детализированных) маршрутов.
- **log-adjacency-changes**: измените состояние соседа и убедитесь, что это изменение записывается, когда отладка отключена.
- **redistribute**: проверьте записи маршрутизации IS-IS.

6.5.15.4. Связанные команды

Настройка максимального количества путей с одинаковой стоимостью

Команда	**maximum-paths** *maximum*
Описание параметра	*maximum*: указывает максимальное количество маршрутов IS-IS равной стоимости, которые можно установить в таблицу маршрутизации. Диапазон значений: от 1 до 32
Командный режим	Режим конфигурации процесса маршрутизации IS-IS и режим конфигурации IS-IS семейства адресов IPv6
Руководство по использованию	Эта команда используется IS-IS для управления количеством путей IS-IS равной стоимости, которые необходимо установить в таблицу маршрутизации. В таблице маршрутизации также есть команда, используемая для управления количеством путей с одинаковой стоимостью. Количество эффективных путей с равной стоимостью определяется любым из двух значений команды, в зависимости от того, какое из них меньше

Настройка максимальной длины, разрешенной для полученных LSP

Команда	**lsp-length receive** *size*
Описание параметра	*size*: указывает максимальную длину, разрешенную для полученных LSP. Согласно RFC, диапазон значений составляет от 1492 до 16 000 в байтах
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Используйте эту команду для управления максимальной длиной, разрешенной для LSP, получаемых локальным устройством. Промежуточные узлы с достаточным объемом памяти должны получать LSP, максимальная длина которых равна MTU интерфейса, чтобы избежать сбоя конвергенции маршрутов. С этой точки зрения команда бессмысленна. Максимальная длина, разрешенная для полученных LSP, не может быть меньше, чем разрешенная для отправленных LSP; в противном случае первое будет автоматически скорректировано так, чтобы оно равнялось второму

Настройка максимальной длины, разрешенной для отправляемых LSP

Команда	**lsp-length originate** *size* [**level-1** | **level-2**]
Описание параметра	*size*: указывает максимальную длину, разрешенную для отправленных LSP. Диапазон значений: от 512 до 16 000 в байтах.

	level-1: применяет настройку только к LSP Level-1. **level-2**: применяет настройку только к LSP Level-2
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	В принципе, максимальная длина LSP и SNP не может превышать MTU интерфейса; в противном случае пакеты будут отброшены при отправке

Настройка пассивного интерфейса

Команда	**passive-interface** [**default**] { *interface-type interface-number* }
Описание параметра	**default**: настраивает все интерфейсы IS-IS, которые не включены в качестве пассивных интерфейсов. *interface-type*: указывает тип интерфейса. *interface-number*: указывает номер интерфейса
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Эта команда запрещает указанному интерфейсу получать и отправлять пакеты IS-IS, но IP-адрес интерфейса будет заполнен другими интерфейсами. Если выбрана опция **default** и более 255 отключенных интерфейсов IS-IS, только первые 255 интерфейсов будут настроены как пассивные интерфейсы. Остальные интерфейсы являются непассивными

Настройка эталонной полосы пропускания

Команда	**bandwidth-reference** *value*
Описание параметра	*value*: указывает значение полосы пропускания. Значение находится в диапазоне от 1 до 4 294 967 в Мбит/с. Значение по умолчанию — 100
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Используйте эту команду для расчета метрики интерфейса в экземпляре в соответствии с эталоном полосы пропускания, настроенным в экземпляре. Если метрика настроена, она имеет преимущественную силу

Настройка поля TLV протокола IS-IS для заполнения на основе протоколов, поддерживаемых интерфейсом

Команда	**interfaces-protocol-compatible**
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Когда устройства, поддерживающие IS-IS для IPv4 или IS-IS для IPv6, а также устройства, поддерживающие как IS-IS для IPv4, так и IS-IS для IPv6 в сети, настроены на установление отношений соседства, рассчитанные маршруты могут быть недоступны из-за black hole маршрутизации. Чтобы предотвратить black hole маршрутизации, поле TLV (#129) протокола QTECH IS-IS дополняется на основе протоколов, поддерживаемых экземпляром, то есть экземпляры IS-IS, которые устанавливают отношения соседства, должны поддерживать один и тот же протокол. Поле TLV (#129) протокола IS-IS, поддерживаемого устройствами некоторых производителей, дополняется в зависимости от протоколов, поддерживаемых интерфейсом. В режиме единой (single) топологии устройство QTECH подключается к устройству другого производителя, на обоих устройствах настроен loopback-интерфейс, включены как IS-IS для IPv4, так и IS-IS для IPv6, и только один стек протоколов (IS-IS для IPv4 или IS-IS для IPv6) настраивается на интерфейсе для соединения двух устройств. Устройство другого производителя отправляет TLV#129 (поддерживает только один стек протоколов) на основе интерфейсов, тогда как устройство QTECH отправляет TLV#129 (поддерживает два стека протоколов) на основе экземпляров. В результате на устройстве другого производителя отображается состояние соседства «Init», но устройство QTECH не может установить отношения соседства с устройством другого производителя. Для этого можно настроить команду **interfaces-protocol-compatible** для включения возможности устройств QTECH устанавливать отношения соседства с устройствами других производителей

Настройка имени IS

Команда	**is-name** *name*
Описание параметра	*name*: указывает имя для замены идентификатора системы. Имя содержит максимум 64 символа
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Используйте эту команду, чтобы заменить системный идентификатор экземпляра настроенным именем. Все системные идентификаторы,

	отображаемые в команде выводе отображения базы данных IS-IS и отображения соседей IS-IS заменяются настроенным именем

Настройка метрики интерфейса IS-IS

Команда	**isis metric** *metric* [**level-1**| **level-2**]
Описание параметра	*metric*: указывает значение метрики. Диапазон значений: от 1 до 63. Значение по умолчанию — 10. **level-1**: применяет настройку к circuit-ам Level-1. **level-2**: применяет настройку к circuit-ам Level-2
Командный режим	Режим настройки интерфейса
Руководство по использованию	Метрика, которая используется при вычислении SPF, хранится в TLV информации о доступности IP. Чем больше метрика, тем больше потребление маршрутизации интерфейсом и тем длиннее путь, полученный в результате расчета SPF. Метрика принадлежит к узкому типу и действительна только в том случае, если для параметра **metric-style** установлено значение **Narrow**

Настройка широкой метрики интерфейса

Команда	**isis wide-metric** *metric* [**level-1** | **level-2**]
Описание параметра	*metric*: указывает значение метрики. Диапазон значений: от 1 до 16 777 214. Значение по умолчанию — 10. **level-1**: применяет настройку к circuit-ам Level-1. **level-2**: применяет настройку к circuit-ам Level-2
Командный режим	Режим настройки интерфейса
Руководство по использованию	Метрика, которая используется при вычислении SPF, хранится в TLV информации о доступности IP. Чем больше метрика, тем больше потребление маршрутизации интерфейсом и тем длиннее путь, полученный в результате расчета SPF. Метрика действительна только в том случае, если для параметра **metric-style** установлено значение **Wide**

Настройка интерфейса как пассивного интерфейса

Команда	**isis passive**
Командный режим	Режим настройки интерфейса
Руководство по использованию	Эта команда запрещает интерфейсу отправлять или получать пакеты IS-IS, но соответствующий IP-адрес будет передаваться через другие интерфейсы. Это действует только на сгенерированный интерфейс IS-IS

Настройка приоритета DIS

Команда	**isis priority** *value* [**level-1** | **level-2**]
Описание параметра	*value*: указывает приоритет. Диапазон значений: от 0 до 127. Значение по умолчанию — 64. **level-1**: применяет настройку к circuit-ам Level-1. **level-2**: применяет настройку к circuit-ам Level-2
Командный режим	Режим настройки интерфейса
Руководство по использованию	Используйте эту команду для изменения приоритета пакетов Hello в локальной сети (LAN). Устройство с более низким приоритетом с меньшей вероятностью будет выбрано в качестве DIS. Команда недействительна на сетевом интерфейсе P2P. Команда **no isis priority** с параметрами или без них восстанавливает приоритет до значения по умолчанию. Чтобы изменить настроенный приоритет, запустите команду **isis priority** с указанным приоритетом, чтобы перезаписать существующую конфигурацию, или вы можете сначала восстановить приоритет до значения по умолчанию, а затем настроить новый приоритет

Создание маршрута по умолчанию

Команда	**default-information originate** [**route-map** *map-name*]
Описание параметра	**route-map** *map-name*: ассоциируется с картой маршрута
Командный режим	Режим конфигурации процесса маршрутизации IS-IS и режим конфигурации IS-IS семейства адресов IPv6

Руководство по использованию	Поскольку домены Level-2 не генерируют маршрут по умолчанию, используйте эту команду, чтобы разрешить маршруту по умолчанию войти в домен Level-2

Настройка цикла расчета SPF

Команда	**spf-interval** [**level-1** | **level-2**] *maximum-interval* [*initial-interval hold-interval*]
Описание параметра	**level-1**: применяет конфигурацию только для Level-1. **level-2**: применяет конфигурацию только для Level-2. *maximum-interval*: указывает максимальный интервал для выполнения двух последовательных вычислений SPF. Диапазон значений: от 1 до 120 (в секундах). Значение по умолчанию — 10. *initial-interval*: указывает время ожидания для первого выполнения расчета SPF. Диапазон значений: от 0 до 60 000 (в миллисекундах). Значение по умолчанию — 50. *hold-interval*: указывает минимальный интервал для выполнения расчета SPF во второй раз. Диапазон значений: от 10 до 60 000 (в миллисекундах). Значение по умолчанию — 200
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Увеличение максимального интервала выполнения вычислений SPF позволяет избежать частых вычислений SPF и пустой траты ресурсов ЦП. Однако, больший минимальный интервал также приводит к более медленному ответу на изменения маршрута. Время ожидания для выполнения вычисления SPF в первый раз является начальным интервалом (initial interval). Если сеть становится нестабильной, интервал вычисления SPF меньше максимального интервала, и интервал для выполнения вычисления SPF во второй раз становится интервалом ожидания (hold interval). К этому интервалу добавляется соответствующий штраф: следующий интервал для расчета SPF удваивает предыдущий интервал для того же расчета SPF, пока интервал расчета SPF не достигнет максимального интервала. Последующие вычисления SPF выполняются с максимальным интервалом. Когда сеть становится стабильной, интервал для выполнения вычисления SPF становится больше максимального интервала, и время ожидания для выполнения вычисления SPF восстанавливается до начального интервала. Изменения канала предъявляют высокие требования к конвергенции. Начальный интервал может быть установлен на небольшое значение. Предыдущие параметры также можно изменить на более высокие значения, чтобы снизить нагрузку на процессор.

	Значение **initial-interval** может быть больше, чем **maximum-interval**. В противном случае значение **initial-interval** будет использоваться в качестве значения **maximum-interval**. Значение **hold-interval** не может быть больше, чем **maximum-interval**. В противном случае значение **hold-interval** будет использоваться в качестве значения **maximum-interval**. Значение **initial-interval** не может быть больше, чем **hold-interval**. В противном случае значение **initial-interval** будет использоваться в качестве значения **hold-interval**

Настройка суммарного маршрута IPv4

Команда	**summary-address** *ip-address net-mask* [**level-1** | **level-2** | **level-1-2**] [**metric** *number*]
Описание параметра	*ip-address*: указывает IP-адрес суммарного маршрута. *net-mask*: указывает маску подсети суммарного маршрута. **level-1**: применяет настройку только к Level-1. **level-2**: применяет настройку только к Level-2. По умолчанию настройка действует для Level-2. **level-1-2**: применяет настройку к Level-1 и Level-2. *number*: указывает метрику суммарного маршрута
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Если настроенный суммарный маршрут содержит информацию о доступном адресе или сегменте сети, суммарный маршрут вместо подробных маршрутов объявляется извне

Настройка суммарного маршрута IPv6

Команда	**summary-prefix** *ipv6-prefix/prefix-length* [**level-1** | **level-2** | **level-1-2**]
Описание параметра	*ipv6-prefix/prefix-length*: указывает сетевой адрес суммарного маршрута и длину его префикса IPv6. Формат адреса: X:X:X:X::X/<0-128>. **level-1**: применяет настройку только к Level-1. **level-2**: применяет настройку только к Level-2. По умолчанию настройка действует для Level-2. **level-1-2**: применяет настройку к Level-1 и Level-2
Командный режим	Режим конфигурации IS-IS семейства адресов IPv6

Руководство по использованию	Если настроенный суммарный маршрут содержит информацию о доступном адресе или сегменте сети, суммарный маршрут вместо подробных маршрутов объявляется извне

Включение вывода событий отношений соседства

Команда	**log-adjacency-changes**
Командный режим	Режим конфигурации процесса маршрутизации IS-IS
Руководство по использованию	Вы также можете использовать команду **debug** для записи изменений состояния соседа IS, но эта команда потребляет много системных ресурсов

Перераспределение других маршрутов на IS-IS

Команда	**redistribute** { **bgp** | **ospf** *process-id* [**match** { **internal** [**external** [**1** | **2**]] [**nssa-external** [**1** | **2**]] | **external** [**1** | **2**] [**internal**] [**nssa-external** [**1** | **2**]] | **nssa-external** [**1** | **2**] [**internal**] [**external** [**1** | **2**]] }] | **rip** | **connected** | **static** } [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-tag*] [**level-1** | **level-1-2** | **level-2**]
Описание параметра	*process-id*: указывает идентификатор процесса OSPF. Диапазон от 1 до 65 535. **match** { **internal** [**external** [**1** | **2**]] [**nssa-external** [**1** | **2**] }: при перераспределении маршрутов OSPF маршруты фильтруются по подтипу. Если опция **match** не выбрана, будут получены маршруты всех типов OSPF. Если после **match external** не следует число **1** или **2**, маршруты OSPF, указанные **external 1** и **external 2**, будут перераспределены. Если после **match nssa-external** не следует число **1** или **2**, маршруты OSPF, указанные в **nssa-external 1** и **nssa-external 2**, будут перераспределены. **metric** *metric-value*: указывает метрику перераспределенных маршрутов. Диапазон значений: от 0 до 4 261 412 864. Метрика внешних маршрутов используется, когда опция **metric** не указана. **metric-type** { **internal** | **external** }: указывает тип метрики перераспределяемых маршрутов. **internal**: указывает, что метрика принадлежит внутреннему типу. **external**: указывает, что метрика принадлежит к внешнему типу. Если **metric-type** не указан, метрика принадлежит внутреннему типу. **route-map** *map-tag*: указывает карту маршрутов, используемую для перераспределения внешних маршрутов. Он используется для фильтрации перераспределяемых маршрутов или настройки атрибутов перераспределяемых маршрутов. Значение *map-tag* не может превышать 32 символов. По умолчанию **route-map** не настроена.

	level-1 | **level-1-2** | **level-2**: указывает уровень перераспределенных маршрутов, полученных IS-IS. Если уровень не указан, маршруты перераспределяются на Level-2. **level-1**: перераспределяет маршруты на Level-1. **level-1-2**: перераспределяет маршруты на Level-1 и Level-2. **level-2**: перераспределяет маршруты на Level-2
Командный режим	Режим конфигурации процесса маршрутизации IS-IS и режим конфигурации IS-IS семейства адресов IPv6
Руководство по использованию	Команда **no redistribute** { **bgp** | **ospf** *processs-id* | **rip** | **connected** | **static** } используется для отмены перераспределения маршрутов, сопоставленных с указанным протоколом. Если после **no redistribute** следуют другие параметры, команда восстановит настройки параметров по умолчанию, а не отменит перераспределение маршрута. Например, команда **no redistribute bgp** отменяет перераспределение маршрутов BGP, тогда как команда **no redistribute bgp route-map aa** отменяет карту маршрутов с именем **aa**, используемую для перераспределения маршрутов BGP. Когда внешние маршруты перераспределяются в режиме IPv4, информация о маршрутизации сохраняется в TLV информации о внешней доступности IP LSP. Когда внешние маршруты перераспределяются в режиме IPv6, информация о маршрутизации сохраняется в TLV IPv6 Reachable LSP. В старых версиях некоторых производителей, если для **metric-type** установлено значение **external**, метрика перераспределяемых маршрутов прибавляется на 64 во время расчета маршрута и используется для определения маршрутизации. Такая практика не соответствует соответствующему протоколу. В действующем приложении внешние маршруты могут быть предпочтительнее внутренних. Если это происходит во время взаимодействия со старыми версиями некоторых производителей, вы можете изменить соответствующие настройки (например, **metric** или **metric-type**) каждого устройства, чтобы гарантировать, что внутренние маршруты предпочтительнее внешних

Перераспределение доступной информации маршрутизации Level-1 указанного экземпляра IS-IS на Level-2 текущего экземпляра

Команда	**redistribute isis** [*tag*] **level-1 into level-2** [**route-map** *route-map-name* | **distribute-list** *access-list-name*]
Описание параметра	*tag*: указывает имя экземпляра IS-IS, информация о маршрутизации которого будет перераспределена. **route-map** *route-map-name*: указывает карту маршрутов, используемую для перераспределения маршрутов. Она используется для фильтрации перераспределяемых маршрутов или настройки атрибутов перераспределяемых маршрутов. Значение *route-map-name*

	не может превышать 32 символов. По умолчанию **route-map** не настроена. **distribute-list** *access-list-name*: фильтрует перераспределяемые маршруты с помощью **distribute-list**. *access-list-name* указывает связанный список префиксов, который может быть стандартным списком префиксов, расширенным списком префиксов или списком префиксов имен. Он имеет формат {<1-99> | <100-199> | <1300-1999> | <2000-2699> | *acl-name* }. При применении режима конфигурации IS-IS семейства адресов IPv6 можно использовать только список префиксов имен в формате *acl-name*
Командный режим	Режим конфигурации процесса маршрутизации IS-IS и режим конфигурации IS-IS семейства адресов IPv6
Руководство по использованию	Вы можете использовать параметр **route-map** или **distribute-list**, чтобы отфильтровать маршруты Level-1 указанного экземпляра для перераспределения. Только маршруты, соответствующие определенным критериям, могут быть перераспределены на Level-2 текущего экземпляра. Параметры **route-map** или **distribute-list** не могут использоваться одновременно. Команда **no redistribute isis** [*tag*] **level-2 into level-1** используется для отмены перераспределения маршрутов указанного экземпляра. Если после **no redistribute** следуют другие параметры, команда восстановит настройки параметров по умолчанию, а не отменит перераспределение маршрута. Например, **no redistribute isis** *tag1* **level-1 into level-2** отменяет перераспределение маршрутов экземпляра IS-IS с именем *tag1*. **no redistribute isis** *tag1* **level-1 into level-2 route-map** *aa* отменяет использование карты маршрутов с именем **aa** для фильтрации перераспределяемых маршрутов

Перераспределение доступной информации маршрутизации Level-2 указанного экземпляра IS-IS на Level-1 текущего экземпляра

Команда	**redistribute isis** [*tag*] **level-2 into level-1** [**route-map** *route-map-name* | **distribute-list** *access-list-name* |(**prefix** *ip-address net-mask* | *ipv6-prefix ipv6-address/length*)]
Описание параметра	*tag*: указывает имя экземпляра IS-IS, информация о маршрутизации которого будет перераспределена. **route-map** *route-map-name*: указывает карту маршрутов, используемую для перераспределения маршрутов. Он используется для фильтрации перераспределяемых маршрутов или настройки атрибутов перераспределяемых маршрутов. Значение *route-map-name* не может превышать 32 символов. По умолчанию **route-map** не настроена. **distribute-list** *access-list-name*: фильтрует перераспределяемые маршруты с помощью **distribute-list**. *access-list-name* указывает

	связанный список префиксов, который может быть стандартным списком префиксов, расширенным списком префиксов или списком префиксов имен. Он имеет формат {<1-99> | <100-199> | <1300-1999> | <2000-2699> | *acl-name* }. При применении режима конфигурации IS-IS семейства адресов IPv6 можно использовать только список префиксов имен в формате *acl-name*. **prefix** *ip-address net-mask*: определяет маршруты, подлежащие перераспределению, по адресу и длине префикса. *ipv6-prefix ipv6-address/length*: определяет маршруты IPv6, которые будут перераспределяться по адресу и длине префикса
Командный режим	Режим конфигурации процесса маршрутизации IS-IS и режим конфигурации IS-IS семейства адресов IPv6
Руководство по использованию	Вы можете использовать параметр **route-map**, **distribute-list** или **prefix** для фильтрации маршрутов Level-2 указанного экземпляра для перераспределения. Только маршруты, соответствующие определенным критериям, могут быть перераспределены на Level-1 текущего экземпляра. Команда **no redistribute isis** [**tag**] **level-2 into level-1** используется для отмены перераспределения маршрутов указанного экземпляра. Если после **no redistribute** следуют другие параметры, команда восстановит настройки параметров по умолчанию, а не отменит перераспределение маршрута. Например: **no redistribute isis** *tag1* **level-2 into level-1** отменяет перераспределение маршрутов экземпляра IS-IS с именем **tag1**. **no redistribute isis** *tag1* **level-2 into level-1 route-map** *aa* отменяет использование карты маршрутов с именем **aa** для фильтрации перераспределяемых маршрутов

6.5.15.5. Пример конфигурации

Настройка максимального количества путей с одинаковой стоимостью

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте максимальное количество путей с равной стоимостью
	A(config)# router isis A(config-router)# maximum-paths 5
Проверка	Проверьте, соответствует ли максимальное количество путей с одинаковой стоимостью, отображаемых в записях маршрутизации, конфигурации
	A# show ip route isis

Настройка максимальной длины, разрешенной для полученных LSP

Конфигурация	• Настройте соседей IS-IS. (опущено) • Настройте максимальную длину, разрешенную для полученных LSP
	A(config)# router isis A(config-router)# lsp-length receive 512
Проверка	Перехватывайте пакеты, чтобы проверить длину полученных LSP

Настройка максимальной длины, разрешенной для отправляемых LSP

Конфигурации	• Настройте соседей IS-IS. (опущено) • Настройте максимальную длину, разрешенную для отправленных LSP
	A# configure terminal A(config)# router isis 1 A(config-router)# lsp-length originate 512 level-2
Проверка	Перехватывайте пакеты, чтобы проверить длину отправленных LSP

Настройка пассивного интерфейса

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте пассивный интерфейс
	A# configure terminal A(config)# router isis 1 A(config-router)# passive-interface GigabitEthernet 0/0
Проверка	Захватывайте пакеты, чтобы проверить, получает ли интерфейс и отправляет пакеты IS-IS

Настройка метрики интерфейса IS-IS

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте метрику интерфейса IS-IS
	A(config)# interface GigabitEthernet 0/1 A(config-if)#isis metric 1
Проверка	Проверьте детали базы данных IS-IS

	A# show isis database detail

Настройка интерфейса как пассивного интерфейса

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте интерфейс как пассивный интерфейс
	A(config)# interface GigabitEthernet 0/1 A(config-if)# isis passive
Проверка	Проверить статус интерфейса IS-IS
	A# show isis interface GigabitEthernet 0/1

Настройка приоритета DIS

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте приоритет DIS
	A(config)# interface GigabitEthernet 0/1 A(config-if)# isis priority 127 level-1
Проверка	Проверьте, выбрано ли устройство с измененной настройкой приоритета в качестве DIS
	A# show isis database detail

Создание маршрута по умолчанию

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Создайте маршрут по умолчанию
	A(config)# router isis A(config-router)# default-information originate
Проверка	Перехватывайте пакеты, чтобы проверить, содержит ли отправленный LSP маршрут по умолчанию

Настройка цикла расчета SPF

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройка цикла расчета SPF
	A(config)# router isis

	A(config-router)# spf-interval 5 100 200
Проверка	Проверьте работает ли цикл расчета SPF

Настройка суммарного маршрута IS-IS

Требования к конфигурации: маршрутизатор A и маршрутизатор B соединены через Ethernet и запукают IS-IS. Настройте маршрутизатор A для объявления только маршрута 172.16.0.0/22 вместо маршрутов 172.16.1.0/24 и 172.16.2.0/24.

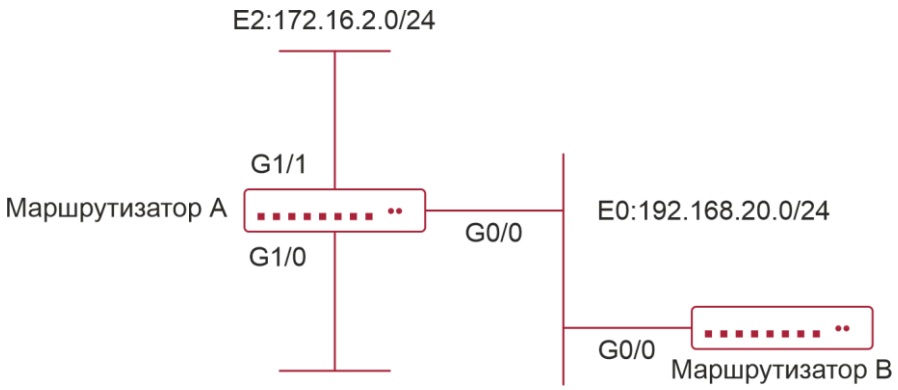


Рисунок 6-20. Сводная топология маршрута IS-IS

Шаги настройки	• Настройте IS-IS. • Настройте интерфейсы Ethernet. • Настройте пароль для аутентификации IS-IS
A	Настройте IS-IS
	A(config)# router isis A(config-router)# net 49.0001.0000.0000.0001.00 A(config-router)# summary-address 172.16.0.0/16 level-1-2
	Настройте интерфейсы Ethernet. A(config)# interface GigabitEthernet 0/0 A(config-if)# ip address 192.168.20.1 255.255.255.0 A(config-if)# ip router isis A(config)# interface GigabitEthernet 1/0 A(config-if)# ip address 172.16.1.1 255.255.255.0 A(config-if)# ip router isis A(config)# interface GigabitEthernet 1/1 A(config-if)# ip address 172.16.2.1 255.255.255.0

	A(config-if)# ip router isis
B	Настройте IS-IS
	B(config)# router isis B(config-router)# net 49.0001.0000.0000.0002.00
	Настройте интерфейс Ethernet
	B(config)# interface GigabitEthernet 0/0 B(config-if)# ip address 192.168.20.2 255.255.255.0 B(config-if)# ip router isis
Проверка	Запустите команду **show ip route** на маршрутизаторе B, чтобы проверить, существует ли только один суммарный маршрут
B	B(config)# show ip route i L1 172.16.0.0/16 [115/20] via 192.168.20.1, FastEthernet0/0

Настройка суммарного маршрута IS-ISv6

Маршрутизатор A и маршрутизатор B соединены через Ethernet и работают под управлением IS-ISv6. Настройте маршрутизатор A для объявления только маршрута 2000::/96 вместо маршрутов 2000::1111:0/112 и 2000::2222::0/112.

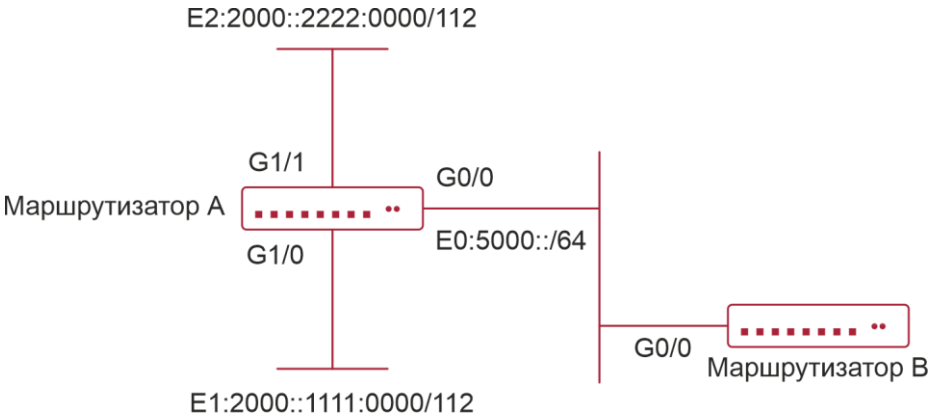


Рисунок 6-21. Сводная топология маршрута IS-ISv6

Шаги настройки	• Настройте IS-IS. • Настройте интерфейсы Ethernet. • Настройте пароль для аутентификации IS-IS

A	Настройте IS-IS
	A(config)# ipv6 unicast-routing A(config)# router isis A(config-router)# net 49.0001.0000.0000.0001.00 A(config-router)# address-family ipv6 unicast A (config-router-af)# summary-prefix 2000::/96 level-1-2 A (config-router-af)# exit-address-family
	Настройте интерфейсы Ethernet. A(config)# interface GigabitEthernet 0/0 A(config-if)# ipv6 address 5000::1/64 A(config-if)# ipv6 router isis A(config)# interface GigabitEthernet 1/0 A(config-if)# ipv6 address 2000::1111:0001/112 A(config-if)# ipv6 router isis A(config)# interface GigabitEthernet 1/1 A(config-if)# ipv6 address 2000::2222:0001/112 A(config-if)# ipv6 router isis
B	Настройте IS-IS
	B(config)# ipv6 unicast-routing B(config)# router isis B(config-router)# net 49.0001.0000.0000.0002.00
	Настройте интерфейс Ethernet
	B(config)# interface GigabitEthernet 0/0 B(config-if)# ipv6 address 5000::2/64 B(config-if)# ipv6 router isis
Проверка	Запустите команду **show ipv6 route** на маршрутизаторе B, чтобы проверить, существует ли только один суммарный маршрут
B	B(config)# show ipv6 route I1 2000::/96 [115/20] via FE80::C800:1BFF:FEF8:1C, FastEthernet1/0

Включение вывода событий отношений соседства

Шаги настройки	• Настройте соседей IS-IS. (пропущено) • Включить вывод событий соседских отношений
	A(config-router)# log-adjacency-changes
Проверка	Измените состояние соседа и убедитесь, что это изменение записывается, когда отладка отключена

Настройка перераспределения маршрутов

Шаги настройки	• Настройте соседей IS-IS. (опущено) • Настройте маршруты OSPF. (опущено) • Настроить перераспределение маршрутов
	A(config)# router isis A(config-router)# redistribute ospf 1 metric 10 level-1
Проверка	Проверьте, существуют ли записи маршрутизации с перераспределенными маршрутами
	A# show ip route isis

6.6. Мониторинг

6.6.1. Очистка

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

Описание	Команда
Очищает все таблицы отношений соседей IS-IS	**clear clns neighbors**
Очищает все структуры данных IS-IS	**clear isis ***
Очищает все счетчики IS-IS	**clear isis** [*tag*] **counter**

6.6.2. Отображение

Описание	Команда
Отображает всех соседей IS и соседские отношения между устройствами	**show clns** [*tag*] **is-neighbors** [*interface-type interface-number*] [**detail**]
Отображает всех соседей IS и предоставляет информацию об устройстве и информацию о соседских отношениях с ES	**show clns** [*tag*] **neighbors** [*interface-type interface-number*] [**detail**]
Отображает все счетчики IS-IS	**show isis** [*tag*] **counter**
Отображает информацию LSDB	**show isis** [*tag*] **database** [*FLAGS*] [*LEVEL*] [*LSPID*]
Отображает информацию о состоянии, связанную с IS-IS GR	**show isis** [*tag*] **graceful-restart**
Отображает связь между именем устройства и идентификатором системы	**show isis** [*tag*] **hostname**
Отображает сведения об интерфейсе IS-IS	**show isis** [*tag*] **interface** [*interface-type interface-number*] [*counter*]
Отображает конфигурацию группы ячеек всех интерфейсов	**show isis** [*tag*] **mesh-groups**
Отображает информацию о соседях IS-IS	**show isis** [*tag*] **neighbors** [**detail**]
Отображает информацию об IS-IS NSR	**show isis** [*tag*] **nsr**
Отображает информацию о соседях виртуальных систем в IS-IS	**show isis** [*tag*] **virtual-neighbors**
Отображает информацию IS-IS	**show isis** [*tag*] **protocol**
Отображает топологию подключения устройств IS-IS	**show isis** [*tag*] **topology** [**frr** { **self-originate** | *WORD* | **all**}] [**l1** | **l2** | **level-1** | **level-2**]

Описание	Команда
Отображает информацию о топологии unicast-рассылки IS-IS IPv6	**show isis** [*tag*] **ipv6 topology** [**l1** | **l2** | **level-1** | **level-2**]

6.6.3. Отладка

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

Описание	Команда
Включает отладку IS-IS	**debug isis** { **all** | **auth** | **events** | **frr** | **gr** | **ifsm** | **lsp** | **mtr** | **nfsm** | **nsm** | **nsr** | **pdu** | **spf** | **warn** }

7. НАСТРОЙКА BGP

7.1. Обзор

Протокол пограничного шлюза (BGP) — это протокол внешнего шлюза (EGP), используемый для связи между маршрутизаторами в различных автономных системах (AS). BGP используется для обмена информацией о доступности сети между различными AS и устранения петель маршрутизации с помощью собственного механизма.

BGP использует TCP в качестве протокола передачи. Надежный механизм передачи TCP используется для обеспечения надежности передачи BGP.

Маршрутизаторы, на которых работает BGP, называются спикерами BGP. Узлы BGP, между которыми устанавливается сеанс BGP, называются peer-ами BPG.

Для установления peer-ов между спикерами BGP можно использовать два режима: внутренний BGP (IBGP) и внешний BGP (EBGP).

- IBGP относится к соединению BGP, установленному внутри AS, и завершает передачу информации о маршрутизации внутри AS.
- EBGP относится к соединению BGP, установленному между разными AS, и обеспечивает обмен информацией о маршрутизации между разными AS.

Правила BGP для выбора оптимального маршрута:

1. Неверные записи таблицы маршрутизации не участвуют в выборе оптимального маршрута.

ПРИМЕЧАНИЕ: недопустимые записи включают записи о недоступных следующих hop-ах и нестабильные (flapping) записи.

2. В противном случае выберите маршрут с большим значением **LOCAL_PREF**.
3. В противном случае выберите маршрут, созданный спикером BGP.

ПРИМЕЧАНИЕ: маршруты, генерируемые спикером BGP, включают маршруты, генерируемые командами **network, redistribute** и **aggregate**.

4. В противном случае выберите маршрут с наименьшей длиной AS.
5. В противном случае выберите маршрут с меньшим значением **ORIGIN**.
6. В противном случае выберите маршрут с наименьшим значением **MED**.
7. В противном случае маршруты EBGP имеют более высокий приоритет, чем маршруты IBGP и маршруты в объединении AS, а маршруты IBGP имеют те же приоритеты, что и маршруты в объединении AS.
8. В противном случае выберите маршрут с наименьшим значением метрики IGP до следующего hop-а.
9. В противном случае выберите маршрут EBGP, который будет получен первым.
10. В противном случае выберите маршрут, объявленный спикером BGP с меньшим идентификатором маршрутизатора.
11. В противном случае выберите маршрут с большой длиной кластера.
12. В противном случае выберите маршрут с большим адресом соседа.

ПРИМЕЧАНИЕ: выше показан процесс выбора маршрута в конфигурациях по умолчанию. С помощью CLI-команд вы можете изменить процесс выбора маршрута. Например, вы можете запустить команду **bgp bestpath as-path ignore**, чтобы шаг 4 процесса выбора

маршрута не действовал, или запустить команду **bgp bestpath compare-routerid**, чтобы шаг 9 не действовал.

7.1.1.1. Протоколы и стандарты

- RFC4271: протокол пограничного шлюза 4 (BGP-4).
- RFC4273: определения управляемых объектов для BGP-4.
- RFC4360: предлагаемый стандарт: атрибут расширенных сообществ BGP.
- RFC4486: предлагаемый стандарт: субкоды для сообщения уведомления о прекращении BGP.
- RFC4724: предлагаемый стандарт: механизм плавного перезапуска для BGP.
- RFC4760: проект стандарта: многопротокольные расширения для BGP-4.
- RFC5492: проект стандарта: объявление возможностей с помощью BGP-4.

7.2. Приложения

Приложение	Описание
Объявление маршрута между AS	Внедрите объявление маршрутов между AS с помощью BGP
Reflection маршрута внутри AS	Настройте топологию отражения маршрутов в AS, чтобы уменьшить количество соединений BGP

7.2.1. Объявление маршрута между AS

7.2.1.1. Сценарий

BGP реализует объявление и обслуживание маршрутов между различными AS.

Как показано на Рисунке 7-1, BGP передает маршрут AS 65536 в AS 65538 через AS 65537.



Рисунок 7-1.

R1 — это устройство на границе сети AS 65536.

R2 и R3 — это устройства на границе сети AS 65537.

R4 — это устройство на границе сети AS 65538.

7.2.1.2. Развертывание

- Установите соседство EBGP между R1 и R2 для реализации объявления маршрутов между AS.
- Установите соседство IBGP между R2 и R3 для реализации объявления маршрутов внутри AS.
- В Интернете используется OSPF, чтобы обеспечить доступность сети между R2 и R3.
- Установите соседство EBGP между R3 и R4 для реализации объявления маршрутов между AS.

7.2.2. Reflection маршрута внутри AS

7.2.2.1. Сценарий

В соответствии с принципами объявления маршрутов BGP, маршруты, изученные соседом IBGP, по умолчанию не будут объявляться следующему соседу IBGP. Поэтому в AS устройство, на котором работает BGP, должно реализовать full-mesh. Когда в AS имеется много устройств BGP, реализация full-mesh может вызвать большие трудности при развертывании сети. В этом случае для решения этой проблемы можно использовать reflection маршрута (route reflection).

Как показано на Рисунке 7-2 reflection маршрута развертывается для реализации full-mesh BGP между R1, R4 и RR.

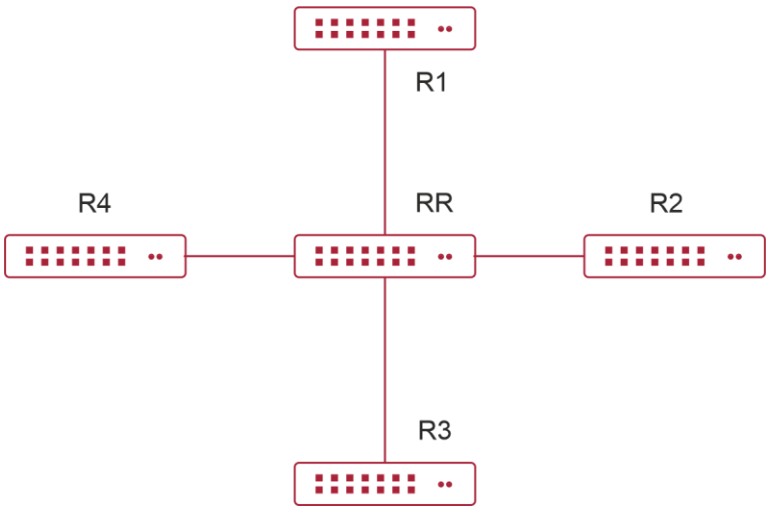


Рисунок 7-2.

RR — reflector маршрута.

R1–R4 — клиенты reflection маршрутов.

7.2.2.2. Развертывание

- Установите соседство IBGP между R1, R4 и RR соответственно.
- Настройте R1–R4 в качестве клиентов reflection маршрутов RR.

7.3. Функции

7.3.1. Основная концепция

Спикер BGP и номер AS

Маршрутизатор с поддержкой BGP называется спикером BGP.

После включения маршрута с помощью BGP для маршрутизатора необходимо указать локальный номер AS. Номер AS — это глобальный уникальный номер, присвоенный IANA, в диапазоне от 1 до 4 294 967 295.

Сосед и peer BGP

Прежде чем будет объявлен маршрут между спикерами BGP, необходимо заранее установить соседство. Вам необходимо вручную настроить соседей BGP на обоих спикерах BGP. То есть настройте peer в качестве соседа на двух спикерах BGP соответственно. Поэтому соседи BGP также называются peer-ами BGP.

Тип соседа и тип маршрута

Соседства BGP подразделяются на следующие типы:

- Соседство IBGP. Соседство между спикерами BGP в AS называется соседством IBGP. Маршруты, изученные от соседей IBGP, называются маршрутами IBGP.
- Соседство EBGP. Соседство между спикерами BGP в разных AS называется соседством EBGP. Маршруты, изученные от соседей EBGP, называются маршрутами EBGP.

Атрибут маршрута BGP

Когда спикер BGP объявляет маршруты своим соседям, спикер BGP также объявляет атрибуты, переносимые маршрутами. Общие атрибуты BGP следующие:

- ORIGIN: указывает происхождение маршрута BGP. Для него может быть установлено значение **IGP**, **EGP** или **INCOMPLETE**.
- AS-PATH: список AS, проходящих по маршруту, в обратном порядке. Последняя AS помещается в начало списка.
- NEXT-HOP: указывает IP-адрес следующего hop-а, к которому будет достигнут маршрут BGP.
- MULTI-EXIT-DISC: различает несколько интерфейсов вывода/ввода для доступа к одному и тому же соседу AS. Меньшее значение означает более высокий приоритет.
- LOCAL-PREF: определяет приоритеты маршрутов IBGP в AS. Большее значение означает более высокий приоритет.

7.3.2. Обзор

Особенность	Описание
Создание соседа BGP	Создайте соседа BGP
Настройка reflector-а маршрута BGP	Настройте топологию reflection маршрутов BGP, чтобы упростить развертывание сети для full-mesh соседей BGP

Особенность	Описание
Настройка объединения BGP	Настройте объединение BGP, чтобы упростить развертывание сети для full-mesh соседей BGP
Перераспределение информации о локальной сети AS в BGP	Перераспределяйте информацию о маршруте в BGP и объявляйте локальные маршруты через BGP
Управление обменом маршрутами между peer-ами BGP	Настройте политику обмена маршрутами для peer-а BGP и контролируйте маршруты, которые будут приниматься и объявляться этому peer-у
Получение доступных сетей других AS из BGP	Перераспределите информацию о маршрутизации в BGP в основную (core) таблицу маршрутизации или IGP
Настройка синхронизации между BGP и IGP	Настройте BGP, чтобы проверить, синхронизированы ли маршруты BGP с маршрутами IGP
Настройка программного сброса BGP	После изменения политики маршрутизации используйте программный сброс, чтобы применить новую политику
Настройка атрибутов маршрута BGP	Настройте алгоритмы выбора маршрута и контроль политики маршрутизации BGP
Настройка агрегации маршрутов BGP	Сократите маршруты с помощью агрегации маршрутов
Настройка подавления маршрутов BGP	Уменьшите влияние flapping-а маршрутов на топологию сети
Настройка расстояния управления BGP	Измените приоритеты маршрутов BGP
Настройка multipath-балансировки нагрузки BGP	Настройте multipath-балансировку нагрузки для BGP, чтобы повысить надежность сети и увеличить пропускную способность сети
Настройка BGP FRR	Настройте быструю перемаршрутизацию для BGP, чтобы повысить надежность сети

Особенность	Описание
Настройка таймеров BGP	Измените время внутреннего таймера BGP
Настройка механизмов обновления маршрутов BGP	Отключите/включите регулярное сканирование маршрутов BGP и настройте интервал сканирования маршрутов
Настройка функции обновления, запускаемого по событию следующего hop-а BGP	Настройте функцию обновления BGP, запускающую следующий hop
Настройка LOCAL AS BGP	Настройте LOCAL AS для соседа BGP
Настройка защиты емкости BGP	Избегайте непредсказуемого состояния работы, вызванного потреблением емкости устройства
Настройка BGP GR	Настройте функцию BGP GR для повышения надежности сети
Настройка 4-байтовых номеров AS BGP	Настройте режим отображения 4-байтового номера AS
Настройка регулярного выражения	Используйте регулярное выражение для фильтрации информации о маршрутизации
Настройка сохранения сеанса BGP	Настройте BGP, чтобы гарантировать, что после обнаружения семейства адресов с неверным атрибутом маршрутизации для соседа, другие маршруты семейства адресов, объявленные соседом, не будут затронуты
Настройка отложенного объявления BGP при перезапуске системы	Настройте BGP для задержки объявления маршрута соседу в течение периода после перезапуска системы
Настройка BGP NSR	Включитье функцию NSR для соседа BGP

Особенность	Описание
Настройка маршрутов BGP как рекурсивные только для маршрутов хоста	Включите, чтобы маршруты IBGP или EBGP были рекурсивными только для маршрутов хоста
Настройка обнаружения исходящей петли для соседа BGP	Включите обнаружение исходящей петли для соседа BGP
Плавное закрытие соединения BGP	Плавно завершите соединение BGP. Убедитесь, что сервисный трафик не прерывается или прерывается на очень короткий период времени
Настройка расширенного импорта маршрутов VPN	Настройте расширенную функцию импорта маршрутов VPN
Атрибут маршрута EVPN	Укажите атрибут маршрута EVPN
Настройка BGP EVPN	Настройте функцию BGP EVPN
Другие связанные конфигурации	Настройте расширенные функции BGP

7.3.3. Создание соседа BGP

Сосед BGP настраивается пользователем вручную. Поддерживаются два режима соединения: IBGP и EBGP. Вы можете определить режим соединения между спикерами BGP на основе AS, в котором находится peer BGP, и AS, в котором находится спикер BGP.

ПРИМЕЧАНИЕ: как правило, спикеры BGP, между которыми устанавливается соединение EBGP, подключаются напрямую, тогда как спикеры BGP, между которыми устанавливается соединение IBGP, могут находиться в любом месте внутри AS.

7.3.3.1. Принцип работы

Спикер BGP может инициировать запрос TCP-соединения к peer-у BGP, указанному пользователем. После успешного создания TCP-соединения peer-ы будут обмениваться пакетами BGP для согласования параметров соединения. Соседство BGP успешно устанавливается после успешного согласования.

Создание TCP-соединения

Спикер BGP инициирует запрос TCP-соединения к соседу. IP-адрес назначения — это IP-адрес peer-а, указанный пользователем, а номер порта зафиксирован на 179.

Спикер BGP также прослушивает порт номер 179 локального TCP-соединения, чтобы получать запросы на соединение от своего peer-а.

Согласование параметров протокола

После успешного создания соединения TCP спикеры BGP обмениваются пакетами OPEN для согласования параметров соединения BGP. Параметры согласования включают в себя:

- Версия: указывает номер версии BGP. На данный момент поддерживается только версия 4.
- Номер соседна AS: определяет, соответствует ли номер AS соседа локальному номеру AS. В противном случае запрос на подключение будет отклонен.
- Время удержания (Hold Time): согласовывает длительность тайм-аута для соединения BGP. Значение по умолчанию — 180 секунд.
- Возможности соседа: согласовывает различные расширенные возможности, поддерживаемые соседом, включая семейство адресов, динамическое обновление маршрута и функции GR.

Обслуживание соседства

Сообщение Keepalive периодически передается между спикерами BGP. Если новый пакет Keepalive не получен от соседа BGP по истечении времени удержания, спикер BGP считает, что сосед недоступен, отключает TCP-соединение от соседа и пытается повторно подключиться к нему. Интервал, в течение которого спикер BGP отправляет сообщение Keepalive, составляет одну треть времени удержания, определенного путем согласования, и по умолчанию составляет 60 секунд.

7.3.3.2. Сопутствующая конфигурация

Создание соседа BGP

По умолчанию спикер BGP не указывает никакого соседа. Вы можете вручную настроить соседа BGP.

Вы можете запустить команду **neighbor** { *peer-address* | *peer-group-name* } **remote-as** *as-number* для ручного создания соседа BGP и указания номера AS соседа.

Настройка TTL соседа

По умолчанию для поля TTL в TCP-пакете, отправленном соседом IBGP, установлено максимальное значение (255). Сосед EBGP установил его в 1.

Вы можете запустить команду **neighbor** { *peer-address* | *peer-group-name* } **ebgp-multihop** [*ttl*] для установки поля TTL пакета TCP, отправленного соседом BGP.

Большее значение TTL означает большее расстояние между соседями BGP. Если TTL равен 1, соседние устройства BGP должны быть подключены напрямую.

Установка адреса источника TCP

По умолчанию BGP автоматически выбирает IP-адрес источника TCP-соединения на основе IP-адреса соседа. Обычно используется IP-адрес локального интерфейса вывода пакетов.

Вы можете запустить команду **neighbor** { *peer-address* | *peer-group-name* } **update-source** {*interface-type interfacenumber* | *address* } для настройки IP-адреса источника TCP-соединения соседа.

Настройка шифрования MD5

По умолчанию соединение BGP не шифруется с помощью MD5.

Вы можете запустить команду **neighbor** { *peer-address* | *peer-group-name* } **password** [**0** | **7**] *string* для установки шифрования для TCP-соединения соседа BGP.

Активация возможности семейства адресов соседа

По умолчанию сосед, созданный в режиме конфигурации BGP, активирует только возможность семейства unicast-адресов IPv4.

Вы можете запустить команду **address-family**, чтобы войти в соответствующий режим семейства адресов, а затем запустить команду **neighbor** { *peer-address* | *peer-group-name* } **activate**, чтобы активировать возможности семейства адресов для соседа BGP.

7.3.4. Настройка reflector-а маршрута BGP

В соответствии с принципом объявления маршрутов BGP для всех спикер-ов BGP в AS должен быть установлен full mesh (между каждыми двумя спикерами BGP необходимо установить соседство). Слишком большое количество спикер-ов BGP в AS увеличит нагрузку на ресурсы спикер-ов BGP, увеличит рабочую нагрузку сетевого администратора и усложнит настройку, а также уменьшит возможности расширения сети.

Использование reflector-а маршрута — это метод сокращения peer-ов IBGP внутри AS.

ПРИМЕЧАНИЕ: методы сокращения peer-ов IBGP внутри AS включают использование reflector-а маршрута и использование объединения AS.

7.3.4.1. Принцип работы

Настройте спикер BGP в качестве reflector-а маршрута, который классифицирует peer-ы IBGP в AS на два типа: клиенты и неклиенты.

Правила реализации reflector-а маршрута в AS следующие:

- Настройте reflector маршрута и укажите клиентов для reflector-а маршрута. Reflector маршрута и его клиенты образуют кластер. Reflector маршрута будет подключаться к своим клиентам.
- Клиенты reflector-а маршрута в кластере не могут подключаться к другим спикерам BGP за пределами кластера.
- Внутри AS между peer-ами IBGP, не являющимися клиентами, устанавливается full mesh. Peer-ы IBGP, не являющиеся клиентами, включают следующие ситуации: Несколько reflector-ов маршрутов в кластере; reflector маршрута в кластере и спикеры BGP (обычно не поддерживающие функцию reflector-а маршрута), не участвующие в функции reflector-а маршрута за пределами кластера; reflector маршрута в кластере и reflector-ы маршрута в других кластерах.

Правила обработки маршрута, полученного reflector-ом маршрута, следующие:

- Сообщение обновления маршрута, полученное спикером EBGP, будет отправлено всем клиентам и неклиентам.
- Сообщение об обновлении маршрута, полученное клиентом, будет отправлено другим клиентам и всем, кто не является клиентами.
- Сообщение об обновлении маршрута, полученное спикером IBGP, будет отправлено всем остальным клиентам.

ПРИМЕЧАНИЕ: обычно в кластере настраивается только один reflector маршрута. В этом случае идентификатор маршрутизатора reflector-а маршрута может использоваться для идентификации этого кластера. Чтобы увеличить резервирование, вы можете установить несколько reflector-ов маршрутов в кластере. В этом случае необходимо настроить

идентификатор кластера, чтобы reflector маршрута мог идентифицировать сообщения обновления маршрута от других reflector-ов маршрута в кластере.

ПРИМЕЧАНИЕ: если для кластера настроено несколько reflector-ов маршрутов, необходимо настроить идентификатор кластера для кластера.

ПРИМЕЧАНИЕ: как правило, нет необходимости создавать соединения между клиентами reflector-а маршрутов в кластере, поскольку reflector маршрутов будет отражать (reflect) маршруты между клиентами. Однако если среди всех клиентов установлен full mesh, вы можете отменить функцию reflection маршрута клиента у reflector-а маршрута.

7.3.4.2. Сопутствующая конфигурация

Настройка reflector-а маршрута BGP и отраженных (reflected) клиентов

По умолчанию в BGP не настроено с reflection-ом маршрутов.

Вы можете запустить команду с **neighbor** *peer-address* **route-reflector-client**, чтобы настроить устройство в качестве reflector-а маршрута, а его соседние устройства в качестве reflected клиентов.

Настройка reflection клиент-клиент BGP

По умолчанию reflection маршрута клиент-клиент включено, что означает, что маршруты, полученные от reflected клиента, могут быть объявлены другим клиентам.

Вы можете запустить команду **bgp client-to-client reflection**, чтобы включить или отключить (используя форму **no** этой команды) reflection клиент-клиент.

Настройка идентификатора кластера reflection BGP

По умолчанию идентификатор кластера reflection BGP — это идентификатор маршрутизатора BGP. Если в AS развернуто несколько кластеров reflection, для этих кластеров reflection необходимо настроить разные идентификаторы кластера reflection.

Вы можете запустить команду **bgp cluster-id** *cluster-id*, чтобы вручную настроить идентификатор кластера reflector-а маршрута.

7.3.5. Настройка объединения BGP

Объединение — это еще один метод сокращения соединения peer-ов IBGP внутри AS.

7.3.5.1. Принцип работы

Разделите AS на несколько sub AS и настройте единый идентификатор объединения (а именно, AS NUMBER объединения) для этих sub AS, чтобы сформировать объединение. За пределами объединения всё объединение по-прежнему считается AS, и виден только номер AS объединения. Внутри объединения для спикер-ов BGP в sub AS может быть установлена full mesh peer-ов IBGP, а для спикер-ов BGP в различных sub AS могут быть установлены соединения EBGP. Хотя соединения EBGP устанавливаются между спикерами BGP внутри sub AS, при обмене информацией NEXT_HOP, MED, LOCAL_PREF и другие атрибуты пути остаются неизменными.

7.3.5.2. Сопутствующая конфигурация

Настройка идентификатора объединения BGP

По умолчанию для спикера BGP не настроен идентификатор объединения.

Вы можете запустить команду **bgp confederation identifier** *as-number*, чтобы настроить идентификатор объединения BGP. После успешной настройки локальная AS (указанная

командой **router bgp** *as-number*) BGP становится приватной AS внутри объединения и невидима для других AS.

Настройка соседа объединения BGP

По умолчанию ни один сосед по объединению не настроен для BGP.

Вы можете запустить команду **bgp confederation peers** *as-number* [… *as-number*], чтобы настроить соседа объединения BGP. После успешной настройки AS, указанная этой командой, и локальная AS принадлежат одному объединениеу.

7.3.6. Перераспределение информации о локальной сети AS в BGP

BGP не может автоматически обнаруживать или изучать доступные сети. Доступная сетевая информация локальной AS должна быть перераспределена в BGP. Затем BGP может объявить эту информацию соседям.

7.3.6.1. Принцип работы

Для этого можно использовать два метода перераспределения информации о локальной сети AS в BGP:

- Статическая настройка вручную: перераспределение доступной сетевой информации в пределах указанного диапазона в BGP.
- Настройка перераспределения маршрутов: перераспределение доступной сетевой информации IGP в BGP.

ПРИМЕЧАНИЕ: кроме того, вы также можете перераспределить информацию о локальной сети AS по маршрутам BGP, настроив агрегацию маршрутов.

7.3.6.2. Сопутствующая конфигурация

Настройка сети BGP

По умолчанию ни одна сеть не настроена для BGP.

Вы можете запустить команду **network** *network-number* [**mask** *mask*] [**route-map** *map-tag*] [**backdoor**], чтобы настроить сеть BGP для перераспределения указанной доступной сетевой информации в BGP. Предпосылкой для успешного перераспределения информации о маршрутизации в BGP является то, что маршрут доступен в основной (core) таблице маршрутизации и этот маршрут может быть IGP, маршрутом с прямым подключением или статическим маршрутом.

Настройка перераспределения маршрутов BGP

По умолчанию в BGP не настроено перераспределение маршрутов.

Запустите команду **redistribute** *protocol-type*, чтобы импортировать маршруты других протоколов в BGP, включая OSPF, RIP, ISIS, статические и прямые маршруты, маршруты хостов, преобразованные с помощью ARP, и маршруты, преобразованные с помощью ND.

Импорт маршрутов с несколькими путями или следующими hop-ами в BGP

По умолчанию маршруты, импортированные в BGP, имеют только один следующий hop.

Запустите команду **bgp sourced-paths *protocol-type* all** для импорта маршрутов с несколькими следующими hop-ами других протоколов к BGP.

7.3.7. Управление обменом маршрутами между peer-ами BGP

BGP предоставляет мощные функции управления маршрутами. Вы можете активно контролировать обмен маршрутами между peer-ами BGP.

7.3.7.1. Принцип работы

Настройте политику обмена маршрутами для peer-а BGP и управляйте маршрутами, которые будут получены и объявлены этому peer-у.

7.3.7.2. Сопутствующая конфигурация

Настройка маршрута по умолчанию для объявления peer-у

По умолчанию BGP не объявляет маршрут по умолчанию.

Вы можете запустить команду **neighbor** { *address* | *peer-group-name* } **default-originate** [**route-map** *map-tag*] для объявления маршрута по умолчанию peer-у (или группе peer-ов).

Настройка Next-Hop-Self для peer-а

По умолчанию BGP не меняет следующий hop маршрута, когда объявляет маршрут соседу IBGP, и устанавливает следующий hop локальному спикер-у BGP, когда объявляет маршрут соседу EBGP.

Вы можете запустить команду **neighbor** { *address* | *peer-group-name* } **next-hop-self** для настройки следующего hop-а маршрута к локальному спикер-у BGP при распределении маршрута указанному peer-у (группе) BGP.

Настройка Remove-Private-AS для peer-а

По умолчанию BGP не удаляет приватную AS в атрибуте AS-PATH, когда объявляет информацию о маршрутизации peer-у.

Вы можете запустить команду **neighbor** { *address* | *peer-group-name* } **remove-private-as**, чтобы номер приватной AS, записанный в атрибуте пути AS, был удален, когда информация о маршрутизации распространяется на peer (группу) EBGP. Эта команда не применяется к соседу IBGP.

Настройка Send-Community для peer-а

По умолчанию BGP не отправляет атрибут сообщества, когда объявляет информацию о маршрутизации peer-у.

Вы можете запустить команду **neighbor** { *address* | *peer-group-name* } **send-community**, чтобы указать, что атрибут сообщества может быть отправлен указанному peer-у (группе) BGP.

Настройка Maximum-Prefix для peer-а

По умолчанию BGP не ограничивает записи информации о маршрутизации, которые может получить peer.

Вы можете запустить команду **neighbor** { *address* | *peer-group-name* } **maximum-prefix** *maximum* [**warning-only**] для указания записей информации о маршрутизации, полученной от указанного peer-а (группы).

Настройка фильтрации маршрутов для соседа BGP

По умолчанию сосед BGP не использует никакую политику фильтрации и получает всю допустимую информацию о маршрутизации, объявленную соседом.

BGP поддерживает несколько методов настройки политик фильтрации маршрутов для соседа, в том числе:

- **neighbor** { peer-address | peer-group-name } **distribute-list** { access-list-number | access-list-name } { **in** | **out** }

Использует ACL для фильтрации маршрутов во входных и выходных направлениях соседа.

- **neighbor** { peer-address | peer-group-name } **filter-list** access-list-number { **in** | **out** }

Использует список AS-PATH для фильтрации маршрутов во входном и выходном направлениях соседа.

- **neighbor** { peer-address | peer-group-name } **prefix-list** prefix-list-name { **in** | **out** }

Использует список префиксов для фильтрации маршрутов во входном и выходном направлениях соседа.

- **neighbor** { *peer-address* | *peer-group-name* } **route-map** *map-tag* { **in** | **out** }

Использует карту маршрутов для фильтрации маршрутов во входных и выходных направлениях соседа.

- **neighbor** { address | peer-group-name } **unsuppress-map** map-tag

Разрешает объявление определенной информации о маршрутизации, ранее подавленной командой **aggregate-address**, при распространении информации о маршрутизации указанному peer-у.

- bgp advertise-map *map-tag*

Использует команду **bgp advertise-map** *map-tag*, чтобы объявить политику маршрутизации всем соседям.

7.3.8. Получение доступных сетей других AS из BGP

Отправляет информацию о маршрутизации других AS, которыми обменивается BGP, в таблицу маршрутизации устройства, чтобы устройство могло пересылать пакеты другим AS.

7.3.8.1. Принцип работы

BGP отправляет информацию о маршрутизации в основную (core) таблицу маршрутизации

BGP управляет информацией о маршрутизации, отправляемой в основную таблицу маршрутизации с помощью **table-map**. **table-map** может изменять атрибуты информации о маршрутизации, отправляемой в основную таблицу маршрутизации. Если маршрут совпадает, BGP изменяет атрибут информации о маршрутизации и отправляет маршрут. Если маршрут не сопоставлен или сопоставление маршрута отклонено, BGP не изменяет атрибут информации о маршрутизации, но отправляет маршрут.

Изменения **table-map** не отражаются в основной таблице маршрутизации немедленно, а отражаются моментом позже. Чтобы немедленно обновить приложение **table-map**, вы можете запустить команду **clear ip bgp** [vrf *vrf-name*] **table-map**, чтобы немедленно обновить информацию о маршрутизации в основной таблице маршрутизации. Эта команда не очищает существующие маршруты в основной таблице маршрутизации, а напрямую применяет **table-map** для отправки обновленной информации о маршрутизации, тем самым не вызывая flapping-а пересылки.

Перераспределение маршрутов BGP в IGP

Перераспределите маршруты BGP на спикере BGP в IGP, чтобы маршрутизаторы внутри AS могли получать маршруты к другим AS.

7.3.8.2. Сопутствующая конфигурация

Настройка table-map

По умолчанию BGP не настроен с table-map и позволяет отправлять все маршруты без изменения атрибутов маршрутов.

Вы можете запустить команду **table-map** *route-map-name*, чтобы установить table-map и управлять информацией о маршрутизации, которая будет отправлена в основную таблицу маршрутизации. *route-map-name* указывает карту маршрутов, которая будет связана.

ПРИМЕЧАНИЕ: запустите команду **table-map** в режиме конфигурации BGP или в режиме семейства адресов IPv4. В table-map поддерживаются следующие операторы Match и Set.

Операторы соответствия (Match): as-path, community, ip address, ip next-hop, metric, origin и route-type.

Операторы установки (Set): metric, tag и next-hop.

ПРИМЕЧАНИЕ: вы можете запустить команду **no table-map**, чтобы удалить конфигурации table-map.

Настройка перераспределения маршрутов BGP с помощью IGP

По умолчанию IGP не перераспределяет маршруты BGP.

Вы можете запустить команду **redistribute bgp** [**route-map** *map-tag*] [**metric** *metric-value*] для перераспределения маршрутов BGP в IGP (RIP\OSPF\ISIS).

Команда **bgp redistribute-internal** контролирует только то, следует ли перераспределять маршруты, изученные из IBGP, в IGP. По умолчанию маршруты, изученные из IBGP, могут быть перераспределены в IGP.

ПРИМЕЧАНИЕ: вы можете запустить команду **bgp redistribute-internal** в режиме конфигурации BGP, режиме семейства адресов IPv4/IPv6 или режиме семейства адресов IPv4 VRF.

ПРИМЕЧАНИЕ: вы можете запустить команду **no bgp redistribute-internal**, чтобы удалить конфигурацию.

7.3.9. Настройка синхронизации между BGP и IGP

Как правило, спикеры BGP, работающие как взаимные соседи IBGP, не связаны напрямую. Устройства IGP между спикерами BGP могут не получить информацию о маршрутизации, ту же, что была получена спикерами BGP. Когда спикер BGP на границе AS пересылает пакеты, полученные из других доменов, соседу IBGP следующего hop-a, пакеты проходят через устройство IGP в середине. В этом случае пакеты могут быть потеряны из-за отсутствия информации о маршрутизации на устройстве IGP.

7.3.9.1. Принцип работы

Чтобы поддерживать синхронизацию между BGP и IGP, вы должны убедиться, что все маршрутизаторы в пределах AS могут изучить информацию о маршрутизации для отправки в другую AS, прежде чем информация о маршрутизации будет объявлена в этой AS.

Синхронизация между BGP и IGP не требуется только в следующих случаях:

- Информация о маршрутизации, проходящая через AS, недоступна. Например, AS является конечной AS.

- Все маршрутизаторы в AS используют BPG. Full mesh устанавливается между всеми спикерами BGP (соседство устанавливается между каждыми двумя спикерами BGP).

7.3.9.2. Сопутствующая конфигурация

Настройка синхронизации маршрутов BGP

По умолчанию синхронизация между маршрутами BGP и IBGP отключена.

Вы можете запустить команду **synchronization**, чтобы включить синхронизацию между BGP и IGP.

ПРИМЕЧАНИЕ: вы можете запустить команду **no synchronization**, чтобы отключить синхронизацию между BGP и IGP.

7.3.10. Настройка программного сброса BGP

Если политики маршрутизации (включая **neighbor distribute-list, neighbor route-map, neighbor prefix-list** и **neighbor filter-list**) изменяются, необходимо предоставить эффективный метод для реализации новых политик маршрутизации. Традиционный метод-— разорвать соединение BGP и затем создать новое соединение BGP. Настроив программный сброс BGP, вы можете выполнить новую политику маршрутизации, не разрывая соединение сеанса BGP.

7.3.10.1. Принцип работы

ПРИМЕЧАНИЕ: политики маршрутизации, влияющие на информацию входящей маршрутизации, называются политиками входящей маршрутизации (например, In-route-map и In-dist-list), а политики маршрутизации, влияющие на информацию исходящей маршрутизации, называются политиками исходящей маршрутизации (например, Out-route-map и Out-dist-list).

При изменении политики исходящей маршрутизации программный сброс BGP повторно объявляет всю информацию о маршрутизации спикера BGP его соседям.

Если изменяются политики входящей маршрутизации, операция становится более сложной, чем при изменении политик исходящей маршрутизации. Это связано с тем, что политики исходящей маршрутизации выполняются в таблице маршрутизации локального спикера BGP, тогда как политики входящей маршрутизации выполняются для информации о маршрутизации, полученной от peer-а BGP. Чтобы снизить затраты, локальный спикер BGP не сохраняет исходную информацию о маршрутизации, полученную от peer-а BGP.

Если политики входящей маршрутизации изменяются и соседнее устройство поддерживает обновление маршрута, вы можете настроить программный сброс для отправки запроса на обновление маршрута соседнему устройству. После получения запроса соседнее устройство повторно объявляет всю информацию о маршрутизации. Вы также можете выполнить настройку, чтобы гарантировать, что каждый peer BGP хранит исходную информацию о маршрутизации на локальном спикере BGP и предоставляет исходную информацию о маршрутизации для последующего изменения политик входящей маршрутизации.

ПРИМЕЧАНИЕ: «возможность обновления маршрута» позволяет изменять и выполнять политики маршрутизации без сохранения исходной информации о маршрутизации. Этот продукт поддерживает возможность обновления маршрута. Вы можете запустить команду **show ip bgp neighbors**, чтобы проверить, поддерживает ли peer BGP обновление маршрута. Если да, вам не нужно запускать команду **neighbor soft-reconfiguration inbound** при изменении политики входящей маршрутизации.

7.3.10.2. Сопутствующая конфигурация

Настройка программного сброса BGP

Запустите команду **clear ip bgp** { ***** | *peer-address* | **peer-group** *peer-group-name* | **external** } **soft out** для мягкого сброса соединения BGP. Вы можете активировать выполнение политики маршрутизации без перезапуска сеанса BGP.

Сохранение исходной информации о маршрутизации соседей

По умолчанию BGP не сохраняет исходную информацию о маршрутизации соседей.

Запустите команду **neighbor** { *address* | *peer-group-name* } **soft-reconfiguration inbound** для сохранения неизмененной информации о маршрутизации, отправленной peer-ом (группой) BGP.

7.3.11. Настройка атрибутов маршрута BGP

BGP предоставляет различные политики управления атрибутами маршрута. Вы можете применять политики в зависимости от реальных условий.

7.3.11.1. Принцип работы

Атрибут AS_PATH

BGP может управлять распределением маршрутной информации в трех режимах:

- IP-адрес. Для реализации можно запустить команды **neighbor distribute-list** и **neighbor prefix-list**.
- Атрибут AS_PATH. Смотрите описание в этом разделе.
- Атрибут COMMUNITY. См. соответствующую конфигурацию атрибута COMMUNITY.

Для управления распределением маршрутной информации можно использовать список управления доступом (ACL) на основе путей AS. При этом ACL на основе пути AS использует регулярное выражение для анализа пути AS.

Согласно стандарту (RFC1771), BGP не учитывает длину пути AS при выборе оптимального пути. Обычно более короткая длина пути AS означает более высокий приоритет пути; поэтому QTECH учитывает длину пути AS при выборе оптимального пути. Вы можете определить, следует ли учитывать длину пути AS при выборе оптимального пути на основе фактических условий.

ПРИМЕЧАНИЕ: при выборе оптимального пути в AS путь AS должен быть единообразным для всех спикеров BGP; в противном случае оптимальные пути, выбранные спикерами BGP, могут отличаться.

Атрибут MULTI_EXIT_DISC

BGP использует значение MED в качестве основы для сравнения приоритетов путей, полученных от peer-ов EBGP. Меньшее значение MED означает более высокий приоритет пути.

- По умолчанию значение MED сравнивается только для путей peer-ов из одной AS, когда выбран оптимальный путь.
- По умолчанию значение MED не сравнивается для путей peer-ов из других sub AS в объединении AS.
- По умолчанию, если получен путь, не настроенный с атрибутом MED, считается, что значение MED этого пути равно 0. Поскольку меньшее значение MED означает более высокий приоритет пути, этот путь имеет наивысший приоритет.

- По умолчанию значение MED не сравнивается с путями от разных AS; вместо этого сравнивается последовательность получения путей.

Атрибут LOCAL_PREF

При отправке маршрутов, полученных от peer-ов EBGP peer-ам IBGP, спикер BGP добавляет атрибут LOCAL_PREF. BGP использует атрибут LOCAL_PREF в качестве основы для сравнения приоритетов путей, изученных от peer-ов IBGP. Большее значение LOCAL_PREF означает более высокий приоритет пути.

Вы также можете запустить команду **set local-preference** карты маршрутов, чтобы изменить атрибут LOCAL_PREF указанного пути.

Атрибут COMMUNITY

Атрибут COMMUNITY — это еще один режим управления распространением информации о маршрутизации.

Сообщество (community) — это набор адресов назначения. Атрибут COMMUNITY предназначен для облегчения выполнения политики маршрутизации на основе сообщества и тем самым упрощает настройку управления распределением маршрутной информации на спикер-ах BGP. Каждый адрес назначения может принадлежать нескольким сообществам. Администратор AS может определить сообщества, которым принадлежит адрес назначения.

По умолчанию все адреса назначения принадлежат интернет-сообществу и передаются в атрибуте пути COMMUNITY.

В настоящее время заранее определены четыре общих значения атрибутов COMMUNITY:

- Internet: указывает на интернет-сообщество. Все пути принадлежат этому сообществу.
- no-export: указывает, что путь не объявляется peer-ам EBGP.
- no-advertise: указывает, что путь не объявляется ни одному peer-у BGP.
- local-as: указывает, что путь не объявляется другим AS. Когда настроено объединение AS, путь не объявляется другим AS или sub AS.

