IR12000 系列智能路由器
配置指南

浪潮思科网络科技有限公司（以下简称“浪潮思科”）为客户提供全方位的技术支持和服务。直接向浪潮思科购买产品的用户，如果在使用过程中有任何问题，可与浪潮思科各地办事处或用户服务中心联系，也可直接与公司总部联系。

读者如有任何关于浪潮思科产品的问题，或者有意进一步了解公司其他相关产品，可通过下列方式与我们联系：

公司网址：http://www.inspur.com/

技术支持热线：400-691-1766

技术支持邮箱：inspur_network@inspur.com

技术文档邮箱：inspur_network@inspur.com

客户投诉热线：400-691-1766

公司总部地址：山东省济南市历下区浪潮路 1036 号

邮政编码：250000

声明

Copyright ©2018

浪潮思科网络科技有限公司

版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

inspur 浪潮 是浪潮思科网络科技有限公司的注册商标。

对于本手册中出现的其它商标，由各自的所有人拥有。

■由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

前言

手册说明

本书介绍IR12000系列产品支持的路由、组播、MPLS、VPN、可靠性等功能的配置过程和配置实例。

读者对象

本书适用于下列人员阅读：

·规划工程师

·调测工程师

·维护工程师

内容介绍

本书的章节名及其概要如下。

章名	概要
第1章 系统管理	介绍了IR12000系列产品与系统管理相关的配置命令与配置实例。
第2章 接口配置	介绍了IR12000系列产品与接口配置相关的配置命令与配置实例。
第3章 IPv4业务	介绍了IR12000系列产品与IPv4业务相关的配置命令与配置实例。
第4章 IPv4路由	介绍了IR12000系列产品与IPv4路由相关的配置命令与配置实例。
第5章 IPv4组播	介绍了IR12000系列产品与IPv4组播相关的配置命令与配置实例。
第6章 MPLS	介绍了IR12000系列产品与MPLS相关的配置命令与配置实例。
第7章 VPN	介绍了IR12000系列产品与VPN相关的配置命令与配置实例。
第8章 QoS	介绍了IR12000系列产品与QoS相关的配置命令与配置实例。
第9章 安全	介绍了IR12000系列产品与安全相关的配置命令与配置实例。
第10章 可靠性	介绍了IR12000系列产品与可靠性相关的配置命令与配置实例。
第11章 策略模板	介绍了IR12000系列产品与策略模板相关的配置命令与配置实例。
第12章 IPv6	介绍了IR12000系列产品与IPv6相关的配置命令与配置实例。
第13章 NAT	介绍了IR12000系列产品与NAT相关的配置命令与配置实例。
第14章 二层交换和WLAN	介绍了IR12000系列产品与二层交换和WLAN相关的配置命令与配置实例。

本书约定

1.安全符号约定

在本书中可能出现下列安全符号，所代表的含义如下。

安全符号	意义
NOTE 说明	表示该内容是正文的附加信息

2.命令格式约定

在本书中可能出现下列命令符号，所代表的含义如下。

命令符号	意义
/* */	注释，不需要输入的内容
粗体字	表示命令或关键字
<*斜体字*>	表示需设置的参数
|	用于分隔若干选项，表示二选一或多选一
[]	方括号中的关键字或参数为可选项
{}	大括号中的关键字或参数为必选项
{**x** | **y** | **z**}	表示必须选择x，y，z中的一个
[**x**{**y** | **z**}]	方括号中的内容是可选的，但如果选择了方括号中的内容，就必须选择大括号中y，z中的一个
*(x)	表示内容x可以循环
{[**x**] ,[**y**] ,[**z**]}	表示多选多参数，x、y、z三个参数可以选择一个，也可以选择 多个，选择顺序任意

目录

前言 iii
目录 1
1 系统管理 18
1.1 设备连接管理 18
1.1.1 配置 Console 口连接 18
1.1.2 配置 Telnet 连接 19
1.1.3 配置 SSH 连接 22
1.1.4 配置设备作为 FTP 服务器 26
1.1.5 配置设备作为 FTP 客户端 28
1.1.6 配置 TFTP 连接 30
1.1.7 配置设备作为 SFTP 服务器 32
1.1.8 配置设备作为 SFTP 客户端 33
1.2 缺省配置 34
1.2.1 缺省用户名和密码配置 34
1.2.2 管理口缺省 IP 配置 37
1.2.3 设备恢复出厂配置 38
1.3 文件系统管理 38
1.3.1 配置文件系统管理 38
1.3.2 文件系统基本配置实例 40
1.3.3 将配置文件备份到 USB 的配置实例 40
1.4 MIM 41
1.4.1 配置 MIM 41
1.4.2 MIM 配置实例 42
1.5 用户管理 43
1.5.1 配置用户管理 43
1.5.2 本地认证授权用户配置实例 47
1.5.3 RADIUS-LOCAL 认证授权用户配置实例 48
1.5.4 TACACS+认证授权用户配置实例 49
1.5.5 密码恢复配置实例 50
1.5.6 OAM 安全管理配置实例 52
1.5.7 密码有效期配置实例 53
1.5.8 首次登录修改密码配置实例 55
1.5.9 用户权限配置实例 56
1.6 命令权限分级 58
1.6.1 配置命令权限 58
1.6.2 命令权限分级配置实例 59
1.7 SNMP 63
1.7.1 配置 SNMP 63
1.7.2 配置 SNMP 防暴力攻击 67

1.7.3 SNMP 配置实例 68
1.7.4 SNMP 防暴力攻击配置实例 71
1.8 告警 72
1.8.1 配置告警 72
1.8.2 告警配置实例 76
1.9 SYSLOG 78
1.9.1 配置 SYSLOG 79
1.9.2 SYSLOG 配置实例 80
1.10 时钟与时钟同步 81
1.10.1 配置 NTP 81
1.10.2 IR12000 作为 NTP 客户端配置实例 83
1.10.3 IR12000 作为 NTP 服务器端配置实例 84
1.11 性能统计 85
1.11.1 配置性能统计 85
1.11.2 性能统计配置实例 86
1.12 NetFlow 87
1.12.1 配置 NetFlow 87
1.12.2 NetFlow V5 版本采集配置实例 92
1.12.3 NetFlow V8 版本采集配置实例 94
1.12.4 NetFlow V9 版本采集配置实例 95
1.12.5 NetFlow IPFIX 版本采集配置实例 97
1.12.6 NetFlow 采样信息支持 IPv6 配置实例 99
1.13 SQA 100
1.13.1 配置 SQA 100
1.13.2 ICMP 类型的 SQA 配置实例 102
1.13.3 FTP 类型的 SQA 配置实例 104
1.13.4 TCP 类型的 SQA 配置实例 105
1.13.5 UDP 类型的 SQA 配置实例 106
1.13.6 DNS 类型的