Используя атрибут COMMUNITY, вы можете контролировать получение, определение приоритетов и распространение информации о маршрутизации. Спикеры BGP могут устанавливать, добавлять или изменять атрибут COMMUNITY при изучении, объявлении или перераспределении маршрутов. Путь агрегации будет содержать значения атрибутов COMMUNITY всех агрегированных путей.

ПРИМЕЧАНИЕ: BGP поддерживает до 32 атрибутов COMMUNITY для каждого маршрута и допускает до 32 атрибутов COMMUNITY, если настроены match и set COMMUNITY карты маршрутов.

Другие

Если во время выбора оптимального пути два пути с одинаковыми атрибутами пути получены от разных peer-ов EBGP, оптимальный путь выбирается на основе последовательности получения по умолчанию. Вы можете отключить сравнение последовательности получения, но использовать путь с меньшим идентификатором маршрутизатора в качестве оптимального пути.

7.3.11.2. Сопутствующая конфигурация

Настройка атрибута AS_PATH

- **ip as-path access-list** *path-list-name* { **permit** | **deny** } *as-regular-expression*

Определяет список путей AS.

- **neighbor** { *address* | *peer-group-name* } filter-list *path-list-name* { **in** | **out** }

По умолчанию для peer-ов BGP политика фильтрации не настроена.

Конфигурация одинакова для получения и отправки информации о маршрутизации для указанного peer-а (группы) BGP. Политики маршрутизации выполняются на основе списка путей AS для объявления или получения только маршрутов, соответствующих политикам.

- **neighbor** { *address* | *peer-group-name* } **route-map** *map-tag* { **in** | **out** }

По умолчанию для peer-ов BGP политика фильтрации не настроена.

Конфигурация одинакова для получения и отправки информации о маршрутизации для указанного peer-а (группы) BGP. Политики маршрутизации выполняются на основе карты маршрутов или набора правил в карте маршрутов и используются для изменения атрибутов маршрутизации.

ПРИМЕЧАНИЕ: в режиме конфигурации карты маршрутов вы можете запустить команду **match as-path** для изменения атрибутов пути AS с помощью списка путей AS или напрямую запустить команду **set as-path** для изменения значений атрибутов AS.

- **bgp bestpath as-path ignore**

Позволяет BGP не учитывать длину пути AS при выборе оптимального пути. Длина пути AS сравнивается по умолчанию.

По умолчанию меньшая длина пути AS означает более высокий приоритет пути.

Настройка атрибута MULTI_EXIT_DISC

- **bgp always-compare-med**

Позволяет сравнивать значения MED путей из разных AS, по умолчанию отключено.

- **bgp bestpath med confed**

Позволяет сравнивать значения MED путей peer-ов из других sub AS в том же объединении AS, по умолчанию отключено.

- **bgp bestpath med missing-as-worst**

Устанавливает для пути, для которого не настроен атрибут MED, самый низкий приоритет, который по умолчанию отключен.

- **bgp deterministic-med**

Позволяет сравнивать пути peer-ов внутри одной AS, по умолчанию отключено.

Настройка атрибута LOCAL_PREF

- **bgp default local-preference** *value*

Изменяет значение локального предпочтения (local-preference) по умолчанию в диапазоне от 0 до 4 294 967 295. Большее значение означает более высокий приоритет. Значение по умолчанию — 100.

Настройка атрибута COMMUNITY

- **ip community-list standard** *community-list-name* { **permit** | **deny** } *community-number*

Создает список сообщества. **community-list-name** указывает имя списка сообщества.

ПРИМЕЧАНИЕ: *community-number*: указывает значение (от 0 до 4 294 967 295), указанное пользователем или известным атрибутом сообщества (internet, local-AS, no-advertise или no-export).

- **neighbor** { *address* | *peer-group-name* } **send-community**

Позволяет отправлять атрибут сообщества указанному peer-у (группе) BGP, который не настроен по умолчанию.

- **neighbor** { *address* | *peer-group-name* } **route-map** *map-tag* { **in** | **out** }

Конфигурация такая же, как и для получения и отправки информации о маршрутизации для указанного peer-а (группы) BGP. Политики маршрутизации выполняются на основе карты маршрутов. По умолчанию для peer-ов не настроена политика фильтрации.

В режиме конфигурации карты маршрутов вы можете запустить команды **match community-list [exact]** и **set community-list delete**, чтобы изменить атрибут сообщества с помощью списка сообщества, или напрямую запустить команду **set community**, чтобы изменить значение сообщества.

Другие

- **bgp bestpath compare-routerid**

Позволяет BGP сравнивать идентификатор маршрутизатора при выборе оптимального пути, который по умолчанию отключен.

7.3.12. Настройка агрегации маршрутов BGP

BGP-4 поддерживает CIDR и, следовательно, позволяет создавать записи агрегации для уменьшения размера таблицы маршрутизации BGP. Записи агрегации BGP можно добавлять в таблицу маршрутизации BGP только в том случае, если в диапазоне агрегации доступны действительные пути.

7.3.12.1. Принцип работы

Агрегирует один или несколько деталлизированных маршрута BGP в маршрут BGP с более короткой маской сети.

ПРИМЕЧАНИЕ: по умолчанию BGP объявляет всю информацию о пути до и после агрегации. Если вы надеетесь, что будет объявлена только агрегированная информация о пути, вы можете запустить команду **aggregate-address summary-only**.

ПРИМЕЧАНИЕ: когда команда **aggregate-address** используется для настройки агрегированного маршрута, агрегированный маршрут вступает в силу немедленно, если в настроенном диапазоне адресов есть маршруты.

7.3.12.2. Сопутствующая конфигурация

Настройка агрегации маршрутов BGP

- **aggregate-address** *address mask*

Настраивает агрегацию маршрутов BGP. По умолчанию BGP не создает агрегированных записей маршрутизации.

- **aggregate-address** *address mask* **as-set**

Настраивает адрес агрегации и сохраняет информацию о пути AS в диапазоне адресов агрегации. По умолчанию BGP не хранит информацию о пути AS.

- **aggregate-address** *address mask* **summary-only**

Настраивает адрес агрегации и объявляет только агрегированный путь. По умолчанию BGP объявляет всю информацию о пути в диапазоне агрегации.

- **aggregate-address** *address mask* **as-set summary-only**

Настраивает адрес агрегации, сохраняет информацию о пути AS в диапазоне адресов агрегации и объявляет только агрегированные пути.

7.3.13. Настройка подавления маршрутов BGP

Если маршрут меняется с действительного на недействительный, происходит flapping маршрута.

Flapping маршрутов часто приводит к передаче нестабильных маршрутов в сети и тем самым вызывает нестабильность сети. Подавление маршрутов BGP — это метод уменьшения flapping-а маршрутов. Это уменьшает возможный flapping маршрутов за счет мониторинга информации о маршрутизации от peer-ов EBGP.

7.3.13.1. Принцип работы

Термины, используемые при подавлении маршрутов BGP, следующие:

- Route Flap: маршрут меняется между действительным и недействительным.
- Penalty: как только происходит flapping маршрута, спикер BGP, включенный с подавлением маршрута, добавляет значение к штрафу (Penalty) для этого маршрута. Штраф накапливается до тех пор, пока не будет достигнут предел подавления (Suppress Limit).
- Suppress Limit: если штраф для маршрута превышает это значение, маршрут будет подавлен.
- Half-life-time: время, за которое штраф будет уменьшен вдвое.
- Reuse Limit: если значение штрафа для маршрута меньше этого значения, подавление маршрута будет отменено.
- Max-suppress-time: максимальное время, в течение которого маршрут может быть подавлен.

Краткое описание обработки подавления маршрутов: спикер BGP наказывает маршрут, как только происходит (добавляется к штрафу) изменение маршрута. Когда штраф достигнет предела подавления (Suppress Limit), маршрут будет подавлен. Когда период Half-life-time достигается, штраф уменьшается вдвое. Когда штраф снижается до Reuse Limit, маршрут снова активируется. Максимальное время подавления (Max-suppress-time) указывает максимальное время, в течение которого маршрут может быть подавлен.

7.3.13.2. Сопутствующая конфигурация

Настройка подавления маршрутов BGP

- **bgp dampening**

Включает подавление BGP, которое по умолчанию отключено.

- **bgp dampening** *half-life-time reuse suppress max-suppress-time*

Настраивает параметры подавления маршрута.

half-life-time (1–45 минут): значение по умолчанию составляет 15 минут. Большее значение означает период подавления и более длительное подавление flapping-а.

reuse (1~10000): значение по умолчанию — 750. Меньшее значение означает больше времени для непрерывной стабилизации, прежде чем flapping маршрута снова будет включен.

suppress (1~20 000): значение по умолчанию — 2000. Меньшее значение означает большее количество раз flapping-а, допустимое перед подавлением.

max-supress-time (1~255 минут): значение по умолчанию — 4×*half-life-time*. Большее значение означает большее максимальное время подавления.

Отображение подавления маршрутов BGP

- **show ip bgp dampening flap-statistics**

Отображает статистику flapping-а по всем маршрутам.

- **show ip bgp dampening dampened-paths**

Отображает статистику о подавленных маршрутах.

Сброс подавления маршрутизации BGP

- **clear ip bgp flap-statistics**

Очищает статистику flapping-а для всех маршрутов, которые не подавлены.

- **clear ip bgp flap-statistics** *address mask*

Очищает статистику flapping-а для указанных маршрутов (исключая подавленные маршруты).

- **clear ip bgp dampening** [*address* [*mask*]]

Очищает статистику flapping-а для всех маршрутов, включая маршруты, подавление которых отменено.

7.3.14. Настройка расстояния управления BGP

Расстояние управления используется для оценки надежности различных источников маршрута. Меньшее расстояние управления означает лучший маршрут.

7.3.14.1. Принцип работы

Расстояние управления BGP

Расстояние управления указывает на надежность источника маршрута в диапазоне от 1 до 255. Большее значение означает меньшую надежность. BGP устанавливает разные расстояния управления для информации о маршрутизации, полученной из разных источников, включая внешнее расстояние (External-distance), внутреннее расстояние (Internal-distance) и локальное расстояние (Local-distance).

- External-distance (Внешнее расстояние): указывает расстояние управления маршрутами, полученными от peer-ов EBGP.
- Internal-distance (Внутреннее расстояние): указывает расстояние управления маршрутами, полученными от peer-ов IBGP.
- Local-distance (Локальное расстояние): указывает расстояние управления для маршрутов, полученных от peer-ов, но считается, что лучшие маршруты можно узнать из IGP. Обычно эти маршруты можно указать с помощью команды **network backdoor**.

ПРИМЕЧАНИЕ: не рекомендуется изменять расстояние управления BGP. Если вам действительно необходимо изменить расстояние управления BGP, помните:

- Внешнее расстояние должно быть короче, чем расстояния управления других протоколов маршрутизации IGP (OSPF и RIP).
- Внутреннее расстояние и локальное расстояние должны быть длиннее, чем расстояния управления других протоколов маршрутизации IGP.

Маршрут backdoor

Если вы предпочитаете маршрут IGP, но не используете маршрут EBGP, вы можете установить маршрут EBGP в качестве маршрута backdoor. По умолчанию расстояние управления для маршрутов, полученных от спикера BGP, для которого установлено

соединение EBGP, составляет 20. Вы можете запустить команду **network backdoor**, чтобы установить расстояние управления сетевой информацией на 200, чтобы та же сетевая информация, изученная из IGP, имела высший приоритет. Сети, изученные от IGP, считаются сетями backdoor и не объявляются.

7.3.14.2. Сопутствующая конфигурация

Настройка расстояния управления BGP

Вы можете запустить команду **distance bgp** *external-distance internal-distance local-distance*, чтобы настроить расстояние управления BGP. Значение варьируется от 1 до 255.

Значение *external-distance* по умолчанию — 20; значение *internal-distance* по умолчанию — 200; значение *local-distance* по умолчанию — 200.

Большее расстояние управления означает меньший приоритет маршрута.

Настройка backdoor-маршрута

Запустите команду **network** *network-number* **mask** *network-mask* **backdoor**, чтобы настроить маршрут backdoor. По умолчанию backdoor-маршрут не настроен.

7.3.15. Настройка multipath-балансировки нагрузки BGP

Multipath-балансировка нагрузки означает, что к одной и той же сети имеется несколько путей, и пакеты данных пересылаются по этим путям равномерно. В таблице маршрутизации один маршрут имеет несколько следующих hop-ов.

По типам эквивалентных маршрутов multipath-балансировка нагрузки BGP классифицируется на следующие типы:

- Балансировка нагрузки EBGP: реализация балансировки нагрузки для маршрутов, полученных от соседей EBGP.
- Балансировка нагрузки IBGP: реализация балансировки нагрузки для маршрутов, полученных от соседей IBGP.

ПРИМЕЧАНИЕ: стеки протоколов IPv4 и IPv6 поддерживают многопутевую балансировку нагрузки.

ПРИМЕЧАНИЕ: балансировку нагрузки нельзя реализовать между маршрутами IBGP и EBGP (включая маршруты EBGP в объединении).

7.3.15.1. Принцип работы

Если таблица маршрутизации BGP содержит несколько путей к одной и той же сети, BGP по умолчанию вычисляет маршрут с наивысшим приоритетом. Если существует несколько оптимальных маршрутов с одинаковыми приоритетами, BGP все равно выбирает уникальный маршрут, используя правила сравнения, уведомляет forwarding plane о маршруте и контролирует пересылку потоков данных. После включения multipath-балансировки нагрузки BGP вычисляет уникальный оптимальный маршрут, а также составляет список путей с теми же приоритетами, что и эквивалентные маршруты. Затем BGP уведомляет forwarding plane об оптимальном маршруте и эквивалентных маршрутах для реализации балансировки нагрузки.

Эквивалентные маршруты имеют одинаковые базовые атрибуты и приоритеты. То есть, в соответствии с правилами оптимального выбора пути BGP, перед сравнением идентификаторов маршрутизаторов пути имеют одинаковые приоритеты.

Свободное сравнение AS_PATH

По умолчанию эквивалентные маршруты должны иметь одинаковые атрибуты AS-PATH. При таких строгих условиях балансировку нагрузки невозможно реализовать в определенных средах. В этом случае вам будет предложено включить режим свободного сравнения AS-PATH. В режиме свободного сравнения AS-PATH, когда выполняются другие условия для эквивалентных маршрутов, при условии, что длины маршрутов AS-PATH и длины маршрутов AS-PATH из объединения одинаковы соответственно, считается, что условия для эквивалентных маршрутов соблюдены.

ПРИМЕЧАНИЕ: когда следующие hop-ы нескольких эквивалентных путей BGP повторяются к одному и тому же выходному интерфейсу IGP, балансировку нагрузки реализовать невозможно.

7.3.15.2. Сопутствующая конфигурация

Настройка multipath-балансировки нагрузки BGP

- **maximum-paths** { **ebgp** | **ibgp** } *number*

Включает функцию multipath-балансировки нагрузки BGP.

number указывает количество эквивалентных следующих hop-ов в диапазоне от 1 до емкости устройства. Значение по умолчанию — 1. Чем больше значение, тем больше разрешено эквивалентных следующих hop-ов.

Настройка свободного сравнения AS_PATH

- **bgp bestpath as-path multipath-relax**

Включает режим свободного сравнения BGP AS-PATH.

7.3.16. Настройка BGP FRR

С быстрым развитием IP-технологий и применением различных сложных сервисов требования к безопасности и стабильности сети становятся все выше. В частности, некоторые сервисы в реальном времени (аудио и видео) чувствительны к состоянию работы сети и могут сильно зависеть от нестабильности сетей. Поэтому все больше внимания и значения уделяется надежности сети. В соответствии с этими требованиями возникает функция IP FRR. Предполагается использовать резервный канал для поддержания пересылки данных во время конвергенции платформы маршрутов после обнаружения неисправного канала, чтобы достичь идеальных целей «нулевой задержки» и «нулевых потерь» при пересылке пакетов.

BGP FRR сокращенно означает Fast Reroute (быстрое изменение маршрута).

7.3.16.1. Принцип работы

Если таблица маршрутизации BGP содержит несколько путей к одной и той же сети, BGP по умолчанию вычисляет маршрут с наивысшим приоритетом. После использования функции BGP FRR BGP выбирает резервный маршрут для каждого оптимального маршрута. После того как BFD FRR обнаруживает, что master-канал неисправен, он переключает данные на первоначально рассчитанный резервный канал для пересылки. После завершения конвергенции маршрутов данные переключаются на оптимальный маршрут, пересчитанный для пересылки. Таким образом, BGP FRR может избежать отключения маршрута из-за сбоя канала до завершения конвергенции маршрутов BGP.

ПРИМЕЧАНИЕ: можно создать только один резервный маршрут, и следующий hop резервного маршрута не может быть таким же, как у предпочтительного маршрута.

ПРИМЕЧАНИЕ: резервный следующий hop не может быть создан для маршрута multipath-маршрутизации с равной стоимостью (ECMP).

ПРИМЕЧАНИЕ: BGP FRR имеет более низкий приоритет, чем VPN FRR. То есть, если VPN FRR включен в режиме VRF, BGP FRR вступает в силу только тогда, когда VPN FRR не удается вычислить резервный маршрут.

7.3.16.2. Сопутствующая конфигурация

Настройка BGP FRR

Запустите команду **bgp fast-reroute**, чтобы включить функцию BGP FRR, которая по умолчанию отключена.

Настройка сеанса BFD для соседа BGP

Запустите команду **neighbor** { *neighbor-address* | *peer-group-name* } **fall-over bfd** для настройки сеанса BFD с соседом BGP, который не настроен по умолчанию.

Настройка сеанса BGP BFD вручную

Если сеанс BFD с соседом BGP не может быть использован для быстрого обнаружения сбоя master-канала, вы можете запустить команду **bfd bind bgp peer-ip** *ip-address* **interface** *interface-type interface-index* **source-ip** *ip-address* для настройки сеанс BGP BFD, который не настроен по умолчанию.

7.3.17. Настройка быстрого изымания (Fast Withdrawal) указанных маршрутов BGP

С быстрым развитием IP-технологий и применением различных сложных сервисов к сети предъявляются все более высокие требования. Клиентам может потребоваться реализовать быструю конвергенцию на определенных маршрутах. Быстрое изымание маршрутов может удовлетворить требования клиентов по предпочтительному изыманию определенных маршрутов.

7.3.17.1. Принцип работы

По умолчанию маршруты изымаются на основе предпочтительного расчета в соответствии с последовательностью в таблице маршрутизации. Быстрое изымание маршрута добавляет маршруты, соответствующие условиям, в очередь с высоким приоритетом для реализации приоритетной обработки указанных маршрутов, чтобы указанные маршруты можно было быстро изымать.

ПРИМЕЧАНИЕ: семейство адресов L2VPN поддерживает только режим карты маршрутов.

ПРИМЕЧАНИЕ: действует только один: список доступа и список префиксов.

7.3.17.2. Сопутствующая конфигурация

Активация возможности семейства адресов

По умолчанию для соседей, созданных в режиме конфигурации BGP, активируется только возможность семейства unicast-адресов IPv4.

Запустите команду **address-family**, чтобы войти в соответствующий режим семейства адресов.

Настройка быстрого изымания указанных маршрутов BGP

Запустите команду **bgp fast-withdraw { access-list {** *access-list-number* | *access-list-name* **} | prefix-list** *prefix-list-name* **| route-map** *map-tag***}**, чтобы включить быстрое изымание указанных маршрутов BGP в семействе адресов. По умолчанию эта функция отключена.

7.3.18. Настройка BGP Multi-path Bypass Protection

Исходный вариант BGP FRR поддерживает только защиту 1:1. После включения функции ECMP FRR становится недоступным. Multi-path Bypass Protection позволяет BGP поддерживать защиту 1:N. Пользователи могут настроить BGP Multi-path Bypass Protection, чтобы система могла выбирать резервный обходной путь (bypass), даже если настроен ECMP. Если все маршруты ECMP терпят неудачу, обходной маршрут становится основным маршрутом пересылки.

7.3.18.1. Принцип работы

По умолчанию, если в таблице маршрутизации BGP имеется несколько путей, доступных к одной и той же сети, BGP вычисляет один маршрут с наивысшим приоритетом. После включения функции BGP Multi-path Bypass Protection BGP предпочтительно выбирает резервный маршрут, если существуют маршруты ECMP. Когда BFD обнаруживает ошибку, возникающую на master-пути, система переключается на выбранный резервный путь для пересылки данных. После завершения конвергенции маршрутов система переключается на оптимальный путь, который пересчитывается на основе маршрутов для пересылки данных.

ПРИМЕЧАНИЕ: создается только один обходной маршрут, и следующий hop обходного маршрута не может совпадать со следующими hop-ами маршрутов ECMP.

ПРИМЕЧАНИЕ: функция BGP FRR конфликтует с функцией BGP Multi-path Bypass Protection. Если какая-либо из них настроена, когда другая функция уже доступна, будет отображено сообщение о конфликте.

7.3.18.2. Сопутствующая конфигурация

Настройка BGP Multi-path Bypass Protection

Запустите команду **bgp install standby-path**, чтобы включить BGP Multi-path Bypass Protection, которая по умолчанию отключена.

Настройка сеанса BFD с соседом BGP

Запустите команду **neighbor** { *neighbor-address* | *peer-group-name* } **fall-over bfd** для настройки сеанса BFD с соседом BGP, который не настроен по умолчанию.

Настройка сеанса BGP BFD вручную

Если неисправности, возникающие на master-пути, не могут быть быстро обнаружены с помощью сеанса BFD соседа BGP, запустите команду **bfd bind bgp peer-ip** *ip-address* **interface** *interface-type interface-index* **source-ip** *ip-address*, чтобы настроить сеанс BGP BFD. По умолчанию сеанс BGP BFD не настроен.

7.3.19. Разрешение reflector-а маршрута BGP для изменения атрибутов маршрута

Согласно RFC4456, reflector маршрутов BGP не может изменять атрибуты маршрутов при отображении (reflecting) маршрутов (цель состоит в том, чтобы предотвратить петли маршрутов). Однако соответствующие атрибуты маршрута необходимо изменить, когда пути сетевого трафика необходимо перепланировать. Эта команда настроена так, чтобы

позволить reflector-у маршрута изменять атрибуты маршрута (включая **route-map** или **nexthop-self**).

7.3.19.1. Принцип работы

Reflector-у маршрута по умолчанию не разрешено изменять атрибуты маршрута. После настройки этой команды reflector-у маршрута разрешено изменять атрибуты маршрута.

7.3.19.2. Сопутствующая конфигурация

Настройка reflector-а маршрутов BGP и клиента reflection

По умолчанию reflector маршрута BGP не настроен.

Запустите команду **neighbor** *neighbor-address* **route-reflector-client**, чтобы настроить локальное устройство в качестве reflector-а маршрута, а соседа — в качестве клиента reflection маршрута.

Настройка reflection клиент-клиент BGP

По умолчанию reflection маршрута клиент-клиент автоматически включается в reflector-е маршрутов BGP, и маршруты, полученные от клиента reflection, могут объявляться другим клиентам.

Запустите команду **bgp client-to-client reflection**, чтобы включить reflection клиент-клиент. Запустите форму **no** этой команды, чтобы отключить reflection клиент-клиент.

Настройка идентификатора кластера reflection BGP

По умолчанию идентификатор кластера reflection BGP напрямую использует идентификатор маршрута BGP. Когда в одном домене AS развернуто несколько кластеров reflection, для них необходимо настроить разные идентификаторы кластера reflection.

Запустите команду **bgp cluster-id** *cluster-id*, чтобы вручную настроить идентификатор кластера для reflector-а маршрута.

Разрешение reflector-у маршрута BGP изменять атрибуты маршрута

По умолчанию BGP не позволяет reflector-у маршрута изменять атрибуты маршрута.

Запустите команду **bgp route-reflector attribute-change**, чтобы позволить reflector-у маршрута изменять атрибуты маршрута.

7.3.20. Настройка устройства BGP для объявления маршрута с самым низким приоритетом при перезапуске

По умолчанию после перезапуска устройства и установления соседства peer BGP может объявлять маршруты своим соседям. Однако в некоторых случаях, например, имеется большое количество соседей или маршрутов, когда устройство запускается, но медленно записывает записи в оборудование. Соседи изучили маршруты и начали пересылку трафика, но локальное устройство не завершило запись записи в оборудование, что привело к сбою пересылки трафика. Поэтому BGP необходимо объявлять маршруты с наименьшим приоритетом после перезапуска устройства. Таким образом, предпочтение отдается другим доступным маршрутам, а не маршрутам, проходящим через локальное устройство.

7.3.20.1. Принцип работы

Настройте устройство BGP для объявления маршрутов с самым низким приоритетом после перезапуска. Таким образом, после перезапуска устройства BGP и установления соседства устройство BGP объявляет своим соседям маршруты с наименьшим

приоритетом. Измените значение **MED** маршрутов на **4 294 967 295** для соседей EBGP и измените значение **local-pref** на **0** для соседей IBGP. После того, как все записи ARP доставлены и все записи пересылки записаны в оборудование, запустите команду **clear bgp advertise lowest-priority on-startup**, чтобы восстановить приоритет объявленных маршрутов. Если пользователь не настроил восстановление приоритета объявленных маршрутов, устройство автоматически восстанавливает приоритет объявленных маршрутов через определенный период времени.

7.3.20.2. Сопутствующая конфигурация

Настройка устройства BGP для объявления маршрутов с наименьшим приоритетом при перезапуске

- **bgp advertise lowest-priority on-startup** [*recover-time*]

Настройте BGP, чтобы при перезагрузке устройства установить самый низкий приоритет объявленных маршрутов. По умолчанию приоритет не регулируется. *recover-time* указывает время (в секундах) таймера восстановления приоритета объявленных маршрутов. Диапазон значений — от 1 до 65 535, значение по умолчанию — 600.

7.3.21. Настройка таймеров BGP

Вы можете вручную настроить различные таймеры в BGP для удовлетворения требований keepalive соседей и управления маршрутами в различных сетевых средах.

7.3.21.1. Принцип работы

Таймер keepalive соседа BGP

BGP использует таймер Keepalive для поддержания допустимого соединения с peer-ом и таймер Holdtime для определения допустимости peer-а. По умолчанию значение таймера Keepalive составляет 60 секунд, а значение таймера Holdtime — 180 секунд. Когда между двумя спикерами BGP устанавливается соединение BGP, два спикера BGP согласовывают значение таймера Holdtime и выбирают меньшее значение. 1/3 согласованного значения таймера Holdtime и настроенного значения таймера Keepalive сравниваются, и меньшее значение используется в качестве значения таймера Keepalive.

Таймер повторного подключения соседа

Чтобы уменьшить влияние частого повторного подключения BGP к соседу на пропускную способность сети, после того, как спикер BGP обнаруживает сбой соединения соседа, спикер BGP пытается повторно подключиться к соседу после истечения таймера повторных попыток подключения. По умолчанию значение таймера повторных попыток подключения составляет 15 с.

Таймер объявления маршрута

Чтобы уменьшить влияние пакетов обновления маршрута на пропускную способность сети, после того, как спикер BGP обнаруживает изменение топологии сети, спикер BGP не объявляет обновление маршрута своим соседям немедленно. Вместо этого спикер BGP использует механизм регулярного обновления для объявления всей измененной информации о маршрутизации своим соседям.

7.3.21.2. Сопутствующая конфигурация

Настройка таймера keepalive соседа BGP

- **timers bgp** *keepalive holdtime*

Регулирует значения *keepalive* и *holdtime* BGP для всех peer-ов.

Значение *keepalive* находится в диапазоне от 0 до 65 535. Значение по умолчанию — 60 секунд.

Значение *holdtime* находится в диапазоне от 0 до 65 535. Значение по умолчанию — 180 секунд.

- **neighbor** { *address* | *peer-group-name* } **timers** *keepalive holdtime*

Настраивает значения *keepalive* и *holdtime*, используемые для подключения к указанному peer-у (группе) BGP.

Значение *keepalive* находится в диапазоне от 0 до 65 535. Значение по умолчанию — 60 секунд.

Значение *holdtime* находится в диапазоне от 0 до 65 535. Значение по умолчанию — 180 секунд.

Настройка таймера повторного подключения соседа

- **neighbor** { *address* | *peer-group-name* } **timers connect** *connect-retry*

Настраивает значение *connect-retry*, используемое для повторного подключения к указанному peer-у (группе) BGP.

Значение *connect-retry* варьируется от 1 до 65 535. Значение по умолчанию — 15 секунд.

Настройка таймера объявления маршрута

- **neighbor** { *address* | *peer-group-name* } **advertisemet-interval** *seconds*

Настраивает минимальный интервал для отправки обновлений маршрута указанному peer-у (группе) BGP. Значение интервала объявления находится в диапазоне от 0 до 600 секунд. Значение по умолчанию для peer-ов IBGP составляет 0 секунд, а значение по умолчанию для peer-ов EBGP — 30 секунд.

- **neighbor** { *address* | *peer-group-name* } **as-origination-interval** *seconds*

Настраивает минимальный интервал для отправки обновлений локального начального маршрута указанному peer-у (группе) BGP. Значение **as-origination-interval** находится в диапазоне от 1 до 65 535. Значение по умолчанию — 1 секунда.

7.3.22. Настройка механизмов обновления маршрутов BGP

7.3.22.1. Принцип работы

BGP предоставляет два механизма обновления маршрутов: обновление с регулярным сканированием и обновление, запускаемое по событию. Обновление регулярного сканирования указывает на то, что BGP использует внутренний таймер для регулярного запуска сканирования и обновления таблицы маршрутизации. Обновление, запускаемое по событию, означает, что BGP начинает сканирование и обновляет таблицу маршрутизации, когда команды конфигурации BGP изменяются из-за конфигурации пользователя или изменения следующего hop-а маршрута BGP.

ПРИМЕЧАНИЕ: эта функция настраивается на основе семейств адресов и может быть настроена в режимах семейства адресов IPv4, IPv6, IPv4 vrf и IPv6 VRF.

ПРИМЕЧАНИЕ: если вы установили механизм обновления маршрута BGP на обновление, запускаемое по событию (путем запуска команды **bgp scan-rib disable**), вы должны отключить синхронизацию (выполнив команду **no synchronization**) и включить функцию обновления запуска следующего hop-а BGP (выполнив команду **bgp nexthop trigger enable**).С другой стороны, если вы включите синхронизацию или отключите функцию

обновление, запускаемое по событию следующего hop-a BGP, таблица маршрутизации BGP должна обновляться в режиме с регулярным сканированием.

7.3.22.2. Сопутствующая конфигурация

Настройка механизмов обновления маршрутов

- **bgp scan-rib disable**

Устанавливает механизм обновления маршрута BGP на обновление, запускаемое по событию.По умолчанию используется обновление с регулярным сканированием.

- **bgp scan-time** *scan-time*

Настраивает интервал регулярного обновления BGP. Значение времени сканирования варьируется от 5 до 60 секунд. Значение по умолчанию — 60 секунд.

7.3.23. Настройка функции обновления, запускаемого по событию следующего hop-a BGP

Функция обновления, запускаемого по событию следующего hop-a BGP, представляет собой метод сокращения времени конвергенции BGP. Эта функция используется для оптимизации метода мониторинга следующего hop-a маршрута, чтобы гарантировать, что BGP может увеличить скорость сходимости маршрутов BGP, когда топология сети стабильна.

7.3.23.1. Принцип работы

Когда BGP подключается к соседу, BGP автоматически отслеживает следующий hop маршрута BGP, полученного от соседа. Когда следующий hop изменяется в основной таблице маршрутизации, BGP получает объявление об изменении следующего hop-a и обновляет таблицу маршрутизации BGP. Эта мера оптимизации повышает производительность конвергенции маршрутов BGP за счет сокращения времени обнаружения изменений следующего hop-a.

Если эта функция отключена, обновление следующего hop-a BGP будет обнаружено посредством регулярного сканирования, заданного таймером сканирования.

ПРИМЕЧАНИЕ: эта функция настраивается на основе семейств адресов и может быть настроена в режимах семейства адресов IPv4, IPv6 и IPv4 vrf.

ПРИМЕЧАНИЕ: **bgp nexthop trigger delay** и **bgp scan-time** управляют одним и тем же таймером. Когда сканирование BGP включено (оно включено по умолчанию и может быть отключено командой **bgp scan-rib disable**), если значение **bgp nexthop trigger delay** превышает 60 с, сканирование BGP не вступает в силу, поскольку таймер сканирования всегда срабатывает раньше задержки.

ПРИМЕЧАНИЕ: если сетевая среда нестабильна (с частыми изменениями следующего hop-a), особенно при наличии большого количества маршрутов, эта функция выполняет ненужные вычисления маршрута, что потребляет больше ресурсов ЦП. Поэтому рекомендуется отключить эту функцию в этой среде.

7.3.23.2. Сопутствующая конфигурация

Настройка функции обновления, запускаемого по событию следующего hop-а BGP

- **bgp nexthop trigger enable**

Включает функцию , запускаемую по событию запуска следующего hop-а BGP, которая включена по умолчанию.

- **bgp nexthop trigger delay** *delay-time*

Настраивает задержку обновления, запускаемого по событию следующего hop-а BGP. Значение времени задержки находится в диапазоне от 0 до 100 секунд. Значение по умолчанию — 5 секунд.

7.3.24. Настройка LOCAL AS BGP

Функция Local AS BGP используется для настройки локальной AS, отличной от AS BGP маршрутизатора, для конкретного peer-а. Это похоже на развертывание новой виртуальной AS между устройствами peer. При изменении локального маршрутизатора BGP AS вы можете установить соединение BGP, не меняя конфигурации BGP на устройстве peer. Эта функция в основном используется для миграции AS и объединения крупных сетей и гарантирует, что конфигурации устройств в других взаимосвязанных AS не будут затронуты.

7.3.24.1. Принцип работы

В BGP, когда локальное устройство подключается к peer-у, локальное устройство объявляет peer-у локальный номер AS с помощью сообщения Open. Peer проверяет, совпадает ли объявленный номер AS BGP с номером локальной AS. Если номера AS разные, peer откажет в соединении BGP. По умолчанию локальной AS в соединении BGP является AS BGP маршрута. Однако если для peer-а настроена локальная AS, настроенная локальная AS заменит AS BGP маршрута, когда между локальным устройством и peer-ом будет установлено соединение BGP.

ПРИМЕЧАНИЕ: за командой **neighbor** *peer-address* **local-as** *as-num* для настройки функции BGP Local AS могут следовать дополнительные опции. Подробности см. в Справочнике команд.

ПРИМЕЧАНИЕ: функция BGP Local AS применяется только к peer-ам EBGP, но не применяется к peer-ам IBGP и peer-ам объединения EBGP. Кроме того, функция BGP Local AS имеет следующие ограничения:

1. Настроенная локальная AS не может совпадать с удаленной AS peer-а.
2. Локальная AS не может быть настроена независимо для участника peer-группы.
3. Настроенная локальная AS не может совпадать с AS маршрута BGP.
4. Если устройство является участником объединения AS, номер локальной AS не может совпадать с номером объединения AS.

7.3.24.2. Сопутствующая конфигурация

Настройка LOCAL AS BGP

- **neighbor** { address | peer-group-name } **local-as** as-number

Настраивает локальную AS для peer-а. По умолчанию ни для одного peer-а не настроена локальная AS. Локальная AS peer-а является AS маршрута BGP.

7.3.25. Настройка защиты емкости BGP

Часто существует большое количество маршрутов BGP, что может привести к перегрузке устройства, особенно устройства с небольшим объемом памяти. Защита емкости BGP помогает избежать непредсказуемого рабочего состояния, вызванного потреблением мощности устройства.

7.3.25.1. Принцип работы

Ограничение количества маршрутов BGP

Ограничьте количество маршрутов BGP, задав максимальное количество маршрутов в семействе адресов BGP и максимальное количество маршрутов, которые могут быть изучены соседом BGP.

Вход в состояние OVERFLOW в случае нехватки памяти (состояние переполнения)

Если памяти недостаточно, BGP может перейти в состояние OVERFLOW. В состоянии OVERFLOW BGP генерирует маршрут по умолчанию, указывающий на NULL-интерфейс (пустой). Если вновь изученный маршрут не является уточненным маршрутом, отличным от маршрута по умолчанию в текущей таблице маршрутизации, этот маршрут отбрасывается. Другими словами, общие вновь изученные маршруты отбрасываются, чтобы обеспечить стабильность системной памяти. Целью отказа от всех маршрутов является избежание петель маршрутов во всей сети. Поэтому для BGP безопасно перейти в состояние OVERFLOW. По умолчанию BGP разрешено переходить в состояние OVERFLOW.

ПРИМЕЧАНИЕ: по умолчанию BGP переходит в состояние OVERFLOW в случае нехватки памяти. Если вы не хотите, чтобы BGP перешел в состояние OVERFLOW, вы можете запустить команду **no overflow-memory-lack**, чтобы отключить эту функцию.

ПРИМЕЧАНИЕ: в состоянии OVERFLOW BGP поддерживает только команду **clear bgp** { *addressfamily* | **all** } * в настоящее время. Вы также можете выйти из состояния OVERFLOW, отключив и снова включив BGP. Когда памяти снова станет достаточно, BGP также может автоматически выйти из состояния OVERFLOW.

7.3.25.2. Сопутствующая конфигурация

Ограничение количества маршрутов BGP

- **neighbor** { *neighbor-address* | *peer-group-name* } **maximum-prefix** *maximum* [**threshold**] [**warning-only**]

Ограничивает максимальное количество маршрутов, которые можно получить от соседа BGP, которое по умолчанию не ограничено.

- **maximum-prefix** *maximum*

Ограничивает максимальное количество маршрутов в семействе адресов BGP, которое по умолчанию не ограничено.

- Запустите команду **bgp maximum-prefix maximum** [**vrf vrf-name**], чтобы ограничить максимальное количество маршрутов в глобальном BGP или указанном VRF. Когда объявление маршрута в семействе адресов приводит к тому, что текущее количество маршрутов BGP превышает максимальное количество, отображается сообщение о переполнении маршрута в глобальном или указанном VRF, а глобальный или указанный VRF BGP переводится в состояние OVERFLOW. По умолчанию эта функция отключена.

Настройка переполнения BGP

- **overflow memory-lack**

Включите BGP для перехода в состояние OVERFLOW в случае нехватки памяти, которое включено по умолчанию.

7.3.26. Настройка BGP GR

Graceful Restart (GR) предназначен для реализации бесперебойной пересылки данных во время перезапуска BGP. Во время переключения плат управления в активный/резервный режим функция GR поддерживает стабильную топологию сети, поддерживает таблицу пересылки и гарантирует, что ключевые сервисы не будут прерываться.

7.3.26.1. Принцип работы

Соответствуйте RFC4724: механизм плавного перезапуска для BGP. [BGP GR] используется в следующем описании для обозначения RFC.

BGP GR не является независимым процессом, а выполняется совместно Restarter-ом и Helper-ом.

- Restarter выполняет перезапуск и поддерживает работоспособность forwarding plane маршрута, когда control plane маршрута неисправна.
- Helper является соседом BGP Restarter-а и помогает Restarter-у завершить GR.

К сообщению OPEN BGP добавляется возможность, указывающая GR, которая называется Graceful Restart Capability («Возможность плавного перезапуска»). Эта возможность используется BGP, чтобы сообщить соседу, что он поддерживает возможность плавного перезапуска. Во время инициализации соединения BGP два соседа согласовывают возможности GR.

ПРИМЕЧАНИЕ: флаг завершения обновления маршрута (End-of-RIB, сокращенно EOR) добавляется к пакету обновления BGP, который указывает, что обновление информации о маршрутизации для соседа завершено.

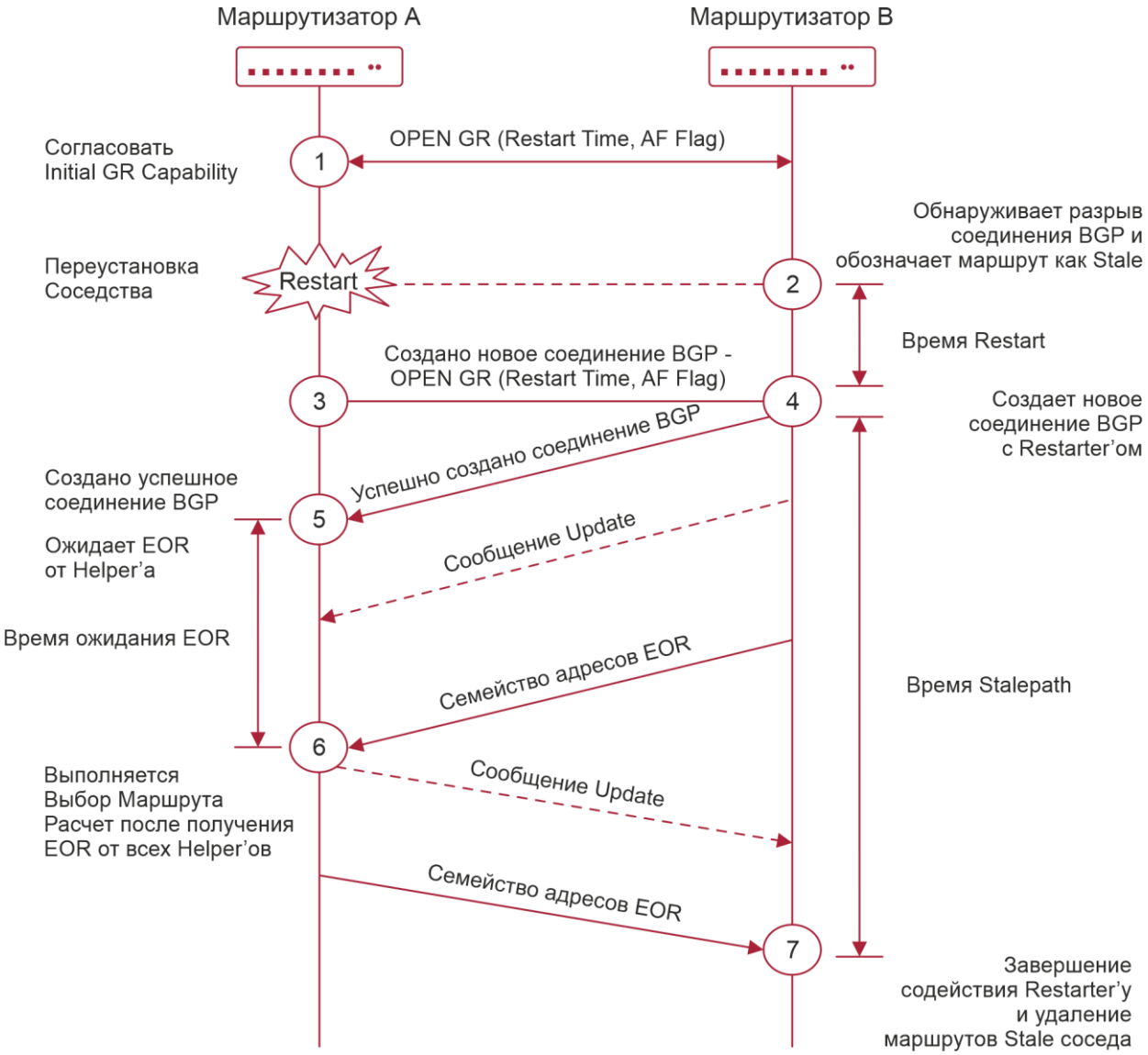


Рисунок 7-3. Процесс взаимодействия с BGP GR

1. ① Когда BGP вначале устанавливает соседство, BGP использует поле возможности GR в сообщении OPEN для согласования возможностей GR двух соседей.
2. ② В какой-то момент Restarter начинает перезагрузку, и сеанс BGP отключается. Helper обнаруживает отключение, сохраняет маршрут перезапуска действительным, но добавляет к маршруту флаг Stale («Устаревший (устаревший, но не обновленный)»).
3. ③ и ④ Restarter завершает перезапуск и снова подключается к Helper-у.
4. ⑤ Restarter ожидает сообщения об обновлении маршрута и флага EOR от Helper”а.
5. ⑥ После получения флага EOR от всех соседей Restarter выполняет расчет маршрута, обновляет записи маршрутизации, а затем отправляет обновленные маршруты Helper-у.
6. ⑦ После получения обновленных маршрутов Helper снимает с маршрутов флаг Stale. После получения флага EOR от Restarter-а Helper удаляет маршруты с флагом Stale

(эти маршруты не обновляются), выполняет расчет маршрута и обновляет записи маршрутизации.Весь процесс GR завершен.

BGP GR определяет несколько расширенных и важных таймеров:

- **Таймер Restart**: GR Restarter объявляет значение времени GR Helper, которое указывает максимальное время ожидания, которое GR Restarter надеется выдержит Helper, прежде чем между ними будет установлено новое соединение. Вы можете запустить команду **bgp graceful-restart restart-time**, чтобы изменить значение времени.
- **Таймер Wait-For-EOR**: указывает максимальное время, в течение которого Restarter GR ожидает флага EOR от всех Helper-ов GR. После получения флага EOR от всех Helper-ов GR или после истечения таймера ожидания EOR Restarter GR вычисляет предпочтительный маршрут и обновляет записи маршрутизации. Вы можете запустить команду **bgp update-delay**, чтобы изменить значение времени.
- **Таймер StalePath**: указывает максимальное время, в течение которого GR-Helper ожидает флага EOR от GR Restarter-а после установления нового соединения между ними. В течение этого периода Helper сохраняет действительным исходный маршрут Restarter-а. После получения флага EOR или по истечении таймера StalePath Helper очищает записи маршрутизации, все еще имеющие тег «Stale». Вы можете запустить команду **bgp graceful-restart stalepath-time**, чтобы изменить значение времени.

7.3.26.2. Сопутствующая конфигурация

Настройка BGP GR

- **bgp graceful-restart**

Включает возможность перезапуска, которая включена по умолчанию.

- **bgp graceful-restart restart-time** *time*

Устанавливает таймер Restart. Значение по умолчанию — 120 секунд.

- **bgp update-delay** *delay*

Устанавливает таймер Wait-For-EOR. Значение по умолчанию — 120 секунд.

- **bgp graceful-restart stalepath-time** *time*

Устанавливает таймер StalePath. Значение по умолчанию — 360 секунд.

- **bgp graceful-restart disable**

Отключает возможность GR семейства адресов. Возможность GR семейства адресов включена по умолчанию. После включения глобального BGP GR возможность GR автоматически включается для всех семейств адресов.

ПРИМЕЧАНИЕ: при реализации BGP GR все peer-ы BGP должны включить возможность BGP GR. Если некоторые peer-ы не поддерживают или не включают GR, BGP GR может быть не реализован. Сбой GR может привести к образованию black hole на коротком маршруте или петли маршрута, что может повлиять на сеть. Поэтому рекомендуется убедиться, что на всех соседях включена возможность BGP GR. Вы можете запустить команду **show ip bgp neighbors**, чтобы отобразить возможности, успешно согласованные между peer- ами BGP, и убедиться, что согласование возможностей GR прошло успешно. В режиме настройки маршрута BGP выполните команду **bgp graceful-restart**, чтобы включить возможность BGP GR.

ПРИМЕЧАНИЕ: команда **bgp graceful-restart** не будет немедленно применена к успешно установленному соединению BGP. То есть, когда соединение BGP находится в состоянии Established («Установлено»), peer-ы BGP не будут немедленно повторно согласовывать возможности GR. Чтобы позволить peer-ам BGP соединения BGP немедленно согласовать возможности GR, вам необходимо принудительно перезапустить peer-ы BGP для повторного согласования возможностей GR, выполнив команду **clear ip bgp** 192.168.195.64 (например). Включение или отключение GR вступает в силу немедленно, необходимо перезапустить соседство для согласования возможностей, что может привести к flapping-у и повлиять на нормальное использование пользователями. Таким образом, вы можете явно контролировать, следует ли перезапускать соседство.

ПРИМЕЧАНИЕ: поддержка BGP GR не означает, что устройство можно использовать в качестве Restarter-а для реализации BGP GR. Реализовать ли BGP GR также зависит от аппаратных возможностей устройства. Устройства QTECH должны поддерживать горячее резервное копирование dual-engine при использовании в качестве Restarter-а GR.

ПРИМЕЧАНИЕ: период перезапуска, настроенный командой **bgp graceful-restar restart-time**, не должен превышать время удержания peer-ов BGP; в противном случае время удержания будет использоваться в качестве времени перезапуска, которое будет объявлено peer-ам BGP во время согласования возможностей GR.

ПРИМЕЧАНИЕ: команда **bgp graceful-restar disable** используется для отключения возможности GR в семействе адресов в режиме конфигурации семейства адресов, которые не настроены по умолчанию.

7.3.27. Настройка 4-байтовых номеров AS BGP

Традиционный номер AS состоит из 2 байтов в диапазоне от 1 до 65 535. Вновь определенный номер AS состоит из 4 байтов в диапазоне от 1 до 4 294 967 295. Вновь определенные номера AS используются, чтобы справиться с исчерпанием ресурсов номеров AS.

7.3.27.1. Принцип работы

4-байтовые номера AS поддерживают два режима выражения: десятичный режим и точечный режим. Десятичный режим аналогичен исходному режиму выражения, то есть выражает 4 байта номера AS в виде десятичных цифр. Режим точки выражается как ([старшие 2 байта.]нижние 2 байта). Если старшие 2 байта равны 0, они не будут отображаться.

Например, номер AS равен 65 534 в десятичном режиме и 65 534 в точечном режиме (0 в начале не отображается).

Например, номер AS равен 65 536 в десятичном режиме и 1,0 в точечном режиме.

Например, номер AS равен 65 538 в десятичном режиме и 1,2 в точечном режиме.

ПРИМЕЧАНИЕ: связанные протоколы: RFC 4893 и RFC 5396.

Настройка режима отображения 4-байтового номера AS

По умолчанию 4-байтовый номер AS отображается в десятичном формате. Вы можете вручную установить точечный режим отображения. После установки регулярное выражение будет использовать точечный режим для соответствия 4-байтовым номерам AS.

Совместимость с устройствами, поддерживающими только 2-байтовые номера AS.

С введением 4-байтовых номеров AS соединения BGP могут быть установлены между старыми peer-ами BPG, поддерживающими только 2-байтовые номера AS, и новыми спикерами BGP, поддерживающими 4-байтовые номера AS. Если AS, в которой находится новый спикер BGP, имеет 4-байтовый номер AS, то когда старый спикер BGP создает соседство с новым спикером BGP, старый спикер BGP использует зарезервированный номер AS 23 456 для замены 4-байтового номера AS нового спикера BGP. В пакетах OPEN, отправляемых новым спикером BGP старому спикеру BGP, 4-байтовый номер AS в поле **My Autonomous System** будет заменен на 23 456. Кроме того, в пакетах UPDATE, отправляемых старому спикеру BGP, 4-байтовый номер AS в атрибутах AS-PATH и AGGREGATOR также будет заменен на 23 456. Кроме того, новые дополнительные атрибуты передачи AS4-PATH и AS4-AGGREGATOR будут использоваться для записи реального 4-байтового номера AS, чтобы реальные атрибуты AS-PATH и AGGREGATOR можно было восстановить, когда маршрут достигнет следующего нового спикера BGP.

В других случаях для создания соседства используется реальный номер AS удаленного конца.

7.3.27.2. Сопутствующая конфигурация

Настройка режима отображения 4-байтового номера AS

- **bgp asnotation dot**

Отображает 4-байтовый номер AS в точечном режиме. По умолчанию используется десятичный режим.

7.3.28. Настройка регулярного выражения

Регулярное выражение — это формула, которая сопоставляет строки на основе шаблона.

Формула используется для оценки текстовых данных и возвращает значение True или False, чтобы указать, может ли выражение правильно описать данные.

7.3.28.1. Принцип работы

Регулярные выражения используются в атрибутах пути BGP. В следующей таблице описано использование специальных символов в регулярном выражении.

Характеристика	Символ	Особое значение
Период		Соответствует любому отдельному символу
Звездочка	*	Соответствует нулю или любой последовательности в строке
Знак плюс	+	Соответствует одной или любой последовательности в строке
Вопросительный знак	?	Соответствует нулю или одному символу в строке

Характеристика	Символ	Особое значение
Карет	^	Соответствует началу строки
Знак доллара	$	Соответствует концу строки
Линия подчеркивания	_	Соответствует началу, концу и пробелу запятых, скобок и строк
Квадратные скобки	[ ]	Соответствует одному символу в диапазоне

7.3.28.2. Сопутствующая конфигурация

Использование регулярного выражения в команде show

- **show ip bgp regexp** *regexp*

Отображает информацию о маршрутизации BGP в указанном регулярном выражении, соответствующем атрибуту AS-PATH.

- **show ip bgp quote-regexp** *regexp*

Отображает информацию о маршрутизации BGP в регулярном выражении в указанных двойных кавычках, соответствующих атрибуту AS-PATH.

7.3.29. Настройка сохранения сеанса BGP

По умолчанию, когда пакет UPDATE получен от соседа, сеанс BGP будет отключен, если обнаружена ошибка в атрибуте многопротокольной маршрутизации. Это приведет к изменению маршрутов во всех адресных семействах этого соседа. То есть ошибка маршрутизации в семействе адресов повлияет на стабильность маршрута в других семействах адресов.

7.3.29.1. Принцип работы

После включения функции сохранения сеанса BGP, если в атрибуте маршрутизации семейства адресов возникает ошибка, удаляется только информация о маршрутизации в этом семействе адресов, связанная с соседом. Кроме того, сеанс BGP и другие семейства адресов не затрагиваются, что повышает стабильность BGP.

recovery-time используется для настройки времени ожидания автоматического восстановления маршрута, для чего требуется, чтобы сосед поддерживал возможность обновления маршрута. По истечении времени **recovery-time** BGP отправляет сообщение обновления маршрута семейства адресов соседу и повторно объявляет всю информацию о маршрутизации в семействе адресов этому соседу.

ПРИМЕЧАНИЕ: в состоянии сохранения сеанса вы можете вручную сбросить соседа, чтобы выйти из состояния сохранения сеанса.

7.3.29.2. Сопутствующая конфигурация

Настройка сохранения сеанса BGP

- **bgp mp-error-handle session-retain** [**recovery-time** *time*]

Включает функцию сохранения сеанса BGP, которая по умолчанию отключена.

recovery-time *time* настраивает время ожидания автоматического восстановления маршрута в диапазоне от 10 до 65 535 секунд. Значение по умолчанию — 120.

7.3.30. Настройка отложенного объявления BGP при перезапуске системы

По умолчанию после установления соседства после перезапуска системы peer BGP может объявлять информацию о маршруте своим соседям. В большинстве случаев это нормально. Однако в некоторых случаях, например, во время запуска имеется много соседей или маршрутов, но запись записей в оборудование происходит медленно. В этом случае соседи изучили маршруты и начали пересылку трафика, но оборудование не завершило запись записей на локальном конце, что приводит к сбою пересылки трафика.

7.3.30.1. Принцип работы

Отложенное объявления BGP при перезапуске системы гарантирует, что маршруты не будут объявлены соседям сразу после установления соседства при перезапуске системы, а также что маршруты будут объявлены через определенный период. Эта функция не влияет на другие действия, такие как получение маршрута соседями. Если задержка не влияет на часть маршрутов, настройте политику списка префиксов для соответствия этой части маршрутов, чтобы объявление маршрутов было более гибким.

delay-time используется для настройки времени ожидания перед объявлением маршрутов соседям. **Startup-time** используется для настройки времени запуска. В течение времени запуска BGP отправляет информацию о маршрутизации соседям с интервалом, заданным временем **delay-time**.

ПРИМЕЧАНИЕ: по истечении времени **startup-time** поведение объявления маршрута по умолчанию восстанавливается.

7.3.30.2. Сопутствующая конфигурация

Настройка отложенного объявления BGP при перезагрузке системы

bgp initial-advertise-delay *delay-time* **[** *startup-time* **] [wait-for-controller]**

Включает отложенное объявление BGP при перезапуске системы, которое по умолчанию отключено.

delay-time настраивает время задержки для объявления маршрутов после установления соседства BGP при перезапуске системы в диапазоне от 1 до 600 секунд. Значение по умолчанию — 1 с.

startup-time настраивает диапазон времени для перезапуска системы в диапазоне от 5 до 58 400 секунд. В этом диапазоне используется механизм отложенного объявления маршрута. Значение по умолчанию — 600 с.

7.3.31. Настройка отложенного объявления BGP для первых маршрутов

По умолчанию после установления соседства peer BGP может объявлять информацию о маршруте своим соседям. Однако соседи с недавно созданным соседством будут отправлять информацию о маршруте через определенный период времени.

7.3.31.1. Принцип работы

После запуска BGP peer-ы BGP договариваются об установлении соседства перед отправкой информации о маршруте (пакеты обновления). Оптимальный маршрут

рассчитывается на локальном конце и отправляется на конец peer-а. По умолчанию маршруты объявляются напрямую. После того как сосед получает лучший маршрут, он обновляет информацию о маршруте peer-у. В результате происходит дополнительное объявление маршрута. **update-delay** можно настроить для сокращения времени обновления информации о маршруте.

Кроме того, после того, как на локальном конце настроена **update-delay**, конкретный сосед отправляет информацию о маршруте на локальный конец, локальный конец выбирает оптимальный маршрут,а потом отправляет информацию о маршруте немедленно другим соседям по умолчанию. В этом случае также возникает дополнительное объявление. Таким образом, значение **update-delay** включает в себя две части: задержку объявления маршрута от локального конца до конкретного соседа и задержку объявления маршрута от локального конца до других соседей после того, как конкретный сосед объявляет информацию о маршруте локальному концу.

ПРИМЕЧАНИЕ: если отложенное объявление BGP при перезапуске системы и отложенное объявление BGP для первых маршрутов включены одновременно, отложенное объявление BGP при перезапуске системы имеет приоритет над отложенным объявлением BGP для первых маршрутов.

ПРИМЕЧАНИЕ: на BGP GR не влияет ни отложенное объявление BGP при перезапуске системы, ни отложенное объявление BGP для первых маршрутов, то есть время задержки не влияет на объявление маршрута BGP GR.

7.3.31.2. Сопутствующая конфигурация

Создание соседа BGP

По умолчанию на спикере BGP соседи не указаны. Вам необходимо вручную настроить соседа BGP.

Запустите команду **neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number* для ручного создания соседа BGP и указания номера AS соседа.

Настройка отложенного объявления BGP для первых маршрутов

По умолчанию отложенное объявление BGP для первых маршрутов отключено для соседей.

Запустите команду **neighbor** { *neighbor-address* | *peer-group-name* } **update-delay** *delay-time*, чтобы включить отложенное объявление BGP для первых маршрутов.

7.3.32. Настройка BGP NSR

Non-Stop-Routing (NSR) используется для обеспечения бесперебойности маршрутов во время перезапуска протокола при переключении между активной и резервной платами управления. Во время переключения между активной и резервной платами управления функция NSR обеспечивает стабильную топологию сети, поддерживает статус соседей и таблицы пересылки, а также гарантирует бесперебойность ключевых сервисов.

7.3.32.1. Принцип работы

В отличие от BGP GR, BGP NSR — это функция, реализуемая индивидуально спикером BGP и не зависящая от соседей.

- Во время переключения между активной и резервной платами управления соединения между соседями BGP не прерываются.
- Соседи не воспринимают поведение перезапуска на локальном конце. Технология GR используется для восстановления перезапуска.

Соседям с включенной функцией BGP NSR не нужно согласовывать возможности GR. Кроме того, содействия соседей не требуется и проблем взаимодействия не существует, поскольку NSR — это технология обеспечения надежности, не воспринимаемая соседями.

7.3.32.2. Сопутствующая конфигурация

Создание соседа BGP

По умолчанию на спикере BGP не указаны соседи. Вам необходимо вручную настроить соседа BGP.

Запустите команду **neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number* для ручного создания соседа BGP и указания номера AS соседа.

Включение функции NSR для соседей BGP

По умолчанию функция NSR отключена для соседей BGP.

Запустите команду **neighbor** { *neighbor-address* | *peer-group-name* } **ha-mode nsr** для включения функции NSR для соседей BGP.

Включение функции NSR для соседей BGP глобально

По умолчанию функция NSR отключена.

Запустите команду **bgp nsr**, чтобы глобально включить функцию NSR для соседей BGP.

ПРИМЕЧАНИЕ: когда функция BGP NSR включена для соседа, соединение с соседом будет сброшено, tcp nss (непрерывный сервис) соседа будет включен, а информация о соответствующем соседе и маршруте будет сохранена на резервной плате управления. В этом случае, если функция NSR включена после установления соседства, соседство будет переустановлено, что приведет к отключению соседа. Рекомендуется включить функцию NSR до установления соседства.

ПРИМЕЧАНИЕ: функция NSR не действует на соседа, которому не удалось установить соединение BGP, то есть, если соединение BGP не находится в состоянии **Established** («Установлено»), сосед не будет выполнять операции резервного копирования, связанные с NSR. Только если соединение BGP находится в состоянии **Established**, сосед выполняет операции резервного копирования, связанные с NSR.

ПРИМЕЧАНИЕ: не все устройства, поддерживающие функцию BGP NSR, могут выполнять переключение между активной и резервной платами управления. Чтобы выполнить переключение между активной и резервной платами управления, аппаратное обеспечение устройства должно соответствовать определенным требованиям. Устройства NSR в сетях QTECH должны поддерживать функцию горячего резервирования dual engine.

ПРИМЕЧАНИЕ: в настоящее время только семейство unicast-адресов IPv4/IPv6 и семейство адресов EVPN поддерживают функцию NSR. Если сосед активирует другие семейства адресов, кроме семейства unicast-адресов, переключения NSR не могут быть выполнены.

ПРИМЕЧАНИЕ: если резервное копирование BGP или TCP не завершено, переключение BGP NSR может не состояться. При возникновении этого состояния BGP GR повторно подключит маршрут. Рекомендуется одновременно включить BGP NSR и BGP GR.

7.3.33. Настройка маршрутов BGP как рекурсивные только для маршрутов хоста

Маршруты BGP по умолчанию используют оптимальное соответствие для рекурсии маршрутов. Таким образом, маршруты BGP могут быть рекурсивными к маршрутам по умолчанию или неправильным маршрутам сегмента сети, что приводит к ошибке выхода

или следующего hop-a. После включения функции рекурсивности маршрутов BGP только к маршрутам хоста маршруты BGP становятся рекурсивными только к маршрутам хостов 32-битного IPv4 или маршрутам хоста 128-битного IPv6. Эта функция применяется к маршрутам, изученным соседями IBGP или multi-hop соседями EBGP, установленными с использованием интерфейса Loopback.

7.3.33.1. Принцип работы

После включения функции рекурсивности маршрутов BGP только к маршрутам хоста функция проверяет достоверность адресов следующего hop-a маршрутов IBGP или multi-hop маршрутов EBGP посредством точного соответствия и выполняет рекурсию маршрута на IBGP или multi-hop маршруты EBGP посредством точного соответствия после их записи в FIB. Например, адрес следующего hop-a маршрута IBGP 192.168.2.0/24 — 1.1.1.1. Адрес следующего hop-a маршрута IBGP 192.168.2.0/24 действителен только тогда, когда маршрут 1.1.1.1/32 существует, а выход маршрута, записанного в FIB, является выходом маршрута 1.1.1.1/32.

7.3.33.2. Сопутствующая конфигурация

Создание соседа BGP

По умолчанию для спикера BGP сосед не указан. Вам необходимо вручную настроить соседа BGP.

Запустите команду **neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number* для ручного создания соседа BGP и указания номера AS для соседа.

Включение маршрутов BGP быть рекурсивными только к маршрутам хоста

По умолчанию рекурсия выполняется на маршрутах BGP посредством точного соответствия.

Запустите команду **bgp recursion host**, чтобы маршруты BGP были рекурсивными только для маршрутов хоста.

7.3.34. Настройка обнаружения исходящей петли для соседа BGP

По умолчанию BGP выполняет обнаружение петель на маршрутах BGP при получении маршрутов BGP от соседа. Если атрибут **AS Path**, передаваемый в маршруте BGP, содержит локальный номер AS, BGP отфильтровывает маршрут BGP. Функция обнаружения исходящей петли соседа заключается в том, чтобы заранее обнаружить петли на маршрутах, когда маршруты передаются соседу, чтобы отфильтровать петли маршрутов.

7.3.34.1. Принцип работы

При отправке маршрута соседу EBGP устройство определяет, содержит ли атрибут **AS Path**, передаваемый в маршруте BGP, номер AS соседа. Если да, маршрут закольцован, и устройство не отправляет маршрут соседу EBGP.

7.3.34.2. Сопутствующая конфигурация

Создание соседа BGP

По умолчанию для спикера BGP сосед не указан. Вам необходимо вручную настроить соседа BGP.

Запустите команду **neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number* для ручного создания соседа BGP и указания номера AS для соседа.

Включение обнаружения исходящей петли для соседа

По умолчанию обнаружение исходящей петли отключено для соседа.

Запустите команду **neighbor** { *neighbor-address* | *peer-group-name* } **as-loop-check out**, чтобы включить обнаружение исходящей петли для соседа BGP.

7.3.35. Плавное закрытие соединения BGP

Требования RFC 6198 к плавному завершению сеансов BGP определяют требование корректного закрытия соединений BGP и требуют, чтобы сосед BGP отключал соединения при условии, что сервисный трафик не прерывается или прерывается на очень короткий период времени.

7.3.35.1. Принцип работы

Эта функция использует режим «Make-Before-Break» для отключения соединений BGP, чтобы гарантировать, что сервисный трафик не прерывается или прерывается на очень короткий период времени в процессе от настройки функции до фактического отключения соединения BGP. Шаги следующие:

- Эта функция позволяет устройству объявлять соседу маршрут с наименьшим приоритетом (значение **local-preference** равно **0** или значение **med** равно 4 294 967 295) и переносить в маршрут атрибут **gshut community**, чтобы сосед обновлял маршруты и переключал трафик на резервный канал или другие эквивалентные каналы заранее.
- Устройство закрывает соединение BGP с соседом через некоторое время.

Период задержки отключения соединения BGP можно указать вручную или рассчитать автоматически. Автоматически рассчитанное время задержки составляет 1 секунду для 1000 маршрутов.

ПРИМЕЧАНИЕ: если атрибут **local-preference** или **med** маршрута с наименьшим приоритетом не может позволить соседу переключиться заранее на резервные каналы или другие эквивалентные каналы, настройте политику входящего трафика на соседе, чтобы изменить приоритет маршрутов, несущих **gshut community** или указанный атрибут **community**, или фильтровать такие маршруты.

7.3.35.2. Сопутствующая конфигурация

Плавное закрытие всех соединений экземпляра BGP

По умолчанию все соединения экземпляров BGP не отключаются.

Запустите команду **bgp shutdown graceful** [**community** *value*] [**delay** *time*] для отключения всех соединений экземпляра BGP.

Плавное закрытие соединений соседа BGP

По умолчанию соединения соседей BGP не отключаются.

Запустите команду **neighbor** { *neighbor-address* | *peer-group-name* } **shutdown graceful** [**community** *value*] [**delay** *time*] для отключения соединений соседа BGP.

7.3.36. Настройка расширенного импорта маршрутов VPN

7.3.36.1. Принцип работы

Во время импорта маршрутов между VRF, импорта удаленных маршрутов L3VPN в VRF или импорта маршрутов EVPN в таблицу IP-маршрутов по умолчанию импортируются только маршруты с предпочтительными следующими hop-ами.

Расширенная функция импорта маршрутов VPN является расширением взаимного импорта предыдущих маршрутов. Это позволяет импортировать все маршруты со следующими hop-ами или эквивалентными следующими hop-ами.

7.3.36.2. Сопутствующая конфигурация

Настройка политики импорта маршрутов

По умолчанию импортируются только маршруты с предпочтительными следующими hop-ами.

Запустите команду **import path selection** { **all** | **bestpath** | **multipath** } для импорта всех маршрутов со следующими hop-ами, маршрутов с предпочтительными следующими hop-ами или маршрутов с эквивалентными следующими hop-ами.

7.3.37. Группа обновления маршрутов BGP

Функция группы обновления маршрутов BGP используется для повышения производительности объявления маршрутов соседям.

7.3.37.1. Принцип работы

Функция группы обновления маршрутов BGP автоматически относит соседей с одинаковой политикой исходящего трафика к одной и той же группе обновления. Когда маршруты отправляются соседям, пакет обновления инкапсулируется на основе группы обновлений и отправляется всем соседям в группе обновлений. В этом случае пакет обновления инкапсулируется один раз и отправляется несколько раз, что повышает производительность объявления маршрута соседям.

7.3.38. Настройка BGP EVPN

Как технологию VPN Level-2 виртуальная приватная сеть Ethernet (EVPN) использует MB-BGP на control plane для распределения информации о маршрутизации уровней 2 и 3 и использует виртуальную расширяемую локальную сеть (VXLAN) на data plane для инкапсуляции сервисного трафика.

7.3.38.1. Принцип работы

EVPN — это технология VPN Level-2, расширенная на основе MP-BPG. MP-BPG расширяет семейство адресов EVPN для передачи необходимой маршрутной информации уровней 2 и 3, а также поддерживает несколько типов data plane. В настоящее время в качестве data plane EVPN может служить только VXLAN.

MP-BGP добавляет не только семейство адресов EVPN, но и информацию о доступности сетевого уровня EVPN, которая включает в себя следующее:

1. Маршрут автоматического обнаружения Ethernet: автоматически обнаруживает информацию о сегменте Ethernet (ES) в сети с несколькими домами.
2. Маршрут объявления MAC/IP: объявляет MAC-адрес и информацию ARP хоста.

3. Маршрут с инклюзивным многоадресным тегом Ethernet (IMET): автоматически обнаруживает конечные точки туннеля VXLAN (VTEP) и создают туннели VXLAN.
4. Маршрут сегмента Ethernet: объявляет информацию ES и информацию о подключенных VTEP.
5. Маршрут с префиксом IP: объявляет информацию о маршрутизации сегментов IP-сети.

В настоящее время маршрут автоматического обнаружения Ethernet и маршрут сегмента Ethernet не поддерживаются.

Предыдущая информация о маршрутизации EVPN включает в себя RD (для маршрутов EVPN различных VNI) и цель маршрута (для импорта маршрутов EVPN между различными устройствами).

7.3.38.2. Сопутствующая конфигурация

Настройка EVPN

По умолчанию режим EVPN не активирован.

Запустите команду **evpn**, чтобы войти в режим EVPN.

Создание экземпляра EVI

По умолчанию экземпляр EVI не настроен.

Запустите команду **vni** *vni-id*, чтобы создать экземпляр EVI и войти в режим настройки экземпляра EVI.

Запустите команду **vni range** *vni-id-list*, чтобы создавать экземпляры EVI в пакетном режиме и войти в режим пакетной настройки экземпляра EVI.

Настройка RD

По умолчанию в режиме EVPN-VNI RD не настроен.

Запустите команду **rd** { **auto** | *rd_value* } для добавления RD.

Настройка цели маршрута

По умолчанию в режиме EVPN-VNI цель маршрута не настроена.

Запустите команду **route-target** { **import** | **export** | **both** } для настройки цели маршрута.

Настройка карты маршрутов для экземпляров EVI

По умолчанию для экземпляров EVI карта маршрутов не настроена.

Запустите команду **export map** *routemap-name*, чтобы настроить карту маршрутов для экспорта расширенного атрибута community маршрутов EVPN с локального устройства на удаленное устройство.

Запустите команду **import map** *routemap-name*, чтобы настроить карту маршрутов для импорта удаленных маршрутов EVPN в локальный экземпляр VNI.

Настройка семейства адресов EVPN

По умолчанию семейство адресов EVPN не активировано.

Запустите команду **address-family l2vpn evpn**, чтобы активировать семейство адресов EVPN.

Настройка параметров мобильности MAC

По умолчанию, если в течение 180 секунд обнаружено пять перемещений MAC-адресов, считается, что произошел конфликт MAC-адресов.

Запустите команду **bgp mac-mobility** *timer count*, чтобы настроить параметры обнаружения мобильности MAC.

7.3.39. Другие связанные конфигурации

ПРИМЕЧАНИЕ: информацию о настройке и применении BGP MCE см. в разделе «Руководство по настройке VRF».

7.4. Конфигурация

Конфигурация	Описание и команда	
Настройка peer-a BGP (группы)	(Обязательно) Используется для создания соседа BGP	
	router bgp	Включает BGP
	neighbor { *peer-address* | *peer-group-name* } **remote-as** *as-number*	Создает соседа BGP
Настройка аутентификации MD5	(Опционально) Используется для выполнения зашифрованной аутентификации для соседа BGP	
	neighbor { *peer-address* | *peer-group-name* } **password** [**0** | **7**] *string*	Настраивает пароль для шифрования
Настройка reflector-а маршрута	(Опционально) Используется для уменьшения количества соседских соединений BGP	
	neighbor { *peer-address* | *peer-group-name* } **route-reflector-client**	Указывает peer (группу) в качестве клиента-reflector-а
Настройка объединения AS	(Опционально) Используется для уменьшения количества соседских соединений BGP	
	bgp confederation identifier *as-number*	Настраивает идентификатор объединения BGP
	bgp confederation peers *as-number* [… *as-number*]	Настраивает соседа объединения BGP

Конфигурация	Описание и команда	
Настройка multipath-балансировки нагрузки BGP	(Опционально) Используется для реализации multipath-балансировки нагрузки	
	maximum-paths ibgp *number*	Настраивает балансировку нагрузки IBGP
	maximum-paths ebgp *number*	Настраивает балансировку нагрузки EBGP
	bgp bestpath as-path multipath-relax	Включает режим свободного сравнения BGP AS-PATH
Настройка EBGP FRR	(Опционально) Используется для увеличения скорости конвергенции при возникновении сбоя в сети	
	bgp fast-reroute	Настраивает BGP FRR
	neighbor { *neighbor-address* | *peer-group-name* } **fall-over bfd**	Настраивает сеанс BFD с соседом BGP
Настройка быстрого изымания указанных маршрутов BGP	(Опционально) Используется для быстрого изымания указанных маршрутов BGP	
	bgp fast-withdraw { **access-list** { *access-list-number* | *access-list-name* } | **prefix-list** *prefix-list-name* | **route-map** *map-tag* }	Настраивает быстрое изымание указанных маршрутов BGP
Настройка локальных AS	(Опционально) Используется для временного развертывания во время миграции сети	
	neighbor { *peer-address* | *peer-group-name* } **local-as** *as-number* [**no-prepend** [**replace-as** [**dual-as**]]]	Настраивает локальную AS для соседа BGP
Настройка BGP GR	(Рекомендуется) Используется для повышения надежности сети	
	bgp graceful-restart	Включает возможность BGP GR
	bgp graceful-restart restart-time *restart-time*	Настраивает максимальное время для BGP GR

Конфигурация	Описание и команда	
Настройка BGP GR	**bgp graceful-restart stalepath-time** *time*	Настраивает максимальное время хранения для стабильного маршрута BGP
Настройка семейства адресов BGP IPv6	(Опционально) Используется для развертывания сети IPv6 с использованием BGP	
	address-family ipv6 unicast	Вход в режим настройки unicast-рассылки BGP IPv6
	neighbor { *peer-address* | *peer-group-name* } **activate**	Активирует возможности семейства адресов соседа BGP в текущем режиме конфигурации
Настройка соединения с устройствами, поддерживающими только 2-байтовые номера AS	(Опционально) Используется для соединения со старым устройством, которое поддерживает только 2-байтовые номера AS	
	neighbor { *peer-address* | *peer-group-name* } **remote-as** *as-number*	Создает соседа BGP

7.4.1. Настройка peer-a BGP (группы)

7.4.1.1. Эффект конфигурации

Настройте BGP и создайте соседей IBGP и EBGP.

7.4.1.2. Примечания

- Если сосед IBGP не подключен напрямую, вам необходимо настроить IGP или протокол статической маршрутизации для реализации соединения.
- Если сосед EBGP не подключен напрямую, вам необходимо настроить для него параметр **ebgp-multihop**.

7.4.1.3. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка интерфейса источника для соседа BGP

(Опционально) Выполните эту настройку в режиме настройки BGP. По умолчанию BGP автоматически выбирает локальный интерфейс, который достигает IP-адреса назначения peer-a, в качестве интерфейса источника.

ПРИМЕЧАНИЕ: для соседа IBGP рекомендуется использовать интерфейс Loopback в качестве интерфейса источника.

7.4.1.4. Проверка

Запустите команду **show**, чтобы отобразить статус соседа.

7.4.1.5. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Создание соседа BGP

Команда	**neighbor** { *peer-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*peer-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *as-number*: указывает номер AS peer-a BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	AS, указанная для peer-a (группы), должна совпадать с номером AS BGP спикера BGP на peer end-e

Создание интерфейса источника для соседа BGP

Команда	**neighbor** { *peer-address* | *peer-group-name* } **update-source** { *interface-type interface-number* | *address* }
Описание параметра	*peer-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *interface-type interface-number*: указывает имя интерфейса. *address*: непосредственно указывает адрес сетевого интерфейса, используемый для создания соединения BGP

Командный режим	Режим конфигурации BGP
Руководство по использованию	Интерфейс источника соседа должен быть локальным допустимым интерфейсом или адресом

7.4.1.6. Пример конфигурации

Настройка peer-а BGP (группы)

Сценарий:

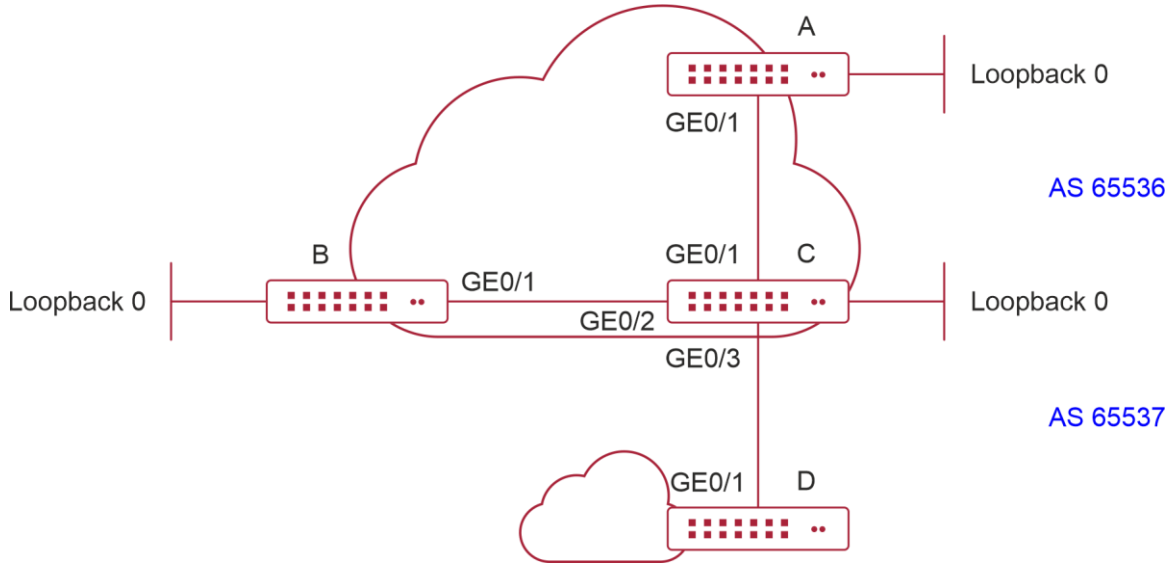


Рисунок 7-4.

Шаги настройки	• Включите BGP на всех устройствах и установите номера AS, как показано на Рисунке 7-4. • Настройте loopback-интерфейс на A, B и C и создайте соседа IBGP на основе loopback-интерфейса. • Создайте соседство EBGP, используя напрямую подключенные интерфейсы на C и D. • Создайте группу peer-ов IBGP на C
A	A# configure terminal A(config)# interface loopback 0 A(config-if-Loopback 0)# ip address 10.1.1.1 255.255.255.255 A(config-if-Loopback 0)# exit A(config)# interface GigabitEthernet 0/1

	A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# exit A(config)# router bgp 65536 A(config-router)# neighbor 10.1.1.3 remote-as 65536 A(config-router)# neighbor 10.1.1.3 update-source loopback 0
B	B# configure terminal B(config)# interface loopback 0 B(config-if-Loopback 0)# ip address 10.1.1.2 255.255.255.255 B(config-if-Loopback 0)# exit B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0 B(config-if-GigabitEthernet 0/1)# exit B(config)# router bgp 65536 B(config-router)# neighbor 10.1.1.3 remote-as 65536 B(config-router)# neighbor 10.1.1.3 update-source loopback 0
C	C# configure terminal C(config)# interface loopback 0 C(config-if-Loopback 0)# ip address 10.1.1.3 255.255.255.255 C(config-if-Loopback 0)# exit C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ip address 192.168.1.3 255.255.255.0 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface GigabitEthernet 0/2 C(config-if-GigabitEthernet 0/2)# ip address 192.168.2.3 255.255.255.0 C(config-if-GigabitEthernet 0/2)# exit C(config)# interface GigabitEthernet 0/3 C(config-if-GigabitEthernet 0/3)# ip address 192.168.3.3 255.255.255.0 C(config-if-GigabitEthernet 0/3)# exit C(config)# router bgp 65536 C(config-router)# neighbor ibgp-group peer-group C(config-router)# neighbor ibgp-group remote-as 65536 C(config-router)# neighbor ibgp-group update-source loopback 0 C(config-router)# neighbor 10.1.1.1 peer-group ibgp-group C(config-router)# neighbor 10.1.1.2 peer-group ibgp-group

	C(config-router)# neighbor 192.168.3.4 remote-as 65537
D	D# configure terminal D(config)# interface GigabitEthernet 0/1 D(config-if-GigabitEthernet 0/1)# ip address 192.168.3.4 255.255.255.0 D(config-if-GigabitEthernet 0/1)# exit D(config)# router bgp 65537 D(config-router)# neighbor 192.168.3.3 remote-as 65536
Проверка	Запустите команду **show**, чтобы отобразить статус соседа BGP
A	A# show ip bgp neighbor BGP neighbor is 10.1.1.3, remote AS 65536, local AS 65536, internal link BGP version 4, remote router ID 10.1.1.3 BGP state = Established, up for 00:00:05 Last read , hold time is 180, keepalive interval is 60 seconds Neighbor capabilities: Route refresh: advertised and received (old and new) Four-octets ASN Capability: advertised and received Address family IPv4 Unicast: advertised and received Received 2 messages, 0 notifications, 0 in queue open message:1 update message:0 keepalive message:1 refresh message:0 dynamic cap:0 notifications:0 Sent 2 messages, 0 notifications, 0 in queue open message:1 update message:0 keepalive message:1 refresh message:0 dynamic cap:0 notifications:0 Route refresh request: received 0, sent 0 Minimum time between advertisement runs is 0 seconds Update source is Loopback 0 For address family: IPv4 Unicast BGP table version 1, neighbor version 1 Index 0, Offset 0, Mask 0x1 0 accepted prefixes 0 announced prefixes

	Connections established 1; dropped 0 Local host: 10.1.1.1, Local port: 1039 Foreign host: 10.1.1.3, Foreign port: 179 Nexthop: 10.1.1.1 Nexthop global: :: Nexthop local: :: BGP connection: non shared network Last Reset: , due to BGP Notification received Notification Error Message: (Cease/Other Configuration Change.)
B	B# show ip bgp neighbor BGP neighbor is 10.1.1.3, remote AS 65536, local AS 65536, internal link BGP version 4, remote router ID 10.1.1.3 BGP state = Established, up for 00:00:07 Last read , hold time is 180, keepalive interval is 60 seconds Neighbor capabilities: Route refresh: advertised and received (old and new) Four-octets ASN Capability: advertised and received Address family IPv4 Unicast: advertised and received Received 2 messages, 0 notifications, 0 in queue open message:1 update message:0 keepalive message:1 refresh message:0 dynamic cap:0 notifications:0 Sent 2 messages, 0 notifications, 0 in queue open message:1 update message:0 keepalive message:1 refresh message:0 dynamic cap:0 notifications:0 Route refresh request: received 0, sent 0 Minimum time between advertisement runs is 0 seconds Update source is Loopback 0 For address family: IPv4 Unicast BGP table version 1, neighbor version 1 Index 0, Offset 0, Mask 0x1 0 accepted prefixes 0 announced prefixes

	Connections established 1; dropped 0 Local host: 10.1.1.2, Local port: 1041 Foreign host: 10.1.1.3, Foreign port: 179 Nexthop: 10.1.1.2 Nexthop global: :: Nexthop local: :: BGP connection: non shared network Last Reset: , due to BGP Notification received Notification Error Message: (Cease/Other Configuration Change.)
C	C# show ip bgp neighbor BGP neighbor is 10.1.1.1, remote AS 65536, local AS 65536, internal link Member of peer-group ibgp-group for session parameters BGP version 4, remote router ID 10.1.1.1 BGP state = Established, up for 00:01:13 Last read , hold time is 180, keepalive interval is 60 seconds Neighbor capabilities: Route refresh: advertised and received (old and new) Four-octets ASN Capability: advertised and received Address family IPv4 Unicast: advertised and received Received 3 messages, 0 notifications, 0 in queue open message:1 update message:0 keepalive message:2 refresh message:0 dynamic cap:0 notifications:0 Sent 3 messages, 0 notifications, 0 in queue open message:1 update message:0 keepalive message:2 refresh message:0 dynamic cap:0 notifications:0 Route refresh request: received 0, sent 0 Minimum time between advertisement runs is 0 seconds Update source is Loopback 0 For address family: IPv4 Unicast BGP table version 1, neighbor version 1 Index 1, Offset 0, Mask 0x2 ibgp-group peer-group member 0 accepted prefixes

```
0 announced prefixes

Connections established 1; dropped 0
Local host: 10.1.1.3, Local port: 179
Foreign host: 10.1.1.1, Foreign port: 1039
Nexthop: 10.1.1.3
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 10.1.1.2, remote AS 65536, local AS 65536, internal link
Member of peer-group ibgp-group for session parameters
  BGP version 4, remote router ID 10.1.1.2
  BGP state = Established, up for 00:01:17
  Last read , hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
  Route refresh: advertised and received (old and new)
  Four-octets ASN Capability: advertised and received
  Address family IPv4 Unicast: advertised and received
Received 3 messages, 0 notifications, 0 in queue
  open message:1 update message:0 keepalive message:2
  refresh message:0 dynamic cap:0 notifications:0
Sent 3 messages, 0 notifications, 0 in queue
  open message:1 update message:0 keepalive message:2
  refresh message:0 dynamic cap:0 notifications:0
Route refresh request: received 0, sent 0
Minimum time between advertisement runs is 0 seconds
Update source is Loopback 0

For address family: IPv4 Unicast
BGP table version 1, neighbor version 1
Index 1, Offset 0, Mask 0x2
ibgp-group peer-group member
0 accepted prefixes
0 announced prefixes
```

Connections established 1; dropped 0
Local host: 10.1.1.3, Local port: 179
Foreign host: 10.1.1.2, Foreign port: 1041
Nexthop: 10.1.1.3
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 192.168.3.4, remote AS 65536, local AS 65536, internal link
Member of peer-group ibgp-group for session parameters
  BGP version 4, remote router ID 192.168.3.4
  BGP state = Established, up for 00:01:01
  Last read , hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
  Route refresh: advertised and received (old and new)
  Four-octets ASN Capability: advertised and received
  Address family IPv4 Unicast: advertised and received
Received 3 messages, 0 notifications, 0 in queue
  open message:1 update message:0 keepalive message:2
  refresh message:0 dynamic cap:0 notifications:0
Sent 3 messages, 0 notifications, 0 in queue
  open message:1 update message:0 keepalive message:2
  refresh message:0 dynamic cap:0 notifications:0
Route refresh request: received 0, sent 0
Minimum time between advertisement runs is 0 seconds
Update source is Loopback 0

For address family: IPv4 Unicast
BGP table version 1, neighbor version 1
Index 1, Offset 0, Mask 0x2
ibgp-group peer-group member
0 accepted prefixes
0 announced prefixes

	Connections established 1; dropped 0 Local host: 192.168.3.3, Local port: 179 Foreign host: 192.168.3.4, Foreign port: 1018 Nexthop: 192.168.3.3 Nexthop global: :: Nexthop local: :: BGP connection: non shared network
D	D# show ip bgp neighbor BGP neighbor is 192.168.3.3, remote AS 65536, local AS 65536, internal link Member of peer-group ibgp-group for session parameters BGP version 4, remote router ID 10.1.1.3 BGP state = Established, up for 00:01:01 Last read , hold time is 180, keepalive interval is 60 seconds Neighbor capabilities: Route refresh: advertised and received (old and new) Four-octets ASN Capability: advertised and received Address family IPv4 Unicast: advertised and received Received 3 messages, 0 notifications, 0 in queue open message:1 update message:0 keepalive message:2 refresh message:0 dynamic cap:0 notifications:0 Sent 3 messages, 0 notifications, 0 in queue open message:1 update message:0 keepalive message:2 refresh message:0 dynamic cap:0 notifications:0 Route refresh request: received 0, sent 0 Minimum time between advertisement runs is 0 seconds Update source is Loopback 0 For address family: IPv4 Unicast BGP table version 1, neighbor version 1 Index 1, Offset 0, Mask 0x2 ibgp-group peer-group member 0 accepted prefixes 0 announced prefixes

	Connections established 1; dropped 0 Local host: 192.168.3.4, Local port: 1018 Foreign host: 192.168.3.3, Foreign port: 179 Nexthop: 192.168.3.4 Nexthop global: :: Nexthop local: :: BGP connection: non shared network

7.4.1.7. Распространенные ошибки

- IGP не включен, и соединение между локальным loopback-адресом и loopback-адресом на соседе IBGP не работает, что приводит к невозможности создания соседа.
- ebgp-multihop не настраивается, если EBGP не подключен напрямую, что приводит к невозможности создания TCP-соединения.

7.4.2. Настройка аутентификации MD5

7.4.2.1. Эффект конфигурации

Настройте MD5 для зашифрованной аутентификации между соседями EBGP и IBGP.

7.4.2.2. Примечания

- Если сосед IBGP не подключен напрямую, вам необходимо настроить IGP или протокол статической маршрутизации для реализации соединения.
- Если сосед EBGP не подключен напрямую, вам необходимо настроить для него параметр **ebgp-multihop**.

7.4.2.3. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

7.4.2.4. Проверка

Запустите команду **show**, чтобы отобразить статус соседа.

7.4.2.5. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме

Командный режим	Режим глобальной конфигурации

Создание соседа BGP

Команда	**neighbor** { *peer-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*peer-address*: указывает адрес peer-а. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *as-number*: указывает номер AS peer-а BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	AS, указанная для peer-а (группы), должна совпадать с номером AS BGP спикера BGP на peer end-е

Настройка пароля MD5 для соседа BGP

Команда	**neighbor** { *peer-address* | *peer-group-name* } **password** [**0** | **7**] *string*
Описание параметра	*peer-address*: указывает адрес peer-а. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. **0**: отображает незашифрованный пароль. **7**: отображает зашифрованный пароль. *string*: указывает пароль для аутентификации TCP MD5, состоящий максимум из 80 символов
Командный режим	Режим конфигурации BGP
Руководство по использованию	На обоих концах соседства BGP должны быть настроены одни и те же пароли

7.4.2.6. Пример конфигурации

Настройка аутентификации BGP MD5

Сценарий:

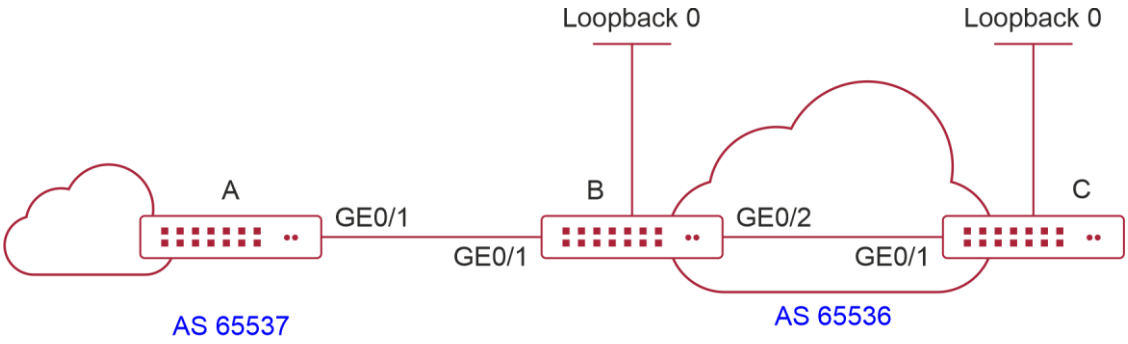


Рисунок 7-5.

Шаги настройки	• Включите BGP на всех устройствах и установите номера AS, как показано на Рисунке 7-5. • Настройте loopback-интерфейс на B и C и создайте соседа IBGP на основе loopback-интерфейса. • Создайте соседство EBGP, используя напрямую подключенные интерфейсы на A и B. • Настройте пароли на A, B и C для их соседей
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# exit A(config)# router bgp 65537 A(config-router)# neighbor 192.168.1.2 remote-as 65536 A(config-router)# neighbor 192.168.1.2 password 7 ebgpneighbor
B	B# configure terminal B(config)# interface loopback 0 B(config-if-Loopback 0)# ip address 10.1.1.1 255.255.255.255 B(config-if-Loopback 0)# exit B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0 B(config-if-GigabitEthernet 0/1)# exit B(config)# interface GigabitEthernet 0/2

	B(config-if-GigabitEthernet 0/2)# ip address 192.168.2.2 255.255.255.0 B(config-if-GigabitEthernet 0/2)# exit B(config)# router bgp 65536 B(config-router)# neighbor 10.1.1.2 remote-as 65536 B(config-router)# neighbor 10.1.1.2 update-source loopback 0 B(config-router)# neighbor 10.1.1.2 password ibgpneighbor B(config-router)# neighbor 192.168.1.1 remote-as 65537 B(config-router)# neighbor 192.168.1.1 password 7 ebgpneighbor
C	C# configure terminal C(config)# interface loopback 0 C(config-if-Loopback 0)# ip address 10.1.1.2 255.255.255.255 C(config-if-Loopback 0)# exit C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ip address 192.168.2.3 255.255.255.0 C(config-if-GigabitEthernet 0/1)# exit C(config)# router bgp 65536 C(config-router)# neighbor 10.1.1.1 remote-as 65536 C(config-router)# neighbor 10.1.1.1 update-source loopback 0 C(config-router)# neighbor 10.1.1.1 password ibgpneighbor
Проверка	Запустите команду **show**, чтобы отобразить статус соседа BGP
A	A#show ip bgp neighbors BGP neighbor is 192.168.1.2, remote AS 65536, local AS 65537, external link BGP version 4, remote router ID 10.1.1.1 BGP state = Established, up for 00:04:54 Last read , hold time is 180, keepalive interval is 60 seconds Neighbor capabilities: Route refresh: advertised and received (old and new) Four-octets ASN Capability: advertised and received Address family IPv4 Unicast: advertised and received Received 7 messages, 0 notifications, 0 in queue open message:1 update message:0 keepalive message:6 refresh message:0 dynamic cap:0 notifications:0 Sent 7 messages, 0 notifications, 0 in queue

	open message:1 update message:0 keepalive message:6 refresh message:0 dynamic cap:0 notifications:0 Route refresh request: received 0, sent 0 Minimum time between advertisement runs is 30 seconds For address family: IPv4 Unicast BGP table version 1, neighbor version 0 Index 1, Offset 0, Mask 0x2 0 accepted prefixes 0 announced prefixes Connections established 2; dropped 1 Local host: 192.168.1.1, Local port: 1026 Foreign host: 192.168.1.2, Foreign port: 179 Nexthop: 192.168.1.1 Nexthop global: :: Nexthop local: :: BGP connection: non shared network Last Reset: 00:04:54, due to BGP Notification sent Notification Error Message: (Cease/Administratively Reset.)
B	B# show ip bgp neighbors BGP neighbor is 10.1.1.2, remote AS 65536, local AS 65536, internal link BGP version 4, remote router ID 10.1.1.2 BGP state = Established, up for 00:04:01 Last read , hold time is 180, keepalive interval is 60 seconds Neighbor capabilities: Route refresh: advertised and received (old and new) Four-octets ASN Capability: advertised and received Address family IPv4 Unicast: advertised and received Received 8 messages, 0 notifications, 0 in queue open message:1 update message:0 keepalive message:7 refresh message:0 dynamic cap:0 notifications:0 Sent 8 messages, 0 notifications, 0 in queue open message:1 update message:0 keepalive message:7

```
  refresh message:0 dynamic cap:0 notifications:0
Route refresh request: received 0, sent 0
Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
BGP table version 1, neighbor version 0
Index 1, Offset 0, Mask 0x2
0 accepted prefixes
0 announced prefixes

Connections established 2; dropped 1
Local host: 10.1.1.1, Local port: 179
Foreign host: 10.1.1.2, Foreign port: 1038
Nexthop: 10.1.1.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:05:27, due to BGP Notification received
Notification Error Message: (Cease/Administratively Reset.)

BGP neighbor is 192.168.1.1, remote AS 65537, local AS 65536, external link
  BGP version 4, remote router ID 192.168.1.1
  BGP state = Established, up for 00:05:27
  Last read , hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
  Route refresh: advertised and received (old and new)
  Four-octets ASN Capability: advertised and received
  Address family IPv4 Unicast: advertised and received
Received 8 messages, 0 notifications, 0 in queue
  open message:1 update message:0 keepalive message:7
  refresh message:0 dynamic cap:0 notifications:0
Sent 8 messages, 0 notifications, 0 in queue
  open message:1 update message:0 keepalive message:7
  refresh message:0 dynamic cap:0 notifications:0
Route refresh request: received 0, sent 0
```

	Minimum time between advertisement runs is 30 seconds For address family: IPv4 Unicast BGP table version 1, neighbor version 0 Index 1, Offset 0, Mask 0x2 0 accepted prefixes 0 announced prefixes Connections established 2; dropped 1 Local host: 192.168.1.2, Local port: 179 Foreign host: 192.168.1.1, Foreign port: 1026 Nexthop: 192.168.1.2 Nexthop global: :: Nexthop local: :: BGP connection: non shared network Last Reset: 00:05:27, due to BGP Notification received Notification Error Message: (Cease/Administratively Reset.)
C	C# show ip bgp neighbors BGP neighbor is 10.1.1.1, remote AS 65536, local AS 65536, internal link BGP version 4, remote router ID 10.1.1.1 BGP state = Established, up for 00:04:01 Last read , hold time is 180, keepalive interval is 60 seconds Neighbor capabilities: Route refresh: advertised and received (old and new) Four-octets ASN Capability: advertised and received Address family IPv4 Unicast: advertised and received Received 8 messages, 0 notifications, 0 in queue open message:1 update message:0 keepalive message:7 refresh message:0 dynamic cap:0 notifications:0 Sent 8 messages, 0 notifications, 0 in queue open message:1 update message:0 keepalive message:7 refresh message:0 dynamic cap:0 notifications:0 Route refresh request: received 0, sent 0 Minimum time between advertisement runs is 30 seconds

	For address family: IPv4 Unicast BGP table version 1, neighbor version 0 Index 1, Offset 0, Mask 0x2 0 accepted prefixes 0 announced prefixes Connections established 2; dropped 1 Local host: 10.1.1.2, Local port: 1038 Foreign host: 10.1.1.1, Foreign port: 179 Nexthop: 10.1.1.2 Nexthop global: :: Nexthop local: :: BGP connection: non shared network Last Reset: 00:05:27, due to BGP Notification received Notification Error Message: (Cease/Administratively Reset.)

7.4.2.7. Распространенные ошибки

Пароли для аутентификации с шифрованием MD5 на двух концах соседства BGP различны.

7.4.3. Настройка reflector-а маршрута

7.4.3.1. Эффект конфигурации

Настройте reflector маршрута в среде IBGP, чтобы уменьшить количество соединений с соседями BGP.

7.4.3.2. Примечания

Если сосед IBGP не подключен напрямую, вам необходимо настроить IGP или протокол статической маршрутизации для реализации соединения.

7.4.3.3. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Создание reflector-а BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

7.4.3.4. Проверка

Запустите команду **show**, чтобы отобразить статус соседа.

7.4.3.5. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Создание соседа BGP

Команда	**neighbor** { *peer-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*peer-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *as-number*: указывает номер AS peer-a BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	AS, указанная для peer-a (группы), должна совпадать с номером AS BGP спикера BGP на peer end-e

Создание reflector-a BGP

Команда	**neighbor** { *peer-address* | *peer-group-name* } **route-reflector-client**
Описание параметра	*peer-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов
Командный режим	Режим конфигурации BGP

7.4.3.6. Пример конфигурации

Настройка reflector-а маршрута BGP

Сценарий:

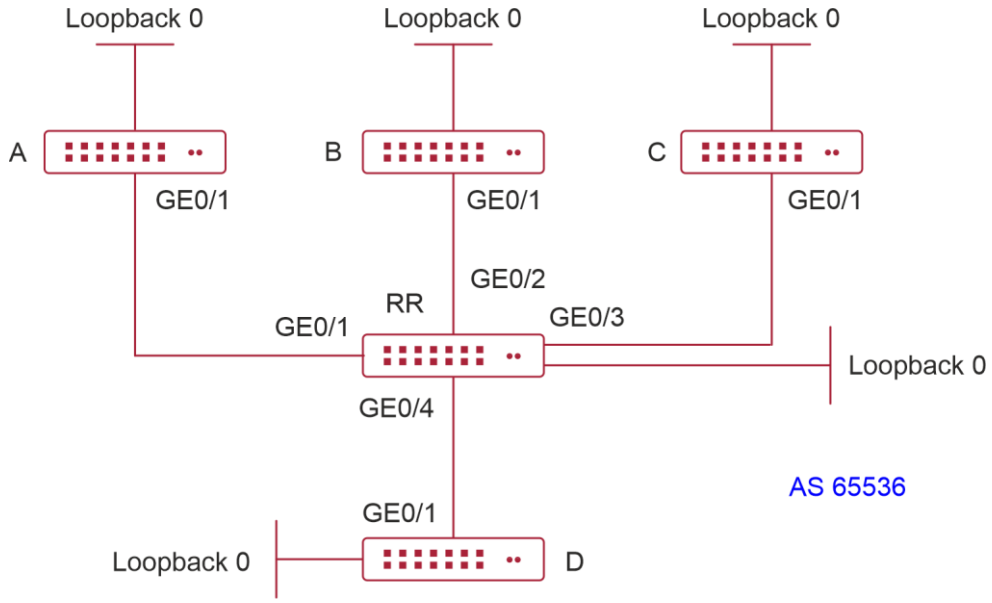


Рисунок 7-6.

Шаги настройки	• Включите BGP на всех устройствах и установите номера AS, как показано на Рисунке 7-6. • Настройте loopback-интерфейс на всех устройствах и создайте соседство IBGP, используя loopback-интерфейс в соответствии с линиям связи подключения, как показано на Рисунке 7-6. • Настройте reflection маршрута на устройстве RR и укажите A, B, C и D в качестве клиентов reflection
A	A# configure terminal A(config)# interface loopback 0 A(config-if-Loopback 0)# ip address 10.1.1.1 255.255.255.255 A(config-if-Loopback 0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# exit A(config)# router bgp 65536 A(config-router)# neighbor 10.1.1.5 remote-as 65536 A(config-router)# neighbor 10.1.1.5 update-source loopback 0

	A(config-router)# network 192.168.1.0 mask 255.255.255.0
B	B# configure terminal B(config)# interface loopback 0 B(config-if-Loopback 0)# ip address 10.1.1.2 255.255.255.255 B(config-if-Loopback 0)# exit B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0 B(config-if-GigabitEthernet 0/1)# exit B(config)# router bgp 65536 B(config-router)# neighbor 10.1.1.5 remote-as 65536 B(config-router)# neighbor 10.1.1.5 update-source loopback 0
C	C# configure terminal C(config)# interface loopback 0 C(config-if-Loopback 0)# ip address 10.1.1.3 255.255.255.255 C(config-if-Loopback 0)# exit C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ip address 192.168.3.3 255.255.255.0 C(config-if-GigabitEthernet 0/1)# exit C(config)# router bgp 65536 C(config-router)# neighbor 10.1.1.5 remote-as 65536 C(config-router)# neighbor 10.1.1.5 update-source loopback 0
D	C# configure terminal C(config)# interface loopback 0 C(config-if-Loopback 0)# ip address 10.1.1.4 255.255.255.255 C(config-if-Loopback 0)# exit C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ip address 192.168.4.4 255.255.255.0 C(config-if-GigabitEthernet 0/1)# exit C(config)# router bgp 65536 C(config-router)# neighbor 10.1.1.5 remote-as 65536 C(config-router)# neighbor 10.1.1.5 update-source loopback 0
RR	RR# configure terminal

	RR(config)# interface loopback 0 RR(config-if-Loopback 0)# ip address 10.1.1.5 255.255.255.255 RR(config-if-Loopback 0)# exit RR(config)# interface GigabitEthernet 0/1 RR(config-if-GigabitEthernet 0/1)# ip address 192.168.1.5 255.255.255.0 RR(config-if-GigabitEthernet 0/1)# exit RR(config)# interface GigabitEthernet 0/2 RR(config-if-GigabitEthernet 0/2)# ip address 192.168.2.5 255.255.255.0 RR(config-if-GigabitEthernet 0/2)# exit RR(config)# interface GigabitEthernet 0/3 RR(config-if-GigabitEthernet 0/3)# ip address 192.168.3.5 255.255.255.0 RR(config-if-GigabitEthernet 0/3)# exit RR(config)# interface GigabitEthernet 0/4 RR(config-if-GigabitEthernet 0/4)# ip address 192.168.4.5 255.255.255.0 RR(config-if-GigabitEthernet 0/4)# exit RR(config)# router bgp 65536 RR(config-router)# neighbor 10.1.1.1 remote-as 65536 RR(config-router)# neighbor 10.1.1.1 update-source loopback 0 RR(config-router)# neighbor 10.1.1.1 route-reflector-client RR(config-router)# neighbor 10.1.1.2 remote-as 65536 RR(config-router)# neighbor 10.1.1.2 update-source loopback 0 RR(config-router)# neighbor 10.1.1.2 route-reflector-client RR(config-router)# neighbor 10.1.1.3 remote-as 65536 RR(config-router)# neighbor 10.1.1.3 update-source loopback 0 RR(config-router)# neighbor 10.1.1.3 route-reflector-client RR(config-router)# neighbor 10.1.1.4 remote-as 65536 RR(config-router)# neighbor 10.1.1.4 update-source loopback 0 RR(config-router)# neighbor 10.1.1.4 route-reflector-client
Проверка	Запустите команду **show**, чтобы отобразить статус соседа BGP
RR	RR# show ip bgp summarywww.qtech.ru BGP router identifier 10.1.1.5, local AS number 65536 BGP table version is 1 0 BGP AS-PATH entries 0 BGP Community entries

	1 BGP Prefix entries (Maximum-prefix:4294967295) Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 10.1.1.1 4 65536 8 9 1 0 0 00:05:11 1 10.1.1.2 4 65536 9 9 1 0 0 00:05:24 0 10.1.1.3 4 65536 8 7 1 0 0 00:05:10 0 10.1.1.4 4 65536 9 8 1 0 0 00:05:14 0 RR# show ip bgp BGP table version is 1, local router ID is 10.1.1.5 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale, b - backup entry Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path *>i192.168.1.0 10.1.1.1 0 100 0 i Total number of prefixes 1
D	D# show ip bgp summary BGP router identifier 10.1.1.4, local AS number 65536 BGP table version is 1 0 BGP AS-PATH entries 0 BGP Community entries 1 BGP Prefix entries (Maximum-prefix:4294967295) Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 10.1.1.5 4 65536 8 9 1 0 0 00:05:20 1 D# show ip bgp BGP table version is 1, local router ID is 10.1.1.4

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop        Metric     LocPrf     Weight Path
* i192.168.1.0    10.1.1.1        0          100        0  i

Total number of prefixes 1
```

7.4.4. Настройка объединения AS

7.4.4.1. Эффект конфигурации

Настройте объединение BGP, чтобы уменьшить количество соединений соседей BGP.

7.4.4.2. Примечания

- Рекомендуется использовать приватные номера AS для sub AS (также называемых AS-участниками) внутри объединения. Номера приватных AS варьируются от 64 512 до 65 535.
- В sub AS объединения для всех спикеров BGP должен быть установлен full mesh (reflector-ы маршрутов могут быть дополнительно настроены внутри sub AS).
- Соседство EBGP должно быть установлено между sub AS в объединении.
- Все спикеры BGP в объединении должны принадлежать к sub AS внутри объединения.

7.4.4.3. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Настройка идентификатора объединения BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка участника объединения BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка нескольких hop-ов для соседа EBGP

Выполните эту настройку в режиме настройки BGP. Это обязательно, когда сосед EBGP не подключен напрямую.

Настройка перераспределения маршрутов BGP в сети

(Опционально) Выполните эту настройку в режиме настройки BGP. Выполните эту настройку, когда необходимо объявить локальный маршрут. Также можно настроить альтернативную сеть посредством перераспределения.

7.4.4.4. Проверка

- Запустите команду **show**, чтобы отобразить статус соседа BGP.
- Запустите команду **show**, чтобы отобразить информацию таблицы маршрутизации BGP.

7.4.4.5. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Включение идентификатора объединения BGP

Команда	**bgp confederation identifier** *as-number*
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим конфигурации BGP

Настройка участника объединения BGP

Команда	**bgp confederation peers** *as-number* [… *as-number*]
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим конфигурации BGP
Руководство по использованию	Все участники AS локального объединения EBGP должны быть идентифицированы

Создание соседа BGP

Команда	**neighbor** { *peer-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*peer-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6.

	peer-group-name: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *as-number*: указывает номер AS peer-а BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	AS, указанная для peer-а (группы), должна совпадать с номером AS BGP спикера BGP на peer end-е

Настройка нескольких hop-ов для соседа EBGP

Команда	**neighbor** { *peer-address* | *peer-group-name* } **ebgp-multihop** [*ttl*]
Описание параметра	*peer-address*: указывает адрес peer-а. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *ttl*: указывает максимальное разрешенное количество hop-ов в диапазоне от 1 до 255
Командный режим	Режим конфигурации BGP
Руководство по использованию	AS, указанная для peer-а (группы), должна совпадать с номером AS BGP спикера BGP на peer end-е

Настройка перераспределения маршрутов BGP в сети

Команда	**network** *network-number* [**mask** *mask*] [**route-map** *map-tag*] [**backdoor**]
Описание параметра	*network-number*: указывает сетевой адрес. *mask*: указывает маску подсети. *map-tag*: указывает название карты маршрутов, состоящее не более чем из 32 символов. **backdoor**: указывает, что маршрут является маршрутом backdoor
Командный режим	Режим конфигурации BGP
Руководство по использованию	Основная (core) таблица маршрутизации должна содержать одинаковые маршруты IGP (или статические и напрямую подключенные) маршруты

7.4.4.6. Пример конфигурации

Настройка объединения BGP

Сценарий:

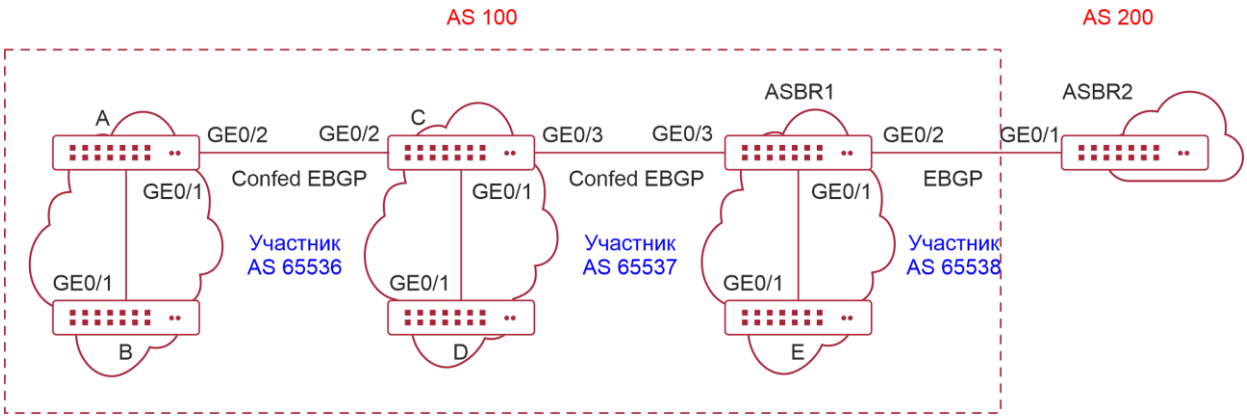


Рисунок 7-7.

Шаги настройки	• Настройте BGP на A и B, установите номер AS равным 65 536 и настройте соседство IBGP. • Настройте BGP на C и D, установите номер AS равным 65 537 и настройте соседство IBGP. • Настройте BGP на ASBR1 и E, установите номер AS равным 65 538 и настройте соседство IBGP. • Настройте идентификатор объединения 100 на A, B, C, D, E и ASBR1. • Настройте участника объединения равным 65 537 на A, настройте C как соседа EBGP и установите номер AS peer-a равным 65 537. • Настройте участников объединения равными 65 536 и 65 538 на C, настройте A как соседа EBGP и установите номер AS peer-a равным 65 536, настройте ASBR1 как соседа EBGP и установите номер AS peer-a равным 65 538. • Настройте участника объединения равным 65 537 на ASBR1, настройте C как соседа EBGP и установите номер AS peer-a равным 65 537, настройте ASBR2 как соседа EBGP и установите номер AS peer-a равным 200. • Настройте BGP на ASBR2 и установите номер AS равным 200; настройте ASBR1 в качестве соседа EBGP и установите номер AS peer-a равным 100
A	A# configure terminal A(config)# interface loopback 0 A(config-if-Loopback 0)# ip address 10.1.1.1 255.255.255.255

	A(config-if-Loopback 0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# exit A(config)# interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0 A(config-if-GigabitEthernet 0/2)# exit A(config)# router bgp 65536 A(config-router)# bgp confederation identifier 100 A(config-router)# bgp confederation peers 65537 A(config-router)# neighbor 10.1.1.2 remote-as 65536 A(config-router)# neighbor 10.1.1.2 update-source loopback 0 A(config-router)# neighbor 10.1.1.3 remote-as 65537 A(config-router)# neighbor 10.1.1.3 ebgp-multihop 2 A(config-router)# neighbor 10.1.1.3 update-source loopback 0 A(config-router)# network 192.168.1.0 mask 255.255.255.0
B	B# configure terminal B(config)# interface loopback 0 B(config-if-Loopback 0)# ip address 10.1.1.2 255.255.255.255 B(config-if-Loopback 0)# exit B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0 B(config-if-GigabitEthernet 0/1)# exit B(config)# router bgp 65536 B(config-router)# neighbor 10.1.1.1 remote-as 65536 B(config-router)# neighbor 10.1.1.1 update-source loopback 0
C	C# configure terminal C(config)# interface loopback 0 C(config-if-Loopback 0)# ip address 10.1.1.3 255.255.255.255 C(config-if-Loopback 0)# exit C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ip address 192.168.3.3 255.255.255.0 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface GigabitEthernet 0/2

	C(config-if-GigabitEthernet 0/2)# ip address 192.168.2.3 255.255.255.0 C(config-if-GigabitEthernet 0/2)# exit C(config)# interface GigabitEthernet 0/3 C(config-if-GigabitEthernet 0/3)# ip address 192.168.4.3 255.255.255.0 C(config-if-GigabitEthernet 0/3)# exit C(config)# router bgp 65537 C(config-router)# bgp confederation identifier 100 C(config-router)# bgp confederation peers 65536 65538 C(config-router)# neighbor 10.1.1.1 remote-as 65536 C(config-router)# neighbor 10.1.1.1 update-source loopback 0 C(config-router)# neighbor 10.1.1.1 ebgp-multihop 2 C(config-router)# neighbor 10.1.1.4 remote-as 65537 C(config-router)# neighbor 10.1.1.4 update-source loopback 0 C(config-router)# neighbor 10.1.1.5 remote-as 65538 C(config-router)# neighbor 10.1.1.5 update-source loopback 0 C(config-router)# neighbor 10.1.1.5 ebgp-multihop 2D
D	D# configure terminal D(config)# interface loopback 0 D(config-if-Loopback 0)# ip address 10.1.1.4 255.255.255.255 D(config-if-Loopback 0)# exit D(config)# interface GigabitEthernet 0/1 D(config-if-GigabitEthernet 0/1)# ip address 192.168.3.4 255.255.255.0 D(config-if-GigabitEthernet 0/1)# exit D(config)# router bgp 65537 D(config-router)# neighbor 10.1.1.3 remote-as 65537 D(config-router)# neighbor 10.1.1.3 update-source loopback 0
E	E# configure terminal E(config)# interface loopback 0 E(config-if-Loopback 0)# ip address 10.1.1.6 255.255.255.255 E(config-if-Loopback 0)# exit E(config)# interface GigabitEthernet 0/1 E(config-if-GigabitEthernet 0/1)# ip address 192.168.5.6 255.255.255.0 E(config-if-GigabitEthernet 0/1)# exit E(config)# router bgp 65538

	E(config-router)# neighbor 10.1.1.5 remote-as 65538 E(config-router)# neighbor 10.1.1.5 update-source loopback 0
ASBR1	ASBR1# configure terminal ASBR1(config)# interface loopback 0 ASBR1(config-if-Loopback 0)# ip address 10.1.1.5 255.255.255.255 ASBR1(config-if-Loopback 0)# exit ASBR1(config)# interface GigabitEthernet 0/1 ASBR1(config-if-GigabitEthernet 0/1)# ip address 192.168.5.5 255.255.255.0 ASBR1(config-if-GigabitEthernet 0/1)# exit ASBR1(config)# interface GigabitEthernet 0/2 ASBR1(config-if-GigabitEthernet 0/2)# ip address 192.168.6.5 255.255.255.0 ASBR1(config-if-GigabitEthernet 0/2)# exit ASBR1(config)# interface GigabitEthernet 0/3 ASBR1(config-if-GigabitEthernet 0/3)# ip address 192.168.4.5 255.255.255.0 ASBR1(config-if-GigabitEthernet 0/3)# exit ASBR1(config)# router bgp 65538 ASBR1(config-router)# bgp confederation identifier 100 ASBR1(config-router)# bgp confederation peers 65537 ASBR1(config-router)# neighbor 10.1.1.3 remote-as 65537 ASBR1(config-router)# neighbor 10.1.1.3 update-source loopback 0 ASBR1(config-router)# neighbor 10.1.1.3 ebgp-multihop 2 ASBR1(config-router)# neighbor 10.1.1.6 remote-65538 ASBR1(config-router)# neighbor 10.1.1.6 update-source loopback 0 ASBR1(config-router)# neighbor 192.168.6.7 remote-as 200
ASBR2	ASBR2# configure terminal ASBR2(config)# interface GigabitEthernet 0/1 ASBR2(config-if-GigabitEthernet 0/1)# ip address 192.168.6.7 255.255.255.0 ASBR2(config-if-GigabitEthernet 0/1)# exit ASBR2(config)# router bgp 200 ASBR2(config-router)# neighbor 192.168.6.5 remote-as 100 ASBR2(config-router)# network 192.168.6.0 mask 255.255.255.0
Проверка	Запустите команду **show**, чтобы отобразить информацию

A	A# show ip bgp summary BGP router identifier 10.1.1.1, local AS number 65536 BGP table version is 1 1 BGP AS-PATH entries 0 BGP Community entries 1 BGP Prefix entries (Maximum-prefix:4294967295) Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 10.1.1.2 4 65536 3 3 1 0 0 00:00:05 0 10.1.1.3 4 65537 3 3 1 0 0 00:00:06 1 Total number of neighbors 1 A# show ip bgp BGP table version is 1, local router ID is 10.1.1.1 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale, b - backup entry Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path * 192.168.6.0 192.168.6.7 0 100 0 (65537 65538) 200 i Total number of prefixes 1
ASBR1	A# show ip bgp summary BGP router identifier 10.1.1.5, local AS number 200 BGP table version is 2 2 BGP AS-PATH entries 0 BGP Community entries 2 BGP Prefix entries (Maximum-prefix:4294967295) Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 10.1.1.3 4 65537 3 3 2 0 0 00:00:10 1

	10.1.1.6 4 65538 3 3 2 0 0 00:00:08 0 192.168.6.7 4 200 3 3 2 0 0 00:00:05 1 Total number of neighbors 1 A# show ip bgp BGP table version is 1, local router ID is 10.1.1.1 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale, b - backup entry Origin codes: i - IGP, e - EGP, ? - incompletewww.qtech.ru Network Next Hop Metric LocPrf Weight Path * 192.168.1.0 10.1.1.1 0 100 0 (65537 65536) i *> 192.168.6.0 192.168.6.7 0 100 0 200 i Total number of prefixes 1
ASBR2	A# show ip bgp summary BGP router identifier 192.168.6.7, local AS number 200 BGP table version is 1 1 BGP AS-PATH entries 0 BGP Community entries 1 BGP Prefix entries (Maximum-prefix:4294967295) Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 192.168.6.5 4 100 3 3 1 0 0 00:00:05 1 Total number of neighbors 1 A# show ip bgp BGP table version is 1, local router ID is 10.1.1.1 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale, b - backup entry

```
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop        Metric     LocPrf     Weight Path
*> 192.168.1.0    192.168.6.5     0          100        0 (65537 65538) 200 i

Total number of prefixes 1
```

7.4.4.7. Распространенные ошибки

- Ни один сосед по объединению BGP не настроен.
- Full mesh не устанавливается в sub AS объединения.

7.4.5. Настройка multipath-балансировки нагрузки BGP

7.4.5.1. Эффект конфигурации

- Внедрите multipath-балансировку нагрузки для маршрутов IBGP.
- Поддержка свободного сравнения AS-PATH.

7.4.5.2. Примечания

Маршруты, полученные от соседа IBGP, должны иметь одинаковый приоритет (идентификатор маршрутизатора не нужно сравнивать).

7.4.5.3. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка балансировки нагрузки BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка свободного сравнения AS-PATH

(Необязательно) Выполните эту настройку в режиме настройки BGP. Выполните эту настройку, если необходимо реализовать балансировку нагрузки для маршрутов, полученных от разных AS.

7.4.5.4. Проверка

- Запустите команду **show**, чтобы отобразить информацию о маршрутизации BGP.
- Запустите команду **show**, чтобы отобразить информацию основной (core) таблицы маршрутизации.

7.4.5.5. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Создание соседа BGP

Команда	**neighbor** { *peer-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*peer-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *as-number*: указывает номер AS peer-a BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	AS, указанная для peer-a (группы), должна совпадать с номером AS BGP спикера BGP на peer end-e

Настройка балансировки нагрузки BGP

Команда	**maximum-paths** { **ebgp** | **ibgp** } *number*
Описание параметра	*number*: указывает максимальное количество эквивалентных путей в диапазоне от 1 до емкости устройства. Если значение равно 1, multipath-балансировка нагрузки IBGP будет отключена
Командный режим	Режим конфигурации BGP

Настройка свободного сравнения AS-PATH

Команда	**bgp bestpath as-path multipath-relax**
Командный режим	Режим конфигурации BGP

7.4.5.6. Пример конфигурации

Настройка multipath-балансировки нагрузки IBGP

Сценарий:

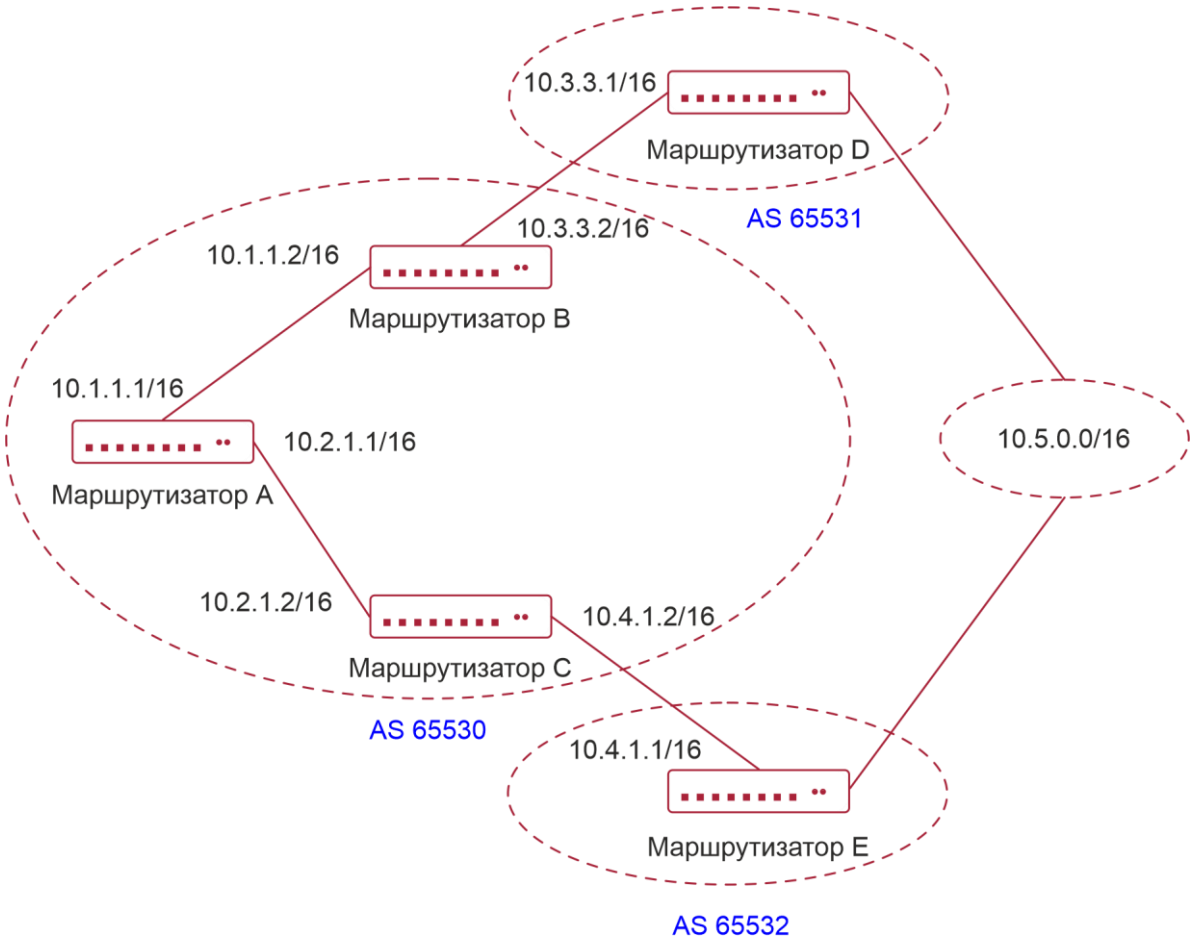


Рисунок 7-8.

Шаги настройки	• Включите BGP на всех устройствах и установите номера AS, как показано на Рисунке 7-8. • Установите соседство IBGP между A и B, а также между A и C, используя интерфейсы с прямым подключением. • Установите соседство EBGP между B и D, а также между C и E, используя интерфейсы с прямым подключением. • Перераспределите одинаковые маршруты на D и E. • Настройте балансировку нагрузки IBGP на A и включите режим свободного сравнения AS-PATH
A	A# conf terminal A(config)# interface fastEthernet 0/0

	A(config-if-FastEthernet 0/0)# ip address 10.1.1.1 255.255.0.0 A(config-if-FastEthernet 0/0)# exit A(config)# interface fastEthernet 0/1 A(config-if-FastEthernet 0/1)# ip address 10.2.1.1 255.255.0.0 A(config-if-FastEthernet 0/1)# exit A(config)# ip route 10.3.0.0 255.255.0.0 10.1.1.2 A(config)# ip route 10.4.0.0 255.255.0.0 10.2.1.2 A(config)# router bgp 65530 A(config-router)# neighbor 10.1.1.2 remote-as 65530 A(config-router)# neighbor 10.2.1.2 remote-as 65530 A(config-router)# bgp maximum-paths ibgp 2 A(config-router)# bgp bestpath as-path multipath-relax
B	B# conf terminal B(config)# interface fastEthernet 0/0 B(config-if-FastEthernet 0/0)# ip address 10.1.1.2 255.255.0.0 B(config-if-FastEthernet 0/0)# exit B(config)# interface fastEthernet 0/1 B(config-if-FastEthernet 0/1)# ip address 10.3.1.2 255.255.0.0 B(config-if-FastEthernet 0/1)# exit B(config)# router bgp 65530 B(config-router)# neighbor 10.1.1.1 remote-as 65530 B(config-router)# neighbor 10.3.1.1 remote-as 65531
C	C# conf terminal C(config)# interface fastEthernet 0/0 C(config-if-FastEthernet 0/0)# ip address 10.2.1.2 255.255.0.0 C(config-if-FastEthernet 0/0)# exit C(config)# interface fastEthernet 0/1 C(config-if-FastEthernet 0/1)# ip address 10.4.1.2 255.255.0.0 C(config-if-FastEthernet 0/1)# exit C(config)# router bgp 65530www.qtech.ru C(config-router)# neighbor 10.2.1.1 remote-as 65530 C(config-router)# neighbor 10.4.1.1 remote-as 65532
D	D# conf terminal

	D(config)# interface fastEthernet 0/0 D(config-if-FastEthernet 0/0)# ip address 10.3.1.1 255.255.0.0 D(config-if-FastEthernet 0/0)# exit D(config)# interface loopback 1 D(config-if)#ip address 10.5.1.1 255.255.0.0 D(config-if-FastEthernet 0/1)# exit D(config)# router bgp 65531 D(config-router)# neighbor 10.3.1.2 remote-as 65530 D(config-router)# redistribute connected
E	E# conf terminal E(config)# interface fastEthernet 0/0 E(config-if-FastEthernet 0/0)# ip address 10.4.1.1 255.255.0.0 E(config-if-FastEthernet 0/0)# exit E(config)# interface loopback 1 E(config-if)#ip address 10.5.1.2 255.255.0.0 E(config-if-FastEthernet 0/1)# exit E(config)# router bgp 65532 E(config-router)# neighbor 10.4.1.2 remote-as 65530 E(config-router)# redistribute connected
Проверка	Запустите команду **show**, чтобы отобразить информацию
A	A# show ip bgp summary BGP router identifier 10.2.1.1, local AS number 65530 BGP table version is 9 2 BGP AS-PATH entries 0 BGP Community entries 3 BGP Prefix entries (Maximum-prefix:4294967295) Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 172.16.23.140 4 65530 29 25 8 0 0 00:18:48 2 172.16.23.141 4 65530 24 21 8 0 0 00:17:58 2

```
A# show ip bgp
BGP table version is 9, local router ID is 10.2.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
        S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop        Metric     LocPrf     Weight Path
*>i10.3.0.0/16   10.3.1.1        0          100        0 65531?
*>i10.4.0.0/16   10.4.1.1        0          100        0 65532 ?
* i10.5.0.0/16   10.3.1.1        0          100        0 65531?
*>i              10.4.1.1        0          100        0 65532 ?

Total number of prefixes 3
A# show ip bgp 10.5.0.0
BGP routing table entry for 10.5.0.0/16
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  65532
  10.4.1.1 from 10.2.1.2 (172.16.24.1)
  Origin incomplete, metric 0, localpref 100, valid, internal, multipath, best
  Last update: Mon Mar 21 03:45:14 2011

65531
  10.3.1.1 from 10.1.1.2 (172.16.25.1)
  Origin incomplete, metric 0, localpref 100, valid, internal, multipath
  Last update: Mon Mar 21 03:45:14 2011

A# show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
```

```
Gateway of last resort is no set
C 10.1.0.0/16 is directly connected, FastEthernet 0/0
C 10.1.1.1/32 is local host.
C 10.2.0.0/16 is directly connected, FastEthernet 0/1
C 10.2.1.1/32 is local host.
S 10.3.0.0/16 [1/0] via 10.1.1.2
S 10.4.0.0/16 [1/0] via 10.2.1.2
B 10.5.0.0/16 [200/0] via 10.3.1.1, 00:27:56
        [200/0] via 10.4.1.1, 00:27:56
```

7.4.5.7. Распространенные ошибки

Приоритеты multi-hop маршрутов BGP различаются, что приводит к сбою балансировки нагрузки.

7.4.6. Настройка EBGP FRR

7.4.6.1. Эффект конфигурации

Внедряет EBGP FRR.

7.4.6.2. Примечания

(Опционально) Настройте сеанс соседа BFD для реализации быстрого обнаружения ошибок канала.

7.4.6.3. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка BGP FRR

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка сеанса соседа BFD

(Опционально) Выполните эту настройку в режиме настройки BGP.

7.4.6.4. Проверка

Запустите команду **show**, чтобы отобразить информацию о маршрутизации.

7.4.6.5. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Настройка BGP FRR

Команда	**bgp fast-reroute**
Командный режим	Режим конфигурации BGP

Создание соседа BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*neighbor-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *as-number*: указывает номер AS peer-a BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	AS, указанная для peer-a (группы), должна совпадать с номером AS BGP спикера BGP на peer end-e

Создание сеанса BFD с соседом BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **fall-over bfd**
Описание параметра	*neighbor-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов
Командный режим	Режим конфигурации BGP

7.4.6.6. Пример конфигурации

Настройка EBGP FRR

Сценарий:

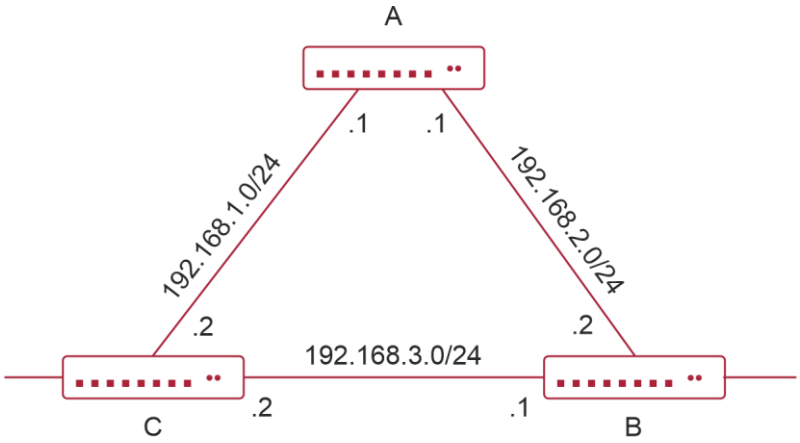


Рисунок 7-9.

Шаги настройки	• Включите BGP на всех устройствах. • Настройте адреса напрямую подключенных интерфейсов на A, B и C, чтобы установить соседство EBGP. • Настройте сеанс BFD для соседства EBGP между B и C. • Настройте FRR на C
A	A# conf terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# exit A(config)# interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0 A(config-if-GigabitEthernet 0/2)# exit A(config)# router bgp 100 A(config-router)# neighbor 192.168.1.2 remote-as 300 A(config-router)# neighbor 192.168.2.2 remote-as 200 A(config-router)# redistribute connect
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip address 192.168.3.1 255.255.255.0 B(config-if-GigabitEthernet 0/1)# bfd interval 200 min_rx 200 multiplier 5

	B(config-if-GigabitEthernet 0/1)# exit B(config)# interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)# ip address 192.168.2.2 255.255.255.0 B(config-if-GigabitEthernet 0/2)# exit B(config)# router bgp 200 B(config-router)# neighbor 192.168.3.2 remote-as 300 B(config-router)# neighbor 192.168.3.2 fall-over bfd B(config-router)# neighbor 192.168.2.1 remote-as 100 B(config-router)# redistribute connect
C	C# configure terminal C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface fastEthernet 0/2 C(config-if-GigabitEthernet 0/2)# ip address 192.168.3.2 255.255.0.0 C(config-if-GigabitEthernet 0/2)# bfd interval 200 min_rx 200 multiplier 5 C(config-if-GigabitEthernet 0/2)# exit C(config)# router bgp 300 C(config-router)# neighbor 192.168.1.1 remote-as 100 C(config-router)# neighbor 192.168.3.1 remote-as 200 C(config-router)# neighbor 192.168.3.1 fall-over bfd C(config-router)# address-family ipv4 unicast C(config-router-af)# bgp fast-reroute C(config-router-af)# redistribute connect
Проверка	Запустите команду **show**, чтобы отобразить информацию
C	C# show ip bgp summary BGP router identifier 10.10.10.10, local AS number 300 BGP table version is 12 4 BGP AS-PATH entries 0 BGP Community entries 3 BGP Prefix entries (Maximum-prefix:4294967295)

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
192.168.1.1	4	100	76	77	12	12	0	00:59:27	3
192.168.3.1	4	200	30	30	12	12	0	00:19:03	3

Total number of neighbors 2

C# show ip bgp

BGP table version is 12, local router ID is 10.10.10.10

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale, b - backup entry

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* 192.168.1.0	192.168.3.1	0	0	200	?
* 192.168.1.1	0	0	100	?	
*> 0.0.0.0	0	32768	?		
*> 192.168.2.0	192.168.3.1	0	0	200	?
*b 192.168.1.1	0	0	100	?	
* 192.168.3.0	192.168.3.1	0	0	200	?
* 192.168.1.1	0	0	100	200	?
*> 0.0.0.0	0	32768	?		

Total number of prefixes 3

C# show ip bgp 192.168.2.0

BGP routing table entry for 192.168.2.0/24

Paths: (2 available, best #1, table Default-IP-Routing-Table)

Advertised to non peer-group peers:

192.168.1.1

200

192.168.3.1 from 192.168.3.1 (3.3.3.3)

Origin incomplete, metric 0, localpref 100, valid, external, best

Last update: Tue Oct 5 00:26:52 1971

100

	192.168.1.1 from 192.168.1.1 (44.44.44.44) Origin incomplete, metric 0, localpref 100, valid, external, backup Last update: Mon Oct 4 23:46:28 1971 C# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 192.168.1.0/24 is directly connected, GigabitEthernet 1/9 C 192.168.1.2/32 is local host. B 192.168.2.0/24 [20/0] via 192.168.3.1, 00:21:39 C 192.168.3.0/24 is directly connected, GigabitEthernet 1/11 C 192.168.3.2/32 is local host

7.4.6.7. Распространенные ошибки

Для соседей BGP не настроен сеанс BFD.

7.4.7. Настройка быстрого изымания указанных маршрутов BGP

7.4.7.1. Эффект конфигурации

Реализуйте быстрое изымание указанных маршрутов BGP.

7.4.7.2. Примечания

Настройте быстрое изымание указанных маршрутов, чтобы предпочтительно объявлять изымание указанных маршрутов.

7.4.7.3. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка быстрого изымания указанных маршрутов BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

7.4.7.4. Проверка

Запустите команду **show**, чтобы отобразить конфигурации.

7.4.7.5. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS. Значение варьируется от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Настройка быстрого изымания указанных маршрутов BGP

Команда	**bgp fast-withdraw** { **access-list** { *access-list-number* | *access-list-name* } | **prefix-list** *prefix-list-name* | **route-map** *map-tag* }
Описание параметра	*access-list-number*: указывает номер ACL. Значение варьируется от 1 до 199 и от 1300 до 2699. *access-list-name*: указывает имя ACL. *prefix-list-name*: указывает имя списка префиксов. *map-tag*: указывает имя карты маршрутов
Командный режим	Режим конфигурации BGP

Создание соседа BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*neighbor-address*: указывает адрес peer-а. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, содержащее не более 32 символов. *as-number*: указывает номер AS peer-а BGP (группы). Значение варьируется от 1 до 4 294 967 295
Командный режим	Режим конфигурации BGP
Руководство по использованию	Номер AS, указанный для peer-а (группы), должен совпадать с номером AS BGP спикера BGP на peer end-е

7.4.7.6. Пример конфигурации

Настройка быстрого изымания указанных маршрутов BGP

Сценарий:



Рисунок 7-10.

Шаги настройки	• Включите BGP на всех устройствах. • Установите отношения соседства BGP между маршрутизаторами A и B. • Настройте ACL на маршрутизаторе A. • Настройте быстрое изымание указанных маршрутов на маршрутизаторе A
A	A# conf terminal
Проверка	Запустите команду **show**, чтобы отобразить конфигурации
A	A#show run router bgp

7.4.8. Настройка локальных AS

7.4.8.1. Эффект конфигурации

Плавно перенесите сетевые конфигурации маршрутизатора A с AS 23 на AS 3600.

7.4.8.2. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка локальной AS для соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

7.4.8.3. Проверка

Запустите команду **show**, чтобы отобразить информацию.

7.4.8.4. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Создание соседа BGP

Команда	**neighbor** { *peer-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*peer-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *as-number*: указывает номер AS peer-a BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	AS, указанная для peer-a (группы), должна совпадать с номером AS BGP спикера BGP на peer end-e

Настройка локальной AS для соседа BGP

Команда	**neighbor** { *peer-address* | *peer-group-name* } **local-as** *as-number* [**no-prepend** [**replace-as** [**dual-as**]]]
Описание параметра	*peer-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *as-number*: указывает локальный номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме. **no-prepend**: не добавляет локальную AS к AS-PATH в информации о маршрутизации, полученной peer-ом. Эта опция недоступна по умолчанию. **replace-as**: для AS-PATH в информации о маршрутизации, отправленной peer-ом, вместо BGP AS используется локальная AS. Эта опция недоступна по умолчанию.

	dual-as: позволяет peer-у использовать BGP AS или Local AS для установки соединения BGP с устройством. Эта опция недоступна по умолчанию
Командный режим	Режим конфигурации BGP

7.4.8.5. Пример конфигурации

Настройка BGP Local-AS

Сценарий:

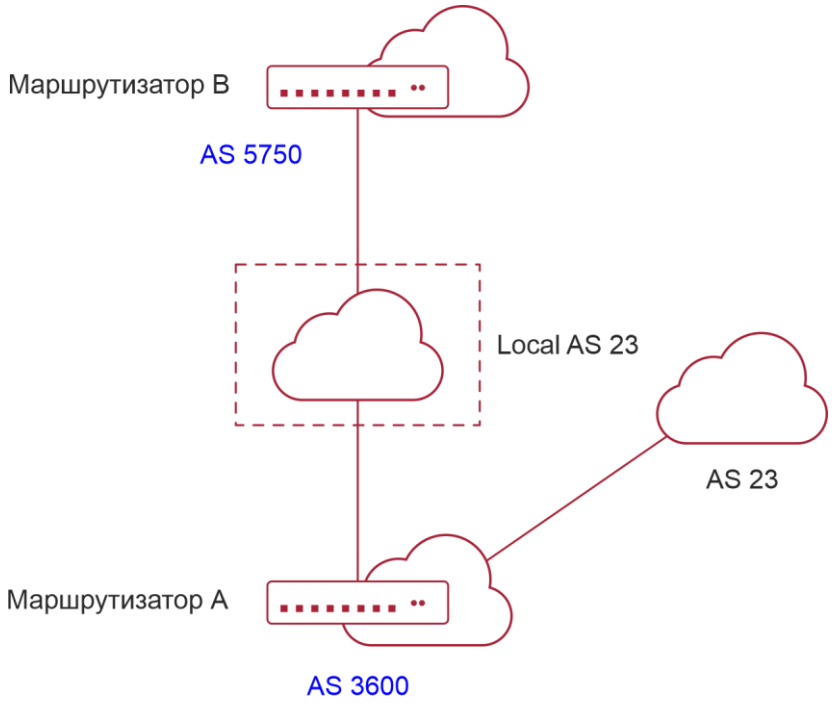


Рисунок 7-11.

Шаги настройки	• Создайте соседство EBGP с B на A и укажите Local-AS для соседства EBGP. • Создайте соседство EBGP для подключения к A на B
A	A# configure terminal A(config)# router bgp 3600 A(config-router)# neighbor 57.50.1.1 remote-as 5750 A(config-router)# neighbor 57.50.1.1 update-source loopback 0 A(config-router)# neighbor 57.50.1.1 ebgp-multihop 255

	A(config-router)# neighbor 57.50.1.1 local-as 23 no-prepend replace-as dual-as
B	B# configure terminal B(config)# router bgp 5750 B(config-router)# neighbor 36.0.1.1 remote-as 23 B(config-router)# neighbor 36.0.1.1 update-source loopback 0 B(config-router)# neighbor 36.0.1.1 ebgp-multihop 255
Проверка	Запустите команду **show**, чтобы отобразить статус соседа BGP
A	A# show ip bgp neighbors 57.50.1.1 BGP neighbor is 57.50.1.1, remote AS 5750, local AS 23(using Peer-s Local AS, noprepend, replace-as, dual-as), external link BGP version 4, remote router ID 0.0.0.0 BGP state = Idle Last read, hold time is 180, keepalive interval is 60 seconds Received 0 messages, 0 notifications, 0 in queue open message:0 update message:0 keepalive message:0 refresh message:0 dynamic cap:0 notifications:0 Sent 0 messages, 0 notifications, 0 in queue

7.4.9. Настройка BGP GR

7.4.9.1. Эффект конфигурации

Настройте BGP GR для реализации развертывания сети с высокой надежностью.

7.4.9.2. Примечания

- Чтобы успешно развернуть функцию BGP GR, вам необходимо использовать соседнее устройство в качестве GR Helper.
- В среде BGP также необходимо настроить IGP GR.
- После включения BGP GR вам необходимо сбросить соседнее соединение BGP, чтобы оно вступило в силу.

7.4.9.3. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Настройка BGP GR

Выполните эту настройку в режиме настройки BGP, который настроен по умолчанию.

Настройка таймера BGP GR

(Опционально) Выполните эту настройку в режиме настройки BGP.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

7.4.9.4. Проверка

Запустите команду **show**, чтобы отобразить статус соседа.

7.4.9.5. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Настройка BGP GR

Команда	**bgp graceful-restart**
Командный режим	Режим конфигурации BGP

Настройка таймера перезапуска BGP GR

Команда	**bgp graceful-restart restart-time** *restart-time*
Описание параметра	*restart-time*: указывает максимальное время ожидания, которое GR Restarter ожидает от GR Helper перед созданием нового соединения, в диапазоне от 1 до 3600 секунд
Командный режим	Режим конфигурации BGP

Настройка таймера Route Stale BGP GR

Команда	**bgp graceful-restart stalepath-time** *time*
Описание параметра	*time*: указывает максимальное время, в течение которого устаревший (stale) маршрут остается действительным после восстановления соединения с соседним устройством GR, в диапазоне от 1 до 3600 секунд

Командный режим	Режим конфигурации BGP

Создание соседа BGP

Команда	**neighbor** { *peer-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*peer-address*: указывает адрес peer-а. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *as-number*: указывает номер AS peer-а BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	AS, указанная для peer-а (группы), должна совпадать с номером AS BGP спикера BGP на peer end-е

7.4.9.6. Пример конфигурации

Настройка BGP GR

Сценарий:

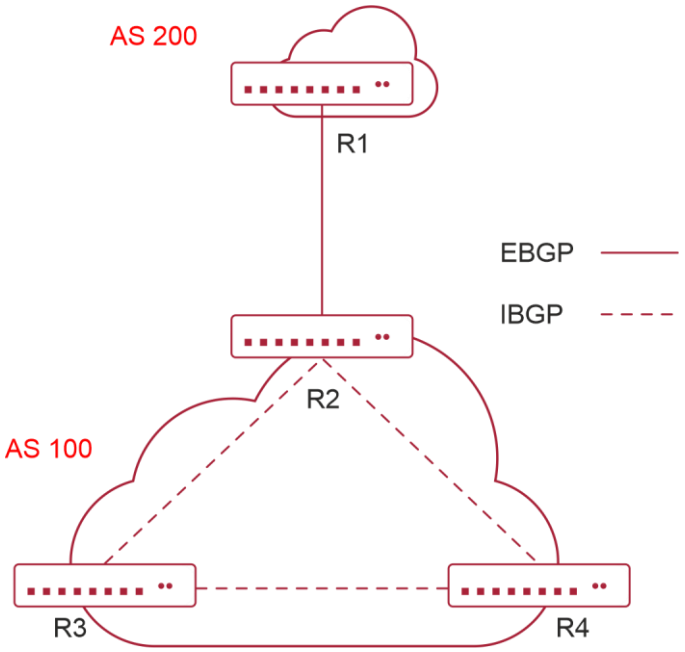


Рисунок 7-12.

Шаги настройки	• Включите BGP на всех устройствах и установите номера AS, как показано на Рисунке 7-12. • Настройте loopback-интерфейс на маршрутизаторах R2, R3 и R4 и создайте соседство IBGP на основе loopback-интерфейса. • Создайте соседство EBGP, используя напрямую подключенные интерфейсы на R1 и R2. • Включите BGP GR на маршрутизаторах R1, R2, R3 и R4
R1	R1# configure terminal R1(config-router)# exit R1(config)# router bgp 100 R1(config-router)# bgp graceful-restart
R2	R2# configure terminal R2(config)# router ospf 1 R2(config-router)# graceful-restart R2(config-router)# exit R2(config)# router bgp 100 R2(config-router)# bgp graceful-restart
R3	R3# configure terminal R3(config)# router ospf 1 R3(config-router)# graceful-restart R3(config-router)# exit R3(config)# router bgp 100 R3(config-router)# bgp graceful-restart
R4	R4# configure terminal R4(config)# router ospf 1 R4(config-router)# graceful-restart R4(config-router)# exit R4(config)# router bgp 100 R4(config-router)# bgp graceful-restart
Проверка	Запустите команду **show**, чтобы отобразить статус соседа BGP
R2	R2# show ip ospf Routing Process "ospf 1" with ID 10.0.0.2

	Process uptime is 4 minutes Process bound to VRF default Conforms to RFC2328, and RFC1583Compatibility flag isenabled Supports only single TOS(TOS0) routes Supports opaque LSA This router is an ASBR (injecting external routing information) SPF schedule delay 5 secs, Hold time between two SPFs 10 secs LsaGroupPacing: 240 secs Number of incomming current DD exchange neighbors 0/5 Number of outgoing current DD exchange neighbors 0/5 Number of external LSA 4. Checksum 0x0278E0 Number of opaque AS LSA 0. Checksum 0x000000 Number of non-default external LSA 4 External LSA database is unlimited. Number of LSA originated 6 Number of LSA received 2 Log Neighbor Adjency Changes : Enabled Graceful-restart enabled Graceful-restart helper support enabled Number of areas attached to this router: 1 Area 0 (BACKBONE) ..... R2# show ip bgp neighbors BGP neighbor is 192.168.195.183, remote AS 200, local AS 100, external link BGP version 4, remote router ID 10.0.0.1 BGP state = Established, up for 00:06:37 Last read 00:06:37, hold time is 180, keepalive interval is 60 seconds Neighbor capabilities: Route refresh: advertised and received (old and new) Address family IPv4 Unicast: advertised and received Graceful restart: advertised and received Remote Restart timer is 120 seconds Address families preserved by peer: None .....

7.4.9.7. Распространенные ошибки

- GR не включен для IGP.
- GR не включен для соседнего устройства BGP.

7.4.10. Настройка семейства адресов BGP IPv6

7.4.10.1. Эффект конфигурации

Настройте маршруты BGP IPv6 для реализации доступа к сети IPv6 в разных AS.

7.4.10.2. Примечания

- Обычно BGP использует адреса IPv6 для создания соседств и реализации обмена маршрутами IPv6.
- Конфигурации, связанные с сервисами BGP IPv6, должны быть настроены в режиме семейства адресов BGP IPv6.

7.4.10.3. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка режима семейства IPv4-адресов BGP

(Опционально) Выполните эту настройку в режиме настройки BGP.

Отключение возможности семейства адресов IPv4 для соседа BGP

(Опционально) Выполните эту настройку в режиме настройки BGP IPv6.

Настройка режима семейства IPv6-адресов BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка возможностей семейства адресов IPv6 для соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP IPv6.

Настройка объявления маршрута IPv6 в BGP

(Опционально) Выполните эту настройку в режиме настройки BGP IPv6.

7.4.10.4. Проверка

- Запустите команду **show**, чтобы отобразить статус соседа.
- Запустите команду **show**, чтобы отобразить статус маршрутизации.

7.4.10.5. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме

Командный режим	Режим глобальной конфигурации

Создание соседа BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*neighbor-address*: указывает адрес peer-a, который обычно является адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *as-number*: указывает номер AS peer-a BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	AS, указанная для peer-a (группы), должна совпадать с номером AS BGP спикера BGP на peer end-e

Настройка режима семейства IPv4-адресов BGP

Команда	**address-family ipv4 unicast**
Командный режим	Режим конфигурации BGP

Отключение возможности семейства адресов IPv4 для соседа BGP

Команда	**no neighbor** { *neighbor-address* | *peer-group-name* } **activate**
Описание параметра	*neighbor-address*: указывает адрес peer-a, который обычно является адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов
Командный режим	Режим семейства адресов BGP IPv4
Руководство по использованию	Соседи с адресами IPv6 используются для обмена маршрутами IPv6. Однако если сосед настроен в режиме BGP, BGP автоматически активирует для соседа возможность семейства unicast-адресов IPv4. Поэтому рекомендуется вручную отключить возможность семейства unicast-адресов IPv4

Настройка режима семейства IPv6-адресов BGP

Команда	**address-family ipv6 unicast**
Командный режим	Режим конфигурации BGP

Настройка возможностей семейства адресов IPv6 для соседа BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **activate**
Описание параметра	*neighbor-address*: указывает адрес peer-а, который обычно является адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов
Командный режим	Семейный режим адресов BGP IPv6

Настройка объявления маршрута IPv6 в BGP

Команда	**network** *network-number* [**mask** *mask*] [**route-map** *map-tag*] [**backdoor**]
Описание параметра	*network-number*: указывает номер сети. *mask*: указывает маску подсети. *map-tag*: указывает название карты маршрутов, состоящее не более чем из 32 символов. **backdoor**: указывает, что маршрут является маршрутом backdoor
Командный режим	Режим семейства адресов BGP IPv6

7.4.10.6. Пример конфигурации

Настройка BGP для реализации обмена маршрутами IPv6 в разных AS

Сценарий:



Рисунок 7-13.

Шаги настройки	• Включите BGP на всех устройствах и установите номера AS, как показано на Рисунке 7-13. • Настройте соседа BGP, отключите для него возможность семейства адресов IPv4 и активируйте возможность семейства адресов IPv6. • Настройте объявление маршрута IPv6 в BGP
A	A# configure terminal A(config)# int loopback 0 A(config-if-Loopback)# ipv6 address 30::1/128 A(config-if-Loopback)# exit A(config)# router bgp 65530 A(config-router)# neighbor 100::1 remote-as 65531 A(config-router)# address-family ipv4 A(config-router-af)# no neighbor 100::1 activate A(config-router-af)# exit-address-family A(config-router)# address-family ipv6 A(config-router-af)# neighbor 100::1 activate A(config-router-af)# network 30::1/128
B	B# configure terminal B(config)# router bgp 65531 B(config-router)# neighbor 100::2 remote-as 65530 B(config-router)# address-family ipv4 B(config-router-af)# no neighbor 100::2 activate B(config-router-af)# exit-address-family B(config-router)# address-family ipv6 B(config-router-af)# neighbor 100::2 activate
Проверка	Запустите команду **show**, чтобы отобразить статус соседа BGP
A	A# show bgp ipv6 unicast summary BGP router identifier 1.1.1.1, local AS number 65530 BGP table version is 1 1 BGP AS-PATH entries 0 BGP Community entries 1 BGP Prefix entries (Maximum-prefix:4294967295)

	Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 100::1 4 65531 4 6 1 0 0 00:01:49 0 Total number of neighbors 1
B	Запустите команду **show**, чтобы отобразить информацию о маршрутизации BGP. B# show bgp ipv6 unicast BGP table version is 4, local router ID is 2.2.2.2 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale, b - backup entry Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path *> 30::1/128 100::2 0 0 65530 i Total number of prefixes 1

7.4.10.7. Распространенные ошибки

- Возможность семейства адресов IPv6 не активирована для соседей BGP.
- В сценариях, отличных от 6PE, адреса IPv4 используются для установления маршрутов IPv6 для обмена между соседями.

7.4.11. Настройка BGP EVPN

7.4.11.1. Примечания

По умолчанию режим маршрутизации BGP находится в семействе unicast-адресов IPv4, а BGP EVPN необходимо настроить в режиме семейства адресов L2VPN EVPN.

7.4.11.2. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Активация возможности EVPN для соседа BGP

(Обязательно) Выполните эту настройку в режиме семейства адресов BGP L2VPN EVPN.

Создание экземпляра EVI

(Обязательно) Выполните эту настройку в режиме настройки EVPN.

Пакетное создание экземпляров EVI

(Опционально) Выполните эту настройку в режиме настройки EVPN.

Создание RD

(Обязательно) Выполните эту настройку в режиме настройки EVPN-VNI.

Создание цели маршрута

(Обязательно) Выполните эту настройку в режиме настройки EVPN-VNI.

Настройка карты маршрутов для экземпляра EVI

(Опционально) Выполните эту настройку в режиме семейства адресов EVPN-VNI.

Настройка параметров мобильности MAC

(Опционально) Выполните эту настройку в режиме конфигурации BGP L2VPN EVPN.

7.4.11.3. Проверка

Запустите команду **show**, чтобы отобразить информацию.

7.4.11.4. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Создание соседа BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*neighbor-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *as-number*: указывает номер AS peer-a BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	AS, указанная для peer-a (группы), должна совпадать с номером AS BGP спикера BGP на peer end-e

Вход в семейство адресов L2VPN EVPN

Команда	**address-family l2vpn evpn**
Командный режим	Режим конфигурации BGP

Активация возможности EVPN для соседа BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **activate**
Описание параметра	*neighbor-address*: указывает адрес peer-а. Этот адрес должен быть адресом IPv4. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов
Командный режим	Режим семейства адресов BGP L2VPN EVPN

Создание экземпляра EVI

Команда	**vni** *vni-id*
Описание параметра	*vni-id*: указывает идентификатор VNI. Диапазон от 1 до16 777 215
Командный режим	Режим конфигурации EVPN
Руководство по использованию	После завершения настройки VNI необходимо настроить соответствующий RD/RT

Пакетное создание экземпляров EVI

Команда	**vni range** *vni-id-list*
Описание параметра	*vni-id-list*: указывает имя списка идентификаторов VNI
Командный режим	Режим конфигурации EVPN
Руководство по использованию	Конфигурация завершается сбоем, если количество настроенных экземпляров VNI превышает емкость или экземпляр VNI удаляется. Значения RD разных экземпляров VNI должны быть разными. Таким образом, для пакетной настройки экземпляров VNI доступен только

	режим автоматической настройки RD, а экземпляры VNI нельзя настроить вручную

Настройка RD

Команда	**rd** { **auto** | *rd_value* }
Описание параметра	**auto**: автоматически генерирует значение RD. *rd_value*: указывает значение RD. Параметр *rd_value* имеет три формы: (1) rd_value = as_num:nn **as_num** указывает 2-байтовый общедоступный (public) номер AS. **nn** определяется пользователем и находится в диапазоне от 0 до 4 294 967 295. (2) rd_value = ip_addr:nn **ip_add** относится к глобальному IP-адресу. **nn** определяется пользователем и находится в диапазоне от 0 до 65 535. (3) rd_value = as4_num:nn **as4_num** указывает 4-байтовый общедоступный (public) номер AS. **nn** определяется пользователем и находится в диапазоне от 1 до 65 535. 4-байтовый номер AS находится в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим конфигурации EVPN VNI
Руководство по использованию	Если EVI определен и для него настроено значение RD, значение RD невозможно изменить. Чтобы изменить его, необходимо сначала удалить EVI, а затем снова определить EVI и настроить для него новое значение RD. Один EVI имеет только одно значение RD. **ПРИМЕЧАНИЕ:** значение RD 4-байтового AS имеет формат **AS4:NN**. **AS4** может быть выражено в десятичном или точечном виде. **AS4** находится в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме. **NN** находится в диапазоне от 1 до 65 535. **ПРИМЕЧАНИЕ:** номер AS в диапазоне от 1 до 65 535 отображается одинаково как в десятичном, так и в точечном режиме. Поэтому сохраните номер AS в диапазоне от 1 до 65 535 как 2-байтовый номер AS. **ПРИМЕЧАНИЕ:** автоматически создаваемое значение RD имеет формат **ip_addr:nn**. **ip_addr** указывает идентификатор маршрутизатора BGP, а **nn** указывает идентификатор VNI. Поскольку идентификатор VNI занимает максимум три байта, а для nn доступно

	только два байта, то, когда идентификатор VNI занимает более 2 байтов, идентификатор VNI разделяется перед заполнением позиции для **nn**. После создания значение RD остается неизменным

Настройка цели маршрута

Команда	**route-target** { **import** | **export** | **both** } { **auto** | *rt_value* }
Описание параметра	**import**: указывает значение импорта RT. **export**: указывает значение экспорта RT. **both**: определяет значения RT для импорта и экспорта. **auto**: автоматически генерирует значение RT. *rt_value*: указывает значение RT. Параметр *rt_value* имеет три формы: (1) rt_value = as_num:nn **as_num** указывает 2-байтовый общедоступный (public) номер AS. **nn** определяется пользователем и находится в диапазоне от 0 до 4 294 967 295. (2) rt_value = ip_addr:nn **ip_add** относится к глобальному IP-адресу. **nn** определяется пользователем и находится в диапазоне от 0 до 65 535. (3) rt_value = as4_num:nn **as4_num** указывает 4-байтовый общедоступный (public) номер AS. **nn** определяется пользователем и находится в диапазоне от 1 до 65 535. 4-байтовый номер AS находится в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим конфигурации EVPN VNI
Руководство по использованию	Один EVI поддерживает несколько значений импорта и экспорта RT. **ПРИМЕЧАНИЕ:** автоматически создаваемое значение RT имеет формат **AS2:nn**. **AS2** указывает 2-байтовый номер AS. Если используется 4-байтовый номер AS, он разделяется, и две 2-байтовые части заполняются в позиции для **nn**, а другая 2-байтовая часть заполняется в позиции для значения RT. **nn** указывает идентификатор VNI. Для размещения 3-байтового идентификатора VNI предусмотрено четыре байта пространства. **ПРИМЕЧАНИЕ:** если номер BGP AS изменится, автоматически сгенерированное значение RT также будет изменено. **ПРИМЕЧАНИЕ:** если вручную настроенное значение RT соответствует автоматически сгенерированному, отображаются оба значения. Если автоматически сгенерированное значение RT равно 100:1, он

	напрямую удаляется. Удаление этого значения не отменяет **auto** режима конфигурации. Чтобы отменить **auto** режима конфигурации запустите форму **no** для команды **route-target auto**

Настройка карты маршрутов для экземпляров EVI

Команда	**export map** *routemap-name*
Описание параметра	*routemap-name*: указывает имя карты маршрутов
Командный режим	Режим конфигурации EVPN VNI
Руководство по использованию	Эта команда используется для изменения атрибута расширенного сообщества, объявленного маршрутом типа 5, преобразованным из локального маршрута EVPN или IP-маршрута. Эта команда поддерживает только одну карту маршрутов, и старая конфигурация заменяется новой

Команда	**import map** *routemap-name*
Описание параметра	*routemap-name*: указывает имя карты маршрутов
Командный режим	Режим конфигурации EVPN VNI
Руководство по использованию	Эта команда используется для фильтрации удаленных (remote) маршрутов EVPN, которые будут импортированы в локальный экземпляр VNI, или для изменения атрибута удаленных маршрутов EVPN, импортированных в локальный экземпляр VNI. Эта команда поддерживает только одну карту маршрутов, и старая конфигурация заменяется новой

Настройка параметров мобильности MAC

Команда	**bgp mac-mobility** *timer count*
Описание параметра	*timer*: указывает продолжительность таймера (в секундах) для обнаружения мобильности MAC. Если в течение этого периода обнаружено несколько перемещений MAC-адресов, считается, что произошел конфликт MAC, и для предупреждения пользователей отображаются системные журналы. По умолчанию значение равно 180 и находится в диапазоне от 1 до 3600.

	count: указывает количество обнаружений. По умолчанию значение равно 5 и находится в диапазоне от 1 до 360
Командный режим	Режим семейства адресов BGP L2VPN EVPN
Руководство по использованию	Один MAC-адрес может меняться много раз. Когда PE обнаруживает перемещение MAC-адреса посредством локального изучения, включается таймер в секундах (значение по умолчанию = 180 с). Если количество перемещений MAC-адреса (значение по умолчанию = 5) обнаружено до истечения времени таймера, считается, что произошел конфликт MAC

7.4.11.5. Пример конфигурации

Настройка семейства адресов BGP EVPN

Сценарий:

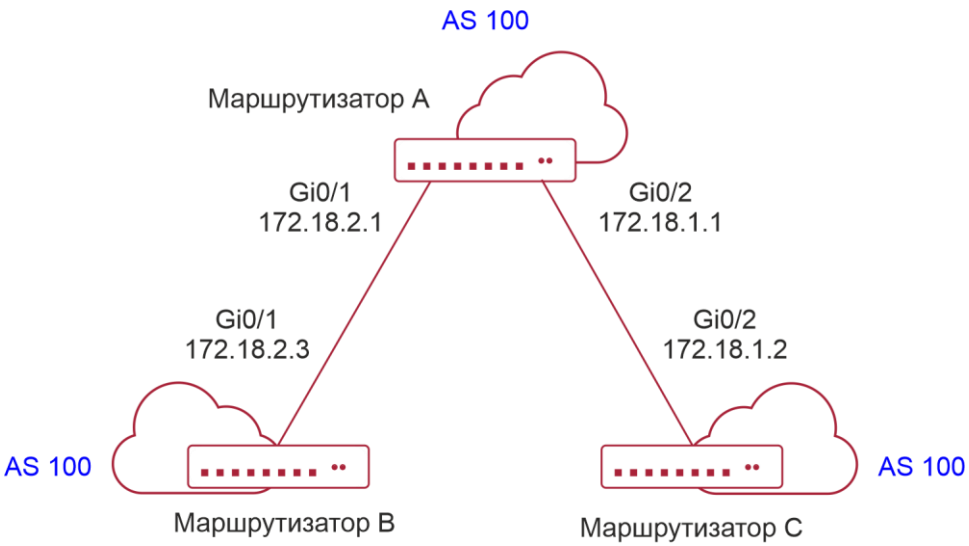


Рисунок 7-14.

Шаги настройки	• Включите BGP на всех устройствах и установите номера AS, как показано на Рисунке 7-14. • Настройте соседство BGP, как показано на Рисунке 7-14. • Активируйте возможность семейства адресов L2VPN EVPN для соседей BGP
A	A# config terminal A(config)# interface gigabitEthernet 0/1 A(config-GigabitEthernet 0/1)# no shutdown

	A(config-GigabitEthernet 0/1)# ip address 172.18.2.1 255.255.255.0 A(config-GigabitEthernet 0/1)# exit A(config)# interface gigabitEthernet 0/2 A(config-GigabitEthernet 0/1)# no shutdown A(config-GigabitEthernet 0/1)# ip address 172.18.1.1 255.255.255.0 A(config-GigabitEthernet 0/1)# exit A(config)# router bgp 100 A(config-router)# neighbor 172.18.2.3 remote-as 100 A(config-router)# neighbor 172.18.1.2 remote-as 100 A(config-router)# address-family l2vpn evpn A(config-router-af)# neighbor 172.18.2.3 activate A(config-router-af)# neighbor 172.18.1.2 activate A(config-router-af)# neighbor 172.18.2.3 route-reflector-client A(config-router-af)# neighbor 172.18.1.2 route-reflector-client A(config-router-af)# exit-address-family
B	B# config terminal B(config)# evpn B(config-evpn)# vni 100 B(config-evpn-vni)# rd auto B(config-evpn-vni)# route-target both auto B(config-evpn-vni)# exit B(config-evpn)# exit B(config)# interface gigabitEthernet 0/1 B(config-GigabitEthernet 0/1)# no shutdown B(config-GigabitEthernet 0/1)# ip address 172.18.2.3 255.255.255.0 B(config-GigabitEthernet 0/1)# exit B(config)# router bgp 100 B(config-router)# neighbor 172.18.2.1 remote-as 100 B(config-router)# address-family l2vpn evpn B(config-router-af)# neighobr 172.18.2.1 activate B(config-router-af)# exit-address-family
C	То же, что и для B
Проверка	Запустите команду **show**, чтобы отобразить информацию

A

```
A#sh bgp l2vpn evpn all summary
For address family: L2VPN EVPN
BGP router identifier 3.3.3.3, local AS number 100
BGP table version is 51
1 BGP AS-PATH entries
0 BGP Community entries
6 BGP Prefix entries (Maximum-prefix:4 294 967 295)

Neighbor        V  AS    MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down
State/PfxRcd
172.18.2.3      4  100   1993     2033     49      0    0     1d04h40m
                3
172.18.1.2      4  100   619      623      51      0    0     08:47:26
                3

Total number of neighbors 2

A#sh bgp l2vpn evpn all
BGP table version is 51, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale, b - backup entry
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric     LocPrf     Weight Path
Route Distinguisher: 1.1.1.1:100
*>i0:6:0011.2233.2016:0:0.0.0.0/128
                 1.1.1.1 0        100          0      i
*>i0:6:0011.2233.2016:32:100.1.1.2/128
                1.1.1.1    0         100      0         i
*>i0:32:1.1.1.1/72 1.1.1.1 0 100 0 i

Total number of prefixes 3
Route Distinguisher: 2.2.2.2:100
*>i0:6:08c6.b322.33df:0:0.0.0.0/128
                2.2.2.2  0         100      0         i
*>i0:6:08c6.b322.33df:32:100.1.1.1/128
```

	2.2.2.2 0 100 0 i *>i0:32:2.2.2.2/72 2.2.2.2 0 100 0 i Total number of prefixes 3
B	B#sh bgp l2vpn evpn all summary For address family: L2VPN EVPN BGP router identifier 1.1.1.1, local AS number 100 BGP table version is 16 1 BGP AS-PATH entrieswww.qtech.ru 0 BGP Community entries 6 BGP Prefix entries (Maximum-prefix:4 294 967 295) Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 172.18.2.1 4 100 639 625 16 0 0 08:55:10 3 Total number of neighbors 1 B#sh bgp l2vpn evpn all BGP table version is 16, local router ID is 1.1.1.1 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale, b - backup entry Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path Route Distinguisher: 1.1.1.1:100 (Default for EVI 100) *> 0:6:0011.2233.2016:0:0.0.0.0/128 0.0.0.0 32768 i *>i0:6:08c6.b322.33df:0:0.0.0.0/128 2.2.2.2 0 100 0 i *> 0:6:0011.2233.2016:32:100.1.1.2/128 0.0.0.0 32768 i *>i0:6:08c6.b322.33df:32:100.1.1.1/128 2.2.2.2 0 100 0 i

	*> 0:32:1.1.1.1/72 0.0.0.0 32768 i *>i0:32:2.2.2.2/72 2.2.2.2 0 100 0 i Total number of prefixes 6

7.4.11.6. Распространенные ошибки

- Сосед семейства адресов L2VPN EVPN не настроен.
- Возможность семейства адресов EVPN не активируется для соседей BGP.

7.4.12. Настройка соединения с устройствами, поддерживающими только 2-байтовые номера AS

7.4.12.1. Эффект конфигурации

Успешно соединяет устройства, поддерживающие 4-байтовые номера AS, с устройствами, поддерживающими только 2-байтовые номера AS.

7.4.12.2. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка режима отображения 4-байтового номера AS

(Опционально) Выполните эту настройку в режиме настройки BGP. По умолчанию 4-байтовый номер AS отображается в виде десятичных цифр.

7.4.12.3. Проверка

Запустите команду **show**, чтобы отобразить статус соседа.

7.4.12.4. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Создание соседа BGP

Команда	**neighbor** { *peer-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*peer-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *as-number*: указывает номер AS peer-a BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	AS, указанная для peer-a (группы), должна совпадать с номером AS BGP спикера BGP на peer end-e

Настройка режима отображения 4-байтового номера AS BGP

Команда	**bgp asnotation dot**
Командный режим	Режим конфигурации BGP

7.4.12.5. Пример конфигурации

Настройка совместимости между устройствами BGP, поддерживающими 4-байтовые номера AS и 2-байтовые номера AS

Сценарий:

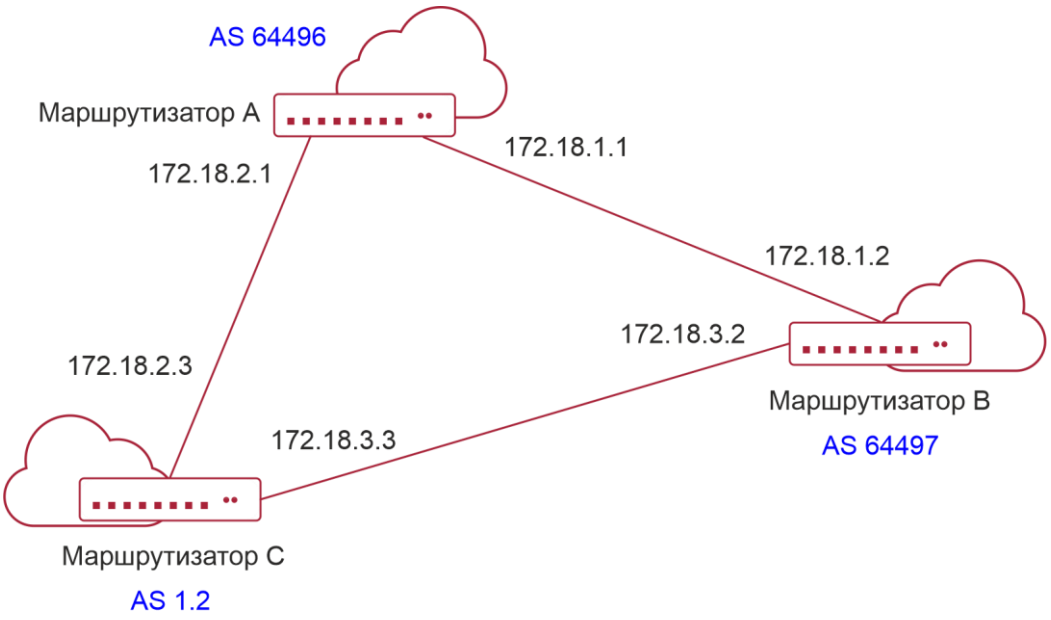


Рисунок 7-15.

Шаги настройки	• Включите BGP на всех устройствах и установите номера AS, как показано на Рисунке 7-15. • Настройте соседство BGP
A	A# configure terminal A(config)# router bgp 64496 A(config-router)# neighbor 172.18.1.2 remote-as 64497 A(config-router)# neighbor 172.18.2.3 remote-as 23456
B	B# configure terminal B(config)# router bgp 64497 B(config-router)# neighbor 172.18.1.1 remote-as 64496 B(config-router)# neighbor 172.18.3.3 remote-as 1.2 B(config-router)# bgp asnotation dot B(config-router)# end
C	C# configure terminal C(config)# router bgp 1.2 C(config-router)# neighbor 172.18.2.1 remote-as 64496 C(config-router)# neighbor 172.18.3.2 remote-as 64497
Проверка	Запустите команду **show**, чтобы отобразить статус соседа BGP
A	A# show ip bgp summary BGP router identifier 172.18.1.1, local AS number 64496 BGP table version is 1, main routing table version 1 Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down Statd 172.18.1.2 4 64497 7 7 1 0 0 00:03:04 0 172.18.2.3 4 23456 4 4 1 0 0 00:00:15 0
B	B# show ip bgp summary BGP router identifier 172.18.3.2, local AS number 64497 BGP table version is 1, main routing table version 1

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	Statd
172.18.1.1	4	64496	7	7	1	0	0	00:00:04	0
172.18.3.2	4	1.2	4	4	1	0	0	00:00:16	0

7.4.13. Использование локальных адресов каналов IPv6 для установления соседства BGP

7.4.13.1. Эффект конфигурации

Используйте локальные адреса каналов IPv6 для установления соседства BGP.

7.4.13.2. Примечания

- Как правило, для установления соседства BGP необходимо использовать глобальные адреса IPv4.
- Локальные адреса каналов IPv6 можно использовать только для установления соседства BGP с одним hop-ом.
- Когда для установления соседства используются локальные адреса каналов IPv6, на peer end-е необходимо указать использование локальных адресов каналов IPv6 в качестве источников информации.
- Если для установления соседства используются локальные адреса каналов IPv6, локальные адреса каналов IPv6 должны быть настроены на обоих концах.

7.4.13.3. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Указание источника сообщения для соседа BGP

Выполните эту настройку в режиме настройки BGP. Если для соседа настроены локальные адреса каналов IPv6, эта конфигурация является обязательной; в противном случае эта конфигурация является необязательной.

Настройка режима семейства IPv4-адресов BGP

(Необязательно) Выполните эту настройку в режиме настройки BGP.

Отключение возможности семейства адресов IPv4 для соседа BGP

(Необязательно) Выполните эту настройку в режиме настройки BGP IPv6.

Настройка режима семейства IPv6-адресов BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка возможностей семейства адресов IPv6 для соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP IPv6.

Настройка объявления маршрута IPv6 в BGP

(Необязательно) Выполните эту настройку в режиме настройки BGP IPv6.

7.4.13.4. Проверка

- Запустите команду **show**, чтобы отобразить статус соседа.
- Запустите команду **show**, чтобы отобразить статус маршрутизации.

7.4.13.5. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Создание соседа BGP

Команда	**neighbor** *peer-address* **remote-as** *as-number*
Описание параметра	*peer-address*: указывает адрес peer-a, который обычно является адресом IPv6. *as-number*: указывает номер AS peer-a BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	AS, указанная для peer-a, должна совпадать с номером AS BGP спикера BGP на peer end-e

Указание источника сообщения для соседа BGP

Команда	**neighbor** *peer-address* **update-source** *interface-type interface-number*
Описание параметра	*peer-address*: указывает адрес peer-a, который обычно является адресом IPv6. *interface-type interface-number*: указывает имя интерфейса
Командный режим	Режим конфигурации BGP
Руководство по использованию	Если локальный адрес канала IPv6 локального интерфейса используется при установлении соседства BGP с соседним устройством, этот интерфейс должен быть указан в качестве источника

	сообщений соседства, когда соседство BGP настроено на локальном устройстве

Настройка режима семейства IPv4-адресов BGP

Команда	**address-family ipv4 unicast**
Командный режим	Режим конфигурации BGP

Отключение возможности семейства адресов IPv4 для соседа BGP

Команда	**no neighbor** *peer-address* **activate**
Описание параметра	*peer-address*: указывает адрес peer-a, который обычно является адресом IPv6
Командный режим	Режим семейства адресов BGP IPv4
Руководство по использованию	Соседи с адресами IPv6 используются для обмена маршрутами IPv6. Однако если сосед настроен в режиме BGP, BGP автоматически активирует для соседа возможность семейства unicast-адресов IPv4. Поэтому рекомендуется вручную отключить возможность семейства unicast-адресов IPv4

Настройка режима семейства IPv6-адресов BGP

Команда	**address-family ipv6 unicast**
Командный режим	Режим конфигурации BGP

Настройка возможностей семейства адресов IPv6 для соседа BGP

Команда	**neighbor** *peer-address* **activate**
Описание параметра	*peer-address*: указывает адрес peer-a, который обычно является адресом IPv6
Командный режим	Режим семейства адресов BGP IPv6

Настройка объявления маршрута IPv6 в BGP

Команда	**network** *network-number* [**mask** *mask*] [**route-map** *map-tag*] [**backdoor**]
Описание параметра	*network-number*: указывает номер сети. *mask*: указывает маску подсети. *map-tag*: указывает название карты маршрутов, состоящее не более чем из 32 символов. **backdoor**: указывает, что маршрут является маршрутом backdoor
Командный режим	Режим семейства адресов BGP IPv6

7.4.13.6. Пример конфигурации

Использование локального адреса канала IPv6 для настройки соседства BGP для реализации обмена маршрутами IPv6 в разных AS

Сценарий:



Рисунок 7-16.

Шаги настройки	• Включите BGP на всех устройствах и установите номера AS, как показано на Рисунке 7-16. • Настройте соседа BGP, укажите источник обновления, отключите возможность семейства адресов IPv4 для соседа и активируйте возможность семейства адресов IPv6. • Настройте объявление маршрута IPv6 в BGP
A	A# configure terminal A(config)# int loopback 0 A(config-if-Loopback)# ipv6 address 30::1/128 A(config-if-Loopback)# exit A(config)# int GigabitEthernet 0/1 A(config-if-Loopback)# ipv6 address fe80:100::2/64

	A(config-if-Loopback)# exit A(config)# router bgp 65530 A(config-router)# neighbor fe80:100::1 remote-as 65531 A(config-router)# neighbor fe80:100::1 update-source GigabitEthernet 0/1 A(config-router)# address-family ipv4 A(config-router-af)# no neighbor fe80:100::1 activate A(config-router-af)# exit-address-family A(config-router)# address-family ipv6 A(config-router-af)# neighbor fe80:100::1 activate A(config-router-af)# network 30::1/128
B	B# configure terminal A(config)# int GigabitEthernet 0/1 A(config-if-Loopback)# ipv6 address fe80:100::1/64 A(config-if-Loopback)# exit B(config)# router bgp 65531 B(config-router)# neighbor fe80:100::2 remote-as 65530 A(config-router)# neighbor fe80:100::2 update-source GigabitEthernet 0/1 B(config-router)# address-family ipv4 B(config-router-af)# no neighbor fe80:100::2 activate B(config-router-af)# exit-address-family B(config-router)# address-family ipv6 B(config-router-af)# neighbor fe80:100::2 activate
Проверка	Запустите команду **show**, чтобы отобразить статус соседа BGP
A	A# show bgp ipv6 unicast summary BGP router identifier 1.1.1.1, local AS number 65530 BGP table version is 1 1 BGP AS-PATH entries 0 BGP Community entries 1 BGP Prefix entries (Maximum-prefix:4 294 967 295) Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd FE80:100::1 4 65531 4 6 1 0 0 00:01:49 0

	Total number of neighbors 1
B	Запустите команду **show**, чтобы отобразить информацию о маршрутизации BGP. B# show bgp ipv6 unicast BGP table version is 4, local router ID is 2.2.2.2 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale, b - backup entry Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path *> 30::1/128 FE80:100::2 0 0 65530 i Total number of prefixes 1

7.4.13.7. Распространенные ошибки

- Когда соседство настроено, для указания соседства используется локальный адрес канала IPv6; однако во время локальной настройки в качестве интерфейса для этого локального адреса канала IPv6 не указан источник обновлений.
- Только один конец использует локальный адрес канала IPv6 для установления соседства.

7.4.14. Настройка BGP NSR

7.4.14.1. Эффект конфигурации

Настройте функцию BGP NSR, чтобы обеспечить высоконадежное развертывание сети.

7.4.14.2. Примечания

- Для успешного развертывания функции BGP NSR устройство должно поддерживать функцию горячего резервирования dual engine.
- После включения функции BGP NSR соединения с соседями BGP будут сброшены, чтобы функция вступила в силу.

7.4.14.3. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка функции NSR для соседей BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

7.4.14.4. Проверка

Запустите команду **show**, чтобы запросить статус соседа BGP.

7.4.14.5. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS в диапазоне от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Создание соседа BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*neighbor-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов. *as-number*: указывает номер AS peer-a BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	AS, указанная для peer-a (группы), должна совпадать с номером AS BGP спикера BGP на peer end-e

Настройка функции NSR для соседей BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **ha-mode nsr**
Описание параметра	*neighbor-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, состоящее не более чем из 32 символов
Командный режим	Режим конфигурации BGP

7.4.14.6. Пример конфигурации

Настройка BGP NSR

Сценарий:



Рисунок 7-17.

Шаги настройки	• Включите BGP на всех устройствах и установите номера AS, как показано на Рисунке 7-17. • Установите соседство EBGP между маршрутизаторами A и B через напрямую подключенный порт. • Включите функцию BGP NSR на A
A	A# configure terminal A(config-router)# exit A(config)# router bgp 65530 A(config-router)# neighbor 192.168.195.182 ha-mode nsr
Проверка	Запустите команду **show**, чтобы запросить статус соседа BGP
A	A# show ip bgp neighbors BGP neighbor is 192.168.195.183, remote AS 65530, local AS 65531, external link Using BFD to detect fast fallover - BFD session state up BGP version 4, remote router ID 10.0.0.1 BGP state = Established, up for 00:06:37 Last read 00:06:37, hold time is 180, keepalive interval is 60 seconds Neighbor capabilities: Route refresh: advertised and received (old and new) Address family IPv4 Unicast: advertised and received Graceful restart: advertised and received Remote Restart timer is 120 seconds Address families preserved by peer: None

	……
B	B# show ip bgp neighbors BGP neighbor is 192.168.195.183, remote AS 65530, local AS 65531, external link Using BFD to detect fast fallover - BFD session state up BGP version 4, remote router ID 10.0.0.1 BGP state = Established, up for 00:06:37 Last read 00:06:37, hold time is 180, keepalive interval is 60 seconds Neighbor capabilities: Route refresh: advertised and received (old and new) Address family IPv4 Unicast: advertised and received Graceful restart: advertised and received Remote Restart timer is 120 seconds Address families preserved by peer: None ……

7.4.14.7. Распространенные ошибки

- IGP не настроен.
- Функция NSR не включена для соседей BGP.

7.4.15. Настройка маршрутов BGP, чтобы быть рекурсивными только для маршрутов хоста

7.4.15.1. Эффект конфигурации

Настройте маршруты BGP так, чтобы они были рекурсивными только для маршрутов хоста, чтобы включить рекурсивность маршрутов IBGP или multi-EBGP только для маршрутов хоста.

7.4.15.2. Примечания

- Эта функция эффективна только для маршрутов IBGP или multi-hop маршрутов EBGP. Невозможно направить маршруты EBGP или маршруты, адреса следующего hop-а которых являются адресами прямого подключения.
- Соседство устройства по протоколу IBGP или multi-hop EBGP должно быть установлено с использованием адреса интерфейса Loopback. В противном случае эта функция недоступна.

7.4.15.3. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Настройка маршрутов BGP, чтобы быть рекурсивными только для маршрутов хоста

(Обязательно) Выполните эту настройку в режиме семейства адресов BGP.

7.4.15.4. Проверка

Запустите команду **show running-config**, чтобы отобразить конфигурацию.

7.4.15.5. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS. Диапазон значений от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Настройка маршрутов BGP, чтобы быть рекурсивными только для маршрутов хоста

Команда	**bgp recursion host**
Командный режим	Режим семейства адресов BGP

7.4.15.6. Пример конфигурации

Настройка маршрутов BGP, чтобы быть рекурсивными только для маршрутов хоста

Сценария:



Рисунок 7-18.

Шаги настройки	• Включите BGP на всех устройствах и установите номера AS, как показано на предыдущем Рисунке. • Установите multi-hop соседства EBGP на маршрутизаторах A и B через интерфейс Loopback.

	• Включите функцию создания рекурсивных маршрутов BGP только для маршрутов хоста на маршрутизаторах A и B
Проверка	Запустите команду **show**, чтобы отобразить статус соседа BGP

7.4.15.7. Распространенные ошибки

Если эта функция включена на устройстве, но соседства IBGP или multi-hop EBGP не установлены с использованием адреса интерфейса Loopback, устройство не сможет найти маршрут хоста, соответствующий адресу следующего hop-а маршрута BGP. В результате следующий hop маршрута BGP недействителен, и приоритетный выбор маршрутов невозможен.

7.4.16. Настройка обнаружения исходящей петли для соседа BGP

7.4.16.1. Эффект конфигурации

Настройка обнаружения исходящей петли для соседа BGP.

7.4.16.2. Примечания

Эта функция доступна только соседям EBGP.

7.4.16.3. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка обнаружения исходящей петли для соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

7.4.16.4. Проверка

Запустите команду **show**, чтобы отобразить статус соседа.

7.4.16.5. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS. Диапазон значений от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Создание соседа BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*neighbor-address*: указывает адрес peer-а. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов,содержащийне более 32 символов. *as-number*: указывает номер AS peer-а BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	Номер AS, указанный для peer-а (группы), должен совпадать с номером AS BGP спикера BGP на peer end-е

Настройка обнаружения исходящей петли для соседа BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **as-loop-check out**
Описание параметра	*neighbor-address*: указывает адрес peer-а. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, содержащее не более 32 символов
Командный режим	Режим конфигурации BGP

7.4.16.6. Пример конфигурации

Настройка обнаружения исходящей петли для соседа BGP

Сценарий:

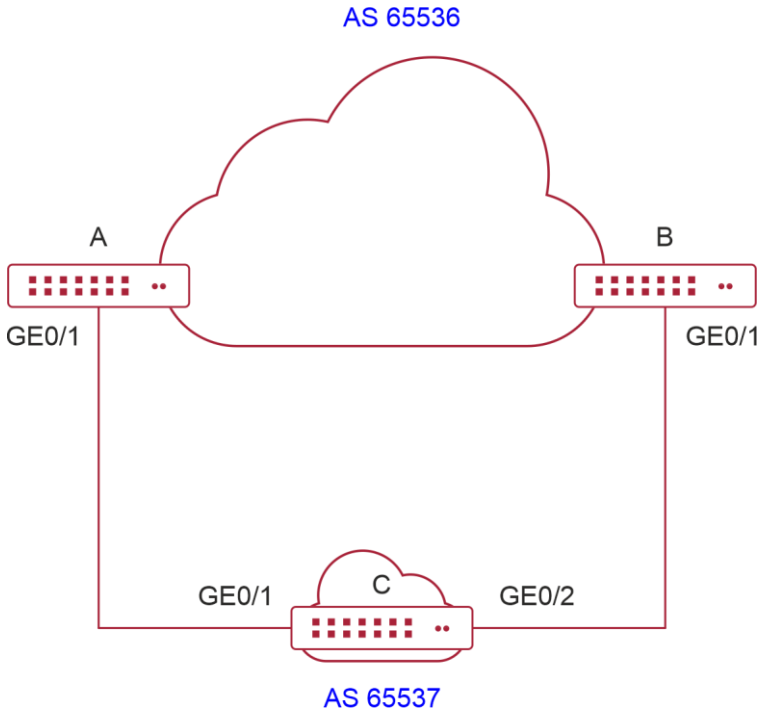


Рисунок 7-19.

Шаги настройки	• Включите BGP на всех устройствах и установите номера AS, как показано на предыдущем Рисунке. • Установите соседство EBGP между устройством A и устройством C, а также между устройством B и устройством C. • На устройстве C включите обнаружение исходящей петли для его соседей: устройства A и устройства B
A	A# configure terminal A(config)# router bgp 65536 A(config-router)# neighbor 10.1.1.1 remote-as 65537
B	B# configure terminal B(config)# router bgp 65536 B(config-router)# neighbor 20.1.1.1 remote-as 65537
C	C# configure terminal C(config)# router bgp 65537 C(config-router)# neighbor 10.1.1.2 remote-as 65536 C(config-router)# neighbor 10.1.1.2 as-loop-check out C(config-router)# neighbor 20.1.1.2 remote-as 65536

	C(config-router)# neighbor 20.1.1.2 as-loop-check out
Проверка	Запустите команду **show**, чтобы отобразить статус соседа BGP
C	C# show ip bgp neighbors 10.1.1.2 BGP neighbor is 10.1.1.2, remote AS 65536, local AS 65537, external link Using as path loop detection in announcing route BGP version 4, remote router ID 10.0.0.1 BGP state = Established, up for 00:06:37 Last read 00:06:37, hold time is 180, keepalive interval is 60 seconds Neighbor capabilities: Route refresh: advertised and received (old and new) Address family IPv4 Unicast: advertised and received Graceful restart: advertised and received Remote Restart timer is 120 seconds Address families preserved by peer: None …

7.4.17. Плавное закрытие соединений BGP

7.4.17.1. Эффект конфигурации

Плавно отключите соединения BGP. Сервисный трафик не прерывается или прерывается на очень короткий период времени в процессе от настройки функции до фактического отключения соединения BGP.

7.4.17.2. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Плавное закрытие соединений соседа BGP

(Опционально) Выполните эту настройку в режиме конфигурации BGP.

Плавное закрытие всех соединений экземпляра BGP

(Опционально) Выполните эту настройку в режиме конфигурации BGP.

7.4.17.3. Проверка

Запустите команду **show**, чтобы отобразить статус соседа.

7.4.17.4. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS. Диапазон значений от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Создание соседа BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*neighbor-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов,содержащее не более 32 символов. *as-number*: указывает номер AS peer-a BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	Номер AS, указанный для peer-a (группы), должен совпадать с номером AS BGP спикера BGP на peer end-e

Плавное закрытие соединений соседа BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **shutdown graceful** [**community** *value*] [**delay** *time*]
Описание параметра	*neighbor-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, содержащее не более 32 символов. **community** *value*: указывает значение сообщества, передаваемое по маршруту соседу. **delay** *time*: указывает время задержки (в секундах) для отключения соединений BGP. Диапазон значения от 1 до 65 535
Командный режим	Режим конфигурации BGP

Плавное закрытие всех соединений экземпляра BGP

Команда	**bgp shutdown graceful** [**community** *value*] [**delay** *time*]
Описание параметра	**community** *value*: указывает значение сообщества, которую несет в себе маршрут, отправленный соседу. **delay** *time*: указывает время задержки (в секундах) для отключения соединений BGP. Диапазон значений от 1 до 65 535
Командный режим	Режим конфигурации BGP

7.4.17.5. Пример конфигурации

Плавное закрытие соединений BGP

Сценарий:

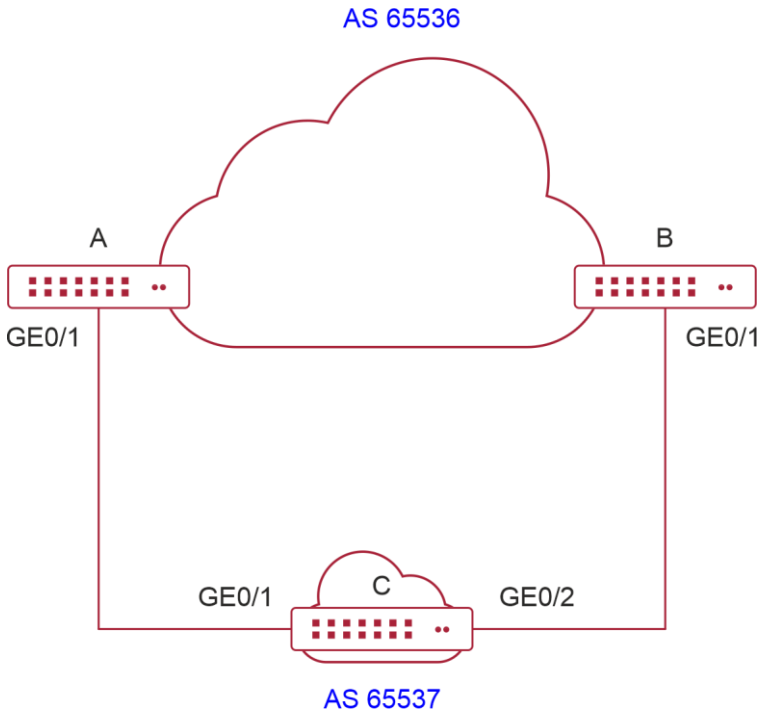


Рисунок 7-20.

Шаги настройки	• Включите BGP на всех устройствах и установите номера AS, как показано на предыдущем Рисунке. • Установите соседство EBGP между устройством A и устройством C, а также между устройством B и устройством C. • На устройстве A плавно закройте все соединения экземпляра BGP
A	A# configure terminal

	A(config)# router bgp 65536 A(config-router)# neighbor 10.1.1.1 remote-as 65537 A(config-router)# bgp shutdown graceful med 4 294 967 295
B	B# configure terminal B(config)# router bgp 65536 B(config-router)# neighbor 20.1.1.1 remote-as 65537
C	C# configure terminal C(config)# router bgp 65537 C(config-router)# neighbor 10.1.1.2 remote-as 65536 C(config-router)# neighbor 10.1.1.2 as-loop-check out C(config-router)# neighbor 20.1.1.2 remote-as 65536 C(config-router)# neighbor 20.1.1.2 as-loop-check out
Проверка	Запустите команду **show**, чтобы отобразить статус соседа BGP
A	A(config)#show ip bgp neighbor 10.1.1.2 For address family: IPv4 Unicast BGP neighbor is 10.10.10.2, remote AS 65537, local AS 65536, external link Administratively graceful shut down BGP version 4, remote router ID 0.0.0.0 BGP state = Idle Last read , hold time is 30, keepalive interval is 1 seconds Configured hold time is 30, keepalive interval is 1 seconds Received 0 messages, 0 notifications, 0 in queue open message:0 update message:0 keepalive message:0 refresh message:0 dynamic cap:0 notifications:0 Sent 0 messages, 0 notifications, 0 in queue open message:0 update message:0 keepalive message:0 refresh message:0 dynamic cap:0 notifications:0 Route refresh request: received 0, sent 0 Minimum time between advertisement runs is 30 seconds Update source is Loopback 0 For address family: IPv4 Unicast

	BGP table version 1, neighbor version 0 Index 1, Offset 0, Mask 0x2 0 accepted prefixes 0 announced prefixes Connections established 0; dropped 0 BGP neighbor may be up to 255 hops away. Sock_fd: -1 Last Reset: , due to BGP Notification received Notification Error Message: (Cease/Other Configuration Change.)

7.4.18. Настройка EBGP Multi-path Bypass Protection

7.4.18.1. Эффект конфигурации

Внедрите EBGP Multi-path Bypass Protection.

7.4.18.2. Примечания

Сеансы BFD можно настроить для соседей, чтобы реализовать быстрое обнаружение сбоев канала.

7.4.18.3. Шаги настройки

Включение BGP

(Обязательно) Выполните эту настройку в режиме глобальной конфигурации.

Создание соседа BGP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка BGP ECMP

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка BGP Multi-path Bypass Protection

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Настройка сеанса BFD для соседа BGP

(Опционально) Выполните эту настройку в режиме конфигурации BGP.

7.4.18.4. Проверка

Запустите команду **show**, чтобы отобразить информацию о маршруте.

7.4.18.5. Связанные команды

Включение BGP

Команда	**router bgp** *as-number*
Описание параметра	*as-number*: указывает номер AS. Диапазон значений от 1 до 4 294 967 295, что составляет от 1 до 65535.65535 в точечном режиме
Командный режим	Режим глобальной конфигурации

Настройка BGP Multi-path Bypass Protection

Команда	**bgp install standby-path**
Командный режим	Режим конфигурации BGP

Создание соседа BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*
Описание параметра	*neighbor-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, содержащее не более 32 символов. *as-number*: указывает номер AS peer-a BGP (группы)
Командный режим	Режим конфигурации BGP
Руководство по использованию	Номер AS, указанный для peer-a (группы), должен совпадать с номером AS BGP спикера BGP на peer end-e

Создание сеанса BFD с соседом BGP

Команда	**neighbor** { *neighbor-address* | *peer-group-name* } **fall-over bfd**
Описание параметра	*neighbor-address*: указывает адрес peer-a. Этот адрес может быть адресом IPv4 или адресом IPv6. *peer-group-name*: указывает имя группы peer-ов, содержащее не более 32 символов
Командный режим	Режим конфигурации BGP

7.4.18.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующем примере конфигурации описана только конфигурация, относящаяся к BGP Multi-path Bypass Protection.

Настройка BGP Multi-path Bypass Protection

Сценарий:

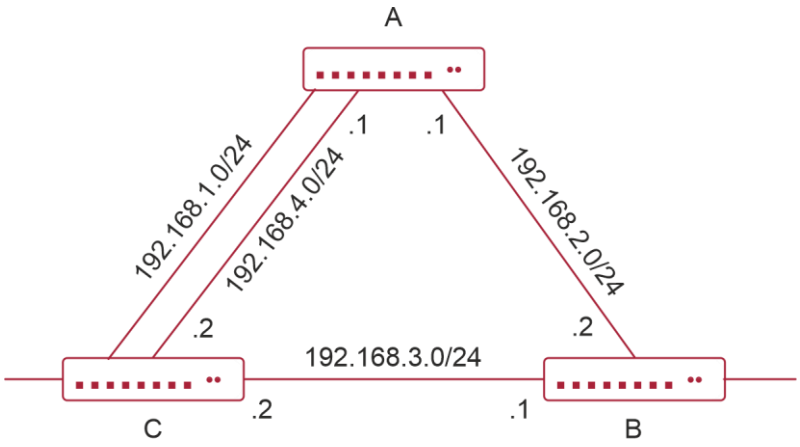


Рисунок 7-21.

Шаги настройки	• Включите BGP на всех устройствах. • Настройте адреса для портов с прямым подключением на устройстве A, устройстве B и устройстве C и взаимно установите соседство EBGP между каждыми двумя из них. • Настройте сеанс BFD для соседства EBGP между устройствами A и C. • Настройте BGP Multi-path Bypass Protection на устройстве C. • Настройте ECMP на устройстве C
A	A# conf terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# exit A(config)# interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)# ip address 192.168.2.1 255.255.255.0 A(config-if-GigabitEthernet 0/2)# exit A(config)# interface GigabitEthernet 0/3 A(config-if-GigabitEthernet 0/3)# ip address 192.168.4.1 255.255.255.0 A(config-if-GigabitEthernet 0/3)# exit A(config)# router bgp 100

	A(config-router)# neighbor 192.168.1.2 remote-as 300 A(config-router)# neighbor 192.168.4.2 remote-as 300 A(config-router)# neighbor 192.168.2.2 remote-as 200 A(config-router)# maximum-paths ebgp 2 A(config-router)# redistribute connect
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip address 192.168.3.1 255.255.255.0 B(config-if-GigabitEthernet 0/1)# bfd interval 200 min_rx 200 multiplier 5 B(config-if-GigabitEthernet 0/1)# exit B(config)# interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)# ip address 192.168.2.2 255.255.255.0 B(config-if-GigabitEthernet 0/2)# exit B(config)# router bgp 200 B(config-router)# neighbor 192.168.3.2 remote-as 300 B(config-router)# neighbor 192.168.3.2 fall-over bfd B(config-router)# neighbor 192.168.2.1 remote-as 100 B(config-router)# redistribute connect
C	C# configure terminal C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0 C(config-if-GigabitEthernet 0/1)# bfd interval 200 min_rx 200 multiplier 5 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface fastEthernet 0/2 C(config-if-GigabitEthernet 0/2)# ip address 192.168.3.2 255.255.0.0 C(config-if-GigabitEthernet 0/2)# bfd interval 200 min_rx 200 multiplier 5 C(config-if-GigabitEthernet 0/2)# exit C(config)# interface fastEthernet 0/3 C(config-if-GigabitEthernet 0/3)# ip address 192.168.4.2 255.255.0.0 C(config-if-GigabitEthernet 0/3)# bfd interval 200 min_rx 200 multiplier 5 C(config-if-GigabitEthernet 0/3)# exit C(config)# router bgp 300 C(config-router)# neighbor 192.168.1.1 remote-as 100 C(config-router)# neighbor 192.168.4.1 remote-as 100

	C(config-router)# neighbor 192.168.3.1 remote-as 200 C(config-router)# neighbor 192.168.1.1 fall-over bfd C(config-router)# neighbor 192.168.4.1 fall-over bfd C(config-router)# maximum-paths ebgp 2 C(config-router)# address-family ipv4 unicast C(config-router-af)# bgp install standby-path C(config-router-af)# redistribute connect
Проверка	Запустите команду **show**, чтобы отобразить конфигурацию
C	C# show ip bgp summary BGP router identifier 10.10.10.10, local AS number 300 BGP table version is 12 4 BGP AS-PATH entries 0 BGP Community entries 4 BGP Prefix entries (Maximum-prefix:4 294 967 295) Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 192.168.1.1 4 100 76 77 12 12 0 00:59:27 3 192.168.3.1 4 200 30 30 12 12 0 00:19:03 3 192.168.4.1 4 100 76 77 12 12 0 00:59:01 3 Total number of neighbors 3 C# show ip bgp BGP table version is 12, local router ID is 10.10.10.10 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale, b - backup entry, m - multipath Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path * 192.168.1.0 192.168.3.1 0 0 200 ? * 192.168.4.1 0 0 100 ? * 192.168.1.1 0 0 100 ? *> 0.0.0.0 0 32768 ?

```
*> 192.168.2.0 192.168.4.1      0                    0 200 ?
*m             192.168.1.1      0                    0 200 ?
*b             192.168.3.1      0                    0 100 ?
* 192.168.3.0  192.168.3.1      0                    0 200 ?
*              192.168.4.1      0                    0 100 200 ?
*              192.168.1.1      0                    0 100 200 ?
*>             0.0.0.0          0                    32768 ?
* 192.168.4.0  192.168.3.1      0                    0 200 ?
*              192.168.4.1      0                    0 100 ?
*              192.168.1.1      0                    0 100 ?
*>             0.0.0.0          0                    32768 ?

Total number of prefixes 4
C# show ip bgp 192.168.2.0
BGP routing table entry for 192.168.2.0/24
Paths: (3 available, best #3, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  192.168.1.1
  200
    192.168.3.1 from 192.168.3.1 (3.3.3.3)
    Origin incomplete, metric 0, localpref 100, valid, external, backup
    Last update: Tue Oct 5 00:26:52 1971

  100
    192.168.1.1 from 192.168.1.1 (44.44.44.44)
    Origin incomplete, metric 0, localpref 100, valid, external, multipath
    Last update: Mon Oct 4 23:46:28 1971

  100
    192.168.4.1 from 192.168.4.1 (44.44.44.44)
    Origin incomplete, metric 0, localpref 100, valid, external, multipath, best
    Last update: Mon Oct 4 23:46:28 1971
C# show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
```

```
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C 192.168.1.0/24 is directly connected, GigabitEthernet 0/1
C 192.168.1.2/32 is local host.
B 192.168.2.0/24 [20/0] via 192.168.1.1, 00:21:39
        [20/0] via 192.168.4.1, 00:21:39
C 192.168.3.0/24 is directly connected, GigabitEthernet 0/2
C 192.168.3.2/32 is local host.
C 192.168.4.0/24 is directly connected, GigabitEthernet 0/3
C 192.168.4.2/32 is local host
```

7.4.19. Настройка Inter-VRF Multi-Path Route Import

7.4.19.1. Эффект конфигурации

Обеспечьте импорт маршрутов inter-VRF и ECMP multi-path для импортированных маршрутов.

7.4.19.2. Шаги настройки

Настройка семейства адресов BGP VRF

(Обязательно) Выполните эту настройку в режиме настройки BGP.

Импорт статических маршрутов в BGP

(Обязательно) Выполните эту настройку в режиме семейства адресов BGP.

Импорт Multi-Path статических маршрутов в BGP

(Обязательно) Выполните эту настройку в режиме семейства адресов BGP.

Настройка BGP ECMP

(Обязательно) Выполните эту настройку в режиме семейства адресов BGP.

Настройка Inter-VRF Import для всех маршрутов

(Обязательно) Выполните эту настройку в режиме семейства адресов BGP.

7.4.19.3. Проверка

Запустите команду **show**, чтобы отобразить информацию о маршруте.

7.4.19.4. Связанные команды

Настройка семейства адресов BGP VRF

Команда	**address-family ipv4 vrf** *vrf-name*
Описание параметра	*vrf-name*: указывает имя экземпляра VRF
Командный режим	Режим конфигурации BGP

Импорт статических маршрутов в BGP

Команда	**redistribute** *protocol-type* [**route-map** *map-tag*] [**metric** *metric-value*]
Описание параметра	*protocol-type*: указывает тип протокола источника перераспределяемого маршрута. **route-map** *map-tag*: указывает имя связанной карты маршрута. **metric** *metric-value*: указывает значение метрики по умолчанию для перераспределяемого маршрута. Диапазон значений: от 0 до 4 294 967 295
Командный режим	Режим семейства адресов BGP

Импорт multi-path статических маршрутов в BGP

Команда	**bgp sourced-paths** *protocol-type* **all**
Описание параметра	*protocol-type*: указывает тип протокола источника перераспределяемого маршрута
Командный режим	Режим семейства адресов BGP
Руководство по использованию	Эту команду необходимо использовать вместе с командой перераспределения для импорта маршрутов с несколькими следующими hop-ами из других протоколов в BGP

Настройка BGP ECMP

Команда	**maximum-paths** { **ebgp** | **ibgp** } *number*
Описание параметра	**ebgp**: указывает количество эквивалентных путей функции multipath-балансировки нагрузки EBGP.

	ibgp: указывает количество эквивалентных путей функции multipath-балансировки нагрузки IBGP. *number*: указывает максимальное количество эквивалентных путей. Минимальное значение — 1, а максимальное значение зависит от возможностей устройства. Если значение равно 1, функция multipath-балансировки нагрузки EBGP отключена
Командный режим	Режим семейства адресов BGP
Руководство по использованию	Команда **maximum-paths ebgp** также используется для настройки эквивалентности объединения нескольких путей EBGP конфедерации и локальных inter-VRF маршрутов импорта. Маршруты IBGP и EBGP не могут образовывать эквивалентные маршруты

Настройка Inter-VRF Import для всех маршрутов

Команда	**import path selection** { **all** | **bestpath** | **multipath** }
Описание параметра	**all**: импортирует все маршруты со следующими hop-ами. **bestpath**: импортирует маршруты с предпочтительными следующими hop-ами. По умолчанию импортируются только маршруты с предпочтительными следующими hop-ами. **multipath**: импортирует маршруты с предпочтительными и эквивалентными следующими hop-ами
Командный режим	Режим семейства адресов BGP
Руководство по использованию	Эту команду можно использовать для управления импортом маршрутов inter-VRF, импортом удаленных маршрутов L3VPN в VRF и импортом маршрутов EVPN в таблицу IP-маршрутов

7.4.19.5. Пример конфигурации

Настройка BGP Multi-Path Bypass Protection

Сценария:

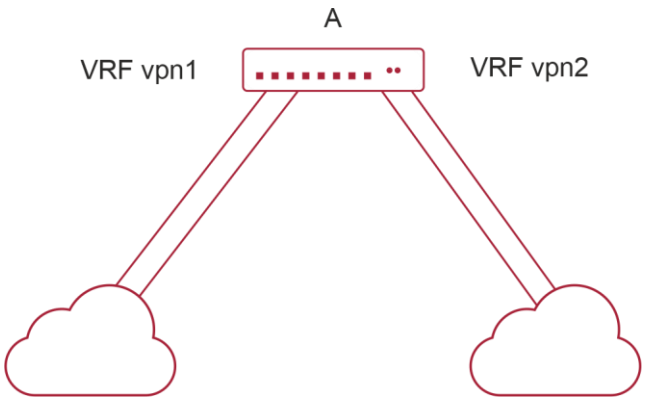


Рисунок 7-22.

Устройство A подключается к двум сетям через VRF vpn1 и vpn2, а cross-VRF доступ реализуется через устройство A.

Шаги настройки	• Настройте VRF. • Настройте статические маршруты VRF. • Настройте семейство адресов VRF. • Импортируйте статические маршруты VRF в BGP. • Включите импорт multi-path статического маршрута в BGP. • Настройте BGP ECMP. • Настройте импорт inter-VRF для всех маршрутов
A	A# conf terminal A(config)# ip vrf vpn1 A(config-vrf)# rd 200:1 A(config-vrf)# route-target both 100:100 A(config-vrf)# exit A(config)# ip vrf vpn2 A(config-vrf)# rd 300:1 A(config-vrf)# route-target both 100:100 A(config-vrf)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# A(config-if-GigabitEthernet 0/1)# ip vrf forwarding vpn1

	A(config-if-GigabitEthernet 0/1)# ip address 44.1.1.2 255.255.255.0 A(config-if-GigabitEthernet 0/1)# exit A(config)# interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)# ip vrf forwarding vpn1 A(config-if-GigabitEthernet 0/2)# ip address 45.1.1.2 255.255.255.0 A(config-if-GigabitEthernet 0/2)# exit A(config)# interface GigabitEthernet 0/3 A(config-if-GigabitEthernet 0/3)# ip vrf forwarding vpn2 A(config-if-GigabitEthernet 0/3)# ip address 46.1.1.2 255.255.255.0 A(config-if-GigabitEthernet 0/3)# exit A(config)# interface GigabitEthernet 0/4 A(config-if-GigabitEthernet 0/4)# ip vrf forwarding vpn2 A(config-if-GigabitEthernet 0/4)# ip address 47.1.1.2 255.255.255.0 A(config-if-GigabitEthernet 0/4)# exit A(config)# ip route vrf vpn1 100.1.1.1 255.255.255.255 44.1.1.1 A(config)# ip route vrf vpn1 100.1.1.1 255.255.255.255 45.1.1.1 A(config)# ip route vrf vpn2 200.1.1.1 255.255.255.255 46.1.1.1 A(config)# ip route vrf vpn2 200.1.1.1 255.255.255.255 47.1.1.1 A(config)# router bgp 100 A(config-router)# address-family ipv4 vrf vpn1 A(config-router-af)# redistribute static A(config-router-af)# maximum-paths ebgp 32 A(config-router-af)# bgp sourced-paths static all A(config-router-af)# import path selection all A(config-router-af)# exit-address-family A(config-router)# address-family ipv4 vrf vpn2 A(config-router-af)# redistribute static A(config-router-af)# maximum-paths ebgp 32 A(config-router-af)# bgp sourced-paths static all A(config-router-af)# import path selection all A(config-router-af)# exit-address-family
Проверка	Запустите команду **show**, чтобы отобразить конфигурации
A	A#show ip route vrf vpn1 Routing Table: vpn1

```
Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V – Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, EV - BGP EVPN, A - Arp to host
       * - candidate default
Gateway of last resort is no set
C 44.1.1.0/24 is directly connected, GigabitEthernet 0/1
C 44.1.1.2/32 is local host.
C 45.1.1.0/24 is directly connected, GigabitEthernet 0/2
C 45.1.1.2/32 is local host.
S 100.1.1.1/32 [1/0] via 44.1.1.1
       [1/0] via 45.1.1.1
B 200.1.1.1/32 [20/0] via 47.1.1.1, 02:32:01
       [20/0] via 46.1.1.1, 02:32:01

A#show ip route vrf vpn2
Routing Table: vpn2

Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V – Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, EV - BGP EVPN, A - Arp to host
       * - candidate default

Gateway of last resort is no set
C 46.1.1.0/24 is directly connected, GigabitEthernet 0/3
C 46.1.1.2/32 is local host.
C 47.1.1.0/24 is directly connected, GigabitEthernet 0/4
C 47.1.1.2/32 is local host.
B 100.1.1.1/32 [20/0] via 45.1.1.1, 03:27:07
```

	[20/0] via 44.1.1.1, 03:27:07 S 200.1.1.1/32 [1/0] via 46.1.1.1 [1/0] via 47.1.1.1

7.5. Мониторинг

7.5.1. Очистка

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

Описание	Команда
Очищает unicast-маршруты BGP IPv4	**clear ip bgp** [**vrf** *vrf-name*] { * | *as-number* | *peer-address* } [**soft**] [**in** | **out**] **clear bgp ipv4 unicast** [**vrf** *vrf-name*] { * | *as-number* | *peer-address* } [**soft**] [**in** | **out**]
Очищает unicast-маршруты BGP IPv6	**clear bgp ipv6 unicast** [**vrf** *vrf-name*] { * | *as-number* | *peer-address* } [**soft**] [**in** | **out**]
Очищает BGP L2VPN EVPN-маршрутов	**clear bgp l2vpn evpn** { * | *as-number* | *neighbor-address*} [**soft**] [**in** | **out**]
Восстанавливает приоритет объявленных маршрутов	**clear bgp advertise lowest-priority on-startup**

7.5.2. Отображение

Описание	Команда
Отображает unicast-маршруты BGP IPv4	**show ip bgp** **show bgp ipv4 unicast**
Отображает unicast-маршруты BGP IPv6	**show bgp ipv6 unicast**
Отображает BGP L2VPN EVPN-маршруты	**show bgp l2vpn evpn all**
Отображает статистику BGP	**show bgp statistics** [**vrf** *vrf-name*]

7.5.3. Отладка

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

Описание	Команда
Включает всю отладку BGP	**debug ip bgp all**
Устраняет flapping маршрута BGP	**debug ip bgp dampening**
Отладка обработки событий BGP	**debug ip bgp event**
Отладка фильтрации маршрутов BGP	**debug ip bgp filter**
Отладка состояния устройства BGP	**debug ip bgp fsm**
Отладка keepalive соседа BGP	**debug ip bgp keepalives**
Отладка обработки core маршрута BGP	**debug ip bgp nsm**
Отладка пакетов BGP UPDATE	**debug ip bgp update**
Отладки BGP EVPN	**debug ip bgp evpn**

8. НАСТРОЙКА RIPNG

8.1. Обзор

RIP следующего поколения (RIPng) — это протокол unicast-маршрутизации, который применяется к сетям IPv6. Маршрутизаторы с поддержкой RIPng обмениваются информацией о маршрутизации для получения маршрутов к удаленным сетям.

Как протокол внутреннего шлюза (IGP), RIPng может работать только внутри автономной системы (AS) и применим к сетям небольшого размера с маршрутами не более 16 hop-ов.

8.1.1. Протоколы и стандарты

RFC2080: определяет RIPng.

8.2. Приложение

RIPng обычно используется в некоторых небольших сетях, например в офисных сетях небольших компаний.

Как показано на следующем Рисунке, компания строит сеть IPv6, в которой все маршрутизаторы поддерживают IPv6. Размер сети небольшой, но рабочая нагрузка по-прежнему велика, если сеть обслуживается вручную. В этом случае RIPng можно настроить для адаптации к топологическим изменениям малоразмерной сети, что снижает рабочую нагрузку.

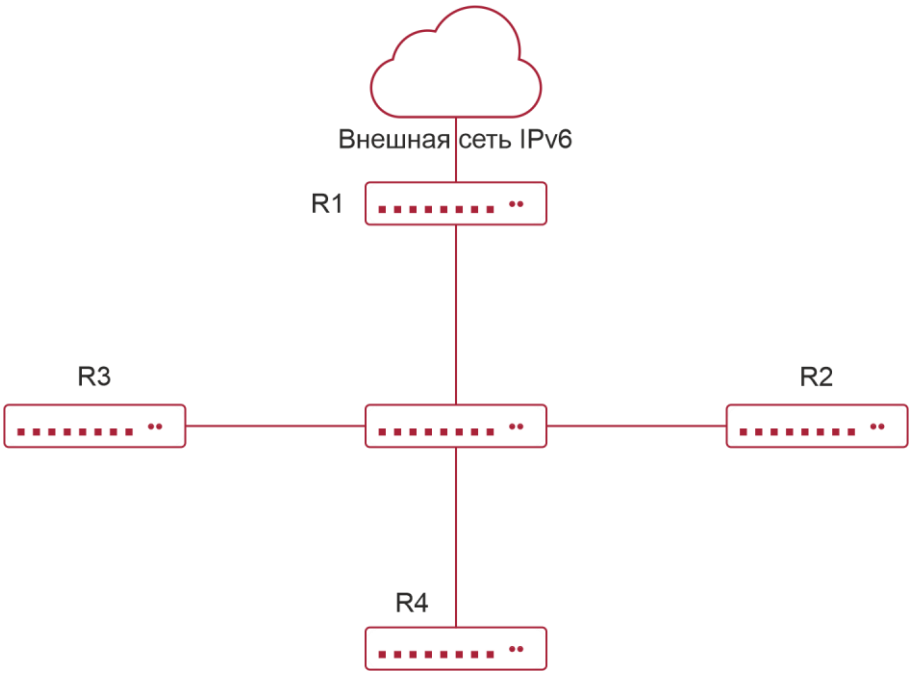


Рисунок 8-1.

8.3. Функции

8.3.1. Базовые определения

IGP и EGP

IGP работает внутри AS. Например, RIPng — это разновидность IGP.

Протокол внешнего шлюза (EGP) работает между AS. Например, BGP — это разновидность EGP.

8.3.2. Особенность

Особенность	Описание
RIPng и RIP	RIPng — это расширение RIPv2 на основе IPv6. Оба схожи по функциям и конфигурациям
Обмен информацией о маршрутизации	Обмениваясь информацией о маршрутизации, устройства с поддержкой RIPng могут автоматически получать маршруты к удаленной сети и обновлять маршруты в режиме реального времени
Алгоритм маршрутизации	RIPng — это протокол, основанный на алгоритме вектора расстояния. Он использует метод сложения векторов для вычисления информации о маршрутизации
Как избежать петель маршрута	RIPng использует такие функции, как split horizon и poison reverse, чтобы избежать петель маршрута

8.3.3. RIPng и RIP

RIP применяется к сетям IPv4. Доступны две версии RIP, включая RIPv1 и RIPv2.

RIPng — это расширение RIPv2 на основе IPv6. Оба схожи по функциям и конфигурациям.

8.3.3.1. Принцип работы

RIPv2

Пакеты RIPv2 являются multicast. Multicast-адрес — 224.0.0.9, а идентификатор порта UDP — 520. RIPv2 может идентифицировать маску подсети.

RIPng

Пакеты RIPng являются multicast. Multicast-адрес — FF02::9, адрес источника — FE80::/10, а идентификатор порта UDP — 521. RIPng может идентифицировать маску подсети.

ПРИМЕЧАНИЕ: в этой главе описаны функции и настройки RIPng. Подробную информацию о RIPv2 см. в разделе Настройка RIP.

8.3.3.2. Сопутствующая конфигурация

Включение процесса RIPng

По умолчанию процесс RIPng отключен.

Запустите команду **ipv6 router rip**, чтобы включить процесс RIPng.

Вы должны включить процесс RIPng на устройстве; в противном случае все функции, связанные с RIPng, не смогут действовать.

Запуск RIPng на интерфейсе

По умолчанию RIPng не запускается на интерфейсе.

Запустите команду **ipv6 rip enable**, чтобы запустить RIPng на интерфейсе.

После запуска RIPng на интерфейсе можно обмениваться пакетами RIPng на интерфейсе, и RIPng может изучать маршруты к сегментам сети, напрямую подключенным к устройству.

Запрет интерфейса на отправку или получение пакетов

По умолчанию интерфейсу с поддержкой RIPng разрешено отправлять и получать пакеты RIPng.

Запустите команду **passive-interface**, чтобы запретить интерфейсу отправлять пакеты RIPng.

8.3.4. Обмен информацией о маршрутизации

По сравнению со статической маршрутизацией протокол динамической маршрутизации имеет существенное преимущество, то есть путем обмена информацией о маршрутизации устройства могут автоматически получать маршруты к удаленной сети и обновлять маршруты в режиме реального времени.

8.3.4.1. Принцип работы

Инициализация

После включения RIPng на маршрутизаторе маршрутизатор отправляет пакет запроса своему соседнему маршрутизатору, запрашивая всю информацию о маршрутизации, то есть таблицу маршрутизации. После получения сообщения запроса соседний маршрутизатор возвращает ответный пакет, содержащий локальную таблицу маршрутизации. После получения ответного пакета маршрутизатор обновляет локальную таблицу маршрутизации и отправляет пакет обновления соседнему маршрутизатору, информируя соседний маршрутизатор об обновлении маршрута. После получения пакета обновления соседний маршрутизатор обновляет локальную таблицу маршрутизации и отправляет пакет обновления другим соседним маршрутизаторам. После серии обновлений все маршрутизаторы смогут получать и сохранять самую свежую информацию о маршрутизации.

Периодическое обновление

По умолчанию для RIPng включено периодическое обновление. Соседние маршрутизаторы обмениваются друг с другом полной информацией о маршрутизации каждые 30 с (таймер обновления), то есть вся таблица маршрутизации отправляется соседним маршрутизаторам.

ПРИМЕЧАНИЕ: если для каждого нелокального маршрута маршрут не обновляется в течение 180 с (таймер неработоспособности), метрика маршрута изменяется на 16 (недоступен). Если маршрут по-прежнему не обновляется в течение следующих 120 с (таймер очистки), маршрут удаляется из таблицы маршрутизации.

Маршрут по умолчанию

В таблице маршрутизации маршрут к сети назначения ::/0 называется маршрутом по умолчанию.

Маршрут по умолчанию можно узнать от соседнего маршрутизатора или отправить на соседний маршрутизатор.

Перераспределение маршрутов

Для RIPng другие типы маршрутов (например, прямые маршруты, статические маршруты и маршруты других протоколов маршрутизации) называются внешними маршрутами.

Внешние маршруты (за исключением маршрута по умолчанию) могут быть перераспределены в RIPng и объявлены соседям.

Фильтрация маршрутов

Условия фильтрации можно настроить для ограничения информации о маршрутизации, которой обмениваются соседние маршрутизаторы. Отправлять или получать можно только ту информацию о маршрутизации, которая соответствует условиям фильтрации.

8.3.4.2. Сопутствующая конфигурация

Таймеры RIPng

По умолчанию таймер обновления составляет 30 с, таймер неработоспособности — 180 с, а таймер очистки — 120 с.

Запустите команду **timers basic**, чтобы изменить продолжительность таймеров RIPng.

Увеличение продолжительности таймера очистки может уменьшить flapping маршрута. Уменьшение продолжительности таймера очистки помогает ускорить сходимость маршрутов.

Длительность таймеров RIPng должна быть одинаковой на соседних маршрутизаторах. Если не требуется иное, не рекомендуется изменять таймеры RIPng.

Маршрут по умолчанию

Запустите команду **ipv6 rip default-information**, чтобы объявить маршрут по умолчанию соседям на интерфейсе.

Перераспределение маршрутов

Запустите команду **redistribute**, чтобы перераспределить внешние маршруты (за исключением маршрута по умолчанию) для RIPng и объявить их соседям.

Фильтрация маршрутов

Запустите команду **distribute-list out**, чтобы установить правила фильтрации для ограничения информации о маршрутизации, отправляемой устройством.

Запустите команду **distribute-list in**, чтобы установить правила фильтрации для ограничения информации о маршрутизации, получаемой устройством.

8.3.5. Алгоритм маршрутизации

RIPng — это протокол, основанный на алгоритме вектора расстояния. Он использует метод сложения векторов для вычисления информации о маршрутизации.

8.3.5.1. Принцип работы

Алгоритм вектора расстояния

RIPng — это протокол, основанный на алгоритме вектора расстояния. Алгоритм вектора расстояния рассматривает маршрут как вектор, состоящий из сети назначения и расстояния (метрики). Маршрутизатор получает маршрут от своего соседа и добавляет к

маршруту вектор расстояния от себя до соседа, чтобы сформировать свой собственный маршрут.

RIPng использует количество hop-ов для оценки расстояния (метрики) до сети назначения. По умолчанию количество hop-ов от маршрутизатора к сети, к которой он подключен напрямую, равно 0, количество hop-ов от маршрутизатора к сети, к которой можно получить доступ через маршрутизатор, равно 1 и так далее. То есть метрика равна количеству маршрутизаторов из локальной сети в сеть назначения. Чтобы ограничить время сходимости, RIPng предусматривает, что метрика должна быть целым числом от 0 до 15. Если метрика равна или больше 16, сеть или хост назначения недоступны. По этой причине RIPng не может применяться в крупномасштабной сети.

Как показано на следующем Рисунке, маршрутизатор A подключен к сети 2::/64. Маршрутизатор B получает маршрут (2::/64, 0) от маршрутизатора A и добавляет метрику 1 к маршруту, чтобы получить свой собственный маршрут (2::/64, 1) и следующий hop указывает на маршрутизатор A.

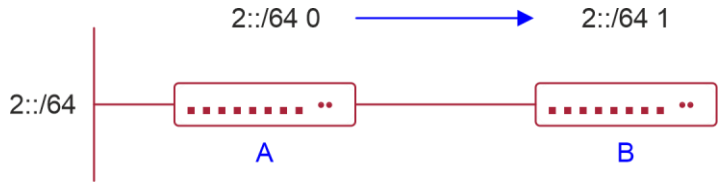


Рисунок 8-2.

Выбор оптимального маршрута

RIPng выбирает оптимальный маршрут на основе следующего принципа: если доступно несколько маршрутов к одной и той же сети назначения, маршрутизатор предпочтительно выбирает маршрут с наименьшей метрикой.

Как показано на следующем Рисунке 8-3, маршрутизатор A подключен к сети 2::/64. Маршрутизатор C получает маршрут (2::/64, 0) от маршрутизатора A и маршрут (2::/64, 1) от маршрутизатора B. Маршрутизатор C выберет маршрут, полученный от маршрутизатора A, и добавит метрику 1 к этому маршруту для формирования собственного маршрута (2::/64, 1), а следующий hop указывает на маршрутизатор A.

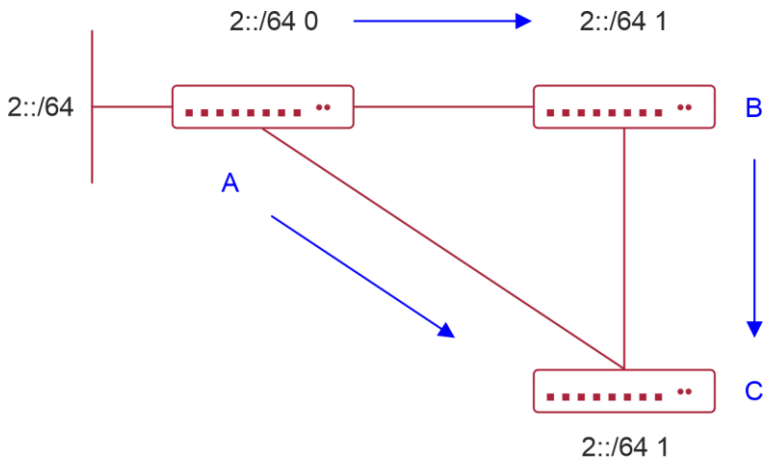


Рисунок 8-3.

ПРИМЕЧАНИЕ: когда на маршрутизаторе существуют маршруты, поступающие из разных источников, предпочтительно выбирается маршрут с меньшим расстоянием.

Источник маршрута	Расстояние по умолчанию
Сеть с прямым подключением	0
Статический маршрут	1
Маршрут OSPF	110
Маршрут IS-IS	115
Маршрут RIPng	120
Недоступный маршрут	255

8.3.5.2. Сопутствующая конфигурация

Изменение расстояния

По умолчанию расстояние маршрута RIPng составляет 120.

Запустите команду **distance**, чтобы изменить расстояние маршрута RIPng.

Изменение метрики

Для маршрута RIPng, который заранее обнаруживается устройством, метрика по умолчанию равна количеству hop-ов из локальной сети в сеть назначения. Смещение метрики интерфейса равно 1.

Для маршрутизатора RIPng, настроенного вручную (маршрут по умолчанию или перераспределенный маршрут), метрика по умолчанию равна 1.

Запустите команду **ipv6 rip metric-offset**, чтобы изменить смещение метрики интерфейса.

Запустите команду **default-metric**, чтобы изменить метрику по умолчанию внешнего маршрута (перераспределенного маршрута).

Запустите команду **redistribute**, чтобы изменить метрику внешнего маршрута (перераспределенного маршрута) при объявлении этого маршрута.

Запустите команду **ipv6 rip default-information**, чтобы изменить метрику маршрута по умолчанию при объявлении маршрута по умолчанию.

8.3.6. Как избежать петель маршрута

RIPng использует такие функции, как split horizon и poison reverse, чтобы избежать петель маршрута.

8.3.6.1. Принцип работы

Петля маршрута

Зацикливание маршрута RIPng возникает из-за присущих алгоритму вектора расстояния дефектов.

Как показано на следующем Рисунке 8-4, маршрутизатор A подключен к сети 2::/64 и отправляет пакет обновления каждые 30 секунд. Маршрутизатор B получает маршрут к 2::/64 от маршрутизатора A каждые 30 секунд. Если маршрутизатор A отключен от 2::/64, маршрут к 2::/64 будет удален из таблицы маршрутизации на маршрутизаторе A. В следующий раз пакет обновления, отправленный маршрутизатором A, больше не будет содержать этот маршрут. Поскольку маршрутизатор B не получает пакет обновления, относящийся к 2::/64, маршрутизатор B определяет, что маршрут к 2::/64 действителен в течение 180 с, и использует пакет обновления для отправки этого маршрута маршрутизатору A. 2::/64 не существует на маршрутизаторе A, маршрут, полученный от маршрутизатора B, добавляется в таблицу маршрутизации. Маршрутизатор B определяет, что данные могут достигать 2::/64 через маршрутизатор A, а маршрутизатор A определяет, что данные могут достигать 2::/64 через маршрутизатор B. Таким образом формируется петля маршрута.

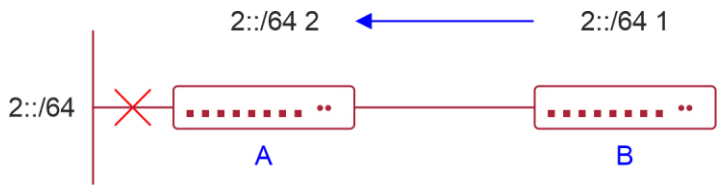


Рисунок 8-4.

Split horizon

Split horizon может предотвратить появление петель на маршруте. После включения split horizon маршрут, полученный на этом интерфейсе, не будет отправляться с этого интерфейса.

Как показано на следующем Рисунке 8-5, после того, как на маршрутизаторе B включен split horizon, маршрутизатор B не будет отправлять маршрут к 2::/64 обратно на маршрутизатор A. Маршрутизатор B узнает через 180 секунд, что 2::/64 не доступен.

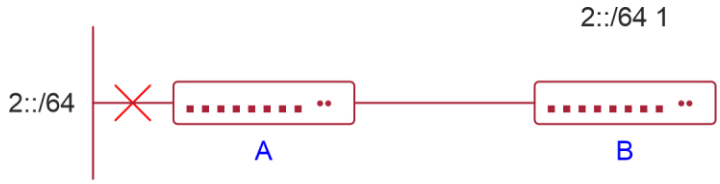


Рисунок 8-5.

Poison reverse

Poison Reverse также может предотвратить появление петель маршрута. По сравнению со split horizon, то poison reverse более надежен, но переносит больше пакетов протокола, что делает перегрузку сети более выраженной.

После включения poison reverse на интерфейсе маршрут, полученный от этого интерфейса, будет снова отправлен с этого интерфейса, но метрика этого маршрутизатора будет изменена на 16 (недоступен).

Как показано на следующем Рисунке, после включения poison reverse на маршрутизаторе A, если маршрут A обнаруживает отключение от 2::/64, маршрутизатор A не удалит маршрут к 2::/64. Вместо этого маршрутизатор A изменяет количество hop-ов на 16 и

объявляет маршрут через пакет обновления. Получив пакет обновления, маршрутизатор B узнает, что 2::/64 недоступен.

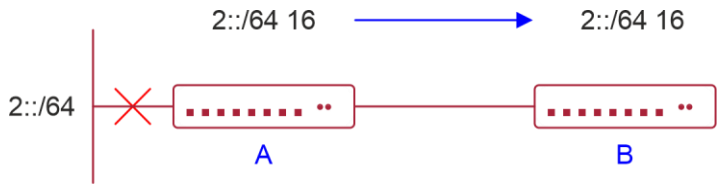


Рисунок 8-6.

8.3.6.2. Сопутствующая конфигурация

Split horizon

По умолчанию split horizon включено.

Запустите команду **no split-horizon**, чтобы отключить split horizon.

Poison reverse

По умолчанию poison reverse отключено.

Запустите команду **split-horizon poisoned-reverse**, чтобы включить poison reverse. (После включения poison reverse split horizon автоматически отключается.)

8.4. Конфигурация

Конфигурация	Связанные команды	
Настройка основных функций RIPng	(Обязательный) Используется для создания домена маршрутизации RIPng	
	ipv6 router rip	Включает процесс маршрутизации RIPng и переходит в режим настройки процесса маршрутизации
	ipv6 rip enable	Запускает RIPng на интерфейсе
	split-horizon	Включает split horizon или poison reverse
	passive-interface	Настраивает пассивный интерфейс
Объявление маршрута по умолчанию или внешних маршрутов	Опционально	
	ipv6 rip default-information	Объявите маршрут по умолчанию соседям на интерфейсе

Конфигурация	Связанные команды	
	redistribute	Перераспределяет маршруты и объявляет внешние маршруты соседям
Настройка правил фильтрации маршрутов	Опционально	
	distribute-list in	Фильтрует полученную информацию о маршрутизации RIPng
	distribute-list out	Фильтрует отправленную информацию о маршрутизации RIPng
Изменение параметров выбора маршрута	Опционально	
	distance	Изменяет административное расстояние маршрута RIPng
	ipv6 rip metric-offset	Изменяет смещение метрики на интерфейсе
	default-metric	Настройте метрику по умолчанию для перераспределения маршрутов
Изменение таймеров	Опционально	
	timers	Изменяет таймер обновления, таймер неработоспособности и таймер очистки RIPng

8.4.1. Настройка основных функций RIPng

8.4.1.1. Эффект конфигурации

- Создайте в сети домен маршрутизации RIPng.
- Маршрутизаторы в домене получают маршруты к удаленной сети через RIPng.

8.4.1.2. Примечания

- Адреса IPv6 должны быть настроены.
- Должны быть включены unicast-маршруты IPv6.

8.4.1.3. Шаги настройки

Включение процесса маршрутизации RIPng

- Обязательный.
- Если не требуется иное, выполните эту настройку на каждом маршрутизаторе в домене маршрутизации RIPng.

Запуск RIPng на интерфейсе

- Обязательный.
- Если не требуется иное, выполните эту настройку на каждом взаимосвязанном интерфейсе маршрутизаторов в домене маршрутизации RIPng.

Включение split horizon или poison reverse

- По умолчанию split horizon включено, а poison reverse отключен.
- Если не требуется иное, включите split horizon на каждом интерфейсе, подключенном к broadcast-сети, например Ethernet. (Сохраните настройки по умолчанию.)
- Если не требуется иное, включите split horizon на каждом интерфейсе, подключенном к сети «точка-точка» (P2P), например PPP и HDLC. (Сохраните настройки по умолчанию.)
- Рекомендуется отключить split horizon и poison reverse на интерфейсе, подключенном к non-broadcast-сети с множественным доступом (multi-access), такой как FR и X.25; в противном случае некоторые устройства не смогут изучить полную информацию о маршрутизации.
- Если дополнительный IP-адрес настроен для интерфейса, подключенного к non-broadcast-интерфейсу, рекомендуется отключить split horizon и poison reverse.

Настройка пассивного интерфейса

- Данная конфигурация рекомендуется.
- Используйте пассивный интерфейс, чтобы установить границу домена маршрутизации RIPng. Сегмент сети пассивного интерфейса принадлежит домену маршрутизации RIPng, но пакеты RIPng не могут отправляться через пассивный интерфейс.
- Если необходимо обмениваться маршрутами RIPng на интерфейсе (например, интерфейсе соединения маршрутизатора) в домене маршрутизации RIPng, этот интерфейс нельзя настроить как пассивный интерфейс.

8.4.1.4. Проверка

Проверьте таблицу маршрутизации маршрутизатора, чтобы убедиться, что маршрут к удаленной сети можно получить через RIPng.

8.4.1.5. Связанные команды

Включение процесса маршрутизации RIPng

Команда	**ipv6 router rip**
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Эта команда используется для создания процесса маршрутизации RIPng и входа в режим настройки процесса маршрутизации

Запуск RIPng на интерфейсе

Команда	**ipv6 rip enable**
Командный режим	Режим настройки интерфейса
Руководство по использованию	Конфигурация для запуска RIPng на интерфейсе отличается от конфигурации RIPv2. В RIPv2 команда **network** настраивается в режиме конфигурации процесса маршрутизации для определения диапазона IP-адресов. Если IP-адрес интерфейса принадлежит этому диапазону IP-адресов, RIP автоматически запускается на этом интерфейсе

Включение split horizon

Команда	**split-horizon** [**poisoned-reverse**]
Описание параметра	**poisoned-reverse**: указывает, что функция split horizon содержит функцию poison reverse
Командный режим	Режим настройки процесса маршрутизации
Руководство по использованию	Запустите команду **show ipv6 rip**, чтобы проверить, включен ли split horizon. Конфигурация отличается от конфигурации RIPv2. В RIPv2 функция split horizon настраивается в режиме конфигурации интерфейса

Настройка пассивного интерфейса

Команда	**passive-interface** { **default** | *interface-type interface-num* }
Описание параметра	**default**: указывает все интерфейсы. *interface-type interface-num*: указывает интерфейс
Командный режим	Режим настройки процесса маршрутизации

Руководство по использованию	Сначала запустите команду **passive-interface default**, чтобы настроить все интерфейсы как пассивные. Затем запустите команду **no passive-interface** *interface-type interface-num*, чтобы интерфейсы, используемые для соединения между маршрутизаторами в домене, не были пассивными интерфейсами

Отображение таблицы IP-маршрутизации

Команда	**show ipv6 route**
Командный режим	Привилегированный режим EXEC или режим глобальной конфигурации
Руководство по использованию	Проверьте, содержит ли таблица маршрутизации какой-либо маршрут к удаленной сети, полученный через RIPng

8.4.1.6. Пример конфигурации

Создание домена маршрутизации RIPng

Сценарий:

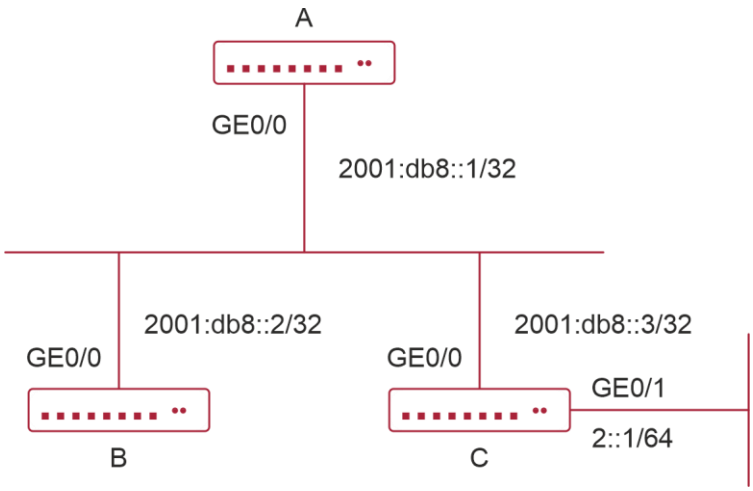


Рисунок 8-7.

Шаги настройки	• Настройте адреса IPv6 на всех маршрутизаторах. • Включите RIPng на всех маршрутизаторах
A	A# configure terminal Введите команды конфигурации, по одной в строке. Закончите с помощью CNTL/Z. A(config)# ipv6 router rip

	A(config-router)# exit A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::1/32 A(config-if-GigabitEthernet 0/0)# ipv6 rip enable
B	B# configure terminal Введите команды конфигурации, по одной в строке. Закончите с помощью CNTL/Z. B(config)# ipv6 router rip B(config-router)# exit B(config)# interface GigabitEthernet 0/0 B(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::2/32 B(config-if-GigabitEthernet 0/0)# ipv6 rip enable
C	C# configure terminal Введите команды конфигурации, по одной в строке. Закончите с помощью CNTL/Z. C(config)# ipv6 router rip C(config-router)# exit C(config)# interface GigabitEthernet 0/0 C(config-if-GigabitEthernet 0/0)# C(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::3/32 C(config-if-GigabitEthernet 0/0)# ipv6 rip enable C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ipv6 address 2::1/64 C(config-if-GigabitEthernet 0/1)# ipv6 rip enable
Проверка	Проверьте таблицы маршрутизации на маршрутизаторах A, B и C. Таблицы маршрутизации должны содержать маршруты к удаленной сети, изученные с помощью RIPng
A	A# show ipv6 route IPv6 routing table name - Default - 6 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2

	SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R 2::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, GigabitEthernet 0/0 C 2001:DB8::/32 via GigabitEthernet 0/0, directly connected L 2001:DB8::1/128 via GigabitEthernet 0/0, local host C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:E7CE/128 via GigabitEthernet 0/0, local host
B	B# show ipv6 route IPv6 routing table name - Default - 6 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R 2::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, GigabitEthernet 0/0 C 2001:DB8::/32 via GigabitEthernet 0/0, directly connected L 2001:DB8::2/128 via GigabitEthernet 0/0, local host C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:C9BA/128 via GigabitEthernet 0/0, local host
C	QTECH# show ipv6 route IPv6 routing table name - Default - 9 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area C 2::/64 via GigabitEthernet 0/1, directly connected

	L 2::2/128 via GigabitEthernet 0/1, local host C 2001:DB8::/32 via GigabitEthernet 0/0, directly connected L 2001:DB8::3/128 via GigabitEthernet 0/0, local host C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:D521/128 via GigabitEthernet 0/0, local host C FE80::/64 via GigabitEthernet 0/1, directly connected L FE80::2D0:F8FF:FEFB:D521/128 via GigabitEthernet 0/1, local host

8.4.1.7. Распространенные ошибки

- Адрес IPv6 не настроен на интерфейсе.
- Интерфейс, используемый для соединения между устройствами, настроен как пассивный интерфейс.

8.4.2. Объявление маршрута по умолчанию или внешних маршрутов

8.4.2.1. Эффект конфигурации

- В домене RIPng введите unicast-маршрут другой AS, чтобы сервис unicast-маршрутизации к этой AS могла быть предоставлена пользователям в домене RIPng.
- В домене RIPng внедрите маршрут по умолчанию в другую AS, чтобы сервис unicast-маршрутизации к этой AS могла быть предоставлена пользователям в домене RIPng.

8.4.2.2. Примечания

Необходимо настроить основные функции RIPng.

8.4.2.3. Шаги настройки

Настройка перераспределения внешних маршрутов

- Необязательный.
- Выполните эту настройку, если внешние маршруты домена RIPng должны быть представлены пограничному маршрутизатору AS (ASBR).

Создание маршрута по умолчанию

- Необязательный.
- Выполните эту настройку, если маршрут по умолчанию должен быть введен в ASBR, чтобы другие маршрутизаторы в домене RIPng получали доступ к другим доменам AS через этот ASBR по умолчанию.

8.4.2.4. Проверка

Запустите команду **show ipv6 route rip** на не ASBR, чтобы проверить, загружены ли внешние маршруты домена и маршрут по умолчанию.

8.4.2.5. Связанные команды

Объявление маршрута по умолчанию соседям на интерфейсе

Команда	**ipv6 rip default-information** { **only**|**originate** } [**metric** *metric-value*]
Описание параметра	**only**: объявляет только маршрут по умолчанию IPv6. **originate**: объявляет маршрут IPv6 по умолчанию и другие маршруты. **metric** *metric-value*: указывает метрику маршрута по умолчанию. Значение варьируется от 1 до 15. Значение по умолчанию — 1
Командный режим	Режим настройки интерфейса
Руководство по использованию	После настройки этой команды на интерфейсе маршрут IPv6 по умолчанию объявляется внешним устройствам через этот интерфейс, но сам маршрут не добавляется в таблицу пересылки маршрутов или в базу данных устройства и маршрутов RIPng. Чтобы предотвратить возникновение петли маршрута, после настройки этой команды на интерфейсе RIPng отказывается получать обновления маршрута по умолчанию, объявленные соседями

Перераспределение маршрутов и объявление внешних маршрутов соседям

Команда	**redistribute** { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static** } [**metric** *metric-value* | **route-map** *route-map-name*]
Описание параметра	**bgp**: указывает на перераспределение из BGP. **connected**: указывает на перераспределение с прямых маршрутов. **isis** [*area-tag*]: указывает на перераспределение из IS-IS. *area-tag* указывает идентификатор процесса IS-IS. **ospf** *process-id*: указывает на перераспределение из OSPF. *process-id* указывает идентификатор процесса OSPF. Значение варьируется от 1 до 65 535. **static**: указывает на перераспределение со статических маршрутов. **metric** *metric-value*: устанавливает метрику маршрута, перераспределяемого в домен RIPng. **route-map** *route-map-name*: устанавливает правила фильтрации перераспределения
Командный режим	Режим настройки процесса маршрутизации

Руководство по использованию	При перераспределении маршрутов нет необходимости преобразовывать метрику одного протокола маршрутизации в метрику другого протокола маршрутизации, поскольку разные протоколы маршрутизации используют совершенно разные методы измерения метрики. RIP измеряет метрику на основе количества hop-ов, а OSPF измеряет метрику на основе полосы пропускания. Поэтому вычисленные метрики нельзя сравнивать друг с другом

8.4.2.6. Пример конфигурации

Сценарий:

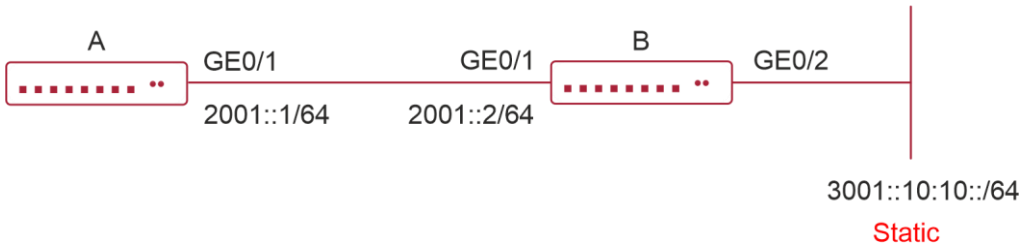


Рисунок 8-8.

Шаги настройки	• Настройте IPv6-адреса интерфейса на всех маршрутизаторах. (опущено) • Настройте базовые функции RIPng на всех маршрутизаторах. (опущено) • На маршрутизаторе B настройте перераспределение статических маршрутов. • На интерфейсе GE0/1 маршрутизатора A настройте объявление маршрута по умолчанию
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ipv6 rip default-information originate
B	B# configure terminal B(config)# ipv6 router rip B(config-router)# redistribute static
Проверка	Проверьте таблицы маршрутизации на маршрутизаторах A и B и убедитесь, что маршрутизатор A может изучить маршрут 3001:10:10::/64, а маршрутизатор B может изучить маршрут по умолчанию ::/0
A	A# show ipv6 route rip

	IPv6 routing table name - Default - 17 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R 3001:10:10::/64 [120/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1
B	B# show ipv6 route rip IPv6 routing table name - Default - 17 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R ::/0 [120/2] via FE80::21A:A9FF:FE41:5B06, GigabitEthernet 0/1

8.4.3. Настройка правил фильтрации маршрутов

8.4.3.1. Эффект конфигурации

Маршруты, не соответствующие критериям фильтрации, не могут быть загружены в таблицу маршрутизации или объявлены соседям. Таким образом, пользователям внутри сети можно запретить доступ к указанным сетям назначения.

8.4.3.2. Примечания

Необходимо настроить основные функции RIPng.

8.4.3.3. Шаги настройки

Фильтрация полученной информации о маршрутизации RIP

Чтобы отказаться от получения некоторых указанных маршрутов, вы можете настроить список управления распределением маршрутов для обработки всех полученных пакетов обновления маршрута. Если интерфейс не указан, будут обработаны пакеты обновления маршрута, полученные на всех интерфейсах.

Фильтрация отправляемой информации о маршрутизации RIP

Если эта команда не содержит каких-либо дополнительных параметров, управление объявлением обновления маршрута вступает в силу на всех интерфейсах. Если команда

содержит параметр интерфейса, управление объявлением обновления маршрута действует только на указанном интерфейсе. Если команда содержит другие параметры процесса маршрутизации, управление объявлением обновления маршрута действует только на указанный процесс маршрутизации.

8.4.3.4. Проверка

Запустите команду **show ipv6 route rip**, чтобы убедиться, что отфильтрованные маршруты не загружены в таблицу маршрутизации.

8.4.3.5. Связанные команды

Команда	**distribute-list prefix-list** *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]
Описание параметра	*prefix-list-name*: указывает имя списка префиксов, который используется для фильтрации маршрутов. **in** | **out**: указывает маршруты обновления (полученные или отправленные маршруты), которые фильтруются. *interface-type interface-name*: указывает, что список рассылки применен к указанному интерфейсу
Командный режим	Режим настройки процесса маршрутизации

8.4.3.6. Пример конфигурации

Сценарий:

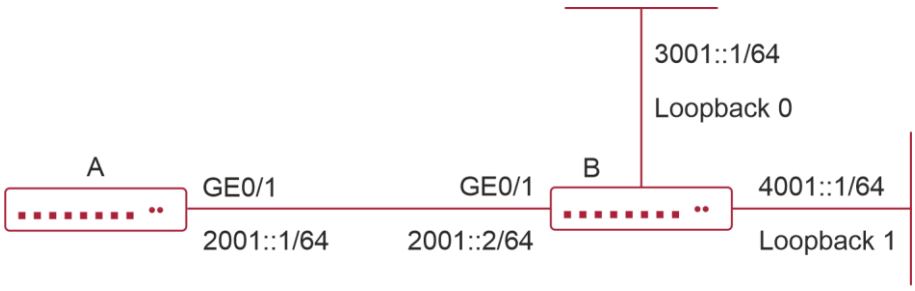


Рисунок 8-9.

Шаги настройки	• Настройте IPv6-адреса интерфейса на всех маршрутизаторах. (опущено) • Настройте базовые функции RIPng на всех маршрутизаторах. (опущено) • На маршрутизаторе A настройте фильтрацию маршрутов
A	**A# configure terminal**

	A(config)# ipv6 prefix-list hello permit 4001::/64 A(config)# ipv6 router rip A(config-router)# distribute-list prefix-list hello in
Проверка	Убедитесь, что маршрутизатор A может изучить только маршрут до 4001::/64
A	A# show ipv6 route rip IPv6 routing table name - Default - 17 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R 4001::/64 [120/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1

8.4.4. Изменение параметров выбора маршрута

8.4.4.1. Эффект конфигурации

- Измените маршруты RIPng, чтобы трафик мог проходить через указанные узлы или избегать прохождения через указанные узлы.
- Измените последовательность выбора маршрутизатором различных типов маршрутов, чтобы изменить приоритеты маршрутов RIPng.

8.4.4.2. Примечания

Необходимо настроить основные функции RIPng.

8.4.4.3. Шаги настройки

Изменение административного расстояния маршрута RIPng

- Опционально.
- Выполните эту настройку, если вы хотите изменить приоритеты маршрутов RIPng на маршрутизаторе, который использует несколько протоколов unicast-маршрутизации.

Изменение смещения метрики на интерфейсе

- Опционально.
- Если не требуется иное, выполните эту настройку на маршрутизаторе, на котором необходимо настроить метрики маршрутов.

Настройка метрики по умолчанию для внешнего маршрута, перераспределенного в RIPng

- Опционально.

- Если не требуется иное, выполните эту настройку на ASBR, к которому введены внешние маршруты.

8.4.4.4. Проверка

- Запустите команду **show ipv6 rip**, чтобы отобразить административное расстояние маршрутов RIPng.
- Запустите команду **show ipv6 rip data**, чтобы отобразить метрики внешних маршрутов, перераспределенных в RIPng.

8.4.4.5. Связанные команды

Изменение административного расстояния маршрута RIPng

Команда	**distance** *distance*
Описание параметра	*distance*: устанавливает административное расстояние маршрута RIPng. Значение представляет собой целое число от 1 до 254
Командный режим	Режим настройки процесса маршрутизации
Руководство по использованию	Запустите эту команду, чтобы установить административное расстояние маршрута RIPng

Изменение смещения метрики на интерфейсе

Команда	**ipv6 rip metric-offset** *value*
Описание параметра	*value*: указывает смещение метрики интерфейса. Значение варьируется от 1 до 16
Командный режим	Режим настройки процесса маршрутизации
Руководство по использованию	Прежде чем маршрут будет добавлен в таблицу маршрутизации, необходимо добавить метрику маршрута со смещением метрики, установленным на интерфейсе. Вы можете контролировать использование маршрута, задав смещение метрики интерфейса

Настройка метрики по умолчанию для внешнего маршрута, перераспределенного в RIPng

Команда	**default-metric** *metric*
Описание параметра	*metric*: указывает метрику по умолчанию. Допустимое значение находится в диапазоне от 1 до 16. Если значение равно или больше 16, ПО определяет, что этот маршрут недоступен

Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если метрика не указана во время перераспределения процесса протокола маршрутизации, RIPng использует метрику, определенную командой **default-metric**. Если метрика указана, метрика, определенная командой **default-metric**, заменяется указанной метрикой. Если эта команда не настроена, значение **default-metric** равно 1

8.4.4.6. Пример конфигурации

Изменение административного расстояния маршрута RIPng

Сценарий:

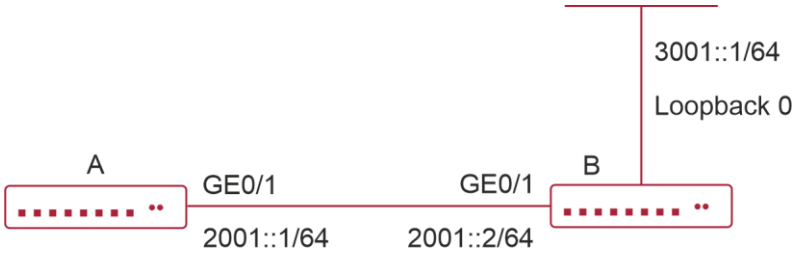


Рисунок 8-10.

Шаги настройки	• Настройте IPv6-адреса интерфейса на всех маршрутизаторах. (опущено) • Настройте базовые функции RIPng на всех маршрутизаторах. (опущено) • На маршрутизаторе A установите административное расстояние маршрута RIPng равным 160
	A# configure terminal A(config)# ipv6 router rip A(config-router)# distance 160
Проверка	На маршрутизаторе A проверьте, равно ли административное расстояние маршрута RIPng 160
	A# show ipv6 route rip | in 3001::/64 R 3001::/64 [160/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1

8.4.5. Изменение таймеров

8.4.5.1. Эффект конфигурации

Изменяйте длительность таймеров RIPng, чтобы ускорить или замедлить изменение состояния протокола или возникновение события.

8.4.5.2. Примечания

- Необходимо настроить основные функции RIPng.
- Изменение параметров управления протоколом может привести к сбоям в работе протокола. Поэтому не рекомендуется изменять таймеры.

8.4.5.3. Шаги настройки

Изменение таймера обновления, таймера неработоспособности и таймера очистки

- Обязательный.
- Если не требуется иное, выполните эту настройку на маршрутизаторе, где необходимо изменить таймеры RIPng.

8.4.5.4. Проверка

Запустите команду **show ipv6 rip**, чтобы отобразить настройки таймеров.

8.4.5.5. Связанные команды

Команда	**timers** *update invalid flush*
Описание параметра	*update*: указывает время обновления маршрута в секундах. Он определяет интервал, с которым устройство отправляет пакет обновления маршрута. Каждый раз при получении пакета обновления таймер неработоспособности и таймер очистки сбрасываются. По умолчанию пакет обновления маршрута отправляется каждые 30 секунд. *invalid*: указывает время неработоспособности маршрута в секундах, отсчитываемое от последнего времени получения действительного пакета обновления. Он определяет время, по истечении которого маршрут в списке маршрутизации становится недействительным, поскольку маршрут не обновляется. Длительность таймера неработоспособности должна быть как минимум в три раза больше длительности таймера обновления. Если пакет обновления не получен до истечения таймера неработоспособности, соответствующий маршрут переходит в недоступное состояние. Если пакет обновления получен до истечения срока действия таймера неработоспособности, таймер сбрасывается. По умолчанию продолжительность таймера неработоспособности составляет 180 с. *flush*: указывает время очистки маршрута в секундах, отсчитываемое с момента, когда маршрут RIPng переходит в недоступное состояние. По истечении времени таймера очистки маршрут в состоянии

	недоступности будет удален из таблицы маршрутизации. По умолчанию продолжительность таймера очистки составляет 120 с
Командный режим	Режим настройки процесса маршрутизации
Руководство по использованию	По умолчанию таймер обновления составляет 30 с, таймер неработоспособности — 180 с, а таймер очистки — 120 с

8.4.5.6. Пример конфигурации

Сценарий:

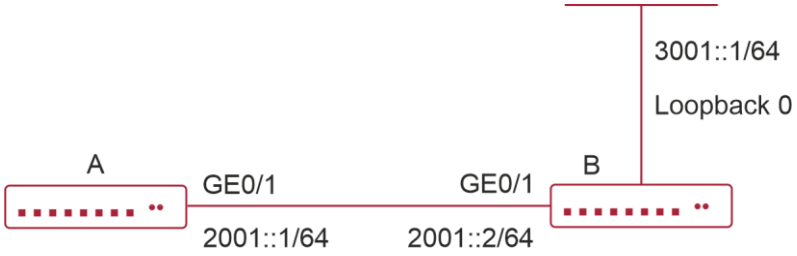


Рисунок 8-11.

Шаги настройки	• Настройте IPv6-адреса интерфейса на всех маршрутизаторах. (опущено) • Настройте базовые функции RIPng на всех маршрутизаторах. (опущено) • На маршрутизаторе A настройте таймер обновления, таймер неработоспособности и таймер очистки
B	B# configure terminal B(config)# ipv6 router rip B(config-router)# timers 10 30 90
Проверка	На маршрутизаторе B проверьте настройки таймеров RIPng
B	B# show ipv6 rip Routing Protocol is "RIPng" Sending updates every 10 seconds with +/-50%, next due in 12 seconds Timeout after 30 seconds, garbage collect after 90 seconds Outgoing update filter list for all interface is: not set Incoming update filter list for all interface is: not setwww.qtech.ru

	Default redistribution metric is 1 Default distance is 120 Redistribution: Redistributing protocol connected Default version control: send version 1, receive version 1 Interface Send Recv GigabitEthernet 0/1 1 1 Routing Information Sources: Gateway: fe80::2d0:f8ff:fe22:334a Distance: 120 Last Update: 00:00:02 Bad Packets: 0 Bad Routes: 0

8.4.5.7. Распространенные ошибки

Настройки таймеров RIPng на устройствах, подключенных к одной сети, несовместимы. Следовательно, маршруты не могут быть изучены должным образом.

8.5. Мониторинг

8.5.1. Отображение

Описание	Команда
Отображает информацию о процессе RIPng	**show ipv6 rip**
Отображает таблицу маршрутизации RIPng	**show ipv6 rip database**

8.5.2. Отладка

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

Описание	Команда
Отладка RIPng	**debug ipv6 rip** [**interface** *interface-type interface-num* | **nsm** | **restart**]

9. НАСТРОЙКА PBR

9.1. Обзор

Маршрутизация на основе политик (PBR) реализуется путем применения карты маршрутов, включая политики, к интерфейсам и устройствам.

Подобно статической маршрутизации, PBR также настраивается вручную и не может автоматически обновляться при изменениях в сети. Кроме того, PBR эффективен только для пакетов, отправленных с локальных интерфейсов и устройств. По сравнению со статической и динамической маршрутизацией PBR более гибкая. Статическая и динамическая маршрутизация может пересылать пакеты только на основе адресов назначения. PBR может пересылать пакеты на основе адресов источника и назначения, длины пакета и входного интерфейса.

9.2. Приложениес

Приложение	Описание
Выбор интернет-провайдера с помощью PBR	Указывает предпочтительные выходные интерфейсы для пакетов из разных подсетей
Реализация классификации трафика с помощью PBR	Указывает значения QoS для пакетов из разных подсетей

9.2.1. Выбор интернет-провайдера с помощью PBR

Существующая пользовательская сеть часто использует ресурсы нескольких провайдеров интернет-серверов (ISP). PBR необходимо использовать, поскольку у разных интернет-провайдеров могут быть запрошены разные полосы пропускания или необходимо защитить сетевые ресурсы ключевых пользователей. Контролируя пересылку определенных пакетов данных, вы можете в полной мере использовать ресурсы интернет-провайдера, а также удовлетворить требования гибких и разнообразных приложений.

9.2.1.1. Сценарий

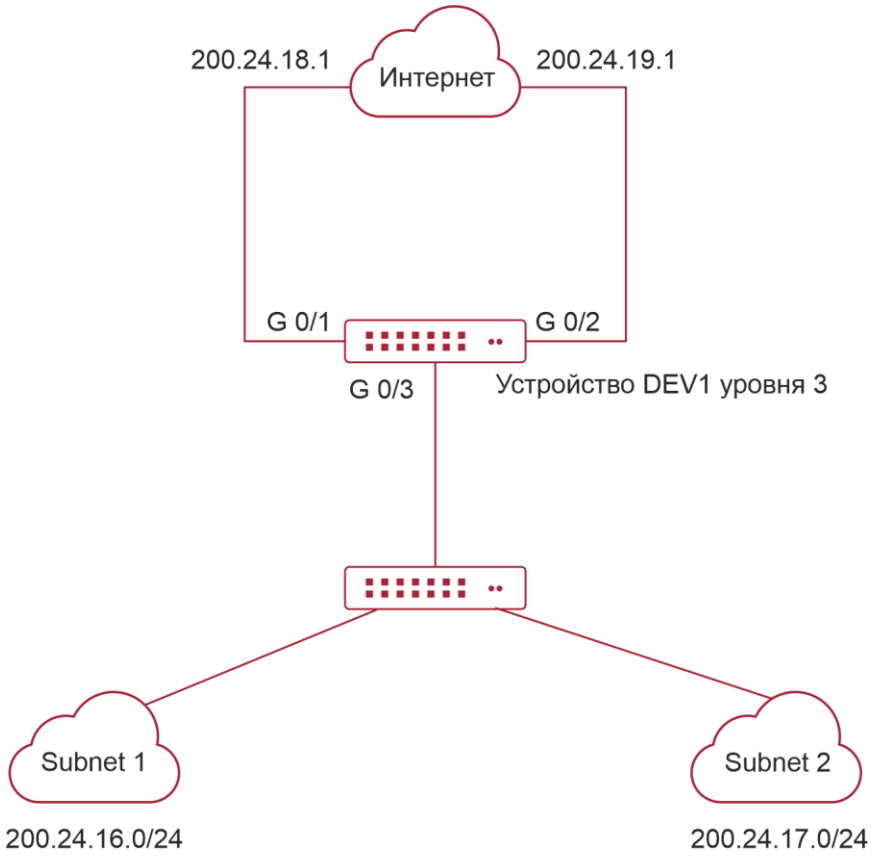


Рисунок 9-1.

Локальная сеть имеет два выходных интерфейса для подключения к Интернету. PBR настроен на устройстве DEV1 уровня 3, чтобы позволить двум выходным интерфейсам реализовать распределение нагрузки и взаимное резервное копирование.

Конкретные требования заключаются в следующем:

- Потоки данных из подсети 1 отправляются из GE 0/1.
- Потоки данных из подсети 2 отправляются из GE 0/2.
- Если канал GE 0/1 отключен, потоки данных на GE 0/1 переключаются на GE 0/2. И наоборот.

9.2.1.2. Развертывание

- Настройте два разных списка ACL на устройстве DEV1 уровня 3:
  ACL1: адреса источника принадлежат подсети 1.
  ACL2: адреса источника принадлежат подсети 2.
- Настройте две политики в карте маршрутов на устройстве уровня 3 DEV1:
  Политика 1: устанавливает следующие переходы для пакетов, соответствующих ACL1, на GE0/1 и GE0/2 (в зависимости от последовательности настройки первым вступает в силу GE0/1, а GE0/ 2 работает в режиме резервного копирования).
  Политика 2: устанавливает следующие переходы для пакетов, соответствующих

ACL2, на GE0/2 и GE0/1 (в зависимости от последовательности настройки сначала вступает в силу GE0/2, а GE0/1 работает в резервном режиме).

- Настройте PBR на GE0/3 (с помощью карты маршрутов). Затем пакеты, полученные на этом интерфейсе, пересылаются на основе политик.

9.2.2. Реализация классификации трафика с помощью PBR

9.2.2.1. Сценарий

Сети средних и малых предприятий имеют простую структуру. Различные узлы филиалов подключаются к центральным узлам через выделенные линии пересылки или в режиме Internet VPN. Корпоративным сетям часто необходимо реализовать интеграцию «три в одном» (аудио, видео и данные), чтобы максимизировать использование существующих IP-сетей и сэкономить затраты. Поскольку весь трафик выводится из одного выходного интерфейса, необходимо настроить политики QoS для выходного интерфейса, чтобы обеспечить предпочтительное качество связи для приложений, чувствительных к полосе пропускания и задержке.

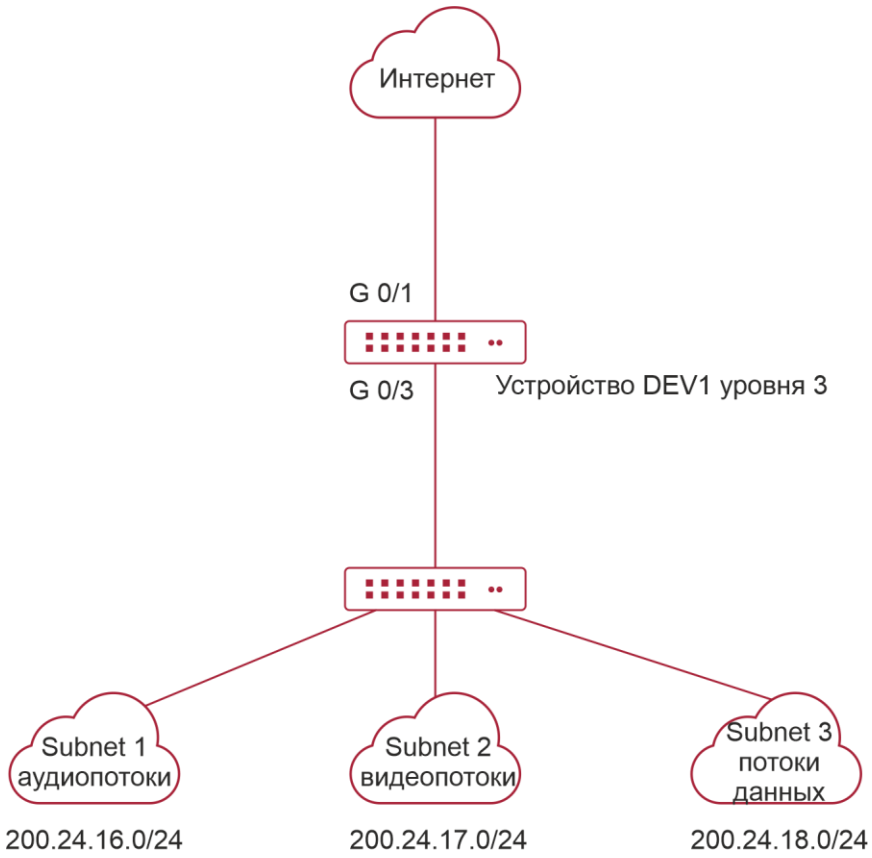


Рисунок 9-2.

LAN имеет выходной интерфейс для подключения к Интернету. PBR настроен на устройстве DEV1 уровня 3 для изменения значений QoS для пакетов из разных сетей.

Конкретные требования заключаются в следующем:

Для потоков данных из подсети 1, представляющих аудиопотоки, установите значение DSCP равным 56.

Для потоков данных из подсети 2, представляющих видеопотоки, установите значение DSCP равным 40.

Для потоков данных из подсети 3, представляющих потоки данных, установите значение DSCP равным 24.

9.2.2.2. Развертывание

- Настройте три разных списка контроля доступа на устройстве DEV1 уровня 3:

ACL1: исходные адреса принадлежат подсети 1.

ACL2: исходные адреса принадлежат подсети 2.

ACL3: исходные адреса принадлежат подсети 3.

- Настройте три политики в карте маршрутов на устройстве уровня 3 DEV1:

Политика 1: устанавливает значение DSCP для пакетов, соответствующих ACL1, равным 56.

Политика 2: устанавливает значение DSCP для пакетов, соответствующих ACL2, равным 40.

Политика 3: устанавливает значение DSCP для пакетов, соответствующих ACL3, равным 24.

- Настройте PBR на GE0/3 (с помощью карты маршрутов). Затем значения DSCP для пакетов, полученных на этом интерфейсе, изменяются в соответствии с политиками.

9.3. Функции

Особенность	Описание
Настройка политики	Перед настройкой PBR настройте политики в карте маршрута
Настройка PBR	Примените карту маршрутов, включая политики, к интерфейсам и устройствам для реализации PBR

9.3.1. Настройка политики

Политика — это оператор «сопоставить…, установить…», который указывает, что «если определенные условия совпадают, выполнить определенные действия по обработке».

ПРИМЕЧАНИЕ: подробное ознакомление с политиками смотрите в разделе Карта маршрута.

9.3.1.1. Выполнение политик

В режиме глобальной конфигурации вы можете запустить команду **route-map** *route-map-name* [**permit** | **deny**] [*sequence-number*] для создания политики в карте маршрутов.

Карта маршрутов может содержать несколько политик. Каждая политика имеет соответствующий порядковый номер. Меньший порядковый номер означает более высокий приоритет. Политики выполняются на основе их порядковых номеров. Как только условие соответствия политики выполнено, необходимо выполнить действие обработки для этой политики и завершить работу карты маршрутов. Если ни одно из условий

соответствия какой-либо политики не выполнено, никакие действия по обработке выполняться не будут.

Политики имеют два режима работы:

- permit: когда условие соответствия политики выполнено, выполните действие обработки для этой политики и выйдите из карты маршрутов.
- deny: если условие соответствия политики выполнено, не выполнять действие обработки для этой политики и выйти из карты маршрутов.

9.3.1.2. Условия соответствия политик

Условия соответствия политики могут содержать 0, 1 или более правил соответствия.

- Если содержится 0 правил соответствия, ни один пакет не будет сопоставлен.
- Если содержится одно или несколько правил соответствия, все правила соответствия должны сопоставляться одновременно, чтобы соответствовать условиям соответствия политики.

В режиме карты маршрутов запустите команду **match**, чтобы настроить правила соответствия. Одна команда **match** сопоставлена с одним правилом соответствия.

PBR поддерживает следующие команды **match**:

	Команда	**Описание**
	match ip address	IPv4-адрес источника (и IPv4-адрес назначения) используется в качестве условия соответствия. **ПРИМЕЧАНИЕ:** в политике можно настроить несколько команд **match ip address**
IPv6 PBR	**match ipv6 address**	IPv6-адрес источника (и IPv6-адрес назначения) используется в качестве условия соответствия. **ПРИМЕЧАНИЕ:** в политике можно настроить только одну команду **match ipv6 address**

ПРИМЕЧАНИЕ: IPv4 PBR определяет диапазоне IP-адресов источника (и IP-адресов назначения) пакетов с использованием стандарта IP или расширенных списков ACL. IPv6 PBR определяет диапазон IPv6-адресов источника (и IPv6-адресов назначения) пакетов с помощью расширенных списков ACL IPv6.

ПРИМЕЧАНИЕ: пересылка пакетов на основе политик интерфейсов PBR IPv4 поддерживает списки ACL уровня эксперта и MAC-имени. Пересылка пакетов на основе локальных политик не поддерживает списки ACL уровня эксперта и MAC-имени.

ПРИМЕЧАНИЕ: когда PBR использует недоступный список ACL, подкарта (sub-map) маршрута не будет сопоставлена, а вместо этого будет сопоставлена следующая подкарта маршрута. Если ни одна подкарта маршрута не соответствует, для пересылки будет выбран общий маршрут. Если настроены только ACL, но не настроен ACE, поведение пересылки PBR такое же, как и в сценарии, где ACL недоступен.

ПРИМЕЧАНИЕ: если на коммутаторе подкарта маршрута использует несколько списков ACL в PBR, сопоставляется только первый ACL.

9.3.1.3. Действие обработки для политики

Действие обработки политики может содержать 0, 1 или несколько правил установок.

- Если содержится 0 правил установок, никаких действий по обработке выполняться не будет, и карта маршрута будет немедленно закрыта.
- Если содержится одно или несколько правил установок, все действия по обработке будут выполнены и карта маршрутов завершится.

ПРИМЕЧАНИЕ: если правила установок имеют разные приоритеты, вступит в силу правило установок с наивысшим приоритетом.

В режиме карты маршрутов выполните команду **set**, чтобы настроить правила установок. Одна команда **set** сопоставляется с одним правилом установок.

PBR поддерживает следующие команды **set**:

	Команда	Описание
IPv4 PBR	**set ip tos**	Изменяет поле **tos** пакета IPv4. **ПРИМЕЧАНИЕ:** команды **set ip** и **dscp** не могут работать друг с другом
IPv4 PBR	**set ip precedence**	Изменяет поле **precedence** пакета IPv4. **ПРИМЕЧАНИЕ:** команды **set ip** и **dscp** не могут работать друг с другом
	set ip dscp	Изменяет поле **dscp** пакета IPv4. **ПРИМЕЧАНИЕ:** команды **set ip tos** и **precedence** не могут работать друг с другом
	set ip next-hop	Настраивает следующий hop для пересылки пакетов IPv4. Следующий hop должен быть подключен напрямую; в противном случае эта команда недействительна. Пакет, соответствующий правилам соответствия, будет перенаправлен на следующий hop первым, указанный параметром set ip next-hop, независимо от того, соответствует ли маршрут, выбранный для пакета в таблице маршрутизации, следующему hop-у, указанному PBR. **ПРИМЕЧАНИЕ:** на коммутаторе выходные интерфейсы для следующих hop-ов, поддерживаемые PBR, включают интерфейсы SVI, маршрутизации и AP уровня 3
	set ip next-hop recursive	Настраивает рекурсивный следующий hop для пересылки пакетов IPv4. Следующий hop может быть подключен напрямую или не подключен напрямую. Следующий hop, не подключенный напрямую, будет

	Команда	Описание
		возвращен к статическому или динамическому маршруту в таблице маршрутизации. Эта команда поддерживает рекурсию к нескольким следующим hop-ам ECMP статического или динамического маршрута. Поддерживается максимум 32 следующих hop-а. Если рекурсивный маршрут является статическим, для статического рекурсивного маршрута поддерживается только один следующий hop. Режим избыточного резервного копирования или балансировки нагрузки для нескольких рекурсивных следующих hop-ов также определяется командой **ip policy** { **redundance** | **load-balance** }. Пакет, соответствующий правилам соответствия, будет перенаправлен на следующий рекурсивный hop первым, указанный в параметре **set ip next-hop recursive**, независимо от того, соответствует ли маршрут, выбранный для пакета в таблице маршрутизации, следующему hop-у, указанному в PBR. **ПРИМЕЧАНИЕ:** только если статический или динамический маршрут имеет выходной интерфейс и IP-адрес следующего hop-а, рекурсивный следующий hop на основе политики может вступить в силу
IPv4 PBR	**set ip default next-hop**	Настраивает следующий hop по умолчанию для пересылки пакетов IPv4. Пакет, соответствующий правилам соответствия, будет перенаправлен на следующий hop по умолчанию, указанный этой командой, если маршрут не может быть выбран или для этого пакета в таблице маршрутизации выбран маршрут по умолчанию
IPv6 PBR	**set ipv6 precedence**	Изменяет поле **precedence** пакета IPv6. **ПРИМЕЧАНИЕ:** IPv6 PBR не поддерживает **set ipv6 tos** или **set ipv6 dscp**
	set ipv6 next-hop	Настраивает следующий hop для пересылки пакетов IPv6. Пакет IPv6, соответствующий правилам соответствия, будет перенаправлен на следующий hop первым , указанный параметром **set ipv6 next-hop**, независимо от того, соответствует ли маршрут,

	Команда	Описание
		выбранный для пакета IPv6 в таблице маршрутизации, следующему hop-у, указанному PBR. Следующий hop должен быть подключен напрямую; в противном случае эта команда недействительна
	set ipv6 default next-hop	Настраивает следующий hop по умолчанию для пересылки пакетов IPv6. Пакет IPv6, соответствующий правилам соответствия, будет перенаправлен на следующий hop по умолчанию, указанный этой командой, если маршрут не может быть выбран или для этого пакета в таблице маршрутизации выбран маршрут по умолчанию. Следующий hop должен быть подключен напрямую; в противном случае эта команда недействительна

ПРИМЕЧАНИЕ: последовательность приоритетов следующая: **set ip next-hop** > **set ip next-hop recursive** > общий маршрут > **set ip default next-hop** > маршрут по умолчанию. Предыдущие команды **set** можно настроить одновременно, но вступает в силу только команда с наивысшим приоритетом.

ПРИМЕЧАНИЕ: последовательность приоритетов следующая: **set ipv6 next-hop** > общий маршрут > **set ipv6 default next-hop** > маршрут по умолчанию. Предыдущие команды **set** можно настроить одновременно, но вступает в силу только команда с наивысшим приоритетом.

ПРИМЕЧАНИЕ: для коммутаторов команда **set ipv6 default next-hop** не действует для адресов IPv6, длина маски которых превышает 64.

9.3.2. Настройка PBR

9.3.2.1. PBR

Примените карту маршрутов, включая политики, к интерфейсам или устройствам для реализации PBR.

- Примените карту маршрутов к интерфейсу, чтобы пакеты, полученные интерфейсом, маршрутизировались в соответствии с политикой. PBR часто используется для управления пользовательскими пакетами, полученными устройством. Эта команда эффективна только для пересылаемых пакетов, но не для локально инициируемых пакетов.
- Примените карту маршрутов к устройству, чтобы локально инициированные пакеты маршрутизировались в соответствии с политикой. PBR часто используется для управления пакетами протоколов, которыми обмениваются устройства (например, пакеты ping, отправляемые локально). Эта команда эффективна только для локально инициируемых пакетов, но не для пересылаемых пакетов.

ПРИМЕЧАНИЕ: по умолчанию PBR доступен на устройстве, и пакеты пересылаются на основе таблицы маршрутизации.

ПРИМЕЧАНИЕ: на коммутаторе интерфейсами, поддерживающими PBR, являются интерфейс Ethernet L3, интерфейс SVI и интерфейс AP L3.

9.3.2.2. Резервное копирование или балансировка нагрузки

В политике можно установить несколько следующих hop-ов. Между несколькими следующими hop-ами можно реализовать либо избыточное резервное копирование, либо балансировку нагрузки. Резервное копирование реализовано по умолчанию.

ПРИМЕЧАНИЕ: резервное копирование или балансировка нагрузки эффективны только для следующих hop-ов, настроенных в командах **set ip next-hop**, **set ip next-hop recursive**, **set ip default next-hop**, **set ipv6 next-hop** и **set ipv6 default next-hop,** и эффективны только для нескольких следующих hop-ов в одном и том же правиле установок.

- Резервное копирование

В зависимости от последовательности настройки вступает в силу первый доступный следующий hop. Когда действующий в данный момент следующий hop (R1) неисправен, трафик автоматически переключается на следующий доступный следующий hop (R2). Когда R1 снова становится доступным, трафик автоматически переключается обратно на R1. Вновь добавленный следующий hop располагается в конце последовательности. Предположим, что исходная последовательность нескольких следующих hop-ов равна R1 > R2 > R3. После удаления и повторного добавления R1 последовательность меняется на R2 > R3 > R1. Если следующий hop недоступен, пакеты будут отброшены.

9.3.2.3. Корреляция с BFD

Корреляция между PBR и BFD эффективна только для следующих hop-ов, настроенных с помощью команды **set ip next-hop** или **set ipv6 next-hop**.

Команды **set ip next-hop** и **set ipv6 next-hop** содержат параметры **verify-availability** и **bfd** [**vrf** *vrfname*] *interface-type interface-number gateway*, которые могут устанавливать корреляцию между PBR и сеансом BFD и следить за доступностью следующих hop-ов.

Корреляция между PBR и BFD помогает улучшить восприятие PBR изменений сетевой среды. Когда BFD обнаруживает, что текущий следующий hop недоступен, BFD немедленно уведомляет PBR о необходимости переключить трафик на другой доступный следующий hop (для реализации избыточного резервного копирования) или на все другие доступные следующие hop-ы (для реализации балансировки нагрузки).

ПРИМЕЧАНИЕ: информацию о конфигурации и связанных с ней командах для корреляции между PBR и BFD см. в разделе «Reliability Configuration/Настройка BFD».

9.3.2.4. Корреляция с Track

Корреляция между PBR и Track эффективна только для следующих hop-ов, настроенных с помощью команды **set ip next-hop**.

Команда **set ip next-hop** содержит параметры **verify-availability** и **track** *track-obj-number*, которые могут устанавливать корреляцию между PBR и сеансом Track и отслеживать доступность следующих hop-ов.

Корреляция между PBR и Track помогает улучшить восприятие PBR изменений сетевой среды. Когда Track обнаруживает, что текущий следующий hop недоступен, Track немедленно уведомляет PBR о необходимости переключить трафик на другой доступный следующий hop (для реализации избыточного резервного копирования) или на все другие доступные следующие hop-ы (для реализации балансировки нагрузки).

ПРИМЕЧАНИЕ: только IPv4 PBR поддерживает корреляцию с Track.

ПРИМЕЧАНИЕ: конфигурацию и соответствующие команды для корреляции между PBR и Track см. в разделе «Reliability Configuration/RNS».

9.3.2.5. PBR на основе адреса источника

Запустите глобальные команды настройки **ip policy-source in-interface** и **ipv6 policy-source in-interface**, чтобы напрямую сгенерировать PBR на основе адреса источника. Вам не нужно настраивать карту маршрутов.

- Если для пакетов, пересылаемых интерфейсом, необходимо сопоставить только адреса IPv4 или IPv6 источника, вы можете применить команду для PBR на основе адреса источника. Процедура настройки этой команды проще, чем для PBR на основе интерфейса.
- Если PBR на основе адреса источника применяется к указанному интерфейсу, пакеты, полученные на этом интерфейсе, будут маршрутизироваться на основе политик в соответствии с адресами источника. PBR часто используется для управления пользовательскими пакетами, полученными устройством. Эта команда эффективна только для пересылаемых пакетов, но не для локально инициируемых пакетов.

ПРИМЕЧАНИЕ: PBR на основе адреса источника имеет более высокий приоритет, чем PBR на основе интерфейса. Если PBR на основе адреса источника и PBR на основе интерфейса применяются к одному и тому же интерфейсу, вступает в силу только PBR на основе интерфейса.

ПРИМЕЧАНИЕ: по умолчанию маршрутизация на основе адреса источника недоступна на устройствах, и пакеты пересылаются на основе таблицы маршрутизации.

9.4. Ограничения

Для продуктов серии QSW-7600:

Если PBR ссылается на несуществующий список ACL, подкарта (submap) маршрута не соответствует, а соответствует следующей подкарте маршрута. Если все подкарты маршрутов не совпадают, они пересылаются по общему маршруту. То же самое происходит, если настроен только ACL, а ACE — нет.

Если на коммутаторе подкарта маршрутов PBR ссылается на несколько списков ACL, она соответствует только первому ACL и не соответствует последующим ACL.

9.5. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций PBR	(Обязательно) Используется для применения PBR для пересылки пакетов	
	ip policy route-map	Применяет PBR для пакетов IPv4, полученных интерфейсом

Конфигурация	Описание и команда	
	ipv6 policy route-map	Применяет PBR для пакетов IPv6, полученных интерфейсом
	ip local policy route-map	Применяет PBR для пакетов IPv4, инициируемых локально
	ipv6 local policy route-map	Применяет PBR для пакетов IPv6, инициируемых локально
Настройка резервного копирования или балансировки нагрузки	(Опционально) Используется для установки, реализует ли PBR избыточное резервное копирование или балансировку нагрузки между несколькими следующими hop-ами	
	ip policy { **redundance** | **load-balance** }	Определяет, реализует ли IPv4 PBR избыточное резервное копирование или балансировку нагрузки между несколькими следующими hop-ами. По умолчанию установлено избыточное резервное копирование
	ipv6 policy { **redundance** | **load-balance** }	Определяет, реализует ли IPv6 PBR избыточное резервное копирование или балансировку нагрузки между несколькими следующими hop-ами. По умолчанию установлено избыточное резервное копирование
Настройка PBR на основе адреса источника	(Опционально) Используется для применения PBR на основе адреса источника для пересылки пакетов	
	ip policy-source in-interface	Применяет PBR на основе адреса источника для пакетов IPv4, полученных интерфейсом

Конфигурация	Описание и команда	
	ipv6 policy-source in-interface	Применяет PBR на основе адреса источника для пакетов IPv6, полученных интерфейсом

9.5.1. Настройка основных функций PBR

9.5.1.1. Эффект конфигурации

Выполняйте персонализированное управление маршрутизацией потоков пользовательских данных, подготавливая гибкие политики.

Выполняйте персонализированное управление взаимодействием протоколов и топологиями сети, подготавливая гибкие политики.

9.5.1.2. Примечания

- Карта маршрутов должна использоваться при настройке PBR; поэтому необходимо настроить карту маршрутов на устройстве.
- Если ACL используется при настройке карты маршрутов, необходимо настроить ACL на устройстве.

9.5.1.3. Шаги настройки

Применение PBR для пакетов IPv4, полученных интерфейсом

- Чтобы выполнить персонализированное управление маршрутизацией для потоков пользовательских данных IPv4, проходящих через устройство, вам следует выполнить эту настройку.
- Выполните эту настройку на входном интерфейсе для потоков пользовательских данных.
- Запустите команду **ip policy route-map**, чтобы применить карту маршрутов к интерфейсу. Затем PBR выполняется для пакетов IPv4, полученных на этом интерфейсе.

Команда	**ip policy route-map** *route-map-name*
Описание параметра	*route-map-name*: указывает имя карты маршрутов
По умолчанию	По умолчанию PBR недоступен на устройстве, и пакеты пересылаются на основе таблицы маршрутизации
Командный режим	Режим настройки интерфейса

Руководство по использованию	Для интерфейса можно настроить только одну команду **ip policy route-map**. Если для интерфейса настроено несколько команд **ip policy route-map**, вступает в силу только последняя конфигурация. Если карта маршрутов, используемая в PBR, недоступна, PBR не вступает в силу. Не вступит в силу, если PBR настроен на интерфейсе DAILER, Loopback или туннельном интерфейсе

Применение PBR для пакетов IPv6, полученных интерфейсом

- Чтобы выполнить персонализированное управление маршрутизацией потоков пользовательских данных IPv6, проходящих через устройство, вам следует выполнить эту настройку.
- Выполните эту настройку на входном интерфейсе для потоков пользовательских данных.
- Запустите команду **ipv6 policy route-map**, чтобы применить карту маршрутов к интерфейсу. Затем PBR выполняется для пакетов IPv6, полученных на этом интерфейсе.

Команда	**ipv6 policy route-map** *route-map-name*
Описание параметра	*route-map-name*: указывает имя карты маршрутов
По умолчанию	По умолчанию PBR недоступен на устройстве, а пакеты пересылаются на основе таблицы маршрутизации
Командный режим	Режим настройки интерфейса
Руководство по использованию	Для интерфейса можно настроить только одну команду **ipv6 policy route-map**. Если для интерфейса настроено несколько команд **ipv6 policy route-map**, вступает в силу только последняя конфигурация. Если карта маршрутов, используемая в PBR, недоступна, PBR не вступает в силу. Не вступит в силу, если PBR настроен на интерфейсе DAILER, Loopback или туннельном интерфейсе

Применение PBR для пакетов IPv4, инициируемых локально

- Чтобы выполнить персонализированное управление взаимодействием протокола IPv4 и топологией сети IPv4, необходимо выполнить данную настройку.
- Запустите команду **ip local policy route-map**, чтобы применить карту маршрутов к устройству. Затем PBR выполняется для локально инициированных пакетов IPv4.

Команда	**ip local policy route-map** *route-map-name*
Описание параметра	*route-map-name*: указывает имя карты маршрутов
По умолчанию	По умолчанию PBR недоступен на устройстве, а пакеты пересылаются на основе таблицы маршрутизации
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Для устройства можно настроить только одну команду **ip local policy route-map**. Если карта маршрутов, используемая в PBR, недоступна, PBR не вступает в силу

Применение PBR для пакетов IPv6, инициируемых локально

- Чтобы выполнить персонализированное управление взаимодействием протокола IPv6 и топологией сети IPv6, необходимо выполнить данную настройку.
- Запустите команду **ipv6 local policy route-map**, чтобы применить карту маршрутов к устройству. Затем PBR выполняется для локально инициированных пакетов IPv6.

Команда	**ipv6 local policy route-map** *route-map-name*
Описание параметра	*route-map-name*: указывает имя карты маршрутов
По умолчанию	По умолчанию PBR недоступен на устройстве, а пакеты пересылаются на основе таблицы маршрутизации
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Для устройства можно настроить только одну команду **ipv6 local policy route-map**. Если карта маршрутов, используемая в PBR, недоступна, PBR не вступает в силу

9.5.1.4. Проверка

- Проверьте конфигурации PBR.
- Проверьте конфигурации карты маршрутов, используемой PBR.
- Если ACL используется при настройке карты маршрутов, вам следует проверить конфигурации ACL.

Проверка конфигурации IPv4 PBR

Команда	**show ip policy** [*route-map-name*]
Описание параметра	*route-map-name*: указывает имя карты маршрутов
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	Проверьте интерфейсы, настроенные с помощью IPv4 PBR, по выходной информации и названию используемой карты маршрутов. QTECH# show ip policy Banlance mode: redundance Interface Route map Local RM_for_PBR_1 GigabitEthernet 0/1 RM_for_PBR_2 **Local** указывает на применение маршрутизации на основе политики для пакетов IPv4, инициируемых локально

Проверка конфигурации IPv6 PBR

Команда	**show ipv6 policy** [*route-map-name*]
Описание параметра	*route-map-name*: указывает имя карты маршрутов
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	Проверьте интерфейсы, настроенные с помощью IPv6 PBR, по выходной информации и названию используемой карты маршрутов. QTECH#show ipv6 policy Banlance mode: redundance Interface Route map Local RM_for_PBR_1 VLAN 1 RM_for_PBR_2 **Local** указывает на применение маршрутизации на основе политики для пакетов IPv6, инициируемых локально

Проверка конфигурации карты маршрутов

Команда	**show route-map** [*route-map-name*]
Описание параметра	*route-map-name*: указывает имя карты маршрутов
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	На устройстве может быть доступно несколько карт маршрутов. Сосредоточьтесь на карте маршрутов, используемой в PBR, и проверьте настройки ее политики. QTECH# show route-map route-map RM_FOR_PBR, permit, sequence 10 Match clauses: ip address acl1 Set clauses: ip next-hop 200.24.18.1 route-map RM_FOR_PBR, permit, sequence 20 Match clauses: ip address acl2 Set clauses: ip next-hop 200.24.19.1

Проверка конфигурации ACL

Команда	**show access-lists** [*acl-id* | *acl-name*]
Описание параметра	*acl-id*: указывает идентификатор ACL. *acl-name*: указывает имя ACL
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	На устройстве может быть доступно несколько списков ACL. Сосредоточьтесь на ACL, используемом картой маршрутов, и проверьте его конфигурации. QTECH# show access-lists 1 ip access-list standard 1 10 permit 200.24.16.0 0.0.0.255

	ip access-list standard 2 10 permit 200.24.17.0 0.0.0.255

Проверка информации о маршрутизации IPv4 PBR

Команда	**show ip pbr route** [**interface** *if-name* | **local**]
Описание параметра	*if-name*: указывает имя интерфейса. **local**: указывает локальный (local)
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	Укажите локальный интерфейс или устройство и проверьте информацию о маршрутизации IPv4 PBR. QTECH# show ip pbr route PBR IPv4 Route Summay : 1 Interface : GigabitEthernet 0/1 Sequence : 10 Min Length : None Max Length : None VRF ID : 0 Route Flags : Route Type : PBR Direct : Permit Priority : High Tos_Dscp : None Precedence : None Tos_Dscp : 0 Precedence : 0 Mode : redundance Nexthop Count : 1 Nexthop[0] : 192.168.8.100 Weight[0] : 1 Ifindex[0] : 2

Проверка информации о маршрутизации IPv6 PBR

Команда	**show ipv6 pbr route** [**interface** *if-name* | **local**]
Описание параметра	*if-name*: указывает имя интерфейса. **local**: указывает локальный (local)
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	Укажите локальный интерфейс или устройство и проверьте информацию о маршрутизации IPv6 PBR. QTECH# show ipv6 pbr route PBR IPv6 Route Summary : 1 Interface : GigabitEthernet 0/1 Sequence : 10 ACL[0] : 2900 ACL_CLS[0] : 5 Min Length : None Max Length : None VRF ID : 0 Route Flags : Route Type : PBR Direct : Permit Priority : High Tos_Dscp : None Precedence : None Tos_Dscp : 0 Precedence : 0 Mode : redundance Nexthop Count : 1 Nexthop[0] : 10::2 Weight[0] : 1 Ifindex[0] : 2

Проверка карты маршрутов, используемой IPv4 PBR

Команда	**show ip pbr route-map** *rmap-name*
Описание параметра	*rmap-name*: указывает имя карты маршрутов
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	Укажите карту маршрутов и проверьте карту маршрутов, используемую IPv4 PBR. QTECH# show ip pbr route-map rm PBR VRF: GLOBAL, ID: 0 Forward Mode: redundance Forwarding: On Route-map rm Route-map index: Sequence 10, permit Match rule: ACL ID : 2900, CLS: 1, Name: acl1 Set rule: Pv4 nexthop: 192.168.8.100, (VRF name: , ID: 0), Weight: 0 PBR state info ifx: 2, Connected: True, Track state: Up

Проверка карты маршрутов, используемой IPv6 PBR

Команда	**show ipv6 pbr route-map** *rmap-name*
Описание параметра	*rmap-name*: указывает имя карты маршрутов
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	Укажите карту маршрутов и проверьте карту маршрутов, используемую IPv6 PBR. QTECH# show ipv6 pbr route-map rm6 PBR VRF: GLOBAL, ID: 0 Forward Mode: redundance Forwarding: On

	Route-map rm6 Route-map index: Sequence 10, permit Match rule: ACL ID : 2901, CLS: 5, Name: acl6 Set rule: IPv6 nexthop: 10::2, (VRF name: , ID: 0), Weight: 0 PBR state info ifx: 2, Connected: True, Track state: Up

Проверка статистики о пакетах, пересылаемых IPv4 PBR

Команда	**show ip pbr statistics** [**interface** *if-name* | **local**]
Описание параметра	*if-name*: указывает имя интерфейса. **local**: указывает локальное (local)
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	QTECH# show ip pbr statistics IPv4 Policy-based route statistic gigabitEthernet 0/1 statistics : 10

Проверка статистики о пакетах, пересылаемых IPv6 PBR

Команда	**show ipv6 pbr statistics** [**interface** *if-name* | **local**]
Описание параметра	*if-name*: указывает имя интерфейса. **local**: указывает локальное (local)
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	QTECH# show ipv6 pbr statistics IPv6 Policy-based route statistic gigabitEthernet 0/1 statistics : 20

9.5.1.5. Пример конфигурации

Настройка IPv4 PBR и выбор выходного канала на основе адресов источника пакетов

Сценарий:

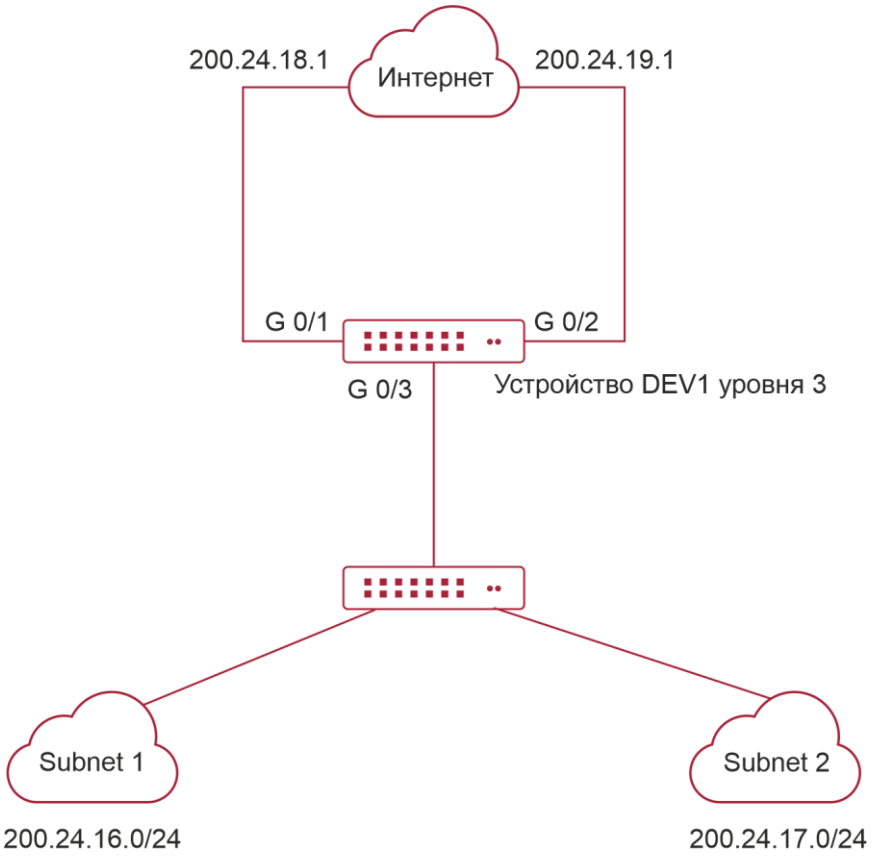


Рисунок 9-3.

	Устройство DEV 1 уровня 3 подключено к подсети 1 и подсети 2 через GE0/3. Сегмент сети, в котором находится подсеть 1, — 200.24.16.0/24, тогда как сегмент сети, в котором находится подсеть 2, — 200.24.17.0/24. DEV 1 подключен к Интернету через GE0/1 и GE0/2, а их следующие hop-ы — 200.24.18.1 и 200.24.19.1
	Эта локальная сеть (LAN) имеет два выходных интерфейса для подключения к Интернету. Требования следующие: • Потоки данных из подсети 1 для выхода в Интернет должны проходить через GE 0/1. • Потоки данных из подсети 2 для выхода в Интернет должны проходить через GE 0/2.

	• Если канал GE 0/1 отключен, потоки данных на интерфейсе GE 0/1 переключаются на интерфейс GE 0/2. И наоборот
Шаги настройки	• Настройте два списка ACL для соответствия пакетов из подсетей 1 и 2 соответственно. • Установите политику, чтобы установить следующие hop-ы для пакетов из подсети 1 в GE0/1 и GE0/2. (Обратите внимание на последовательность настройки.) • Установите политику, чтобы установить следующие hop-ы для пакетов из подсети 2 в GE0/2 и GE0/1. (Обратите внимание на последовательность настройки.) • Примените политику к GE 0/3. • Установите PBR для реализации избыточного резервного копирования между несколькими следующими hop-ами. (Настройка по умолчанию — избыточное резервное копирование.) **ПРИМЕЧАНИЕ:** во время избыточного резервного копирования, в зависимости от последовательности конфигурации, первым вступает в силу первый следующий hop
	DEV1(config)# access-list 1 permit 200.24.16.0 0.0.0.255 DEV1(config)# access-list 2 permit 200.24.17.0 0.0.0.255 DEV1(config)# route-map RM_FOR_PBR 10 DEV1(config-route-map)# match ip address 1 DEV1(config-route-map)# set ip next-hop 200.24.18.1 DEV1(config-route-map)# set ip next-hop 200.24.19.1 DEV1(config-route-map)# exit DEV1(config)# route-map RM_FOR_PBR 20 DEV1(config-route-map)# match ip address 2 DEV1(config-route-map)# set ip next-hop 200.24.19.1 DEV1(config-route-map)# set ip next-hop 200.24.18.1 DEV1(config-route-map)# exit DEV1(config)# interface GigabitEthernet 0/3 DEV1(config-if-GigabitEthernet 0/3)# ip policy route-map RM_FOR_PBR DEV1(config-if-GigabitEthernet 0/3)# exit DEV1(config)# ip policy redundance
Проверка	• Проверьте настройки IPv4 PBR. • Проверьте настройки карты маршрутов. • Проверьте конфигурации ACL

	DEV1# show ip policy Interface Route map GigabitEthernet 0/3 RM_FOR_PBR
	DEV1# show route-map route-map RM_FOR_PBR, permit, sequence 10 Match clauses: ip address 1 Set clauses: ip next-hop 200.24.18.1 200.24.19.1 route-map RM_FOR_PBR, permit, sequence 20 Match clauses: ip address 2 Set clauses: ip next-hop 200.24.19.1 200.24.18.1
	DEV1# show access-lists ip access-list standard 1 10 permit 200.24.16.0 0.0.0.255 ip access-list standard 2 10 permit 200.24.17.0 0.0.0.255

Настройка IPv6 PBR и выбор выходного канала на основе адресов источника пакетов

Сценарий:

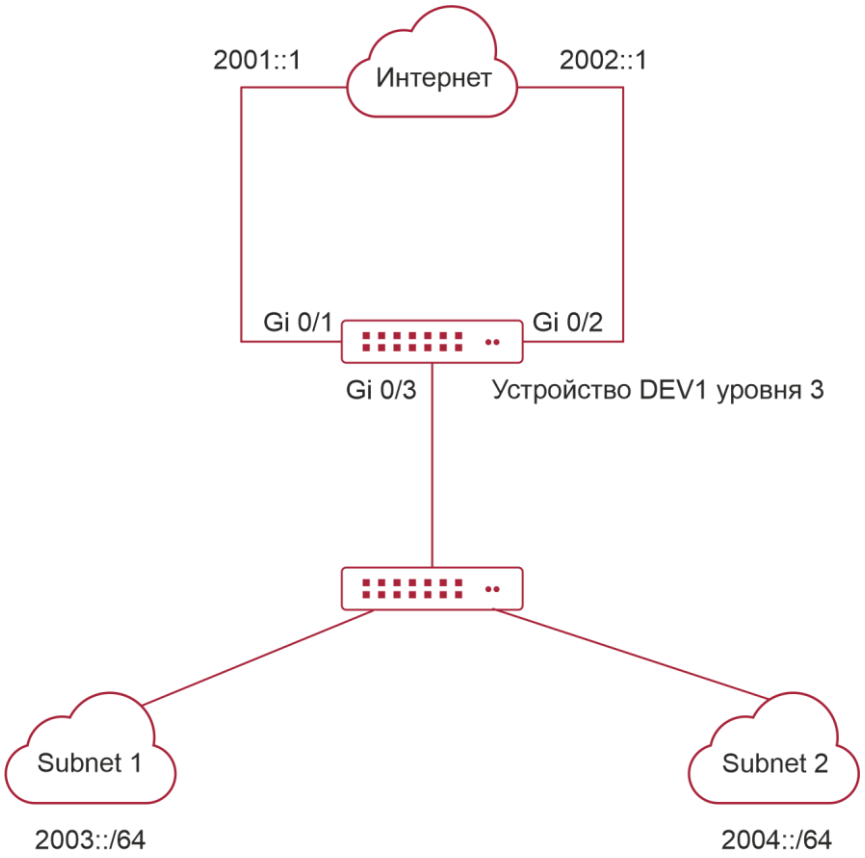


Рисунок 9-4.

	DEV 1 подключен к подсети 1 и подсети 2 через GE0/3. Сегмент сети, в котором находится подсеть 1, — это 2003::/64, тогда как сегмент сети, в котором находится подсеть 2, — 2004::/64. DEV1 подключен к Интернету через GE0/1 и GE0/2, а их следующие hop-ы — 2001::1/64 и 2002::1/64
	Эта LAN имеет два выходных интерфейса для подключения к Интернету. Требования следующие: • Потоки данных из подсети 1 для выхода в Интернет должны проходить GE 0/1. • Потоки данных из подсети 2 для выхода в Интернет должны проходить GE 0/2. • Если канал GE 0/1 отключен, потоки данных на интерфейсе GE 0/1 переключаются на интерфейс GE 0/2. И наоборот

Шаги настройки	• Настройте два списка ACL для соответствия пакетов из подсетей 1 и 2 соответственно. • Установите политику, чтобы установить следующие hop-ы для пакетов из подсети 1 в GE0/1 и GE0/2. (Обратите внимание на последовательность настройки.) • Установите политику, чтобы установить следующие hop-ы для пакетов из подсети 2 в GE0/2 и GE0/1. (Обратите внимание на последовательность настройки.) • Примените политику к GE 0/3. • Установите PBR для реализации избыточного резервного копирования между несколькими следующими hop-ами. **ПРИМЕЧАНИЕ:** во время избыточного резервного копирования, в зависимости от последовательности конфигурации, сначала вступает в силу первый следующий hop
	DEV1(config)# ipv6 access-list net1 DEV1(config-ipv6-acl)# permit ipv6 2003::/64 any DEV1(config-ipv6-acl)# exit DEV1(config)# ipv6 access-list net2 DEV1(config-ipv6-acl)# permit ipv6 2004::/64 any DEV1(config-ipv6-acl)# exit DEV1(config)# route-map RM_FOR_PBR 30 DEV1(config-route-map)# match ipv6 address net1 DEV1(config-route-map)# set ipv6 next-hop 2001::1 DEV1(config-route-map)# set ipv6 next-hop 2002::1 DEV1(config-route-map)# exit DEV1(config)# route-map RM_FOR_PBR 40 DEV1(config-route-map)# match ipv6 address net2 DEV1(config-route-map)# set ipv6 next-hop 2002::1 DEV1(config-route-map)# set ipv6 next-hop 2001::1 DEV1(config-route-map)# exit DEV1(config)# interface GigabitEthernet 0/3 DEV1(config-if-GigabitEthernet 0/3)# ipv6 policy route-map RM_FOR_PBR DEV1(config-if-GigabitEthernet 0/3)# exit DEV1(config)# ipv6 policy redundance
Проверка	• Проверьте настройки IPv6 PBR. • Проверьте настройки карты маршрутов. • Проверьте конфигурации ACL

	DEV1# show ipv6 policy Interface Route map GigabitEthernet 0/3 RM_FOR_PBR
	DEV1# show route-map route-map RM_FOR_PBR, permit, sequence 11 Match clauses: ipv6 address net1 Set clauses: ipv6 next-hop 2001::1 2002::1 route-map RM_FOR_PBR, permit, sequence 21 Match clauses: ipv6 address net2 Set clauses: ipv6 next-hop 2002::1 2001::1
	DEV1# show access-lists ipv6 access-list net1 10 permit ipv6 2003::/64 any (0 packets matched) ipv6 access-list net2 10 permit ipv6 2004::/64 any (0 packets matched)

Настройка корреляции между IPv4 PBR и Track

Сценарий:

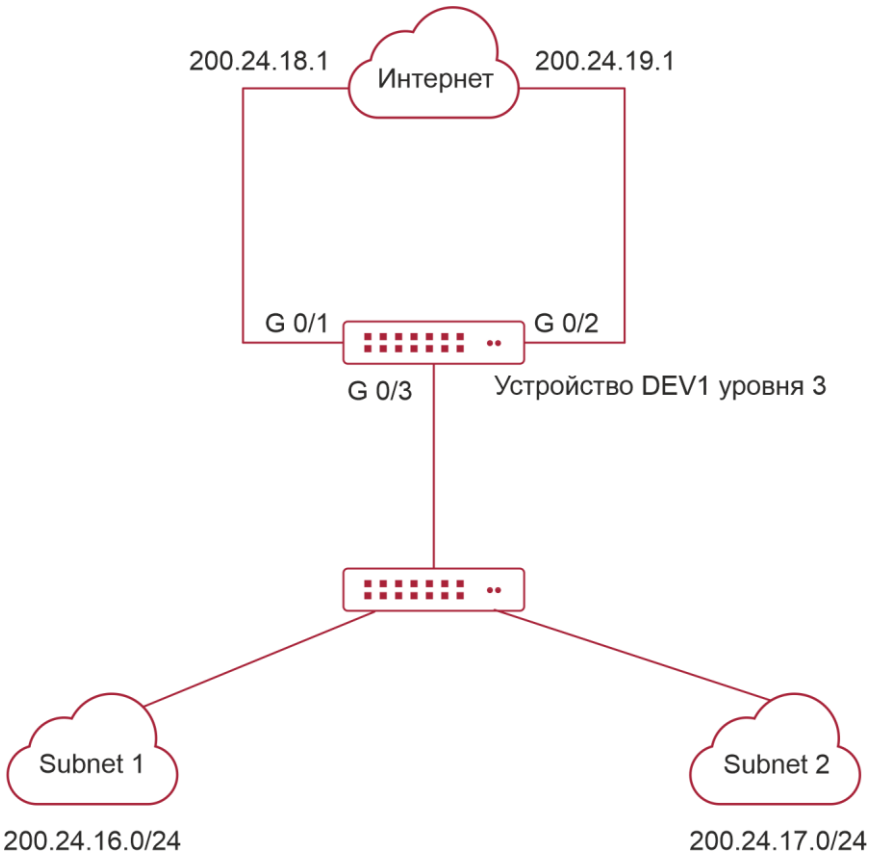


Рисунок 9-5.

	Устройство DEV 1 уровня 3 подключено к подсети 1 и подсети 2 через GE0/3. Сегмент сети, в котором находится подсеть 1, — 200.24.16.0/24, тогда как сегмент сети, в котором находится подсеть 2, — 200.24.17.0/24. DEV 1 подключен к Интернету через GE0/1 и GE0/2, а их следующие hop-ы — 200.24.18.1 и 200.24.19.1
	DEV1 может быстро обнаружить неисправный выходной канал и переключиться на резервный канал
Шаги настройки	При настройке IPv4 PBR и выбора выходного канала на основе адресов источника пакетов, добавьте или измените следующие конфигурации: • Установите два объекта Track и отслеживайте доступность следующих hop-ов двух выходных интерфейсов. • При настройке политики установите корреляцию между следующими hop-ами и объектами Track

DEV1	DEV1(config)# ip access-list extended 101 DEV1(config-ip-acl)# permit ip 200.24.16.0 0.0.0.255 any DEV1(config-ip-acl)# exit DEV1(config)# ip access-list extended 102 DEV1(config-ip-acl)# permit ip 200.24.17.0 0.0.0.255 any DEV1(config-ip-acl)# exit DEV1(config)#ip rns 1 DEV1(config-ip-rns)#icmp-echo 200.24.18.1 DEV1(config)#ip rns schedule 1 start-time now life forever DEV1(config)#track 1 rns 1 DEV1(config)#ip rns 2 DEV1(config-ip-rns)#icmp-echo 200.24.19.1 DEV1(config)#ip rns schedule 2 start-time now life forever DEV1(config)#track 2 rns 2 DEV1(config)# route-map RM_FOR_PBR 10 DEV1(config-route-map)# match ip address 101 DEV1(config-route-map)# set ip next-hop verify-availability 200.24.18.1 track 1 DEV1(config-route-map)# set ip next-hop verify-availability 200.24.19.1 track 2 DEV1(config-route-map)# exit DEV1(config)# route-map RM_FOR_PBR 20 DEV1(config-route-map)# match ip address 102 DEV1(config-route-map)# set ip next-hop verify-availability 200.24.19.1 track 2 DEV1(config-route-map)# set ip next-hop verify-availability 200.24.18.1 track 1 DEV1(config-route-map)# exit DEV1(config)# interface GigabitEthernet 0/3 DEV1(config-if-GigabitEthernet 0/3)# ip policy route-map RM_FOR_PBR DEV1(config-if-GigabitEthernet 0/3)# exit DEV1(config)# ip policy redundance
Проверка	Проверьте, что объекты Track в состоянии Up
DEV1	QTECH#show track Track 1 Reliable Network Service 1 The state is Up 1 change, current state last: 120 secs

	Delay up 30 secs, down 50 secs Track 2 Reliable Network Service 2 The state is Up 1 change, current state last: 130 secs Delay up 30 secs, down 50 secs

Настройка рекурсивного PBR IPv4, выбор выходного канала на основе адресов источника пакетов и повторяющееся обращение к выходному каналу динамического маршрута

Сценарий:

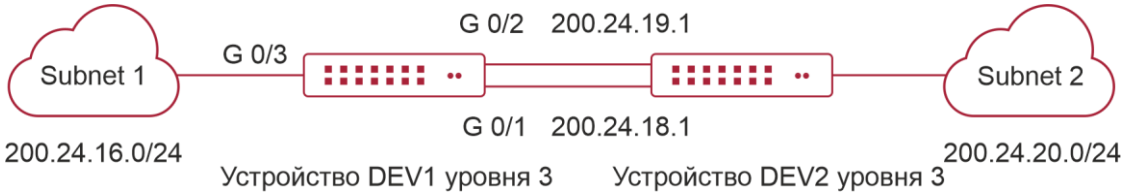


Рисунок 9-6.

	Устройство DEV 1 уровня 3 подключено к подсети 1 через GE0/3. Сегмент сети, в котором находится подсеть 1, — 200.24.16.0/24. DEV 1 подключен к подсети 2 через GE0/1 и GE0/2, а их следующие hop-ы — 200.24.18.1 и 200.24.19.1
	Подсеть 1 подключена к подсети 2 через два выходных интерфейса DEV1. Требования следующие: • Заранее настройте статические или динамические маршруты, чтобы гарантировать, что статические или динамические маршруты в сегменте сети 200.24.20.0 доступны в таблице маршрутизации DEV1. • Потоки данных из подсети 1 для доступа в Интернет могут повторяться по динамическому маршруту с IP-адресом 200.24.20.1. • Если канал GE 0/1 отключен, потоки данных на GE 0/1 переключаются на GE 0/2. И наоборот
Шаги настройки	• Настройте ACL для соответствия пакетов из подсети 1. • Установите политику для установки рекурсивного следующего hop-а для пакетов из подсети 1 в 200.24.20.1. • Примените политику к GE 0/3.

	• Установите PBR для реализации избыточного резервного копирования между несколькими следующими hop-ами. (Настройка по умолчанию — избыточное резервное копирование.) **ПРИМЕЧАНИЕ:** во время избыточного резервного копирования последовательность вступления в силу следующих hop-ов связана с последовательностью вступления в силу статических или динамических маршрутов
	DEV1(config)# access-list 1 permit 200.24.16.0 0.0.0.255 DEV1(config)# route-map RM_FOR_PBR 10 DEV1(config-route-map)# match ip address 1 DEV1(config-route-map)# set ip next-hop recursive 200.24.20.1 DEV1(config-route-map)# exit DEV1(config)# interface GigabitEthernet 0/3 DEV1(config-if-GigabitEthernet 0/3)# ip policy route-map RM_FOR_PBR DEV1(config-if-GigabitEthernet 0/3)# exit DEV1(config)# ip policy redundance
Проверка	• Проверьте настройки IPv4 PBR. • Проверьте настройки карты маршрутов. • Проверьте конфигурации списков ACL
	DEV1# show ip policy Interface Route map GigabitEthernet 0/3 RM_FOR_PBR
	DEV1# show route-map route-map RM_FOR_PBR, permit, sequence 10 Match clauses: ip address 1 Set clauses: ip next-hop recursive 200.24.20.1
	DEV1# show access-lists ip access-list standard 1 10 permit 200.24.16.0 0.0.0.255

9.5.1.6. Распространенные ошибки

- Карта маршрутов используется, когда PBR настроен, но карта маршрутов не существует.

- ACL используется, когда карта маршрутов настроена, но ACL не существует.

9.5.2. Настройка резервного копирования или балансировки нагрузки

9.5.2.1. Эффект конфигурации

- Использование нескольких следующих hop-ов в режиме взаимного резервного копирования может повысить надежность сети.
- Реализация балансировки нагрузки между несколькими следующими hop-ами может расширить пропускную способность сети.

9.5.2.2. Примечания

- Необходимо настроить основные функции PBR.
- Резервное копирование и балансировка нагрузки эффективны только для следующих hop-ов, заданных следующими командами **set**.

Команда	Описание
set ip next-hop	Настраивает следующий hop пакетов IPv4. Эта команда содержит параметр *weight*, который используется для установки веса WCMP. Значение по умолчанию — 1
set ip default next-hop	Настраивает следующий hop по умолчанию для пакетов IPv4. Эта команда содержит параметр *weight*, который используется для установки веса WCMP. Значение по умолчанию — 1
set ipv6 next-hop	Настраивает следующий hop пакетов IPv6. Эта команда содержит параметр *weight*, который используется для установки веса WCMP. Значение по умолчанию — 1
set ipv6 default next-hop	Настраивает следующий hop по умолчанию для пакетов IPv6. Эта команда содержит параметр *weight*, который используется для установки веса WCMP. Значение по умолчанию — 1
set ip next-hop recursive	Настраивает рекурсивный следующий hop пакетов IPv4. Для карты маршрутов можно настроить только одну команду, и пакеты могут повторяться на нескольких следующих hop-ах (до 32 следующих hop-ов) статического или динамического маршрута ECMP. Режим резервного копирования или балансировки нагрузки для повторения нескольких следующих hop-ов также определяется командой **ip policy** { **redundance** | **load-balance** }

ПРИМЕЧАНИЕ: для WCMP можно установить до восьми следующих hop-ов, а для ECMP — до 32 следующих hop-ов.

9.5.2.3. Шаги настройки

Настройка того, реализует ли IPv4 PBR избыточное резервное копирование или балансировку нагрузки между несколькими следующими hop-ами

- Если необходимо реализовать балансировку нагрузки между несколькими следующими hop-ами, необходимо выполнить эту настройку.
- Если в настоящее время настроена балансировка нагрузки, вам также необходимо выполнить эту настройку для сброса избыточного резервного копирования.
- Эта конфигурация действительна для всех PBR, настроенных на устройстве.

Команда	**ip policy** { **redundance** | **load-balance** }
Описание параметра	**redundance**: указывает избыточное резервное копирование. **load-balance**: указывает балансировку нагрузки
По умолчанию	Резервное копирование настроено по умолчанию
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если выбрано избыточное резервное копирование, вступает в силу первый следующий hop в зависимости от последовательности конфигурации. Если выбрана балансировка нагрузки, все следующие hop-ы вступают в силу одновременно и распределяют трафик по весу

Настройка того, реализует ли Ipv6 PBR избыточное резервное копирование или балансировку нагрузки между несколькими следующими hop-ами

- Если необходимо реализовать балансировку нагрузки между несколькими следующими hop-ами, необходимо выполнить эту настройку.
- Если в настоящее время настроена балансировка нагрузки, вам также необходимо выполнить эту настройку для сброса избыточного резервного копирования.
- Эта конфигурация действительна для всех PBR, настроенных на устройстве.

Команда	**ipv6 policy** { **redundance** | **load-balance** }
Описание параметра	**redundance**: указывает избыточное резервное копирование. **load-balance**: указывает балансировку нагрузки
По умолчанию	Резервное копирование настроено по умолчанию

Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если выбрано избыточное резервное копирование, вступает в силу первый следующий hop в зависимости от последовательности конфигурации. Если выбрана балансировка нагрузки, все следующие hop-ы вступают в силу одновременно и распределяют трафик по весу

9.5.2.4. Проверка

Проверьте, реализовано ли избыточное резервное копирование или балансировка нагрузки между несколькими следующими hop-ами.

Проверка того, реализует ли IPv4 PBR избыточное резервное копирование или балансировку нагрузки между несколькими следующими hop-ами

Команда	**show ip policy** [*route-map-name*]
Описание параметра	*route-map-name*: указывает карту маршрута
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	QTECH# show ip policy Banlance mode: redundance Interface Route map Local test GigabitEthernet 0/3 test

Проверка того, реализует ли IPv6 PBR избыточное резервное копирование или балансировку нагрузки между несколькими следующими hop-ами

Команда	**show ipv6 policy** [*route-map-name*]
Описание параметра	*route-map-name*: указывает карту маршрута
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации

Руководство по использованию	PE#show ipv6 policy Banlance mode: redundance Interface Route map VLAN 1 RM_for_Vlan_1 VLAN 2 RM_for_Vlan_2

9.5.2.5. Пример конфигурации

Настройка PBR IPv4 для реализации избыточного резервного копирования между несколькими следующими hop-ами

См. предыдущий пример: Настройка IPv4 PBR и выбор выходного канала на основе адресов источника пакетов в разделе 9.5.1.5.

Настройка IPv6 PBR для реализации избыточного резервного копирования между несколькими следующими hop-ами

См. предыдущий пример: Настройка IPv6 PBR и выбор выходного канала на основе адресов источника пакетов в разделе 9.5.1.5.

Настройка PBR IPv4 для реализации балансировки нагрузки между несколькими следующими hop-ами

Сценарий:

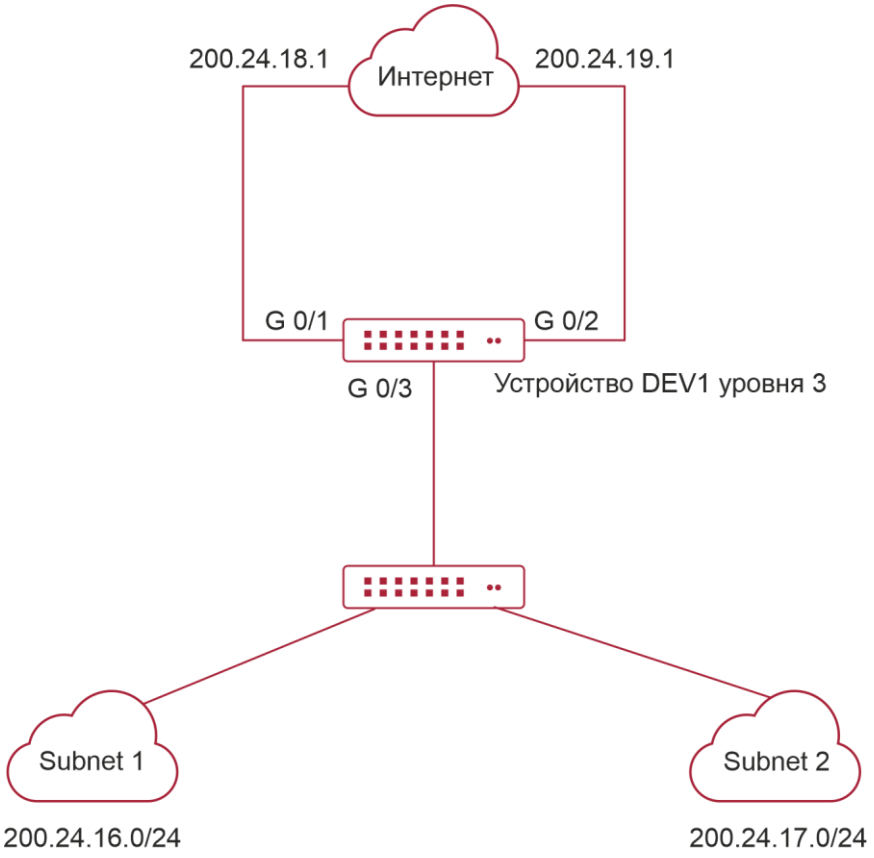


Рисунок 9-7.

	Устройство DEV 1 уровня 3 подключено к подсети 1 и подсети 2 через GE0/3. Сегмент сети, в котором находится подсеть 1, — 200.24.16.0/24, тогда как сегмент сети, в котором находится подсеть 2, — 200.24.17.0/24. DEV 1 подключен к Интернету через GE0/1 и GE0/2, а их следующие hop-ы — 200.24.18.1 и 200.24.19.1
	Эта LAN сеть имеет два выходных интерфейса для подключения к Интернету. Требования следующие: Трафик поровну распределяется между GE0/1 и GE0/2
Шаги настройки	• Настройте основные функции PBR. Укажите несколько следующих hop-ов. • Установите режим балансировки нагрузки
	DEV1(config)# route-map RM_LOAD_PBR 10 DEV1(config-route-map)# set ip next-hop 200.24.18.1 DEV1(config-route-map)# set ip next-hop 200.24.19.1 DEV1(config-route-map)# exit DEV1(config)# interface GigabitEthernet 0/3 DEV1(config-if-GigabitEthernet 0/3)# ip policy route-map RM_LOAD_PBR DEV1(config-if-GigabitEthernet 0/3)# exit DEV1(config)# ip policy load-balance
Проверка	• Проверьте настройки IPv4 PBR. • Проверьте настройки карты маршрутов
	DEV1# show ip policy Balance mode: load-balance Interface Route map GigabitEthernet 0/3 RM_LOAD_PBR
	DEV1# show route-map route-map PBR-VRF-Selection, permit, sequence 10 Match clauses: Set clauses: ip next-hop 200.24.18.1 8 ip next-hop 200.24.19.1 8

Настройка PBR IPv6 для реализации балансировки нагрузки между несколькими следующими hop-ами

Сценарий:

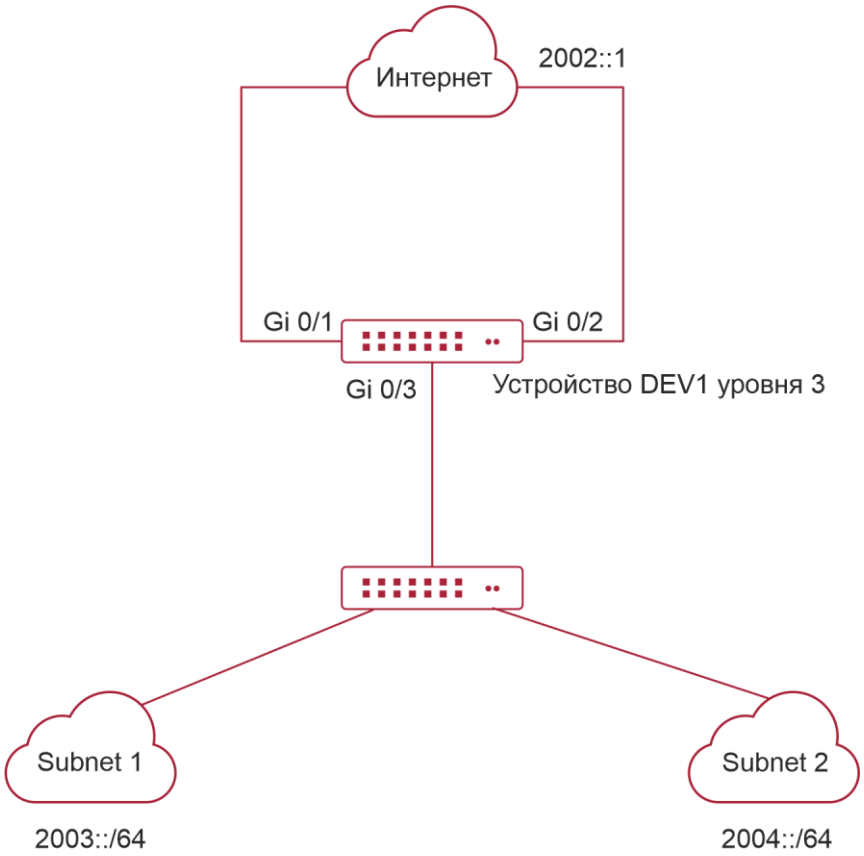


Рисунок 9-8.

	DEV 1 подключен к подсети 1 и подсети 2 через GE0/3. Сегмент сети, в котором находится подсеть 1, — это 2003::/64, тогда как сегмент сети, в котором находится подсеть 2, — 2004::/64. DEV1 подключен к Интернету через GE0/1 и GE0/2, а их следующие hop-ы — 2001::1/64 и 2002::1/64
	Эта LAN имеет два выходных интерфейса для подключения к Интернету. Требования следующие: Трафик поровну распределяется между GE0/1 и GE0/2
Шаги настройки	• Настройте основные функции PBR. Укажите несколько следующих hop-ов. • Установите режим балансировки нагрузки
	DEV1(config)# route-map RM_LOAD_PBR 20

	DEV1(config-route-map)# set ipv6 next-hop 2001::1 DEV1(config-route-map)# set ipv6 next-hop 2002::1 DEV1(config-route-map)# exit DEV1(config)# interface GigabitEthernet 0/3 DEV1(config-if-GigabitEthernet 0/3)# ipv6 policy route-map RM_LOAD_PBR DEV1(config-if-GigabitEthernet 0/3)# exit DEV1(config)# ipv6 policy load-balance
Проверка	• Проверьте настройки IPv6 PBR. • Проверьте настройки карты маршрутов
	DEV1# show ipv6 policy Balance mode: load-balance Interface Route map GigabitEthernet 0/3 RM_LOAD_PBR DEV1# show route-map route-map PBR-VRF-Selection, permit, sequence 10 Match clauses: Set clauses: ipv6 next-hop 2001::1 ipv6 next-hop 2002::1

9.5.3. Настройка PBR на основе адреса источника

9.5.3.1. Эффект конфигурации

Выполняйте персонализированное управление маршрутизацией для адресов IPv4 или IPv6 потоков пользовательских данных, подготавливая гибкие политики.

9.5.3.2. Примечания

PBR на основе адреса источника имеет более высокий приоритет, чем PBR на основе интерфейса. Когда они применяются к интерфейсу одновременно, PBR на основе интерфейса вступает в силу, тогда как PBR на основе адреса источника не вступает в силу.

9.5.3.3. Шаги настройки

Применение PBR на основе адреса источника для пакетов IPv4, полученных интерфейсом

- Чтобы выполнить персонализированное управление маршрутизацией на основе исходных IPv4-адресов для потоков пользовательских данных IPv4, проходящих через устройство, вам следует выполнить эту настройку.
- Глобальная конфигурация влияет на входной интерфейс указанных потоков пользовательских данных.

- Запустите команду **ip policy-source in-interface**, чтобы выполнить PBR на основе адреса источника для пакетов IPv4, полученных указанным интерфейсом.

Команда	**ip policy-source in-interface** *interface-type sequence* {*source-address mask* | *source-address/mask*} {[**default**] **next-hop** *ip-address* [*weight*] | [**default**] *interface out-interface-type* | **vrf** *vrf-name*}
Описание параметра	*interface-type*: указывает тип интерфейса, к которому применяется PBR адреса источника. *sequence*: указывает порядковый номер политики. Меньший порядковый номер означает более высокий приоритет. *source-address*: указывает исходный IPv4-адрес. *mask*: указывает маску исходного IPv4-адреса. *ip-address*: указывает IPv4-адрес следующего hop-a. *weight*: указывает вес следующего hop-a. *out-interface-type*: указывает тип выходного интерфейса следующего hop-a. *vrf-name*: указывает имя экземпляра VRF
По умолчанию	По умолчанию PBR на основе адреса источника недоступен на устройстве, а пакеты пересылаются на основе таблицы маршрутизации
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Настройте несколько команд **ip policy-source in-interface** для одного и того же интерфейса. Порядковые номера разных адресов источника различны. Меньший порядковый номер означает более высокий приоритет PBR на основе адреса источника. Когда порядковый номер один и тот же, приоритеты следующих hop-ов следующие: **vrf** *vrf-name* > **next-hop** *ip-address* > **interface** *out-interface-type* > **default next-hop** *ip-address* > **default interface** *out-interface-type*. PBR на основе адреса источника имеет более высокий приоритет, чем PBR на основе интерфейса. Когда они применяются к интерфейсу одновременно, PBR на основе интерфейса вступает в силу, тогда как PBR на основе адреса источника не вступает в силу

Применение PBR на основе адреса источника для пакетов IPv6, полученных интерфейсом

- Чтобы выполнить персонализированное управление маршрутизацией на основе исходных IPv6-адресов для потоков пользовательских данных IPv6, проходящих через устройство, необходимо выполнить эту настройку.
- Глобальная конфигурация влияет на входной интерфейс указанных потоков пользовательских данных.

- Запустите команду **ipv6 policy-source in-interface**, чтобы выполнить PBR на основе адреса источника для пакетов IPv6, полученных указанным интерфейсом.

Команда	**ipv6 policy-source in-interface** *interface-type sequence* {*source-address*/*prefix-length*} {[**default**] **next-hop** *ipv6-address* [*weight*] | [**default**] **interface** *out-interface-type* | **vrf** *vrf-name*}
Описание параметра	*interface-type*: указывает тип интерфейса, к которому применяется PBR адреса источника. *sequence*: указывает порядковый номер политики. Меньший порядковый номер означает более высокий приоритет. *source-address*: указывает исходный IPv6-адрес. *prefix-length*: указывает длину префикса исходного IPv6-адреса. *ipv6-address*: указывает IPv6-адрес следующего hop-a. *weight*: указывает вес следующего hop-a. *out-interface-type*: указывает тип выходного интерфейса следующего hop-a. *vrf-name*: указывает имя экземпляра VRF
По умолчанию	По умолчанию PBR на основе адреса источника недоступен на устройстве, а пакеты пересылаются на основе таблицы маршрутизации
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Настройте несколько команд **ipv6 policy-source in-interface** для одного и того же интерфейса. Порядковые номера разных адресов источника различны. Меньший порядковый номер означает более высокий приоритет PBR на основе адреса источника. Если порядковый номер один и тот же, приоритеты следующих hop-ов следующие: **vrf** *vrf-name* > **next-hop** *ipv6-address* > **interface** *out-interface-type* > **default next-hop** *ipv6-address* > **default interface** *out-interface-type*. PBR на основе адреса источника имеет более высокий приоритет, чем PBR на основе интерфейса. Когда они применяются к интерфейсу одновременно, PBR на основе интерфейса вступает в силу, тогда как PBR на основе адреса источника не вступает в силу

9.5.3.4. Проверка

Проверка информации о маршрутизации IPv4 PBR на основе адреса источника

Команда	**show ip pbr source-route** [**interface** *if-name*]
Описание параметра	*if-name*: указывает имя интерфейса
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	Укажите интерфейс и проверьте информацию о маршрутизации PBR на основе адреса источника IPv4. QTECH# show ip pbr source-route PBR IPv4 Source Route Interface : GigabitEthernet 0/1 Sequence : 10 Source address : 10.1.1.1/24 VRF ID : 0 Route Flags : Route Type : PBR Direct : Permit Priority : High Match_ipaddr : Exist Mode : redundance Nexthop Count : 1 Nexthop[0] : 192.168.8.100 Weight[0] : 1 Ifindex[0] : 2

Проверка информации о маршрутизации IPv6 PBR

Команда	**show ipv6 pbr source-route** [**interface** *if-name*]
Описание параметра	*if-name*: указывает имя интерфейса
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации

Руководство по использованию	Укажите интерфейс и проверьте информацию о маршрутизации IPv6 PBR. QTECH# show ipv6 pbr source-route PBR IPv6 Source Route Interface : GigabitEthernet 0/1 Sequence : 10 Source address : 1000::1/64 VRF ID : 0 Route Flags : Route Type : PBR Direct : Permit Priority : High Match_ipaddr : Exist Mode : redundance Nexthop Count : 1 Nexthop[0] : 1001::2 Weight[0] : 1 Ifindex[0] : 3

9.5.3.5. Пример конфигурации

Настройка PBR на основе адреса источника IPv4 и выбор выходного канала на основе адресов источника пакетов

Сценарий:

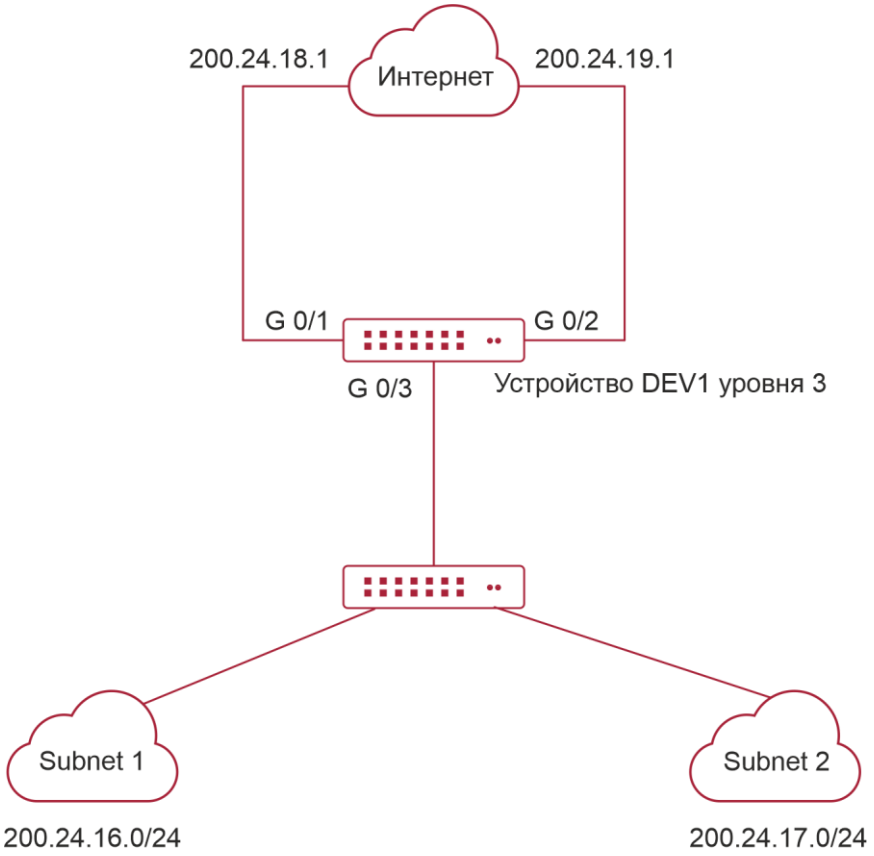


Рисунок 9-9.

	Устройство DEV 1 уровня 3 подключено к подсети 1 и подсети 2 через GE0/3. Сегмент сети, в котором находится подсеть 1, — 200.24.16.0/24, тогда как сегмент сети, в котором находится подсеть 2, — 200.24.17.0/24. DEV 1 подключен к Интернету через GE0/1 и GE0/2, а их следующие hop-ы — 200.24.18.1 и 200.24.19.1
	Эта LAN имеет два выходных интерфейса для подключения к Интернету. Требования следующие: • Потоки данных из подсети 1 для выхода в Интернет должны проходить через GE 0/1. • Потоки данных из подсети 2 для выхода в Интернет должны проходить через GE 0/2. • Если канал GE 0/1 отключен, потоки данных на GE 0/1 переключаются на GE 0/2. И наоборот

Шаги настройки	• Установите PBR на основе адреса источника и установите следующие hop-ы для пакетов из подсети 1 GE0/3 в GE0/1 и GE0/2. (Обратите внимание на последовательность настройки.) • Установите PBR на основе адреса источника и установите следующие hop-ы для пакетов из подсети 2 GE0/3 в GE0/2 и GE0/1. (Обратите внимание на последовательность настройки.) • Установите PBR для реализации избыточного резервного копирования между несколькими следующими hop-ами. (Настройка по умолчанию — избыточное резервное копирование.) **ПРИМЕЧАНИЕ:** во время избыточного резервного копирования, в зависимости от последовательности конфигурации, первым вступает в силу первый следующий hop
	DEV1(config)# ip policy-source in-interface gigabitEthernet 0/3 1 200.24.16.0/24 next-hop 200.24.18.1 200.24.19.1 DEV1(config)# ip policy-source in-interface gigabitEthernet 0/3 2 200.24.17.0/24 next-hop 200.24.19.1 200.24.18.1 DEV1(config)# ip policy redundance
Проверка	Проверьте информацию о маршрутизации PBR IPv4 на основе адреса источника
	DEV1# show ip pbr source-route PBR IPv4 Source Route Interface : GigabitEthernet 0/3 Sequence : 1 Source address : 200.24.16.0/24 VRF ID : 0 Route Flags : Route Type : PBR Direct : Permit Priority : High Match_ipaddr : Exist Mode : redundance Nexthop Count : 2 Nexthop[0] : 200.24.18.1 Weight[0] : 1 Ifindex[0] : 1 Nexthop[1] : 200.24.19.1

	Weight[1] : 1 Ifindex[1] : 2 Interface : GigabitEthernet 0/3 Sequence : 2 Source address : 200.24.17.0/24 VRF ID : 0 Route Flags : Route Type : PBR Direct : Permit Priority : High Match_ipaddr : Exist Mode : redundance Nexthop Count : 2 Nexthop[0] : 200.24.19.1 Weight[0] : 1 Ifindex[0] : 2 Nexthop[1] : 200.24.18.1 Weight[1] : 1 Ifindex[1] : 1

Настройка PBR на основе адреса источника IPv6 и выбор выходного канала на основе адресов источника пакетов

Сценарий:

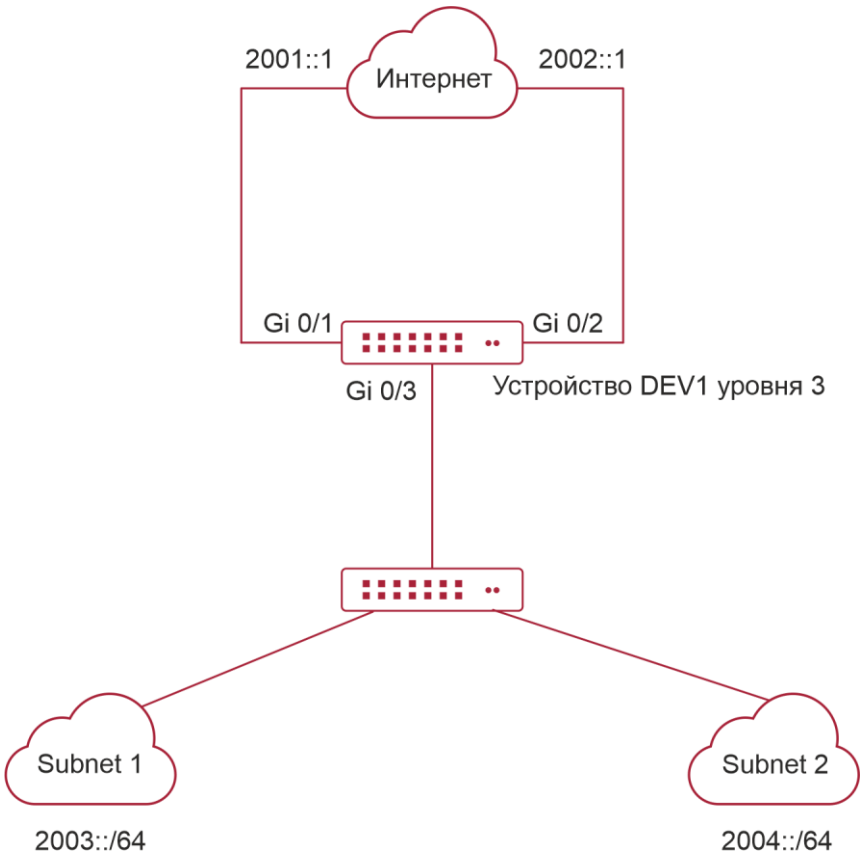


Рисунок 9-10.

	DEV 1 подключен к подсети 1 и подсети 2 через GE0/3. Сегмент сети, в котором находится подсеть 1, — это 2003::/64, тогда как сегмент сети, в котором находится подсеть 2, — 2004::/64. DEV1 подключен к Интернету через GE0/1 и GE0/2, а их следующие hop-ы — 2001::1/64 и 2002::1/64
	Эта LAN имеет два выходных интерфейса для подключения к Интернету. Требования следующие: • Потоки данных из подсети 1 для выхода в Интернет должны проходить через GE 0/1. • Потоки данных из подсети 2 для выхода в Интернет должны проходить через GE 0/2. • Если канал GE 0/1 неисправен, потоки данных на GE 0/1 переключаются на GE 0/2. И наоборот

Шаги настройки	• Установите PBR на основе адреса источника и установите следующие hop-ы для пакетов из подсети 1 GE0/3 в GE0/1 и GE0/2. (Обратите внимание на последовательность настройки.) • Установите PBR на основе адреса источника и установите следующие hop-ы для пакетов из подсети 2 GE0/3 в GE0/2 и GE0/1. (Обратите внимание на последовательность настройки.) • Установите PBR для реализации избыточного резервного копирования между несколькими следующими hop-ами. **ПРИМЕЧАНИЕ:** во время избыточного резервного копирования, в зависимости от последовательности конфигурации, первым вступает в силу первый следующий hop
	DEV1(config)# ipv6 policy-source in-interface gigabitEthernet 0/3 1 2003::/64 next-hop 2001::1 2002::1 DEV1(config)# ip policy-source in-interface gigabitEthernet 0/3 2 2004::/64 next-hop 2002::1 2001::1 DEV1(config)# ipv6 policy redundance
Проверка	Проверьте конфигурацию PBR на основе адреса источника IPv6
	DEV1# show ipv6 pbr source-route PBR IPv6 Source Route Interface : GigabitEthernet 0/3 Sequence : 1 Source address : 2003::/64 VRF ID : 0 Route Flags : Route Type : PBR Direct : Permit Priority : High Match_ipaddr : Exist Mode : redundance Nexthop Count : 2 Nexthop[0] : 2001::1 Weight[0] : 1 Ifindex[0] : 1 Nexthop[1] : 2002::1 Weight[1] : 1 Ifindex[1] : 2

	Interface :	GigabitEthernet 0/3
	Sequence :	2
	Source address :	2004::/64
	VRF ID :	0
	Route Flags :	
	Route Type :	PBR
	Direct :	Permit
	Priority :	High
	Match_ipaddr :	Exist
	Mode :	redundance
	Nexthop Count :	2
	Nexthop[0] :	2002::1
	Weight[0] :	1
	Ifindex[0] :	2
	Nexthop[1] :	2001::1
	Weight[1] :	1
	Ifindex[1] :	1

9.6. Мониторинг

9.6.1. Очистка

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

Описание	Команда
Очищает статистику о пакетах, пересылаемых IPv4 PBR	**clear ip pbr statistics** [**interface** *if-name* | **local**]
Очищает статистику о пакетах, пересылаемых IPv6 PBR	**clear ipv6 pbr statistics** [**interface** *if-name* | **local**]

9.6.2. Отображение

Описание	Команда
Отображает конфигурации IPv4 PBR	**show ip policy**
Отображает конфигурации IPv6 PBR	**show ipv6 policy**

Описание	Команда
Отображает конфигурации карты маршрута	**show route-map** [*name*]
Отображает конфигурации ACL	**show access-list**
Отображает корреляцию между IPv4 PBR и BFD	**show ip pbr bfd**
Отображает корреляцию между IPv6 PBR и BFD	**show ipv6 pbr bfd**
Отображает информацию о маршрутизации IPv4 PBR	**show ip pbr route** [**interface** *if-name* | **local**]
Отображает информацию о маршрутизации IPv6 PBR	**show ipv6 pbr route** [**interface** *if-name* | **local**]
Отображает карту маршрутов, используемую IPv4 PBR	**show ip pbr route-map** *rmap-name*
Отображает карту маршрутов, используемую IPv6 PBR	**show ipv6 pbr route-map** *rmap-name*
Отображает информацию о маршрутизации PBR на основе адреса источника IPv4	**show ip pbr source–route** [**interface** *if-name*]
Отображает информацию о маршрутизации PBR на основе адреса источника IPv6	**show ipv6 pbr source-route** [**interface** *if-name*]
Отображает статистику по IPv4 PBR	**show ip pbr statistics** [**interface** *if-name* | **local**]
Отображает статистику IPv6 PBR	**show ipv6 pbr statistics** [**interface** *if-name* | **local**]

9.6.3. Отладка

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

Описание	Команда
Отладка ошибки PBR	**debug pbr error**
Отладка события PBR	**debug pbr events**
Отладка нескольких сервисных карт, поддерживаемых PBR	**debug pbr ms**
Отладка передачи сообщений PBR	**debug pbr msg**
Отладка взаимодействия между PBR и NSM	**debug pbr nsm**
Отладка пересылки пакетов PBR	**debug pbr packet**
Отладка PBR GR	**debug pbr restart**

10. УПРАВЛЕНИЕ МАРШРУТАМИ

10.1. Обзор

Модуль сетевых служб (NSM) управляет таблицей маршрутизации, объединяет маршруты, отправленные различными протоколами маршрутизации, а также выбирает и отправляет предпочтительные маршруты в таблицу маршрутизации. Маршруты, обнаруженные различными протоколами маршрутизации, сохраняются в таблице маршрутизации. Эти маршруты обычно подразделяются по источникам на три типа:

- Прямой маршрут: это маршрут, обнаруженный протоколом канального уровня, который также называется маршрутом интерфейса.
- Статический маршрут: настраивается администратором сети вручную. Статический маршрут легко настроить, он менее требователен к системе и, следовательно, применим к сети небольшого размера, стабильной и имеющей простую топологию. Однако при изменении топологии сети статический маршрут необходимо переконфигурировать вручную, и он не может автоматически адаптироваться к топологическим изменениям.
- Динамический маршрут: это маршрут, обнаруженный протоколом динамической маршрутизации.

10.2. Приложения

Приложение	Описание
Основные функции статического маршрута	Настройте маршрут вручную
Плавающий статический маршрут	Настройте резервный маршрут в multipath-сценарии
Статический маршрут балансировки нагрузки	Настройте балансировку нагрузки статических маршрутов в multipath-сценарии
Корреляция статических маршрутов с Track, BFD или ARP	Используйте функцию обнаружения двусторонней переадресации (BFD), чтобы проверить, доступен ли следующий hop статического маршрута
Быстрое перенаправление статических маршрутов	Используйте функцию быстрого перенаправления, чтобы улучшить производительность переключения в multipath-сценарии
Преобразование ARP-to-host	Используйте ARP-хост преобразование (ARP-to-host), чтобы не передавать ARP-пакеты, отправленные хостами через всю сеть

10.2.1. Основные функции статического маршрута

10.2.1.1. Сценарий

В сети с простой топологией можно настроить только статические маршруты для реализации сетевого взаимодействия. Соответствующая конфигурация и использование статических маршрутов могут улучшить производительность сети и гарантировать пропускную способность для важных сетевых приложений.

Как показано на Рисунке 10-1, чтобы реализовать взаимодействие между ПК 1, ПК 2 и ПК 3, вы можете настроить статические маршруты на маршрутизаторах R1, R2 и R3.

- На R1 настройте маршрут к сегменту сети ПК 2 через R2 и маршрут к сегменту сети ПК 3 через R3.
- На R2 настройте маршрут к сегменту сети от ПК 1 через R1 и маршрут к сегменту сети от ПК 3 через R3.
- На R3 настройте маршрут к сегменту сети от ПК 1 через R1 и маршрут к сегменту сети от ПК 2 через R2.

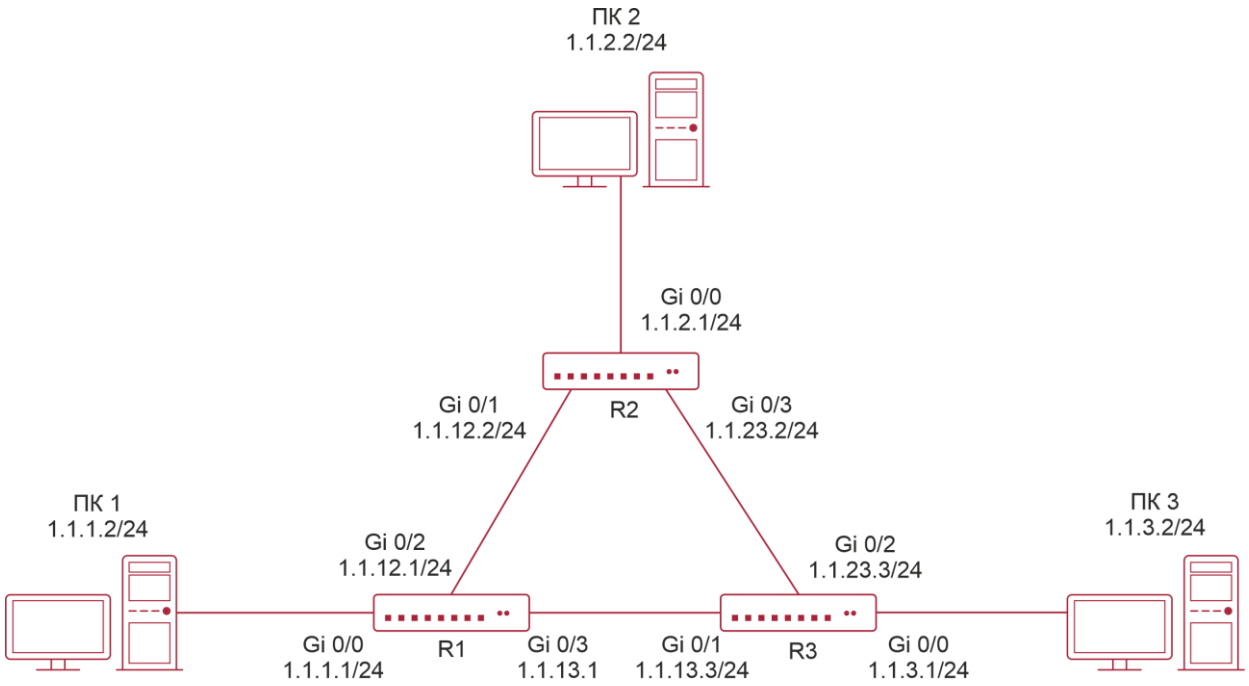


Рисунок 10-1.

10.2.1.2. Развертывание

- Настройте адрес и маску подсети каждого интерфейса.
- Настройте статические маршруты на маршрутизаторах R1, R2 и R3.

10.2.2. Плавающий статический маршрут

10.2.2.1. Сценарий

Если протокол динамической маршрутизации не настроен, вы можете настроить плавающие статические маршруты для реализации динамического переключения маршрутов во избежание прерывания связи, вызванного сбоями сетевого подключения.

Как показано на Рисунке 10-2, чтобы предотвратить прерывание связи, вызванное сбоем линии связи между R1 и R3, вы можете настроить плавающий статический маршрут соответственно на R1 и R3. Обычно пакеты пересылаются по пути с небольшим административным расстоянием. Если канал на этом пути не работает, маршрут автоматически переключается на путь с большим административным расстоянием.

- На маршрутизаторе R1 настройте два маршрута к сегменту сети ПК 3, включая маршрут через маршрутизатор R3 (расстояние по умолчанию = 1) и маршрут через маршрутизатор R2 (расстояние по умолчанию = 2).
- На маршрутизаторе R3 настройте два маршрута к сегменту сети ПК 1, включая маршрут через маршрутизатор R1 (расстояние по умолчанию = 1) и маршрут через маршрутизатор R2 (расстояние по умолчанию = 2).

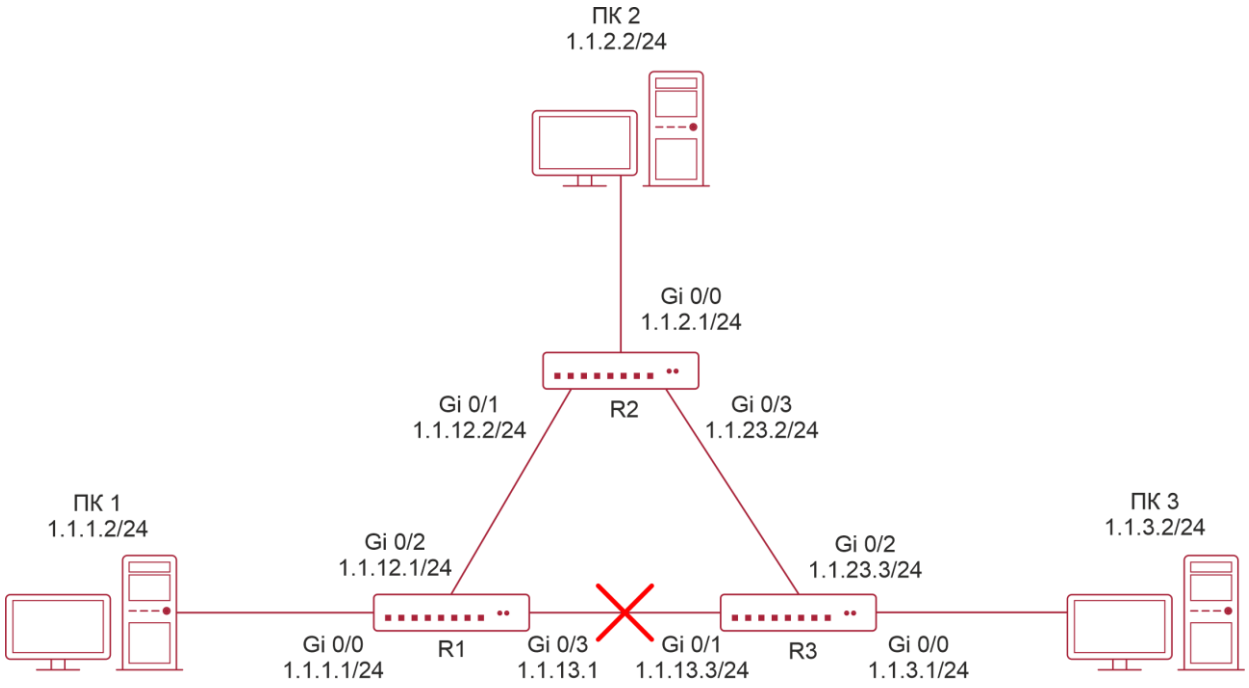


Рисунок 10-2.

10.2.2.2. Развертывание

- Настройте адрес и маску подсети каждого интерфейса.
- Настройте статические маршруты на маршрутизаторах R1, R2 и R3.

10.2.3. Статический маршрут балансировки нагрузки

10.2.3.1. Сценарий

Если к одному и тому же месту назначения существует несколько путей, вы можете настроить маршруты балансировки нагрузки. В отличие от плавающих маршрутов, административные расстояния маршрутов балансировки нагрузки одинаковы. Пакеты распределяются по этим маршрутам на основе политики сбалансированной пересылки.

Как показано на Рисунке 10-3 маршруты балансировки нагрузки настраиваются соответственно на маршрутизаторах R1 и R3, чтобы пакеты, отправляемые в сегмент сети ПК 3 или ПК 1, были сбалансированы между двумя маршрутами, включая маршрут через R2 и маршрут через R4.

- На R1 настройте два маршрута к сегменту сети ПК 3, включая маршрут через R2 и маршрут через R4.
- На R3 настройте два маршрута к сегменту сети ПК 1, включая маршрут через R2 и маршрут через R4.

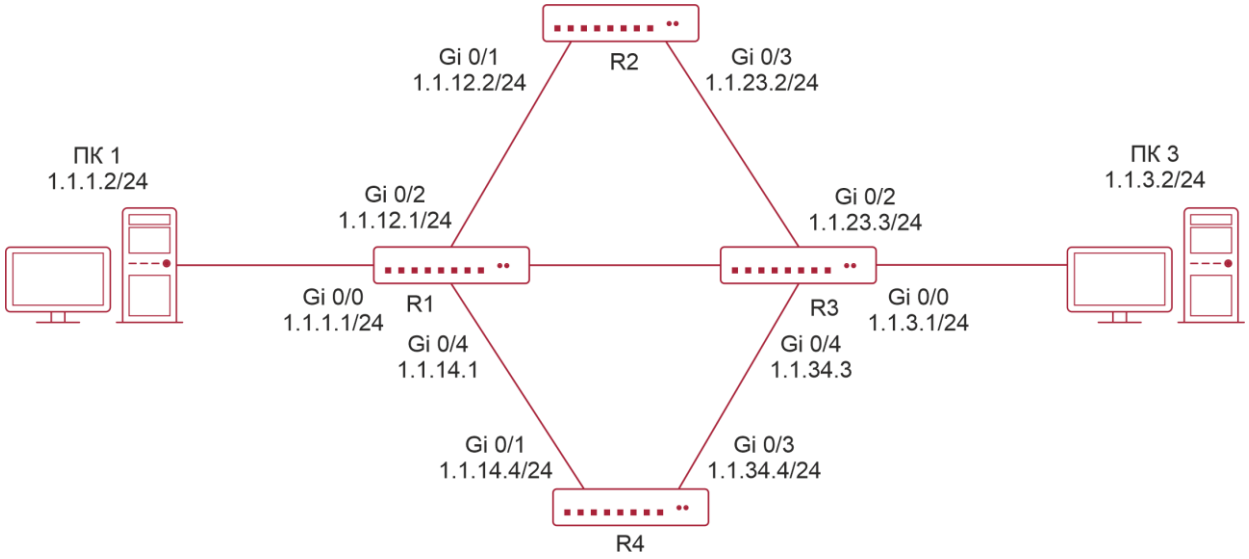


Рисунок 10-3.

На коммутаторе балансировка нагрузки по умолчанию осуществляется на основе IP-адреса назначения.

10.2.3.2. Развертывание

- Настройте адрес и маску подсети каждого интерфейса.
- Настройте статические маршруты на маршрутизаторах R1, R2, R3 и R4.
- Настройте политику балансировки нагрузки на маршрутизаторах R1 и R3.

10.2.4. Корреляция статических маршрутов с Track, BFD или ARP

10.2.4.1. Сценарий

Если настроены плавающие статические маршруты или статические маршруты с балансировкой нагрузки, статические маршруты могут не обнаружить сбои маршрута, если

линия связи неисправна, но состояние интерфейса нормальное. Чтобы решить эту проблему, устройству необходимо проверить, доступен ли следующий hop статического маршрута. Если следующий hop недоступен, устройство может переключить трафик на резервный маршрут.

Вы можете использовать функцию Track, BFD или ARP, чтобы проверить, доступен ли следующий hop статического маршрута. В следующем сценарии в качестве примера используется BFD.

ПРИМЕЧАНИЕ: все три режима могут проверить, доступен ли следующий hop статического маршрута. Если настроено более одного режима, когда один из режимов проверяет, что следующий hop статического маршрута недоступен, статический маршрут является недействительным. Поэтому рекомендуется использовать только один режим.

Как показано на Рисунке 10-4, чтобы предотвратить прерывание связи, вызванное сбоем линии связи между R1 и R3, вы можете настроить плавающий статический маршрут соответственно на R1 и R3 и сопоставить статические маршруты с BFD.

- На маршрутизаторе R1 настройте два маршрута к сегменту сети ПК 3, включая маршрут через маршрутизатор R3 (расстояние по умолчанию = 1) и маршрут через маршрутизатор R2 (расстояние по умолчанию = 2). BFD включен на первом маршруте, чтобы проверить, доступен ли следующий hop 1.1.13.3, а на втором маршруте — чтобы проверить, доступен ли следующий hop 1.1.12.2.
- На маршрутизаторе R3 настройте два маршрута к сегменту сети ПК 1, включая маршрут через маршрутизатор R1 (расстояние по умолчанию = 1) и маршрут через маршрутизатор R2 (расстояние по умолчанию = 2). BFD включен на первом маршруте, чтобы проверить, доступен ли следующий hop 1.1.13.1, а на втором маршруте — чтобы проверить, доступен ли следующий hop 1.1.23.2.

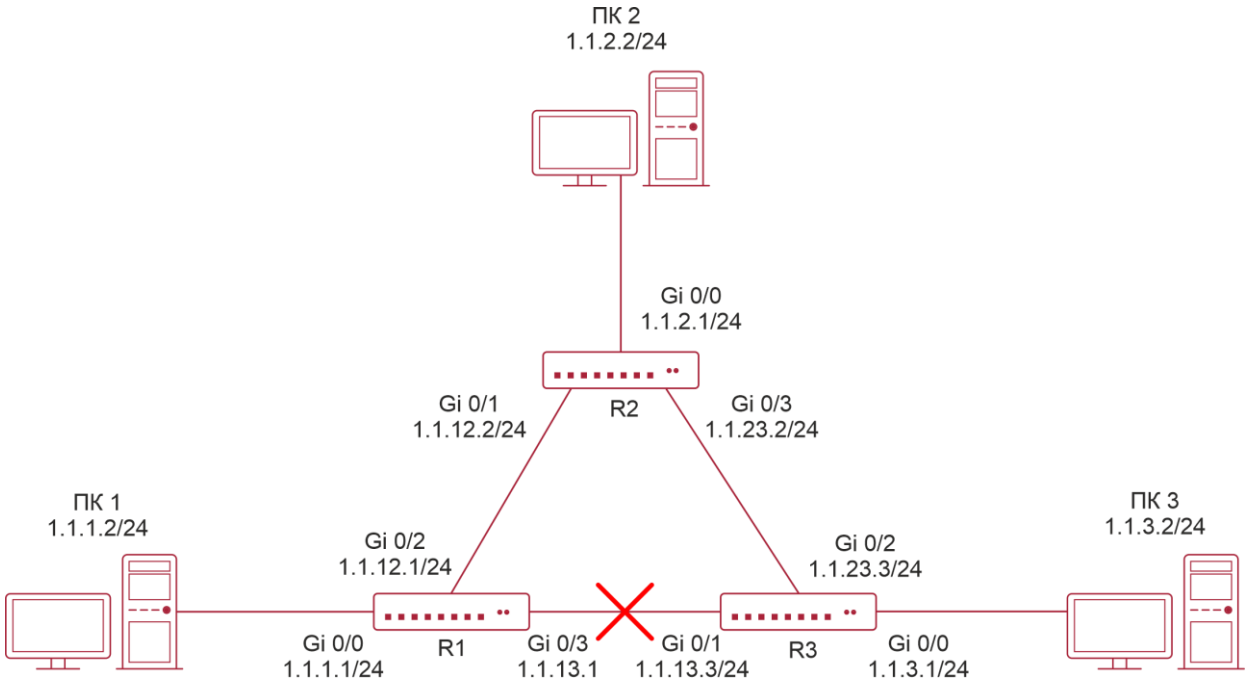


Рисунок 10-4.

10.2.4.2. Развертывание

- Настройте адрес и маску подсети каждого интерфейса.
- Настройте параметры BFD на каждом интерфейсе.
- Настройте статические маршруты и сопоставьте эти статические маршруты с BFD на маршрутизаторах R1, R2 и R3.

10.2.5. Быстрое перенаправление статических маршрутов

10.2.5.1. Сценарий

Чтобы ускорить переключение маршрутов и сократить время прерывания связи, когда протокол динамической маршрутизации не настроен, вы можете сопоставить статические маршруты с Track, BFD или ARP, чтобы проверить, доступен ли следующий hop. Кроме того, вы можете настроить быстрое перенаправление для дальнейшего улучшения производительности конвергенции.

Как показано на Рисунке 10-5, чтобы предотвратить прерывание связи, вызванное сбоем линии связи между R1 и R3, вы можете настроить статическое быстрое перенаправление соответственно на R1 и R3. Обычно пакеты пересылаются по пути между R1 и R3. Когда соединение включено, этот маршрут не работает, пакеты автоматически перенаправляются на R2.

- На маршрутизаторе R1 настройте маршрут с выходным интерфейсом, установленным на Gi0/3, и следующим hop-ом, установленным на 1.1.13.3, а также резервный маршрут с выходным интерфейсом, установленным на Gi0/2, и следующим hop-ом, установленным на 1.1.12.2.
- На маршрутизаторе R3 настройте маршрут с выходным интерфейсом, установленным на Gi0/1, и следующим hop-ом, установленным на 1.1.13.1, а также резервный маршрут с выходным интерфейсом, установленным на Gi0/2, и следующим hop-ом, установленным на 1.1.23.2.

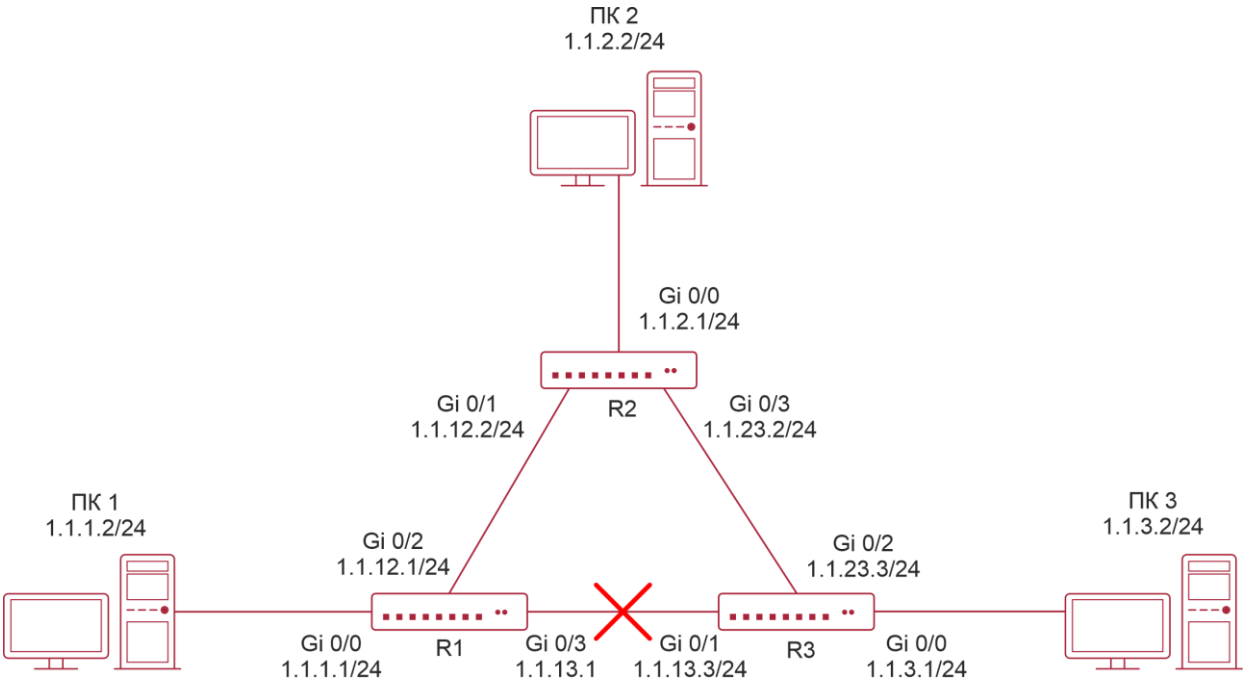


Рисунок 10-5.

10.2.5.2. Развертывание

- Настройте адрес и маску подсети каждого интерфейса.
- Настройте статические маршруты на маршрутизаторах R1, R2 и R3.
- Настройте статическое быстрое перенаправление на маршрутизаторах R1, R2 и R3.

10.2.6. Преобразование ARP-to-host

10.2.6.1. Сценарий

В сценариях с особыми требованиями требуется связь между хостами, но пакеты ARP, отправленные хостами, нежелательно передавать по всей сети. В этом случае вы можете запустить команду **arp-to-host** на устройствах, подключенных к хостам, чтобы преобразовать записи ARP в маршруты хоста, чтобы удаленные устройства изучали маршруты хоста посредством перераспределения BGP, чтобы соответствовать требованиям сценария.

Как показано на следующем рисунке, ПК1 и ПК2 — это два хоста в одном сегменте сети. ПК1 и ПК2 должны обмениваться данными друг с другом, но пакеты ARP не желательно передавать по всей сети. Запустите команду **arp-to-host** на маршрутизаторах R1 и R2, чтобы сгенерировать маршруты хостов ARP, установить отношения соседства BGP между R1 и R2 и включить перераспределение маршрутов хостов ARP. В этом случае и R1, и R2 могут получить маршруты к ПК1 и ПК2 для реализации сетевого соединения.

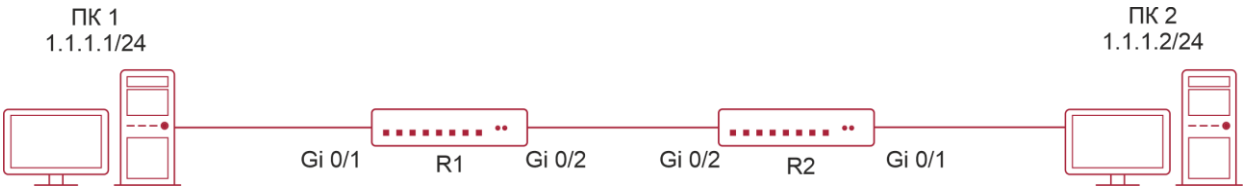


Рисунок 10-6.

10.2.6.2. Развертывание

- Настройте IP-адреса и маски для интерфейсов.
- Включите преобразование ARP-to-host на интерфейсах R1 и R2.
- Установите отношения соседства BGP между R1 и R2 и перераспределите маршруты хостов ARP.

10.3. Функции

Особенность	Описание
Расчет маршрута	Создайте действительный (valid) маршрут на устройстве
Оптимальный выбор маршрута	Выберите оптимальный маршрут для пересылки пакетов
Маршрут по умолчанию	Пересылайте все пакеты и помогайте уменьшить размер таблицы маршрутизации
Надежность маршрута	Быстро обнаруживайте сбой маршрута и восстанавливайте связь

10.3.1. Расчет маршрута

10.3.1.1. Функция маршрутизации

Функции маршрутизации подразделяются на функции маршрутизации IPv4 и IPv6. Если функции маршрутизации отключены, устройство эквивалентно хосту и не может пересылать маршруты.

10.3.1.2. Динамический маршрут

Протокол динамической маршрутизации изучает удаленные маршруты и динамически обновляет маршруты путем обмена маршрутами с соседями. Если сосед является следующим hop-ом маршрута и этот сосед выходит из строя, маршрут также выходит из строя.

10.3.1.3. Статический маршрут

В сети с простой топологией можно настроить только статические маршруты для реализации сетевого взаимодействия. Соответствующая конфигурация и использование

статических маршрутов могут улучшить производительность сети и гарантировать пропускную способность для важных сетевых приложений.

Активность статического маршрута определяется на основе состояния локального интерфейса. Когда выходной интерфейс статического маршрута расположен на уровне 3 (L3) и находится в состоянии Up (состояние канала — Up и IP-адрес настроен), этот маршрут активен и может использоваться для пересылки пакетов.

Статический маршрут может проходить через экземпляры маршрутизации и пересылки VPN (VRF). Интерфейс следующего hop-а или выхода статического маршрута VRF 1 можно настроить на VRF 2.

10.3.1.4. Преобразование ARP-to-host

Включите преобразование ARP-to-host на указанном интерфейсе. Если интерфейс является интерфейсом уровня 3 в состоянии Up, записи ARP будут преобразованы в 32-битные маршруты хоста на интерфейсе.

10.3.2. Оптимальный выбор маршрута

10.3.2.1. Административное расстояние

Когда несколько протоколов маршрутизации генерируют маршруты к одному и тому же пункту назначения, приоритеты этих маршрутов можно определить на основе административного расстояния. Меньшее административное расстояние указывает на более высокий приоритет.

10.3.2.2. Маршрут равной стоимости

Если несколько маршрутов к одному и тому же пункту назначения имеют разные следующие hop-ы, но одинаковое административное расстояние, эти маршруты являются маршрутами с одинаковой стоимостью. Пакеты распределяются по этим маршрутам для реализации балансировки нагрузки на основе политики сбалансированной пересылки.

На конкретном устройстве общее количество маршрутов одинаковой стоимости ограничено. Маршруты, превышающие это ограничение, не участвуют в пересылке пакетов.

10.3.2.3. Плавающий маршрут

Если несколько маршрутов к одному и тому же пункту назначения имеют разные следующие hop-ы и разные административные расстояния, эти маршруты являются взаимно плавающими маршрутами. Для пересылки пакетов сначала будет выбран маршрут с наименьшим административным расстоянием. В случае сбоя этого маршрута для пересылки выбирается маршрут с большим административным расстоянием, что предотвращает прерывание связи, вызванное сбоем сетевой линии связи.

10.3.3. Маршрут по умолчанию

В таблице маршрутизации пересылки маршрут с сегментом сети назначения 0.0.0.0 и маской подсети 0.0.0.0 является маршрутом по умолчанию. Пакеты, которые не могут быть перенаправлены по другим маршрутам, будут пересылаться по маршруту по умолчанию. Маршрут по умолчанию может быть настроен статически или создан с помощью протокола динамической маршрутизации.

10.3.3.1. Статический маршрут по умолчанию

На коммутаторе L3 статический маршрут с сегментом сети 0.0.0.0 и маской подсети 0.0.0.0 настроен для создания маршрута по умолчанию.

10.3.3.2. Сеть по умолчанию

Сеть по умолчанию настроена на создание маршрута по умолчанию. Если команда **ip default-network** настроена для указания сети (классовой сети, например сети класса A, B или C), и эта сеть существует в таблице маршрутизации, маршрутизатор будет использовать эту сеть в качестве сети по умолчанию. и следующий hop этой сети — шлюз по умолчанию. Поскольку сеть, указанная командой **ip default-network**, является классовой, если эта команда используется для идентификации подсети в классовой сети, маршрутизатор автоматически генерирует статический маршрут классовой сети вместо любого маршрута по умолчанию.

10.3.4. Надежность маршрута

Когда устройство в сети неисправно, некоторые маршруты становятся недоступными, что приводит к прерыванию трафика. Если возможность подключения следующего peer-а может быть обнаружена в режиме реального времени, маршрут может быть пересчитан в случае возникновения сбоя или трафик может быть переключен на резервный маршрут.

10.3.4.1. Корреляция с Track

Объект Track — это абстрактное понятие. Его можно использовать для отслеживания того, доступен ли IP-адрес или работает ли интерфейс. Если протокол динамической маршрутизации или статический маршрут коррелируют с функцией Track, протокол динамической маршрутизации или статический маршрут могут быстро узнать, доступен ли следующий hop, чтобы быстро отреагировать.

10.3.4.2. Корреляция с BFD

Протокол BFD обеспечивает легкий и быстрый метод обнаружения соединения пути пересылки между двумя смежными маршрутизаторами. Если протокол динамической маршрутизации или статический маршрут коррелируют с функцией BFD, протокол динамической маршрутизации или статический маршрут могут быстро узнать, доступен ли следующий hop, чтобы быстро отреагировать.

ПРИМЕЧАНИЕ: производительность обнаружения BFD лучше, чем у Track.

10.3.4.3. Корреляция с ARP

Если статический маршрут коррелирует с функцией ARP, а ARP не существует, статический маршрут может быстро узнать, что следующий hop недоступен, чтобы быстро отреагировать.

10.3.4.4. Быстрое перенаправление

Быстрое перенаправление обеспечивает резервный маршрут. Когда протокол динамической маршрутизации или статический маршрут обнаруживает, что следующий hop недоступен, он немедленно переключает трафик на резервный маршрут для восстановления связи.

10.4. Конфигурация

Элемент конфигурации	Описание и команда	
Настройка статического маршрута	(Обязательный) Используется для настройки записи статического маршрута	
	ip route	Настраивает статический маршрут IPv4
	ipv6 route	Настраивает статический маршрут IPv6
Настройка маршрута по умолчанию	(Опционально) Используется для настройки шлюза по умолчанию	
	ip route 0.0.0.0 0.0.0.0 *gateway*	Настраивает шлюз IPv4 по умолчанию на устройстве L3
	ipv6 route ::/0 *ipv6-gateway*	Настраивает шлюз IPv6 по умолчанию на устройстве L3
	ip default network	Настраивает сеть IPv4 по умолчанию на устройстве L3
Настройка ограничений маршрута	(Опционально) Используется для ограничения количества маршрутов с равной стоимостью и количества статических маршрутов или отключения маршрутизации	
	maximum-paths	Настраивает максимальное количество маршрутов с равной стоимостью
	ip static route-limit	Настраивает максимальное количество статических маршрутов IPv4
	ipv6 static route-limit	Настраивает максимальное количество статических маршрутов IPv6
	no ip routing	Отключает маршрутизацию IPv4

Элемент конфигурации	Описание и команда	
Настройка ограничений маршрута	**no ipv6 unicast-routing**	Отключает маршрутизацию IPv6
	no ip route static inter-vrf	Запрещает статическую маршрутизацию между VRF
Сопоставление статического маршрута с BFD	(Опционально) Используется для корреляции статического маршрута с BFD	
	ip route static bfd	Сопоставляет статический маршрут IPv4 с BFD
	ipv6 route static bfd	Сопоставляет статический маршрут IPv6 с BFD
Настройка статического быстрого перенаправления	(Опционально) Используется для настройки статического быстрого перенаправления	
	route-map	Настраивает карту маршрутов
	set fast-reroute backup-nexthop	Настраивает резервный интерфейс и резервный следующий hop для быстрого перенаправления
	ip fast-reroute	Настраивает статическое быстрое перенаправление
Настройка преобразования ARP-to-host	**ip route arp-to-host interface** *interface-name*	Настраивает преобразование ARP-to-host на указанном интерфейсе
	redistribute arp-host [**route-map** *map-tag*] [**metric** *metric-value*]	Настраивает перераспределение BGP для маршрута хоста ARP

10.4.1. Настройка статического маршрута

10.4.1.1. Эффект конфигурации

Создайте статический маршрут в таблице маршрутизации. Используйте статический маршрут для пересылки пакетов в удаленную сеть.

10.4.1.2. Примечания

- Если на коммутаторе L3 настроена команда **no ip routing**, вы не сможете настроить статические маршруты IPv4 на этом коммутаторе, а существующие статические маршруты IPv4 также будут удалены. Перед перезапуском устройства перенастройка команды **ip routing** может восстановить удаленные статические маршруты IPv4. После перезапуска устройства удаленные статические маршруты IPv4 невозможно восстановить.
- Если на коммутаторе L3 настроена команда **no ipv6 unicast-routing**, вы не сможете настроить статические маршруты IPv6 на этом коммутаторе, а существующие статические маршруты IPv6 также будут удалены. Перед перезапуском устройства перенастройка команды **ipv6 unicast-routing** может восстановить удаленные статические маршруты IPv6. После перезапуска устройства удаленные статические маршруты IPv6 невозможно восстановить.
- Чтобы сопоставить статический маршрут с функцией отслеживания, необходимо запустить команду **track** для настройки объекта track.

10.4.1.3. Шаги настройки

Настройка статического маршрута IPv4

Настройте следующую команду на маршрутизаторе с поддержкой IPv4.

Команда	**ip route** [**vrf** *vrf_name*] *network net-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent** | **track** *object-number*| **arp**] [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**] [**global**]
Описание параметра	**vrf** *vrf_name*: (Опционально) указывает VRF маршрутизации, который может быть VRF с одним протоколом IPv4 или VRF с несколькими протоколами настроенного семейства адресов IPv4. По умолчанию VRF является глобальным VRF. *network*: указывает адрес сети назначения. *net-mask: у*казывает маску сети назначения. *ip-address*: (Опционально) указывает адрес следующего hop-а статического маршрута. Вы должны указать хотя бы один из *ip-address* и *interface* или оба из них. Если *ip-address* не указан, настроен статический прямой маршрут. *interface:* (Опционально) указывает выходной интерфейс следующего hop-а статического маршрута. Вы должны указать хотя бы один из *ip-address* и *interface* или оба из них. Если *interface* не указан, настраивается рекурсивный статический прямой маршрут. Выходной интерфейс получается следующим hop-ом в таблице маршрутизации. *distance:* (Опционально) указывает административное расстояние статического маршрута. По умолчанию административное расстояние равно 1. *tag*: (Опционально) указывает тег статического маршрута. По умолчанию тег имеет значение 0.

	permanent: (Опционально) указывает флаг постоянного маршрута. Статический маршрут по умолчанию не является постоянным маршрутом. **track** *object-number*: (Опционально) указывает корреляцию с Track-ом. *object-number* указывает идентификатор объекта track. По умолчанию статический маршрут не коррелирует с функцией Track. **weight** *number*: (Опционально) указывает вес статического маршрута. По умолчанию вес равен 1. **description** *description-text*: (Опционально) указывает описание статического маршрута. По умолчанию описание не настроено. Текст описания — это строка длиной от одного до 60 символов. **disabled** | **enabled**: (Опционально) указывает флаг включения статического маршрута. Флаг включен по умолчанию. **global**: (Опционально) указывает, что следующий hop принадлежит глобальному VRF. По умолчанию VRF следующего hop-а совпадает с VRF, указанным *vrf name*. **arp**: (Опционально) соотнесите статический маршрут с функцией ARP. По умолчанию он не коррелирован (не соотнесен)
По умолчанию	По умолчанию статический маршрут не настроен
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Самая простая конфигурация этой команды — **ip route** *network net-mask ip-address*. Если статический маршрут коррелирует с Track и обнаружено состояние Down объекта отслеживания, статический маршрут не активен и не участвует в пересылке пакетов. Если статический маршрут коррелирует с ARP, но не обнаружено информации ARP, статический маршрут не активен и не участвует в пересылке пакетов

Настройка статического маршрута IPv6

Настройте следующую команду на маршрутизаторе с поддержкой IPv6.

Команда	**ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix/prefix-length* { *ipv6-address* [**nexthop-vrf** {*vrf-name1*| **default**}] | *interface* [*ipv6-address* [**nexthop-vrf** {*vrf-name1*| **default**}]] } [*distance*] [**weight** *number*] [**description** *description-text*]
Описание параметра	**vrf** *vrf-name*: (Опционально) указывает VRF маршрутизации, который должен быть многопротокольным VRF настроенного семейства адресов IPv6. По умолчанию VRF является глобальным VRF. *ipv6-prefix*: указывает префикс IPv6, который должен соответствовать выражению адреса, указанному в RFC4291.

	prefix-length: указывает длину префикса IPv6. Обратите внимание, что перед длиной необходимо добавить косую черту (/). *ipv6-address*: (Опционально) указывает адрес следующего hop-а статического маршрута. Необходимо указать хотя бы один из *ipv6-address* и *interface* или оба из них. Если *ipv6-address* не указан, настроен статический прямой маршрут. *interface*: (Опционально) указывает выходной интерфейс следующего hop-а статического маршрута. Необходимо указать хотя бы один из *ipv6-address* и *interface* или оба из них. Если *interface* не указан, настраивается рекурсивный статический прямой маршрут. Выходной интерфейс получается следующим hop-ом в таблице маршрутизации. **nexthop-vrf** *vrf-name1*: (Опционально) указывает VRF маршрутизации следующего hop-а, который должен быть многопротокольным VRF настроенного семейства адресов IPv6. По умолчанию VRF следующего hop-а совпадает с VRF, заданным именем VRF. **nexthop-vrf default** указывает, что VRF следующего hop-а является глобальным VRF. *distance*: (Опционально) указывает административное расстояние статического маршрута. По умолчанию административное расстояние равно 1. **weight** *number*: (Опционально) указывает вес статического маршрута, который необходимо указать при настройке маршрутов с равной стоимостью. Вес варьируется от 1 до 8. Когда веса всех маршрутов с одинаковой стоимостью суммируются, сумма не может превышать максимальное количество маршрутов с одинаковой стоимостью, которые можно настроить для маршрута. Взвешивание равноценных маршрутов маршрута указывает на соотношение трафика на этих маршрутах. По умолчанию вес равен 1. **description** *description-text*: (Опционально) указывает описание статического маршрута. По умолчанию описание не настроено. Текст описания — это строка длиной от одного до 60 символов
По умолчанию	По умолчанию статический маршрут не настроен
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Самая простая конфигурация этой команды — **ipv6 route** *ipv6-prefix* / *prefix-length ipv6-address*

10.4.1.4. Проверка

- Запустите команду **show ip route**, чтобы отобразить таблицу маршрутизации IPv4 и проверить, вступает ли в силу настроенный статический маршрут IPv4.
- Запустите команду **show ipv6 route**, чтобы отобразить таблицу маршрутизации IPv6 и проверить, вступает ли в силу настроенный статический маршрут IPv6.

10.4.1.5. Пример конфигурации

Настройка статических маршрутов для реализации взаимодействия сети IPv4

Сценарий:

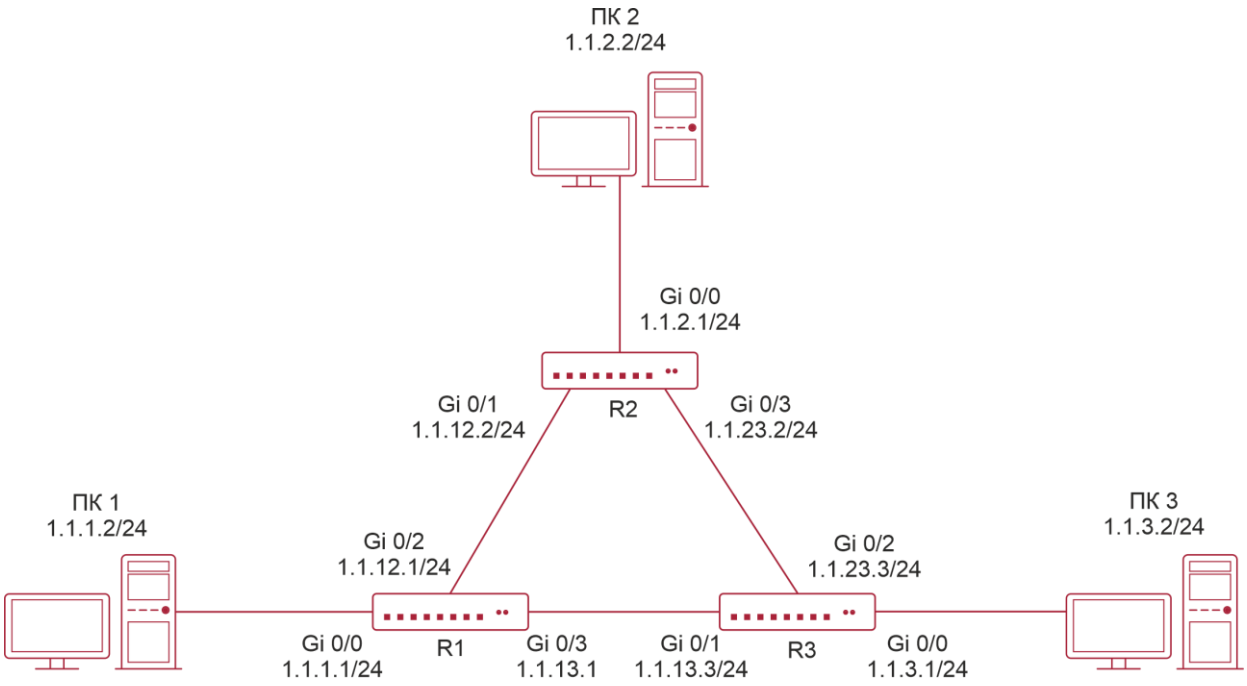


Рисунок 10-7.

Шаги настройки	Настройте адреса интерфейсов на каждом устройстве
R1	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/2 R1(config-if-GigabitEthernet 0/2)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/3 R1(config-if-GigabitEthernet 0/3)# ip address 1.1.13.1 255.255.255.0
R2	R2#configure terminal R2(config)#interface gigabitEthernet 0/0

	R2(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/3 R2(config-if-GigabitEthernet 0/3)# ip address 1.1.23.2 255.255.255.0
R3	R3#configure terminal R3(config)#interface gigabitEthernet 0/0 R3(config-if-GigabitEthernet 0/0)# ip address 1.1.3.1 255.255.255.0 R3(config-if-GigabitEthernet 0/0)# exit R3(config)#interface gigabitEthernet 0/1 R3(config-if-GigabitEthernet 0/1)# ip address 1.1.13.3 255.255.255.0 R3(config-if-GigabitEthernet 0/0)# exit R3(config)#interface gigabitEthernet 0/2 R3(config-if-GigabitEthernet 0/2)# ip address 1.1.23.3 255.255.255.0
	Настройте статические маршруты на каждом устройстве
R1	R1#configure terminal R1(config)#ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.12.2 R1(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.13.3
R2	R2#configure terminal R2(config)#ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.12.1 R2(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.23.3
R3	R3#configure terminal R3(config)#ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.23.2 R3(config)# ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.13.1
Проверка	Отобразите таблицу маршрутизации
R1	R1# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS

	N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate defaultwww.qtech.ru Gateway of last resort is no set C 1.1.1.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.1.1/32 is local host. S 1.1.2.0/24 [1/0] via 1.1.12.2, GigabitEthernet 0/2 S 1.1.3.0/24 [1/0] via 1.1.13.3, GigabitEthernet 0/2 C 1.1.12.0/24 is directly connected, GigabitEthernet 0/2 C 1.1.12.1/32 is local host. C 1.1.13.0/24 is directly connected, GigabitEthernet 0/3 C 1.1.13.1/32 is local host
R2	R2# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set S 1.1.1.0/24 [1/0] via 1.1.12.1, GigabitEthernet 0/0 C 1.1.2.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.2.1/32 is local host. S 1.1.3.0/24 [1/0] via 1.1.23.3, GigabitEthernet 0/3 C 1.1.12.0/24 is directly connected, GigabitEthernet 0/1 C 1.1.12.2/32 is local host. C 1.1.23.0/24 is directly connected, GigabitEthernet 0/3 C 1.1.23.2/32 is local host
R3	R3# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS

	N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2www.qtech.ru SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set S 1.1.1.0/24 [1/0] via 1.1.13.1, GigabitEthernet 0/2 S 1.1.2.0/24 [1/0] via 1.1.23.2, GigabitEthernet 0/2 C 1.1.3.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.3.1/32 is local host. C 1.1.13.0/24 is directly connected, GigabitEthernet 0/1 C 1.1.13.3/32 is local host. C 1.1.23.0/24 is directly connected, GigabitEthernet 0/2 C 1.1.23.3/32 is local host

Корреляция статических маршрутов IPv4 с Track

Сценарий:

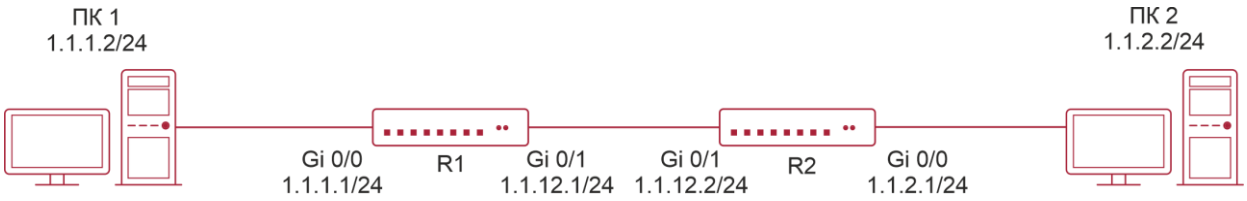


Рисунок 10-8.

Шаги настройки	• Настройте статические маршруты на маршрутизаторах R1 и R2 и укажите выходной интерфейс или следующий hop в качестве интерфейса взаимодействия (interworking interface). • Сопоставьте статические маршруты с Track на R1 и R2 и проверьте связь следующих hop-ов статических маршрутов
R1	R1#configure terminal R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/1)# exit R1(config)#track 2 interface gigabitEthernet 0/1 line-protocol R1(config)# ip route 1.1.2.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.2 track 2

R2	R2#configure terminal R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0 R1(config-if-GigabitEthernet 0/1)# exit R1(config)#track 2 interface gigabitEthernet 0/1 line-protocol R1(config)# ip route 1.1.1.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.1 track 2
Проверка	• Отображение статуса Track-a. • Отображение статических маршрутов, связанных с Track. R1# show track 2 Track 2 Interface gigabitEthernet 0/1 The state is Up, delayed Down (5 secs remaining) 1 change, current state last: 300 secs Delay up 0 secs, down 0 secs R1#show ip route track-table ip route 1.1.2.0 255.0.0.0 GigabitEthernet 0/1 1.1.12.2 track 2 up

Настройка статических маршрутов для реализации взаимодействия сети IPv6

Сценарий:

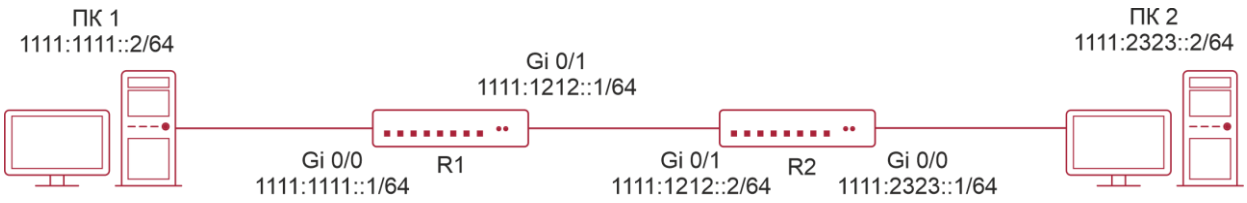


Рисунок 10-9.

Шаги настройки	Настройте адреса интерфейсов на каждом устройстве
R1	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ipv6 address 1111:1111::1/64 R1(config-if-GigabitEthernet 0/0)# exit

	R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)# ipv6 address 1111:1212::1/64
R2	R2#configure terminal R2(config)#interface gigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)#ipv6 address 1111:2323::1/64 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# ipv6 address 1111:1212::2/64
	Настройте статические маршруты на каждом устройстве
R1	R1#configure terminal R1(config)# ipv6 route 1111:2323::0/64 gigabitEthernet 0/1
R2	R2#configure terminal R2(config)#ipv6 route 1111:1111::0/64 gigabitEthernet 0/1
Проверка	Отобразите таблицу маршрутизации
R1	R1# show ipv6 route IPv6 routing table name - Default - 10 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area C 1111:1111::/64 via GigabitEthernet 0/0, directly connected L 1111:1111::1/128 via GigabitEthernet 0/0, local host C 1111:1212::/64 via GigabitEthernet 0/1, directly connected L 1111:1212::1/128 via GigabitEthernet 0/1, local host S 1111:2323::/64 [1/0] via GigabitEthernet 0/1, directly connected C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected

	L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/0, local host C FE80::/64 via GigabitEthernet 0/1, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/1, local host
R2	R2# show ipv6 route IPv6 routing table name - Default - 10 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area C 1111:2323::/64 via GigabitEthernet 0/0, directly connected L 1111:2323::1/128 via GigabitEthernet 0/0, local host C 1111:1212::/64 via GigabitEthernet 0/1, directly connected L 1111:1212::1/128 via GigabitEthernet 0/1, local host S 1111:1111::/64 [1/0] via GigabitEthernet 0/1, directly connected C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/0, local host C FE80::/64 via GigabitEthernet 0/1, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/1, local host

10.4.1.6. Распространенные ошибки

- Канал на интерфейсе не работает.
- Для интерфейса не настроен IP-адрес.
- Статический маршрут коррелирует с Track, но объект Track не настроен.

10.4.2. Настройка маршрута по умолчанию

10.4.2.1. Эффект конфигурации

Создайте маршрут по умолчанию в таблице маршрутизации. Маршрут по умолчанию используется для пересылки пакетов, которые не могут быть перенаправлены другими маршрутами.

10.4.2.2. Примечания

- На коммутаторе L3 запустите команду **ip route** 0.0.0.0 0.0.0.0 *gateway* или **ipv6 route** ::/0 *ipv6-gateway*, чтобы настроить шлюз по умолчанию.
- Если на коммутаторе L3 настроена команда **no ip routing** или **no ipv6 unicast-routing**, вы можете запустить команду **ip default gateway** или **ipv6 default gateway**, чтобы настроить шлюз по умолчанию.

10.4.2.3. Шаги настройки

Настройка шлюза IPv4 на коммутаторе L2

Команда	**ip default-gateway** *gateway*
Описание параметра	*gateway*: указывает адрес шлюза IPv4
По умолчанию	По умолчанию статический маршрут по умолчанию не настроен
Командный режим	Режим глобальной конфигурации

Настройка шлюза IPv6 на коммутаторе L2

Команда	**ipv6 default-gateway** *gateway*
Описание параметра	*gateway*: указывает адрес шлюза IPv6
По умолчанию	По умолчанию статический маршрут по умолчанию не настроен
Командный режим	Режим глобальной конфигурации

Настройка шлюза по умолчанию IPv4 на коммутаторе L3

Команда	**ip route** [**vrf** *vrf_name*]**0.0.0.0 0.0.0.0**{*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent**] [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**] [**global**]
Описание параметра	**vrf** *vrf_name*: (Опционально) указывает VRF маршрутизации, который может быть VRF с одним протоколом IPv4 или VRF с несколькими протоколами настроенного семейства адресов IPv4. По умолчанию VRF является глобальным VRF. **0.0.0.0**: указывает адрес сети назначения. **0.0.0.0**: указывает маску сети назначения. *ip-address*: (Опционально) указывает адрес следующего hop-а статического маршрута. Вы должны указать хотя бы один из *ip-address*

	и *interface* или оба из них. Если *ip-address* не указан, настроен статический прямой маршрут. *interface*: (Опционально) указывает выходной интерфейс следующего hop-а статического маршрута. Вы должны указать хотя бы один из *ip-address* и *interface* или оба из них. Если *interface* не указан, настраивается рекурсивный статический прямой маршрут. Выходной интерфейс получается следующим hop-ом в таблице маршрутизации. *distance*: (Опционально) указывает административное расстояние статического маршрута. По умолчанию административное расстояние равно 1. *tag*: (Опционально) указывает тег статического маршрута. По умолчанию тег имеет значение 0. **permanent**: (Опционально) указывает флаг постоянного маршрута. Статический маршрут по умолчанию не является постоянным маршрутом. **weight** *number*: (Опционально) указывает вес статического маршрута. По умолчанию вес равен 1. **description** *description-text*: (Опционально) указывает описание статического маршрута. По умолчанию описание не настроено. *description-text* : это строка длиной от одного до 60 символов. **disabled** | **enabled**: (Опционально) указывает флаг включения статического маршрута. Флаг включен по умолчанию. **global**: (Опционально) указывает, что следующий hop принадлежит глобальному VRF. По умолчанию VRF следующего hop-а совпадает с VRF, указанным *rf name*
По умолчанию	По умолчанию статический маршрут по умолчанию не настроен
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Самая простая конфигурация этой команды — **ip route 0.0.0.0 0.0.0.0** *ip-address*

Настройка шлюза по умолчанию IPv6 на коммутаторе L3

Команда	**ipv6 route** [**vrf** *vrf-name*] **::/0** { *ipv6-address* [**nexthop-vrf** {*vrf-name1*| **default**}] | *interface* [*ipv6-address* [**nexthop-vrf** {*vrf-name1*| **default**}]] } [*distance*] [**weight** *number*] [**description** *description-text*]
Описание параметра	**vrf** *vrf-name*: (Опционально) указывает VRF маршрутизации, который должен быть многопротокольным VRF настроенного семейства адресов IPv6. По умолчанию VRF является глобальным VRF. **::** указывает префикс IPv6, который должен соответствовать выражению адреса, указанному в RFC4291.

	0: указывает длину префикса IPv6. Обратите внимание, что перед длиной необходимо добавить косую черту (/). *ipv6-address*: (Опционально) указывает адрес следующего hop-а статического маршрута. Необходимо указать хотя бы один из *ipv6-address* и *interface* или оба из них. Если *ipv6-address* не указан, настроен статический прямой маршрут. *interface*: (Опционально) указывает выходной интерфейс следующего hop-а статического маршрута. Необходимо указать хотя бы один из *ipv6-address* и *interface* или оба из них. Если *interface* не указан, настраивается рекурсивный статический прямой маршрут. Выходной интерфейс получается следующим hop-ом в таблице маршрутизации. **nexthop-vrf** *vrf-name1*: (Опционально) указывает VRF маршрутизации следующего hop-а, который должен быть многопротокольным VRF настроенного семейства адресов IPv6. По умолчанию VRF следующего hop-а совпадает с VRF, заданным *vrf-name*. **nexthop-vrf default** указывает, что VRF следующего hop-а является глобальным VRF. *distance*: (Опционально) указывает административное расстояние статического маршрута. По умолчанию административное расстояние равно 1. **weight** *number*: (Опционально) указывает вес статического маршрута, который необходимо указать при настройке маршрутов с равной стоимостью. Вес варьируется от 1 до 8. Когда веса всех маршрутов с одинаковой стоимостью суммируются, сумма не может превышать максимальное количество маршрутов с одинаковой стоимостью, которые можно настроить для маршрута. Взвешивание равноценных маршрутов маршрута указывает на соотношение трафика на этих маршрутах. По умолчанию вес равен 1. **description** *description-text*: (Опционально) указывает описание статического маршрута. По умолчанию описание не настроено. *description-text*: это строка длиной от одного до 60 символов
По умолчанию	По умолчанию статический маршрут по умолчанию не настроен
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Самая простая конфигурация этой команды — **ipv6 route** ::/0 *ipv6-gateway*

Настройка сети по умолчанию IPv4 на коммутаторе L3

Команда	**ip default-network** *network*
Описание параметра	*network*: указывает адрес сети. (Сеть должна быть сетью класса A, B или C.)

По умолчанию	По умолчанию сеть по умолчанию не настроена
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если сеть, указанная командой **ip default-network**, существует, создается маршрут по умолчанию, и следующим hop-ом к этой сети является шлюз по умолчанию. Если сеть, указанная командой **ip default-network**, не существует, маршрут по умолчанию не генерируется

10.4.2.4. Проверка

- На коммутаторе L2 (или коммутаторе L3, где маршрутизация отключена) запустите команду **show ip redirects** или **show ipv6 redirects**, чтобы отобразить шлюз по умолчанию.
- На коммутаторе L3, где включена маршрутизация, запустите команду **show ip route** или **show ipv6 route**, чтобы отобразить маршрут по умолчанию.

10.4.2.5. Пример конфигурации

Настройка маршрутов IPv4 по умолчанию на коммутаторах L3 для реализации сетевого взаимодействия

Сценарий:

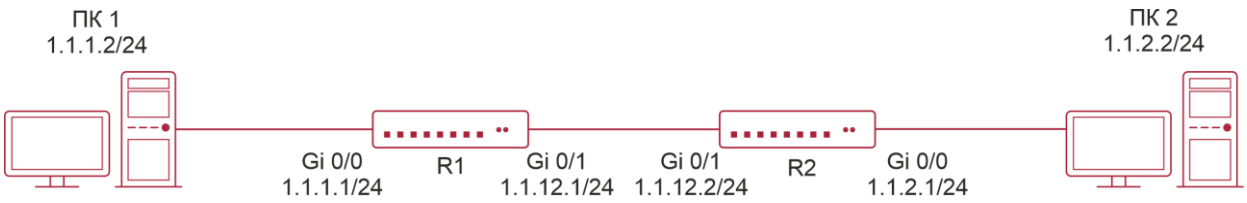


Рисунок 10-10.

Шаги настройки	Настройте IP-адреса на устройствах L3
R1	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit

R2	R2#configure terminal R2(config)#interface gigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit
R1	Настройте шлюз IPv6 по умолчанию на маршрутизаторе R1. R1#configure terminal R1(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 1.1.12.2
R2	R2#configure terminal R2(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 1.1.12.1
Проверка	Отобразите таблицу маршрутизации
R1	R1# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is 1.1.12.2 S* 0.0.0.0/0 [1/0] via 1.1.12.2, GigabitEthernet 0/1 C 1.1.1.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.1.1/32 is local host. C 1.1.12.0/24 is directly connected, GigabitEthernet 0/1 C 1.1.12.1/32 is local host

10.4.3. Настройка ограничений маршрута

10.4.3.1. Эффект конфигурации

Ограничьте количество маршрутов с равной стоимостью и количество статических маршрутов или отключите маршрутизацию.

10.4.3.2. Примечания

Ограничения маршрутов невозможно настроить на коммутаторе L2.

10.4.3.3. Шаги настройки

Настройка максимального количества маршрутов с одинаковой стоимостью

Команда	**maximum-paths** *number*
Описание параметра	*number*: указывает максимальное количество маршрутов с одинаковой стоимостью. Значение варьируется от 1 до 64
По умолчанию	Значение по умолчанию варьируется в зависимости от продукта
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы настроить максимальное количество следующих hop-ов в маршруте с равной стоимостью. В режиме балансировки нагрузки количество маршрутов, на которых балансируется трафик, не превышает настроенное количество маршрутов равной стоимости

Настройка максимального количества статических маршрутов IPv4

Команда	**ip static route-limit** *number*
Описание параметра	*number*: указывает верхний предел маршрутов. Значение варьируется от 1 до 10 000
По умолчанию	По умолчанию можно настроить максимум 1024 статических IP-маршрута
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы настроить максимальное количество статических маршрутов IPv4. Если достигнуто максимальное количество статических маршрутов IPv4, больше статических маршрутов IPv4 настроить невозможно

Настройка максимального количества статических маршрутов IPv6

Команда	**ipv6 static route-limit** *number*
Описание параметра	*number*: указывает верхний предел маршрутов. Значение варьируется от 1 до 10 000
По умолчанию	По умолчанию можно настроить максимум 1000 статических маршрутов IPv6
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы настроить максимальное количество статических маршрутов IPv6. Если достигнуто максимальное количество статических маршрутов IPv6, больше статических маршрутов IPv6 настроить невозможно

Отключение маршрутизации IPv4

Команда	**no ip routing**
По умолчанию	По умолчанию маршрутизация IPv4 включена
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы отключить маршрутизацию IPv4. Если устройство функционирует только как мост или шлюз передачи голоса по IP (VoIP), устройству не требуется использовать функцию маршрутизации IPv4 программного обеспечения. В этом случае вы можете отключить функцию маршрутизации IPv4 программного обеспечения

Отключение маршрутизации IPv6

Команда	**no ipv6 unicast-routing**
По умолчанию	По умолчанию маршрутизация IPv6 включена
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Запустите эту команду, чтобы отключить маршрутизацию IPv6. Если устройство функционирует только как мост или шлюз VoIP, устройству не требуется использовать функцию маршрутизации IPv6 программного обеспечения. В этом случае вы можете отключить функцию маршрутизации IPv6 программного обеспечения

Запрет статической маршрутизации между VRF

Команда	**no ip route static inter-vrf**
По умолчанию	По умолчанию разрешена статическая маршрутизация IP или IPv6 между VRF
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы запретить статическую IP-маршрутизацию между VRF. После настройки этой команды статический IP-маршрут между VRF не активен и не может участвовать в пересылке пакетов

10.4.3.4. Проверка

Запустите команду **show run**, чтобы отобразить файл конфигурации, и убедитесь, что предыдущие команды конфигурации существуют.

10.4.3.5. Пример конфигурации

Настройка не более двух ограничений статической маршрутизации

Сценарий:

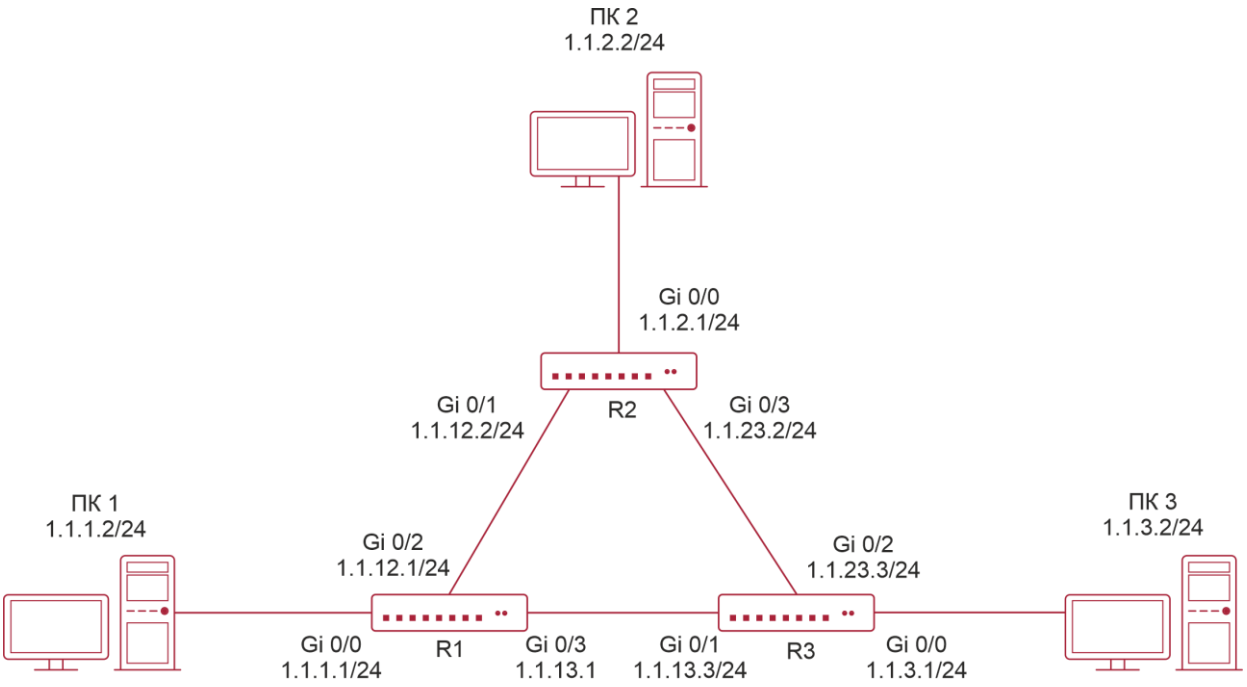


Рисунок 10-11.

Шаги настройки	На маршрутизаторе R1 настройте IP-адреса, статические маршруты и максимальное количество статических маршрутов
	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/2 R1(config-if-GigabitEthernet 0/2)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/3 R1(config-if-GigabitEthernet 0/3)# ip address 1.1.13.1 255.255.255.0 R1(config-if-GigabitEthernet 0/3)# exit R1(config)#ip route 1.1.3.0 255.255.255.0 1.1.13.3 R1(config)#ip route 1.1.4.0 255.255.255.0 1.1.12.2 R1(config)#ip route 1.1.5.0 255.255.255.0 1.1.12.2

	R1(config)#ip static route-limit 2 % Exceeding maximum static routes limit
Проверка	Проверьте статические маршруты, которые действительно действуют, в таблице маршрутизации
	R1(config)# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set C 1.1.1.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.1.1/32 is local host. S 1.1.3.0/24 [1/0] via 1.1.13.3 S 1.1.4.0/24 [1/0] via 1.1.12.2 C 1.1.12.0/24 is directly connected, GigabitEthernet 0/2 C 1.1.12.1/32 is local host. C 1.1.13.0/24 is directly connected, GigabitEthernet 0/3 C 1.1.13.1/32 is local host

10.4.4. Сопоставление статического маршрута с BFD

10.4.4.1. Эффект конфигурации

Статический маршрут может быстро обнаружить сбой маршрута с помощью BFD.

10.4.4.2. Примечания

- Корреляция BFD не может быть настроена на коммутаторе L2.
- Вам необходимо настроить статический маршрут.
- Вы должны настроить параметры сеанса BFD, выполнив команду **bfd interval** *x***min_rx** *x***multiplier** *x*.

10.4.4.3. Шаги настройки

Сопоставление статического маршрута IPv4 с BFD

Команда	**ip route static bfd** [**vrf** *vrf-name*]*interface-type interface-number gateway*[**source** *ip-addess*]
Описание параметра	**vrf** *vrf-name*: (Опционально) указывает имя VRF, которому принадлежит статический маршрут. По умолчанию VRF является глобальным VRF. *interface-type*: указывает тип интерфейса. *interface-number*: указывает номер интерфейса. *gateway*: указывает IP-адрес шлюза, то есть IP-адрес соседа BFD. Если следующим hop-ом статического маршрута является этот сосед, BFD используется для проверки возможности подключения пути пересылки. **source** *ip-addess*: (Опционально) указывает IP-адрес источника, используемый для сеанса BFD. Этот параметр необходимо настроить, если IP-адрес соседа включает несколько hop-ов. По умолчанию IP-адрес источника не указан
По умолчанию	По умолчанию статический маршрут не коррелирует с BFD
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы сопоставить статический маршрут IPv4 с BFD. Если обнаружено состояние отключения сеанса BFD, статический маршрут IPv4 не активен и не участвует в пересылке пакетов

Сопоставление статического маршрута IPv6 с BFD

Команда	**ipv6 route static bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway* [**source** *ipv6-address*]
Описание параметра	**vrf** *vrf-name*: (Опционально) указывает имя VRF, которому принадлежит статический маршрут. По умолчанию VRF является глобальным VRF. *interface-type*: указывает тип интерфейса. *interface-number*: указывает номер интерфейса. *gateway*: указывает IP-адрес шлюза, то есть IP-адрес соседа BFD. Если следующим hop-ом статического маршрута является этот сосед, BFD используется для проверки возможности подключения пути пересылки. **source** *ipv6-address*: (Опционально) указывает IP-адрес источника, используемый для сеанса BFD. Этот параметр необходимо настроить, если IP-адрес соседа включает несколько hop-ов. По умолчанию

	IP-адрес соседа сеанса BFD представляет собой один hop, а IP-адрес источника не используется
По умолчанию	По умолчанию статический маршрут не коррелирует с BFD
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы сопоставить статический маршрут IPv6 с BFD. Если обнаружено состояние Down сеанса BFD, статический маршрут IPv6 не активен и не участвует в пересылке пакетов

10.4.4.4. Проверка

- Запустите команду **show bfd neighbors**, чтобы отобразить информацию о соседях BFD.
- Запустите команду **show ip route static bfd** или **show ipv6 route static bfd**, чтобы отобразить информацию о корреляции статических маршрутов с BFD.

10.4.4.5. Пример конфигурации

Сопоставление статического маршрута IPv4 с BFD

Сценарий:

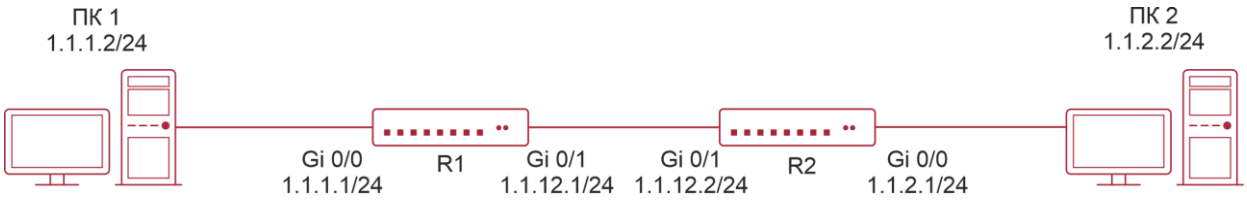


Рисунок 10-12.

Шаги настройки	• Настройте сеанс BFD на интерфейсе соединения между R1 и R2. • Настройте статические маршруты на маршрутизаторах R1 и R2 и укажите выходной интерфейс или следующий hop в качестве интерфейса взаимодействия. • Сопоставьте статические маршруты с BFD на маршрутизаторах R1 и R2 и проверьте связь следующих hop-ов статических маршрутов
R1	R1#configure terminal R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)# no switchport R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/1)#bfd interval 50 min_rx 50 multiplier 3

	R1(config-if-GigabitEthernet 0/1)# exit R1(config)# ip route 1.1.2.0 255.0.0.0 FastEthernet 0/1 1.1.12.2 R1(config)#ip route static bfd gigabitEthernet 0/1 1.1.12.2
R2	R2#configure terminal R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)# no switchport R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0 R1(config-if-GigabitEthernet 0/1)#bfd interval 50 min_rx 50 multiplier 3 R1(config-if-GigabitEthernet 0/1)# exit R1(config)# ip route 1.1.1.0 255.0.0.0 FastEthernet 0/1 1.1.12.1 R1(config)#ip route static bfd gigabitEthernet 0/1 1.1.12.1
Проверка	• Отобразите статус соседей BFD. • Отобразите статические маршруты, связанные с BFD
R1	R1#show bfd neighbors OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int 1.1.12.1 1.1.12.2 8192/0 Up 0(3) Up GigabitEthernet 0/1 R1#show ip route static bfd S 1.1.2.0/24 via 1.1.12.2, GigabitEthernet 0/1, BFD state is Up

10.4.4.6. Распространенные ошибки

- Канал на интерфейсе не работает.
- Для интерфейса не настроен IP-адрес.
- Параметры сеанса BFD не настроены.
- Статический маршрут не настроен.

10.4.5. Настройка статического быстрого перенаправления

10.4.5.1. Эффект конфигурации

Настройте и включите статическое быстрое перенаправление.

10.4.5.2. Примечания

- Статическое быстрое перенаправление невозможно настроить на коммутаторе L2.
- Вам необходимо настроить статический маршрут.
- Необходимо настроить карту маршрутов.

10.4.5.3. Шаги настройки

Определение резервного маршрута на карте маршрутов

Команда	**set fast-reroute backup-nexthop** *interface ip-address*
Описание параметра	*interface*: указывает резервный выходной интерфейс. *ip-address* : указывает резервный следующий hop
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите команду **route-map** *name* [**permit** | **deny**] *sequence* для создания дорожной карты. Запустите команду **match**, чтобы определить условия соответствия. Запустите команду **set fast-reroute backup-nexthop** *interface ip-address*, чтобы определить резервный выходной интерфейс и резервный следующий hop. Если маршрут соответствует условиям соответствия, для этого маршрута создается резервный маршрут. Если команда **match** не настроена, резервные маршруты генерируются для любого статического маршрута с выходным интерфейсом и следующим hop-ом

Включение быстрого перенаправления и ссылка на карту маршрутов

Команда	**ip fast-reroute** [**vrf** *vrf-name*] **static route-map** *route-map-name*
Описание параметра	*vrf-name*: (Необязательно) указывает VRF. Если VRF не указан, команда выполняется на всех VRF. *route-map-name*: указывает название дорожной карты резервного маршрута
По умолчанию	По умолчанию статическое быстрое перенаправление не настроено
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы включить быстрое изменение маршрута и свериться с картой маршрута

10.4.5.4. Проверка

Запустите команду **show ip route fast-reroute**, чтобы отобразить активные и резервные маршруты, которые вступят в силу.

10.4.5.5. Пример конфигурации

Настройка быстрой повторной маршрутизации

Сценарий:

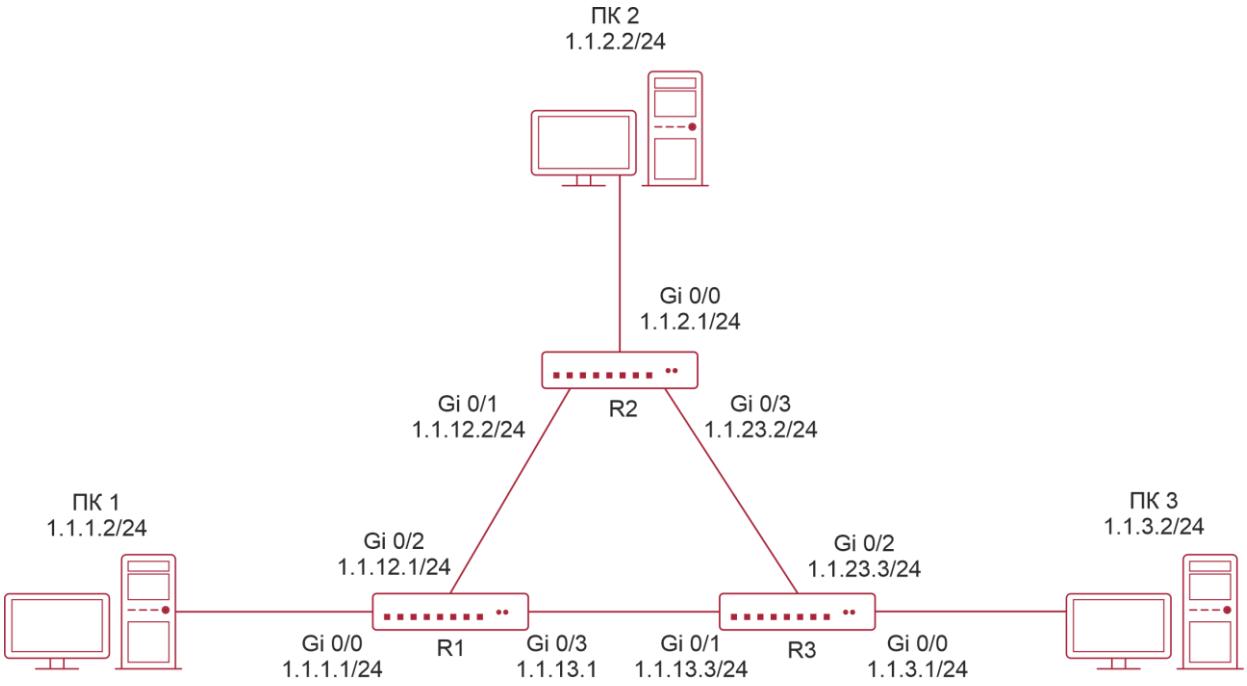


Рисунок 10-13.

Шаги настройки	На R1 настройте статический маршрут к сетевому сегменту ПК 3, а следующим hop-ом выходного интерфейса будет R3. На маршрутизаторе R1 настройте статическое быстрое перенаправление. Следующий hop выходного интерфейса резервного маршрута — R2
	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/2 R1(config-if-GigabitEthernet 0/2)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/3 R1(config-if-GigabitEthernet 0/3)# ip address 1.1.13.1 255.255.255.0 R1(config-if-GigabitEthernet 0/3)# exit R1(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.13.3

	R1(config)#route-map fast-reroute R1(config-route-map)# set fast-reroute backup-interface GigabitEthernet 0/2 backupnexthop 1.1.12.2 R1(config-route-map)# exit R1(config)#ip fast-reroute static route-map fast-reroute
Проверка	Отображение активных и резервных маршрутов на R1. R1#show ip route fast-reroute Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Status codes: m - main entry, b - backup entry, a - active entry Gateway of last resort is no set S 1.1.3.0 /24 [ma] via 1.1.13.3, GigabitEthernet 0/3 [b] via 1.1.12.2, GigabitEthernet 0/2

10.4.5.6. Распространенные ошибки

- Канал на интерфейсе не работает.
- Статический маршрут не настроен.
- Условия соответствия не настроены или неправильно настроены в дорожной карте.

10.4.6. Настройка преобразования ARP-to-host

10.4.6.1. Эффект конфигурации

Включите преобразование ARP-to-host на указанном интерфейсе.

10.4.6.2. Примечания

- Эту настройку невозможно выполнить на коммутаторе уровня 2.
- Интерфейс должен быть интерфейсом уровня 3 в состоянии Up.

10.4.6.3. Шаги настройки

Включение преобразования ARP-to-host на указанном интерфейсе

Команда	**ip route arp-to-host interface** *interface-name*
Описание параметра	*interface-name*: указывает имя интерфейса
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Эта команда используется для преобразования записей ARP в 32-битные маршруты хоста на указанном интерфейсе

Включение ARP-прокси

Команда	**local-proxy-arp**
Командный режим	Режим настройки интерфейса
Руководство по использованию	После получения запроса ARP, устройство использует прокси для отправки ответа ARP со своим собственным MAC-адресом Ethernet. В этом случае хосты общаются друг с другом через маршруты уровня 3

Настройка перераспределения BGP маршрутов хоста ARP

Команда	**redistribute arp-host**[**route-map** *map-tag*] [**metric** *metric-value*]
Описание параметра	**route-map** *map-tag*: указывает имя связанной карты маршрутов. Ни одна карта маршрутов не связана по умолчанию. **metric** *metric-value*: указывает значение метрики по умолчанию для перераспределения маршрутов в диапазоне от 0 до 4 294 967 295. Значение не установлено по умолчанию
Командный режим	Режим конфигурации BGP
Руководство по использованию	Эта команда используется для настройки перераспределения BGP маршрутов хостов ARP

10.4.6.4. Проверка

Запустите команду **show ip route arphost**, чтобы отобразить сгенерированные маршруты хоста.

10.4.6.5. Пример конфигурации

Настройка преобразования ARP-to-host

Сценарий:

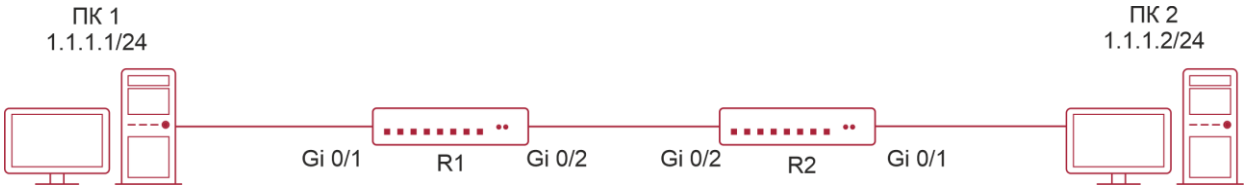


Рисунок 10-14.

Шаги настройки	Настройте адреса интерфейсов на R1 и R2. Включите преобразование ARP-to-host на указанных интерфейсах R1 и R2, настройте отношения соседства BGP и перераспределите маршруты хостов ARP
R1	R1#configure terminal R1(config)#interface vlan 40 R1(config-if-VLAN 40)#ip address 1.1.1.3 24 R1(config-if-VLAN 40)#local-proxy-arp R1(config-if-VLAN 40)#exit R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)#switchport R1(config-if-GigabitEthernet 0/1)#switchport mode trunk R1(config-if-GigabitEthernet 0/1)#switchport trunk allowed vlan only 40 R1(config-if-GigabitEthernet 0/1)#exit R1(config)#interface gigabitEthernet 0/2 R1(config-if-GigabitEthernet 0/2)# ip address 10.10.10.1 255.255.255.0 R1(config-if-GigabitEthernet 0/2)# exit R1(config)#router bgp 1 R1(config-router)#neighbor 10.10.10.2 remote-as 1 R1(config-router)#redistribute arp-host R1(config-router)#address-family ipv4 R1(onfig-router-af)#neighbor 10.10.10.2 next-hop-self R1(onfig-router-af)#exit R1(config-router)#exit R1(config)#ip route arp-to-host vlan 40

	R1(config)#ip route arp-to-host delay-time 1
R2	R2#configure terminal R2(config)#interface vlan 40 R2(config-if-VLAN 40)#ip address 1.1.1.4 24 R2(config-if-VLAN 40)#local-proxy-arp R2(config-if-VLAN 40)#exit R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# switchport R2(config-if-GigabitEthernet 0/1)#switchport mode trunk R2(config-if-GigabitEthernet 0/1)# switchport trunk allowed vlan only 40 R2(config-if-GigabitEthernet 0/1)#exit R2(config)#interface gigabitEthernet 0/2 R2(config-if-GigabitEthernet 0/2)# ip address 10.10.10.2 255.255.255.0 R2(config-if-GigabitEthernet 0/2)# exit R2(config)#router bgp 1 R2(config-router)#neighbor 10.10.10.1 remote-as 1 R2(config-router)#redistribute arp-host R2(config-router)#address-family ipv4 R2(onfig-router-af)#neighbor 10.10.10.1 next-hop-self R2(onfig-router-af)#exit R2(config-router)#exit R2(config)#ip route arp-to-host vlan 40 R2(config)#ip route arp-to-host delay-time 1
Проверка	Отобразите маршруты хоста ARP маршрутизатора R1, чтобы убедиться, что ПК1 может пинговать ПК2. R1(config)#show ip route arphost A 1.1.1.1/32 [1/0] via 1.1.1.1, gigabitEthernet 0/1 R1#show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, EV - BGP EVPN, A - Arp to host

	* - candidate default Gateway of last resort is 0.0.0.0 to network 0.0.0.0 S* 0.0.0.0/0 is directly connected, Null 0 C 10.10.10.0/24 is directly connected, GigabitEthernet 0/2 C 10.10.10.1/32 is local host. C 1.1.1.0/24 is directly connected, VLAN 40 A 1.1.1.1/32 [1/0] via 1.1.1.1, VLAN 40 C 1.1.1.3/32 is local host. B 1.1.1.2/32 [200/0] via 10.10.10.2, 00:57:12

10.4.6.6. Распространенные ошибки

Функция прокси-сервера ARP не включена на указанных интерфейсах.

10.5. Мониторинг

10.5.1. Отображение

Описание	Команда
Отображает таблицу маршрутизации IPv4	**show ip route**
Отображает таблицу маршрутизации IPv6	**show ipv6route**

10.5.2. Отладка

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

Описание	Команда
Отладка управления маршрутами IPv4	**debug nsm kernel ucast- v4**
Отладка управления маршрутами IPv6	**debug nsm kernel ucast-v6**
Отладка быстрого управления перенаправлением	**debug nsm kernel frr**

Описание	Команда
Отладка управления сетью по умолчанию	**debug nsm kernel default-network**
Отладка внутренних событий управления маршрутами	**debug nsm events**
Отладка отправки сообщений управления маршрутами и протоколов маршрутизации	**debug nsm packet send**
Отладка получения сообщений управления маршрутами и протоколов маршрутизации	**debug nsm packet recv**

11. НАСТРОЙКА VRF

11.1. Обзор

Таблица маршрутизации и пересылки (VRF) виртуальной приватной сети (VPN) используется для пересылки пакетов VPN. Каждая VPN соответствует таблице VRF.

Устройство, предоставляющее сервис VPN, имеет несколько таблиц маршрутизации, включая таблицу маршрутизации общедоступной сети (public) и одну или несколько таблиц VRF. Таблица маршрутизации общедоступной сети используется для пересылки пакетов общедоступной сети, а таблицы VRF используются для пересылки пакетов VPN. Эти таблицы маршрутизации создаются для разделения маршрутов в общедоступной сети от маршрутов в VPN, а также для разделения маршрутов в разных VPN.

ПРИМЕЧАНИЕ: VPN — это приватная выделенная сеть встроенная в общедоступную сеть. «Виртуальный» означает, что VPN является логически исключающим, а не физически исключающим.

11.2. Приложения

Приложение	Описание
Локальный доступ Inter-VPN	Предоставьте сервис VPN на устройстве маршрутизации и разрешите VPN-сетям доступ друг к другу
VRF только на границах провайдера (PE)	Предоставьте сервис VPN в IP-сеть и подключите один Customer Edge (CE) к одной VPN
VRF на CE и PE (приложение MCE)	Предоставьте сервис VPN в IP-сеть и подключите один CE к нескольким VPN

ПРИМЕЧАНИЕ: CE: периферийное устройство в сети клиента.

ПРИМЕЧАНИЕ: PE: граничное устройство в сети поставщика услуг (SP).

11.2.1. Локальный доступ Inter-VPN

11.2.1.1. Сценарий

Предоставьте сервис VPN на устройстве маршрутизации и разрешите VPN-сетям получать доступ друг к другу.

На Рисунке 11-1 Sub a запускает протокол информации о маршрутизации (RIP), Sub b запускает протокол Open Shortest Path First (OSPF), а Серверы (Servers) — это сегмент сети, напрямую подключенный к C. Предоставьте сервис VPN на C для Sub a, Sub b и Серверов, а также включите Sub a и Sub b для доступа к Серверам.

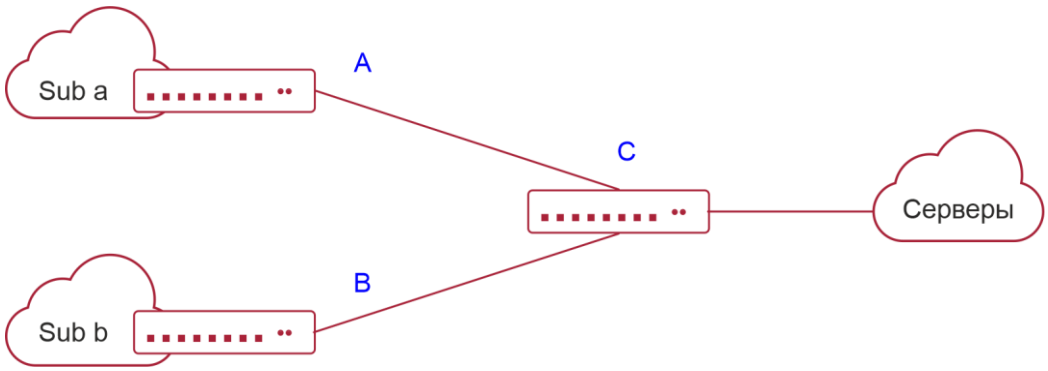


Рисунок 11-1.

11.2.1.2. Сопутствующая конфигурация

- На C создайте таблицу VRF для Sub a, привяжите интерфейс, напрямую подключенный к A, и соотнесите таблицу VRF с A с помощью RIP.
- На C создайте таблицу VRF для Sub b, привяжите интерфейс, напрямую подключенный к B, и соотнесите таблицу VRF с B с помощью OSPF.
- В C создайте таблицу VRF для Серверов и привяжите интерфейс, напрямую подключенный к Серверам.
- На C настройте цели маршрута (RT) таблиц VRF для Sub a, Sub b и Серверов. Импортируйте маршруты из таблиц VRF для Sub a и Sub b в таблицу VRF для Серверов и импортируйте маршруты из таблицы VRF для Серверов в таблицы VRF для Sub a и Sub b.
- Настройте протокол пограничного шлюза (BGP) на C. Добавьте маршруты RIP в таблицу VRF для Sub a, введите маршруты OSPF в таблицу VRF для Sub b и введите прямые маршруты в таблицу VRF для Серверов.

11.2.2. VRF только на границах провайдера (PE)

11.2.2.1. Сценарий

Поставщик интернет-услуг (ISP) предоставляет сервис VPN в магистральной IP-сети.

На Рисунке 11-2 VPN1 использует RIP, а VPN2 — OSPF.

- Один CE подключен к одной VPN, и все маршруты на CE используются исключительно подключенной VPN. Таким образом, для разделения маршрутов не требуется создавать таблицу VRF.
- На каждом PE необходимо создать таблицы VRF, чтобы разделить маршруты в VPN1, VPN2 и в общедоступной сети друг от друга.

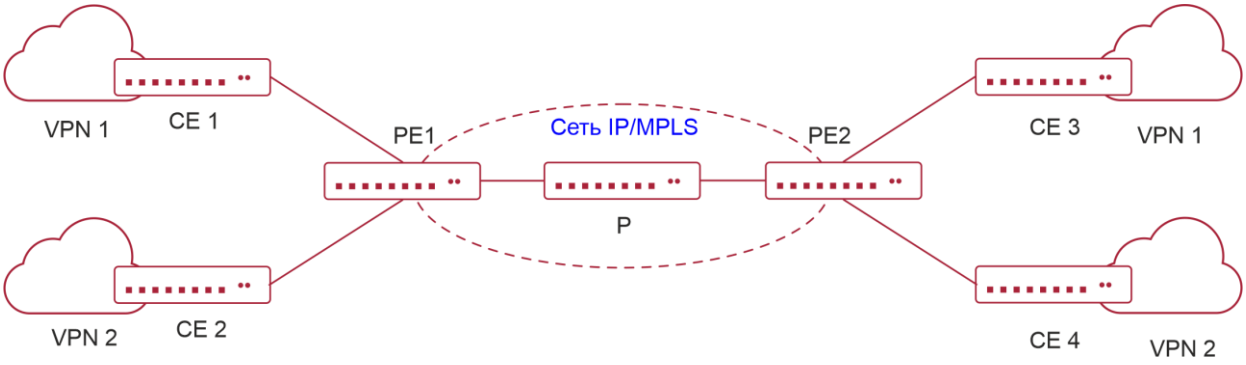


Рисунок 11-2.

11.2.2.2. Развертывание

- На PE1 создайте таблицу VRF для VPN1 и привяжите интерфейс, напрямую подключенный к CE1. На PE2 создайте таблицу VRF для VPN1 и привяжите интерфейс, напрямую подключенный к CE3.
- На PE1 создайте таблицу VRF для VPN2 и привяжите интерфейс, напрямую подключенный к CE2. На PE2 создайте таблицу VRF для VPN2 и привяжите интерфейс, напрямую подключенный к CE4.
- На PE1 свяжите таблицу VRF для VPN1 с CE1 с помощью RIP. На PE2 свяжите таблицу VRF для VPN1 с CE3 с помощью RIP.
- На PE1 свяжите таблицу VRF для VPN2 с CE2 с помощью OSPF. На PE2 свяжите таблицу VRF для VPN2 с CE4 с помощью OSPF.
- В экземпляре VRF для VPN1 на PE1 перераспределите маршруты RIP в BGP и перераспределите маршруты BGP в RIP. Конфигурация PE2 аналогична.
- В экземпляре VRF для VPN2 на PE1 перераспределите маршруты OSPF в BGP и перераспределите маршруты BGP в OSPF. Конфигурация PE2 аналогична.

11.2.3. VRF на CE и PE (приложение MCE)

11.2.3.1. Сценарий

ISP предоставляет сервис VPN в магистральной IP-сети.

На Рисунке 11-3 VPN a использует RIP, VPN b использует OSPF, а PE1 и PE2 подключены к BGP.

- Один мульти-VPN-экземпляр CE (MCE) подключен к нескольким VPN. Таблицы VRF должны быть созданы для разделения маршрутов в VPN a и маршрутов в VPN b.
- На каждом PE необходимо создать таблицы VRF, чтобы разделить маршруты в VPN a, VPN b и в общедоступной сети друг от друга.

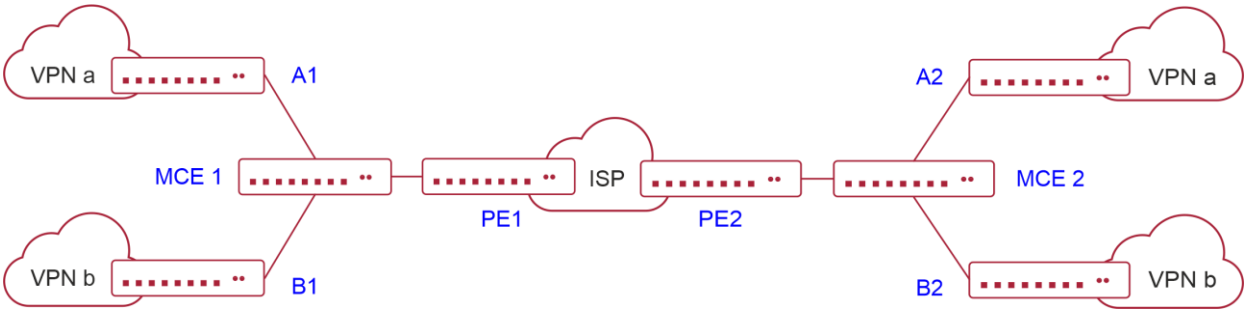


Рисунок 11-3.

11.2.3.2. Развертывание

- Один MCE1 создает таблицы VRF для VPN a и VPN b соответственно, привязывает интерфейсы, напрямую подключенные к VPN a и VPN b, и привязывает интерфейс VLAN, подключенный к PE1. Конфигурация MCE2 аналогична.
- На PE1 создайте таблицы VRF для VPN a и VPN b соответственно и привяжите интерфейс VLAN, подключенный к MCE1. Конфигурация PE2 аналогична.
- На MCE1 свяжите таблицу VRF для VPN a с VPN a с помощью RIP. Конфигурация MCE2 аналогична.
- На MCE1 свяжите таблицу VRF для VPN b с VPN b с помощью OSPF. Конфигурация MCE2 аналогична.
- В экземпляре VRF для VPN a на MCE1 перераспределите маршруты RIP в BGP и перераспределите маршруты BGP в RIP. Конфигурация MCE2 аналогична.
- В экземпляре VRF для VPN b на MCE1 перераспределите маршруты OSPF в BGP и перераспределите маршруты BGP в OSPF. Конфигурация MCE2 аналогична.

11.3. Функции

11.3.1. Обзор

Особенность	Описание
VPN-экземпляр	Экземпляр VPN используется для предоставления сервиса VPN. Обычно он представлен таблицей VRF
VPN-маршрут	Маршрут VPN используется для пересылки пакетов VPN
Атрибут VPN-маршрута	Отличитель маршрута (Route distinguisher (RD)): указывает VPN, которой принадлежит маршрут. RT: указывает trade-off режим маршрута VRF

11.3.2. VPN-экземпляр

Экземпляр VPN используется для предоставления сервиса VPN. На устройстве, предоставляющем сервис VPN, экземпляр VPN состоит из таблицы VRF, интерфейсов, процессов протокола маршрутизации и конфигурации, принадлежащих одной и той же VPN. Экземпляр VPN обычно представлен таблицей VRF.

11.3.2.1. Принцип работы

PE обменивается маршрутами с CE, используя соответствующий протокол маршрутизации в соответствующем экземпляре VPN. Таблица VRF привязана к определенному интерфейсу для создания набора интерфейсов. Пакеты, полученные на этих интерфейсах, будут связаны с таблицей VRF и перенаправлены по соответствующим маршрутам.

11.3.2.2. Сопутствующая конфигурация

ПРИМЕЧАНИЕ: таблицы VRF с одним протоколом и таблицы VRF с несколькими протоколами нельзя создавать одновременно. Таблицы VRF с одним протоколом поддерживают только IPv4, тогда как таблицы VRF с несколькими протоколами поддерживают IPv4 и IPv6.

Настройка таблицы VRF для одного протокола

По умолчанию у устройства нет таблицы VRF.

Запустите команду **ip vrf**, чтобы создать таблицу VRF с одним протоколом.

Запустите команду **ip vrf forwarding**, чтобы привязать интерфейс.

В настоящее время таблицы VRF с одним протоколом поддерживают только IPv4.

Настройка многопротокольной таблицы VRF

По умолчанию у устройства нет таблицы VRF.

Запустите команду **vrf definition**, чтобы создать многопротокольную таблицу VRF.

Запустите команду **address-family ipv4**, чтобы включить семейство адресов IPv4.

Запустите команду **address-family ipv6**, чтобы включить семейство адресов IPv6.

Запустите команду **vrf forwarding**, чтобы привязать интерфейс.

Многопротокольные таблицы VRF поддерживают IPv4 и IPv6.

11.3.3. VPN-маршрут

Маршрут VPN используется только для пересылки пакетов VPN. Он берется из:

- Прямой маршрут и маршрут хоста на связанном интерфейсе.
- Прямой маршрут и маршрут хоста в настроенном интерфейсе импорта (не привязано).
- Статические и динамические маршруты (RIP, RIPng, OSPFv2, OSPFv3, ISIS и BGP) в настроенном экземпляре VPN.

ПРИМЕЧАНИЯ:

- Подробную информацию о RIP в экземпляре VPN см. в разделе «Руководство по настройке RIP».
- Подробную информацию о RIPng в экземпляре VPN см. в «Руководстве по настройке RIPng».

- Подробную информацию об OSPFv2 в экземпляре VPN см. в разделе «Руководство по настройке OSPFv2».
- Подробную информацию об OSPFv3 в экземпляре VPN см. в разделе «Руководство по настройке OSPFv3».
- Подробную информацию об ISIS в экземпляре VPN см. в разделе «Руководство по настройке ISIS».
- Подробную информацию о BGP в экземпляре VPN см. в разделе «Руководство по настройке BGP».

11.3.4. Атрибут VPN-маршрута

Расширенные атрибуты BGP включают два атрибута, специфичные для маршрутов VPN: RD и RT.

11.3.4.1. Принцип работы

RD

Два маршрута с одним и тем же адресом, но разными RD в двух таблицах VRF могут объявляться отдельно между PE, поскольку маршруты отправляются вместе со своими RD через многопротокольный BGP (MP-BGP).

RT

По сути, RT указывает компромисс и предпочтения маршрута каждой таблицы VRF. В основном он используется для управления политиками объявления и установки VPN-маршрутов. RT разделен на атрибут импорта и атрибут экспорта. Атрибут импорта указывает интересующий маршрут, а атрибут экспорта указывает объявленный маршрут. PE объявляет маршрут к другим PE на основе правила экспорта RT в соответствующей таблице VRF. Peer PE проверяет все полученные маршруты на соответствие правилу импорта RT в каждой таблице VRF. Если маршрут соответствует правилу экспорта RT (правило экспорта содержит правило импорта), он будет добавлен в соответствующую таблицу VRF.

11.3.4.2. Сопутствующая конфигурация

RD

По умолчанию в режиме VRF не настроен RD.

Запустите команду **rd**, чтобы настроить RD.

RT

По умолчанию RT не настроен в режиме VRF или режиме семейства адресов.

Запустите команду **route-target** { **import | export | both** } для настройки RT.

11.4. Конфигурация

Конфигурация	Описание и команда	
Настройка таблицы VRF для одного протокола	Таблицы VRF с одним протоколом и таблицы VRF с несколькими протоколами нельзя создавать одновременно. Если поддерживается IPv6, настройте многопротокольную таблицу VRF; в противном случае вы можете настроить таблицу VRF с одним протоколом или таблицу VRF с несколькими протоколами. Этот элемент конфигурации создает таблицу VRF в сети IPv4. IPv6 не поддерживается	
	ip vrf *vrf-name*	Создает таблицу VRF
	rd *rd_value*	Настраивает RD
	route-target { **import** | **export** | **both** } *rt_value*	Настраивает RT
	ip vrf forwarding *vrf-name*	Привязывает интерфейс и добавляет прямой маршрут и маршрут хоста на интерфейсе в таблицу VRF
	ip vrf receive *vrf_name*	Добавляет прямой маршрут и маршрут хоста на интерфейсе в таблицу VRF без привязки интерфейса
Настройка многопротокольной таблицы VRF	Таблицы VRF с одним протоколом и таблицы VRF с несколькими протоколами нельзя создавать одновременно. Если поддерживается IPv6, настройте многопротокольную таблицу VRF. В противном случае вы можете настроить таблицу VRF с одним протоколом или таблицу VRF с несколькими протоколами. Этот элемент конфигурации создает таблицу VRF в сети IPv4 или IPv6	
	vrf definition *vrf-name*	Создает таблицу VRF
	description *string*	Настраивает описание VRF
	rd *rd_value*	Настраивает RD
	route-target { **import** | **export** | **both** } *rt_value*	Настраивает RT

Конфигурация	Описание и команда	
	address-family ipv4	Включает семейство адресов IPv4
	address-family ipv6	Включает семейство адресов IPv6
	vrf forwarding *vrf-name*	Привязывает интерфейс и добавляет прямой маршрут и маршрут peer-a на интерфейсе в таблицу VRF
	vrf receive *vrf-name*	Добавляет прямой маршрут и маршрут хоста на интерфейсе в таблицу VRF без привязки интерфейса

11.4.1. Настройка таблицы VRF для одного протокола

11.4.1.1. Эффект конфигурации

- Предоставьте сервис VPN на устройстве.
- С помощью BGP можно гибко контролировать разделение и доступ между VPN.
- С помощью BGP предоставьте сервис VPN в магистральной IP-сети.
- Поддерживается только IPv4.

11.4.1.2. Примечания

- Таблицу VRF создавать не нужно, если устройство пересылает пакеты только из одной VPN или из общедоступной сети.
- Если устройству необходимо пересылать пакеты общедоступной сети и пакеты VPN или пересылать пакеты из нескольких VPN, необходимо создать таблицы VRF для разделения маршрутов.
- Во многих случаях в таблицы VRF необходимо добавить статические или динамические маршруты (RIP, OSPF, ISIS и BGP).

11.4.1.3. Шаги настройки

Создание таблицы VRF

- Обязательный.
- Создайте таблицу VRF для каждой VPN.

Настройка RD

- Опционально.
- Когда информацию о маршрутизации необходимо объявить через BGP в магистральной сети, BGP может выбрать лучший маршрут для объявления, если в разных VPN существуют перекрывающиеся сетевые адреса, из-за чего

некоторые VPN не смогут получить соответствующую информацию о маршрутизации. Чтобы решить эту проблему, вы можете настроить RD для маршрутов, чтобы BGP мог принимать решения о маршрутизации на основе этих RD, гарантируя тем самым, что каждая VPN сможет получать соответствующую информацию о маршрутизации.

- Запустите команду **rd** в однопротокольном режиме VRF.

Настройка RT

- Опционально.
- Вы можете запустить команду **route-target export**, чтобы указать атрибуты объявляемого маршрута, и запустить команду **route-target import**, чтобы указать атрибуты получаемого маршрута. Вы также можете запустить команду **route-target both**, чтобы указать атрибуты экспорта и импорта.
- Запустите команду **route-target** в однопротокольном режиме VRF.

Привязка интерфейса и добавление прямого маршрута и маршрута хоста на интерфейсе в таблицу VRF

- Обязательный.
- Если физический канал для передачи VPN-пакетов занят исключительно VPN, привяжите физический интерфейс к соответствующей таблице VRF.
- Если физический канал для передачи VPN-пакетов используется несколькими VPN, необходимо создать независимый логический канал для каждого VPN и привязать логический интерфейс к соответствующей таблице VRF. Логический интерфейс может быть субинтерфейсом или интерфейсом VLAN.
- Прежде чем настраивать IPv4-адрес интерфейса, необходимо привязать интерфейс к соответствующей таблице VRF с одним протоколом. Если вы привязываете интерфейс после настройки его IPv4-адреса, IPv4-адрес будет недействительным (IPv6-адрес интерфейса сохраняется).
- Если вы привяжете интерфейс к соответствующей однопротокольной таблице VRF и включите IPv6 на интерфейсе, устройство не сможет пересылать пакеты IPv6, полученные на интерфейсе.

Добавление прямого маршрута и маршрута хоста на интерфейсе в таблицу VRF без привязки интерфейса

- Опционально.
- Если для выбора таблицы VRF требуется маршрутизация на основе политик (PBR), запустите команду **ip vrf receive** на интерфейсе, к которому применяется PBR, и импортируйте прямой маршрут и маршрут хоста на интерфейсе в каждую таблицу VRF, доступную для выбора.

11.4.1.4. Проверка

Проверьте, правильно ли созданы таблицы VRF на маршрутизаторе.

11.4.1.5. Связанные команды

Создание таблицы VRF

Команда	**ip vrf** *vrf-name*
Описание параметра	*vrf-name*: указывает имя создаваемой таблицы VRF. Оно не может превышать 31 символ
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После выполнения команды система войдет в режим VRF

Настройка RD

Команда	**rd** *rd_value*
Описание параметра	*rd_value* имеет следующие три разных формы параметра: (1) *rd_value* = as_num: nn as_num указывает 2-байтовое число, которое идентифицирует общедоступную автономную систему (AS). nn настраивается в диапазоне от 0 до 4 294 967 295. (2) *rd_value* "= ip_addr: nn ip_addr должен быть глобальным IP-адресом. nn настраивается в диапазоне от 0 до 65 535. (3) *rd_value* = as4_num: nn as4_num указывает 4-байтовый номер, идентифицирующий общедоступную AS. nn настраивается в диапазоне от 1 до 65 535
Командный режим	Режим конфигурации VRF
Руководство по использованию	Вы не можете напрямую изменить RD существующей таблицы VRF. Вам необходимо сначала удалить таблицу VRF, а затем настроить новый RD. Таблица VRF имеет только один RD. Вы не можете настроить несколько RD для одной таблицы VRF

Настройка RT

Команда	**route-target** { **import** | **export** | **both** } *rt_value*
Описание параметра	*rt_value* имеет следующие три разных формы параметра:

	(1) *rt_value* = as_num: nn as_num указывает 2-байтовый номер, идентифицирующий общедоступную AS. nn настраивается в диапазоне от 0 до 4 294 967 295. (2) *rt_value* = ip_addr: nn ip_addr должен быть глобальным IP-адресом. nn настраивается в диапазоне от 0 до 65 535. (3) *rt_value* = as4_num: nn as4_num указывает 4-байтовый номер, идентифицирующий общедоступную AS. nn настраивается в диапазоне от 1 до 65 535
Командный режим	Режим конфигурации VRF
Руководство по использованию	Таблицу VRF можно настроить с использованием нескольких атрибутов импорта и экспорта RT

Привязка интерфейса

Команда	**ip vrf forwarding** *vrf-name*
Описание параметра	*vrf-name*: указывает имя таблицы VRF
Командный режим	Режим настройки интерфейса
Руководство по использованию	По умолчанию интерфейс не принадлежит ни одной таблице VRF. После привязки интерфейса к соответствующей таблице VRF прямой маршрут и маршрут хоста на интерфейсе будут автоматически добавлены в таблицу VRF. Прежде чем настраивать IPv4-адрес интерфейса, необходимо привязать интерфейс к соответствующей таблице VRF с одним протоколом. Если вы привязываете интерфейс после настройки его IPv4-адреса, IPv4-адрес будет недействительным (IPv6-адрес интерфейса сохраняется)

Добавление прямого маршрута и маршрута хоста на интерфейсе в таблицу VRF без привязки интерфейса

Команда	**ip vrf receive** *vrf-name*
Описание параметра	*vrf-name*: указывает имя таблицы VRF

Командный режим	Режим настройки интерфейса
Руководство по использованию	Эта команда используется для добавления маршрута хоста и прямого маршрута на интерфейсе в таблицу VRF. Если вам нужно добавить маршрут хоста и прямой маршрут на интерфейсе в несколько таблиц VRF, выполните команду несколько раз. В отличие от команды **ip vrf forwarding**, команда **ip vrf receive** не привязывает интерфейс к соответствующей таблице VRF. Интерфейс по-прежнему является глобальным и не принадлежит ни одной таблице VRF. Команды **ip vrf forwarding** и **ip vrf receive** являются взаимоисключающими на одном и том же интерфейсе

Отображение информации VRF на устройстве

Команда	**show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*]
Описание параметра	**brief**: отображает краткую информацию. **detail**: отображение подробной информации. **interfaces**: отображает информацию о привязке интерфейса. *vrf-name*: указывает имя таблицы VRF
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	Эта команда используется для отображения информации указанной таблицы VRF, чтобы проверить, связана ли таблица VRF с верным интерфейсом

Отображение маршрутов в таблице VRF

Команда	**show ip route vrf** *vrf-name*
Описание параметра	*vrf-name*: указывает имя таблицы VRF
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	Эта команда используется для проверки того, содержит ли указанная таблица VRF соответствующие маршруты

11.4.1.6. Пример конфигурации

Локальный доступ Inter-VPN

Сценарий:

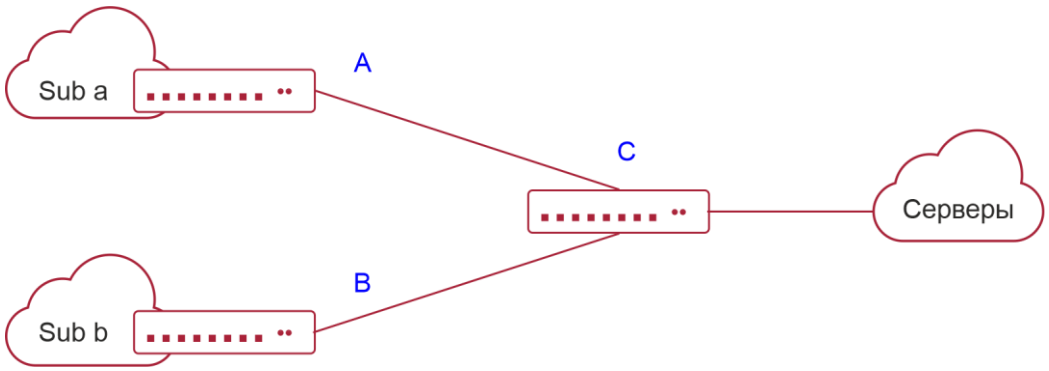


Рисунок 11-4.

	Sub a, Sub b и Серверы (Servers) — это три VPN с отдельными адресными пространствами. Sub a запускает RIP, Sub b запускает OSPF, а Серверы — это сегмент сети, напрямую подключенный к C
Требования к конфигурации	Маршруты в Sub a отделены от тех, что находятся в Sub b, но оба Sub a и Sub b могут получить доступ к Серверам
Шаги настройки	• На C создайте таблицу VRF для Sub a, привяжите интерфейс, напрямую подключенный к A, и свяжите таблицу VRF с A с помощью RIP. • На C создайте таблицу VRF для Sub b, привяжите интерфейс, напрямую подключенный к B, и свяжите таблицу VRF с B с помощью OSPF. • В C создайте таблицу VRF для Серверов и привяжите интерфейс, напрямую подключенный к Серверам. • На C настройте RT таблиц VRF для Sub a, Sub b и Серверов. Импортируйте маршруты из таблиц VRF для Sub a и Sub b в таблицу VRF для Серверов и импортируйте маршруты из таблицы VRF для Серверов в таблицы VRF для Sub a и Sub b. • Настройте протокол пограничного шлюза (BGP) на C. Добавьте маршруты RIP в таблицу VRF для Sub a, введите маршруты OSPF в таблицу VRF для Sub b (с поддержкой семейства адресов) и введите прямые маршруты в таблицу VRF для Серверов (включена с семейством адресов). Планирование интерфейсов и адресов:

<table>
<tr><td></td><td>
<table>
<tr><th>Описание интерфейса</th><th>Имя интерфейса</th><th>IP-адрес/ маска</th><th>Таблица VRF</th></tr>
<tr><td>Интерфейс на C подключен к A</td><td>GE0/1</td><td>10.10.1.1/24</td><td>Таблица VRF для Sub a</td></tr>
<tr><td>Интерфейс C подключен к B</td><td>GE0/2</td><td>10.10.2.1/24</td><td>Таблица VRF для Sub b</td></tr>
<tr><td>Интерфейс на C, подключенный к Серверам</td><td>GE0/3</td><td>10.10.3.1/24</td><td>Таблица VRF для Серверов</td></tr>
<tr><td>Интерфейс на A подключен к C</td><td>GE0/1</td><td>10.10.1.2/24</td><td>-</td></tr>
<tr><td>Интерфейс на B подключен к C</td><td>GE0/2</td><td>10.10.2.2/24</td><td>-</td></tr>
</table>
</td></tr>
<tr><td>A</td><td>A(config)#interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)#no switchport port
A(config-if-GigabitEthernet 0/1)#ip address 10.10.1.2 255.255.255.0
A(config-if-GigabitEthernet 0/1)#exit
A(config)#router rip
A(config-router)#version 2
A(config-router)#no auto-summary
A(config-router)#network 10.10.1.0 0.0.0.255</td></tr>
<tr><td>B</td><td>B(config)#interface GigabitEthernet 0/2
B(config-if-GigabitEthernet 0/2)#no switchport port
B(config-if-GigabitEthernet 0/2)#ip address 10.10.2.2 255.255.255.0
B(config-if-GigabitEthernet 0/2)#exit
B(config)#router ospf 1
B(config-router)#network 10.10.2.0 0.0.0.255 area 0</td></tr>
<tr><td>C</td><td>C(config)# ip vrf Suba
C(config-vrf)# rd 100:1
C(config-vrf)# route-target import 100:3
C(config-vrf)# route-target export 100:1
C(config-vrf)# exit
C(config)#interface GigabitEthernet 0/1
C(config-GigabitEthernet 0/1)#ip vrf forwarding Suba</td></tr>
</table>

	C(config-GigabitEthernet 0/1)#ip address 10.10.1.1 255.255.255.0 C(config-GigabitEthernet 0/1)# exit C(config)#router rip C(config-router)#address-family ipv4 vrf Suba C(config-router-af)# version 2 C(config-router-af)# no auto-summary C(config-router-af)#network 10.10.1.0 0.0.0.255 C(config-router-af)#exit
	C(config)# ip vrf Subb C(config-vrf)# rd 100:2 C(config-vrf)# route-target import 100:3 C(config-vrf)# route-target export 100:2 C(config-vrf)# exit C(config)#interface gigabitEthernet 0/2 C(config-GigabitEthernet 0/2)#ip vrf forwarding Subb C(config-GigabitEthernet 0/2)# ip address 10.10.2.1 255.255.255.0 C(config-GigabitEthernet 0/2)# exit C(config)# router ospf 2 vrf Subb C(config-router)# network 10.10.2.0 0.0.0.255 area 0 C(config-router)# exit
	C(config)# ip vrf Servers C(config-vrf)# rd 100:3 C(config-vrf)# route-target import 100:1 C(config-vrf)# route-target import 100:2 C(config-vrf)# route-target export 100:3 C(config-vrf)# exit C(config)# interface gigabitEthernet 0/3 C(config-GigabitEthernet 0/3)# ip vrf forwarding Servers C(config-GigabitEthernet 0/3)# ip address 10.10.3.1 255.255.255.0 C(config-GigabitEthernet 0/3)# exit
	C(config)# router bgp 200 C(config-router)# address-family ipv4 vrf vpna C(config-router-af)# redistribute rip

	C(config-router-af)# exit C(config-router)# address-family ipv4 vrf vpnb C(config-router-af)# redistribute ospf 1 C(config-router-af)# exit C(config-router)# address-family ipv4 vrf Servers C(config-router-af)# redistribute connected subnets C(config-router-af)# exit
Проверка	Запустите команду **show ip vrf interface** на C, чтобы проверить информацию о привязке интерфейса. Запустите команду **show ip route vrf** на C, чтобы проверить, созданы ли две таблицы VRF для разделения маршрутов в Sub a от маршрутов в Sub b и содержат ли обе таблицы VRF маршруты на Серверах
C	C# show ip vrf interfaces Interface IP-Address VRF Protocol GigabitEthernet 0/1 10.10.1.1 Suba up GigabitEthernet 0/2 10.10.2.1 Subb up GigabitEthernet 0/3 10.10.3.1 Servers up
	C# show ip route vrf Subb Routing Table: Subb Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set O 10.2.0.0/16 [20/0] via 0.0.0.0, 00:10:46, GigabitEthernet 0/2 O 10.10.2.0/24 [20/0] via 0.0.0.0, 00:10:46, GigabitEthernet 0/2 C 10.10.2.1/32 is local host. C 10.10.3.0/24 is directly connected, GigabitEthernet 0/3 C 10.10.3.1/32 is local host

11.4.1.7. Распространенные ошибки

- Интерфейс привязывается к таблице VRF после настройки IP-интерфейса интерфейса.
- Когда физический канал используется для пересылки пакетов из нескольких VPN, соответствующий физический интерфейс привязывается к таблице VRF.
- Маршруты VPN не представлены в BGP.

11.4.2. Настройка многопротокольной таблицы VRF

11.4.2.1. Эффект конфигурации

- Предоставьте сервис VPN на устройстве.
- С помощью BGP можно гибко контролировать разделение и доступ между VPN.
- С помощью BGP предоставьте сервис VPN в магистральной IP-сети.
- Поддержка IPv4 и IPv6 посредством настройки семейства адресов.

11.4.2.2. Примечания

- Таблицу VRF создавать не нужно, если устройство пересылает пакеты только из одной VPN или из общедоступной сети.
- Если устройству необходимо пересылать пакеты общедоступной сети и пакеты VPN или пересылать пакеты из нескольких VPN, необходимо создать таблицы VRF для разделения маршрутов.
- Во многих случаях в таблицы VRF необходимо добавить статические или динамические маршруты (RIP, OSPF, ISIS и BGP).

11.4.2.3. Шаги настройки

Создание таблицы VRF

- Обязательный.
- Создайте таблицу VRF для каждой VPN.

Настройка семейства адресов

- Обязательный.
- Включите соответствующее семейство адресов для каждой созданной таблицы VRF.

Настройка RD

- Опционально.
- Когда информацию о маршрутизации необходимо объявить через BGP в магистральной сети, BGP может выбрать лучший маршрут для объявления, если в разных VPN существуют перекрывающиеся сетевые адреса, из-за чего некоторые VPN не смогут получить соответствующую информацию о маршрутизации. Чтобы решить эту проблему, вы можете настроить RD для маршрутов, чтобы BGP мог принимать решения о маршрутизации на основе этих RD, гарантируя тем самым, что каждая VPN сможет получать соответствующую информацию о маршрутизации.

Настройка RT

- Опционально.

- Вы можете запустить команду **route-target export**, чтобы указать атрибуты объявляемого маршрута, и запустить команду **route-target import**, чтобы указать атрибуты получаемого маршрута. Вы также можете запустить команду **route-target both**, чтобы указать атрибуты экспорта и импорта.
- Запустите команду **route-target** в многопротокольном режиме VRF или в режиме семейства многопротокольных адресов VRF.

Привязка интерфейса и добавление прямого маршрута и маршрута хоста на интерфейсе в таблицу VRF

- Обязательный.
- Если физический канал для передачи VPN-пакетов занят исключительно VPN, привяжите физический интерфейс к соответствующей таблице VRF.
- Если физический канал для передачи VPN-пакетов используется несколькими VPN, необходимо создать независимый логический канал для каждого VPN и привязать логический интерфейс к соответствующей таблице VRF. Логический интерфейс может быть субинтерфейсом или интерфейсом VLAN.
- Прежде чем привязать интерфейс к многопротокольной таблице VRF, включите для этой таблицы семейство адресов. Если вы заранее не включите семейство адресов IPv4, вы не сможете настроить адрес IPv4 и адрес IPv4 VRRP привязанного интерфейса. Если вы заранее не включите семейство адресов IPv6, вы не сможете настроить адрес IPv6 и адрес IPv6 VRRP привязанного интерфейса.
- Прежде чем настраивать адрес IPv4 или IPv6 интерфейса, необходимо привязать интерфейс к соответствующей многопротокольной таблице VRF. Если вы привяжете интерфейс после настройки его адреса IPv4 или IPv6, адрес будет недействительным.

Добавление прямого маршрута и маршрута хоста на интерфейсе в таблицу VRF без привязки интерфейса

- Опционально.
- Если для выбора таблицы VRF требуется PBR, запустите команду **ip vrf receive** на интерфейсе, к которому применяется PBR, и импортируйте прямой маршрут и маршрут хоста на интерфейсе в каждую таблицу VRF, доступную для выбора.

11.4.2.4. Проверка

Проверьте, правильно ли созданы многопротокольные таблицы VRF на маршрутизаторе и включены ли соответствующие семейства адресов.

11.4.2.5. Связанные команды

Создание таблицы VRF

Команда	**vrf definition** *vrf-name*
Описание параметра	*vrf-name*: указывает имя создаваемой таблицы VRF. Оно не может превышать 31 символ
Командный режим	Режим глобальной конфигурации

Руководство по использованию	После выполнения команды система войдет в режим VRF

Включение семейства адресов IPv4

Команда	**address-family ipv4**
Командный режим	Режим VRF
Руководство по использованию	После выполнения команды система войдет в подрежим семейства адресов IPv4 VRF

Включение семейства адресов IPv6

Команда	**address-family ipv6**
Командный режим	Режим VRF
Руководство по использованию	После запуска команды система перейдет в подрежим семейства адресов IPv6 VRF

Настройка RD

Команда	**rd** *rd_value*
Описание параметра	*rd_value* имеет следующие три разных формы параметра: (1) *rd_value* = as_num: nn as_num указывает 2-байтовый номер, идентифицирующий общедоступную AS. nn настраивается в диапазоне от 0 до 4 294 967 295. (2) *rd_value* = ip_addr: nn ip_addr должен быть глобальным IP-адресом. nn настраивается в диапазоне от 0 до 65 535. (3) *rd_value* = as4_num: nn ac4_num указывает 4-байтовый номер, идентифицирующий общедоступную AS. nn настраивается в диапазоне от 1 до 65 535
Командный режим	Режим конфигурации VRF

Руководство по использованию	Вы не можете напрямую изменить RD существующей таблицы VRF. Вам необходимо сначала удалить таблицу VRF, а затем настроить новый RD. Таблица VRF имеет только один RD. Вы не можете настроить несколько RD для одной таблицы VRF

Настройка RT

Команда	**route-target** { **import** | **export** | **both** } *rt_value*
Описание параметра	*rt_value* имеет следующие три разных формы параметра: (1) *rt_value* = as_num: nn as_num указывает 2-байтовое число, которое идентифицирует общедоступную AS. nn настраивается в диапазоне от 0 до 4 294 967 295. (2) *rt_value* = ip_addr: nn ip_addr должен быть глобальным IP-адресом. nn настраивается в диапазоне от 0 до 65 535. (3) *rt_value* = as4_num: nn as4_num указывает 4-байтовый номер, идентифицирующий общедоступную AS. nn настраивается в диапазоне от 1 до 65 535
Командный режим	Режим конфигурации VRF или подрежим семейства адресов VRF
Руководство по использованию	В одной таблице VRF можно настроить несколько атрибутов импорта и экспорта RT

Привязка интерфейса

Команда	**vrf forwarding** *vrf-name*
Описание параметра	*vrf-name*: указывает имя таблицы VRF
Командный режим	Режим настройки интерфейса
Руководство по использованию	По умолчанию интерфейс не принадлежит ни одной таблице VRF. После привязки интерфейса к соответствующей таблице VRF прямой маршрут и маршрут хоста на интерфейсе будут автоматически добавлены в таблицу VRF. Прежде чем привязать интерфейс к многопротокольной таблице VRF, включите для этой таблицы семейство адресов. Если вы заранее не

	включите семейство адресов IPv4, вы не сможете настроить адрес IPv4 и адрес IPv4 VRRP привязанного интерфейса. Если вы заранее не включите семейство адресов IPv6, вы не сможете настроить адрес IPv6 и адрес IPv6 VRRP привязанного интерфейса. Прежде чем настраивать адреса IPv4, IPv6, VRRP IPv4 и VRRP IPv6 интерфейса, необходимо привязать интерфейс к многопротокольной таблице VRF; в противном случае эти адреса будут недействительны, и протокол IPv6 на интерфейсе будет отключен. Если семейство адресов IPv4 будет удалено из многопротокольной таблицы VRF, адреса IPv4 и VRRP IPv4 всех интерфейсов, привязанных к таблице VRF, будут удалены, а также будут удалены статические маршруты IPv4 в таблице VRF или маршруты следующего hop-a. Если семейство адресов IPv6 будет удалено из многопротокольной таблицы VRF, адреса IPv6 и VRRP IPv6 всех интерфейсов, привязанных к таблице VRF, будут удалены, протокол IPv6 на интерфейсах будет отключен, а статические маршруты IPv6 в таблице VRF или маршруты следующего hop-a также удаляются

Добавление прямого маршрута и маршрута хоста на интерфейсе в таблицу VRF без привязки интерфейса

Команда	**vrf receive** *vrf-name*
Описание параметра	*vrf-name*: указывает имя таблицы VRF
Командный режим	Режим настройки интерфейса
Руководство по использованию	Эта команда используется для добавления маршрута хоста и прямого маршрута на интерфейсе в таблицу VRF. Если вам нужно добавить маршрут хоста и прямой маршрут на интерфейсе в несколько таблиц VRF, выполните команду несколько раз. В отличие от команды **vrf forwarding**, команда **vrf receive** не привязывает интерфейс к соответствующей таблице VRF. Интерфейс по-прежнему является глобальным и не принадлежит ни одной таблице VRF. Команды **vrf forwarding** и **vrf receive** являются взаимоисключающими на одном и том же интерфейсе

Отображение информации VRF на устройстве

Команда	**show vrf** [**brief** | **detail** | **ipv4** | **ipv6**] [*vrf-name*]
Описание параметра	**brief**: отображает краткую информацию. **detail**: отображение подробной информации.

	ipv4: отображает краткую информацию таблицы IPv4 VRF. **ipv6**: отображает краткую информацию таблицы IPv6 VRF. *vrf-name*: указывает имя таблицы VRF
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	Эта команда используется для отображения информации об указанной таблице VRF, чтобы проверить, связана ли таблица VRF с верным интерфейсом

Отображение маршрутов в таблице VRF

Команда	**show ip route vrf** *vrf-name*
Описание параметра	*vrf-name*: указывает имя таблицы VRF
Командный режим	Режимы привилегированной, глобальной и интерфейсной конфигурации
Руководство по использованию	Эта команда используется для проверки того, содержит ли указанная таблица VRF соответствующие маршруты

11.4.2.6. Пример конфигурации

ПРИМЕЧАНИЕ: в следующем примере описывается только конфигурация, связанная с VRF, на A1, B1, MCE1 и PE1. Конфигурация A2, B2, MCE2 и PE2 аналогична.

VRF на CE и PE (приложение MCE)

Сценарий:

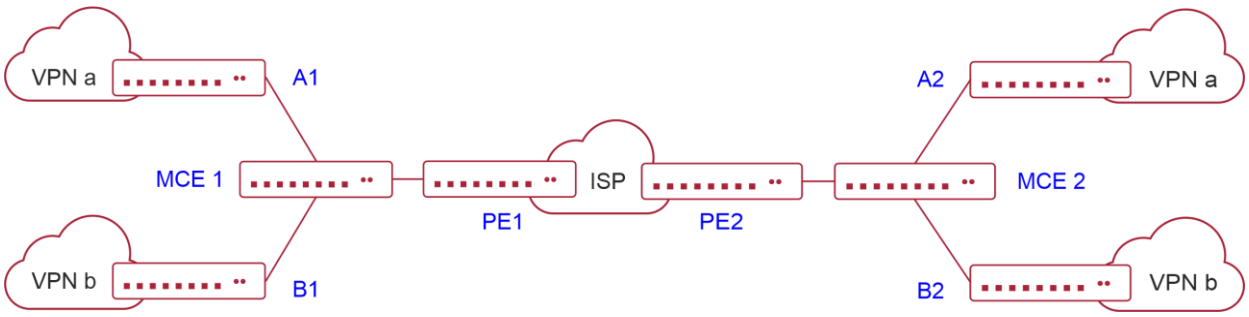


Рисунок 11-5.

<table>
<tr><td></td><td>VPN a и VPN b имеют независимые адресные пространства.
VPN a использует RIP, а VPN b использует OSPF</td></tr>
<tr><td>Требования к конфигурации</td><td>Маршруты в VPN a отделены от маршрутов в VPN b. A1 и A2 могут получить доступ друг к другу, а B1 и B2 могут получить доступ друг к другу</td></tr>
<tr><td>Шаги настройки</td><td>

Соедините MCE1 и A1 через RIP. Расширьте маршруты RIP на A1. На MCE1 создайте таблицу VRF для VPN a, привяжите напрямую подключенный интерфейс и настройте маршруты RIP.
Подключите MCE1 и B1 через OSPF. Расширьте маршруты OSPF на B1. На MCE1 создайте таблицу VRF для VPN b, привяжите напрямую подключенный интерфейс и настройте маршруты OSPF.
Соедините MCE1 и PE1 через BGP. На MCE1 и PE1 создайте таблицу VRF для каждой VPN, привяжите интерфейс VLAN и настройте маршруты BGP.
Настройте физическое соединение между MCE1 и PE1 в режиме Trunk.
В экземпляре VRF для VPN a на MCE1 перераспределите маршруты RIP в BGP и перераспределите маршруты BGP в RIP.
В экземпляре VRF для VPN b на MCE1 перераспределите маршруты OSPF в BGP и перераспределите маршруты BGP в OSPF.

Планирование интерфейсов и адресов:
<table>
<tr><th>Описание интерфейса</th><th>Имя интерфейса</th><th>IP-адрес/маска</th><th>Таблица VRF</th></tr>
<tr><td>Физический интерфейс на A1, подключенный к MCE1</td><td>GE0/1</td><td>10.10.1.2/24</td><td>-</td></tr>
<tr><td>Физический интерфейс на B1, подключенный к MCE1</td><td>GE0/2</td><td>10.10.2.2/24</td><td>-</td></tr>
<tr><td>Физический интерфейс на MCE1, подключенный к A1</td><td>GE0/1</td><td>10.10.1.1/24</td><td>Таблица VRF для VPN a</td></tr>
</table>
</td></tr>
</table>

	Физический интерфейс на MCE1, подключенный к B1	GE0/2	10.10.2.1/24	Таблица VRF для VPN b
	Логический интерфейс на MCE1, подключенном к PE1	VLAN10	10.10.10.1/24	Таблица VRF для VPN a
	Логический интерфейс на MCE1, подключенном к PE1	VLAN20	10.10.20.1/24	Таблица VRF для VPN b
	Логический интерфейс на PE1, подключенном к MCE1	VLAN10	10.10.10.2/24	Таблица VRF для VPN a
	Логический интерфейс на PE1, подключенном к MCE1	VLAN20	10.10.20.2/24	Таблица VRF для VPN b

A1

```
A1(config)#interface GigabitEthernet 0/1
A1(config-if-GigabitEthernet 0/1)#no switchport port
A1(config-if-GigabitEthernet 0/1)#ip address 10.10.1.2 255.255.255.0
A1(config-if-GigabitEthernet 0/1)#exit
A1(config)#router rip
A1(config-router)#version 2
A1(config-router)#no auto-summary
A1(config-router)#network 10.10.1.0 0.0.0.255
```

B1

```
B1(config)#interface GigabitEthernet 0/2
B1(config-if-GigabitEthernet 0/1)#no switchport port
B1(config-if-GigabitEthernet 0/1)#ip address 10.10.2.2 255.255.255.0
B1(config-if-GigabitEthernet 0/1)#exit
B1(config)#router ospf 1
B1(config-router)#network 10.10.2.0 0.0.0.255 area 0
```

MCE1	#Создайте таблицу VRF для VPN a и таблицу VRF для VPN b и включите семейство адресов IPv4. MCE1(config)#vrf definition vpna MCE1(config-vrf)#address-family ipv4 MCE1(config-vrf-af)#exit MCE1(config-vrf)#exit MCE1(config)#vrf definition vpnb MCE1(config-vrf)#address-family ipv4 MCE1(config-vrf-af)#exit MCE1(config-vrf)#exit
	#Привязываем интерфейсы к таблицам VRF. MCE1(config)#interface GigabitEthernet 0/1 MCE1(config-if-GigabitEthernet 0/1)#no switchport port MCE1(config-if-GigabitEthernet 0/1)#vrf forwarding vpna MCE1(config-if-GigabitEthernet 0/1)#ip address 10.10.1.1 255.255.255.0 MCE1(config-if-GigabitEthernet 0/1)#exit MCE1(config)#interface GigabitEthernet 0/2 MCE1(config-if-GigabitEthernet 0/2)#no switchport port MCE1(config-if-GigabitEthernet 0/2)#vrf forwarding vpnb MCE1(config-if-GigabitEthernet 0/2)#ip address 10.10.2.1 255.255.255.0 MCE1(config-if-GigabitEthernet 0/2)#exit MCE1(config)#interface vlan 10 MCE1(config-if-VLAN 10)#vrf forwarding vpna MCE1(config-if-VLAN 10)#ip address 10.10.10.1 255.255.255.0 MCE1(config-if-VLAN 10)#exit MCE1(config)#interface vlan 20 MCE1(config-if-VLAN 20)#vrf forwarding vpnb MCE1(config-if-VLAN 20)#ip address 10.10.20.1 255.255.255.0 MCE1(config-if-VLAN 20)#exit
	#Настройте интерфейс, подключенный к PE1, в режиме Trunk. MCE1(config)#interface GigabitEthernet 0/3 MCE1(config-if-GigabitEthernet 0/3)#switchport mode trunk MCE1(config-if-GigabitEthernet 0/3)#exit

	#Настройте маршруты RIP и BGP в таблице VRF для VPN a и представьте маршруты в двух таблицах VRF друг другу. MCE1(config)#router rip MCE1(config-router)#address-family ipv4 vrf vpna MCE1(config-router-af)# version 2 MCE1(config-router-af)# no auto-summary MCE1(config-router-af)#network 10.10.1.0 0.0.0.255 MCE1(config-router-af)#redistribute bgp subnets MCE1(config-router-af)#exit MCE1(config)# router bgp 100 MCE1(config-router)#address-family ipv4 vrf vpna MCE1(config-router-af)#neighbor 10.10.10.2 remote-as 200 MCE1(config-router-af)#redistribute rip MCE1(config-router-af)#exit
	#Настройте маршруты OSPF и BGP в таблице VRF для VPN b и представьте маршруты в двух таблицах VRF друг другу. MCE1(config)#router ospf 1 vrf vpnb MCE1(config-router)#network 10.10.2.0 0.0.0.255 area 0 MCE1(config-router)#redistribute bgp subnets MCE1(config-router)#exit MCE1(config)# router bgp 100 MCE1(config-router)#address-family ipv4 vrf vpnb MCE1(config-router-af)#neighbor 10.10.20.2 remote-as 200 MCE1(config-router-af)#redistribute ospf 1 MCE1(config-router-af)#exit
PE1	#Создайте таблицу VRF для VPN a и таблицу VRF для VPN b и включите семейство адресов IPv4. PE1(config)#vrf definition vpna PE1(config-vrf)#address-family ipv4 PE1(config-vrf-af)#exit PE1(config-vrf)#exit PE1(config)#vrf definition vpnb PE1(config-vrf)#address-family ipv4 PE1(config-vrf-af)#exit PE1(config-vrf)#exit

	#Привязываем интерфейсы к таблицам VRF. PE1(config)#vlan 10 PE1(config-vlan)#exit PE1(config)#vlan 20 PE1(config-vlan)#exit PE1(config)#interface vlan 10 PE1(config-if-VLAN 10)#vrf forwarding vpna PE1(config-if-VLAN 10)#ip address 10.10.10.2 255.255.255.0 PE1(config-if-VLAN 10)#exit PE1(config)#interface vlan 20 PE1(config-if-VLAN 20)#vrf forwarding vpnb PE1(config-if-VLAN 20)#ip address 10.10.20.2 255.255.255.0 PE1(config-if-VLAN 20)#exit
	#Настройте интерфейс PE1, подключенного к MCE1, в режиме Trunk. PE1(config)#interface GigabitEthernet 0/3 PE1(config-if-GigabitEthernet 0/3)#switchport mode trunk PE1(config-if-GigabitEthernet 0/3)#exit
	#Настройте маршруты BGP в таблице VRF для VPN a. PE1(config)# router bgp 200 PE1(config-router)#address-family ipv4 vrf vpna PE1(config-router-af)#neighbor 10.10.10.1 remote-as 100 PE1(config-router-af)#exit
	#Настройте маршруты BGP в таблице VRF для VPN b. PE1(config)# router bgp 200 PE1(config-router)#address-family ipv4 vrf vpnb PE1(config-router-af)#neighbor 10.10.20.1 remote-as 100 PE1(config-router-af)#exit
Проверка	• На A1 запустите команду **show ip route**, чтобы отобразить маршруты в VPN a. • На B2 запустите команду **show ip route**, чтобы отобразить маршруты в VPN b. • На MCE1 запустите команду **show ip route vrf vpna**, чтобы отобразить маршруты в VPN a, и запустите команду **show ip route vrf vpnb**, чтобы отобразить маршруты в VPN b.

	• На PE1 запустите команду **show ip route vrf vpna**, чтобы отобразить маршруты в VPN a, и выполните команду **show ip route vrf vpnb**, чтобы отобразить маршруты в VPN b

11.4.2.7. Распространенные ошибки

- Многопротокольная таблица VRF настроена, но семейство адресов не включено.
- Интерфейс привязывается к таблице VRF после настройки IP-интерфейса интерфейса.
- Когда физический канал используется для пересылки пакетов из нескольких VPN, соответствующий физический интерфейс привязывается к таблице VRF.
- Маршруты VPN не представлены в BGP.

11.5. Мониторинг

11.5.1. Очистка

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

Описание	Команда
Очищает маршруты в указанной таблице VRF	**clear ip route vrf** *vrf-name*

11.5.2. Отображение

Описание	Команда
Отображает информацию таблицы VRF для одного протокола	**show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*]
Отображает информацию многопротокольной таблицы VRF	**show vrf** [**ipv4** | **ipv6** | **brief** | **detail**] [*vrf-name*]

11.5.3. Отладка

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

Описание	Команда
Отображает отладочную информацию во время процессов создания таблицы VRF и включения семейства адресов, и привязки интерфейс к таблице VRF	**debug vrf**
Выводит информацию об отладке работы VRF, связанной с интерфейсом	**debug vrf interface**

12. НАСТРОЙКА L3MAC

12.1. Обзор

MAC-адрес уровня 3 для пересылки можно настроить для устройства таким образом, чтобы пакеты, MAC-адреса назначения которых совпадают с настроенным MAC-адресом уровня 3, пересылались на уровень 3. В сценариях центров обработки данных этот MAC-адрес можно настроить в статических записях ARP соседей, чтобы маршрутизацию можно было запустить на любом соседнем устройстве.

12.2. Приложения

Приложение	Описание
Сценарий центра обработки данных	Маршрутизация уровня 3 может быть запущена на любом соседе без получения MAC-адреса уровня 3 устройства

12.2.1. Сценарий центра обработки данных

12.2.1.1. Сценарий

В качестве примера используется центр обработки данных, использующий топологию, показанную на Рисунке ниже:

- Глобальный MAC-адрес уровня 3 настроен на SW2 и SW3.
- Статическая запись ARP настроена на SW1.
- MAC-адрес в статической записи ARP, настроенной на SW1, является глобальным MAC-адресом уровня 3 его соседей, то есть SW2 и SW3.

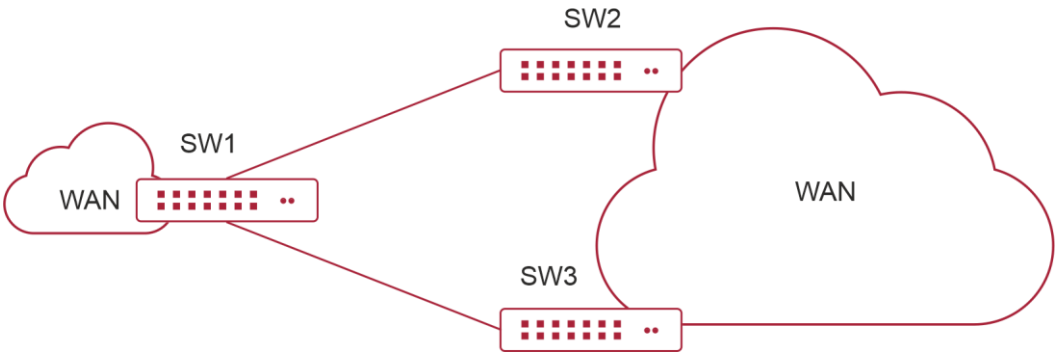


Рисунок 12-1.

12.2.1.2. Развертывание

- Пакеты от SW1 могут быть перенаправлены на уровне 3 через его соседей: SW2 и SW3.

12.3. Конфигурация

Конфигурация	Описание и команда	
Добавление MAC-адреса уровня 3	Обязательный	
	l3intf-mac-add	Добавляет MAC-адрес уровня 3

12.3.1. Добавление MAC-адреса уровня 3

12.3.1.1. Эффект конфигурации

Добавьте глобальный MAC-адрес уровня 3, чтобы маршрутизация уровня 3 могла запускаться при получении пакетов, соответствующих этому MAC-адресу уровня 3.

12.3.1.2. Примечания

Можно добавить до двух MAC-адресов уровня 3.

12.3.1.3. Шаги настройки

Добавление MAC-адреса уровня 3

Команда	**l3intf-mac-add** *mac*
Описание параметра	*mac*: указывает MAC-адрес уровня 3
Командный режим	Режим глобальной конфигурации

Удаление MAC-адреса уровня 3

Команда	**no l3intf-mac-add** *mac*
Описание параметра	*mac*: указывает MAC-адрес уровня 3
Командный режим	Режим глобальной конфигурации

12.3.1.4. Проверка

1. Запустите команду **show run**, чтобы проверить правильность текущей конфигурации.
2. Запустите команду **show l3intf-mac-add**, чтобы проверить правильность текущей конфигурации.

12.3.1.5. Пример конфигурации

Добавление MAC-адреса уровня 3

Сценарий:

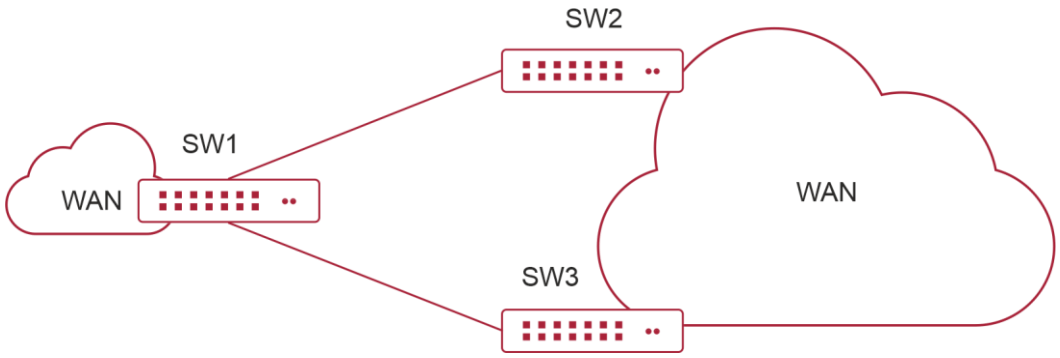


Рисунок 12-2.

Шаги настройки	Настройте статическую запись ARP на SW1 и глобальный MAC-адрес уровня 3 на SW2 и SW3. Другие конфигурации опущены
SW2	SW2# configure terminal SW2#(config)#l3intf-mac-add 0000.0001.2233
SW3	SW3# configure terminal SW3#(config)#l3intf-mac-add 0000.0001.2233
SW1	SW1# configure terminal SW1(config)# arp 192.168.22.20 0000.0001.2233 arpa
Проверка	Запустите команду **show**, чтобы отобразить глобальный MAC-адрес, настроенный на SW2 и SW3. Прокачайте трафик и убедитесь, что пакеты от SW1 пересылаются на уровне 3 независимо от того, что следующий hop SW1 является SW2 или SW3
SW2	SW2(config)#show l3intf-mac-add l3intf mac address: 0000.0001.2235
SW3	SW3(config)#show l3intf-mac-add l3intf mac address: 0000.0001.2235

12.4. Мониторинг

12.4.1. Отображение

Описание	Команда
Отображает настроенный глобальный MAC-адрес уровня 3 устройства	**show l3intf-mac-add**

13. НАСТРОЙКА ЗАПРОСА МОЩНОСТИ ОБОРУДОВАНИЯ

13.1. Обзор

Запрос мощности оборудования обеспечивает функцию запроса мощности и условий использования оборудования базы пересылочной информации (FIB).

13.2. Функции

13.2.1. Базовые определения

Аппаратные ресурсы маршрута подразделяются на ресурсы маршрута IPv4 и ресурсы маршрута IPv6 по протоколу, а также ресурсы маршрута хоста и ресурсы сетевого маршрута по префиксу маршрута.

Распределение ресурсов маршрута зависит от типа аппаратного обеспечения чипа.

- Серия QSW-7600

Ресурсы маршрутов хоста и ресурсы сетевых маршрутов управляются отдельно, и их пропускная способность фиксирована. Маршруты хоста IPv4 и IPv6 совместно используют ресурсы маршрута хоста, а сетевые маршруты IPv4 и IPv6 совместно используют ресурсы сетевого маршрута. Один маршрут IPv6 занимает в два раза больше ресурсов одного маршрута IPv4. Например, если общая емкость маршрутов хоста составляет 200 000, то поддерживаются 200 000 маршрутов хоста IPv4, 100 000 маршрутов хоста IPv6 или 100 000 маршрутов хоста IPv4 и 50 000 маршрутов хоста IPv6.

Сетевые маршруты IPv6 включают сетевые маршруты с длиной префикса 0–64 и сетевые маршруты с длиной префикса 65–127. Два типа ресурсов сетевых маршрутов управляются отдельно, и их пропускная способность фиксирована.

ПРИМЕЧАНИЕ: когда во время настройки маршрутов хоста возникает конфликт хэша, ресурсы сетевых маршрутов заняты, и фактически используемая мощность сетевого маршрута может быть больше, чем отображаемая используемая мощность.

13.3. Мониторинг

13.3.1. Отображение

Описание	Команда
Отображает емкость и условия использования оборудования FIB коммутатора	**show route-res usage**

ПРИМЕЧАНИЕ: приведенная выше команда мониторинга также применима к устройствам chassis-type и box-type, автономным устройствам и VSU.

14. ОБЩАЯ ИНФОРМАЦИЯ

14.1. 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.

14.2. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться разделом технической поддержки пользователей QTECH на нашем сайте www.qtech.ru/support/.

Телефон Технической поддержки +7 (495) 269-08-81

Центральный офис +7 (495) 477-81-18

14.3. Электронная версия документа

Дата публикации 28.04.2025

https://files.qtech.ru/upload/switchers/QSW-7600/QSW-7600_ip_routing_config_guide.pdf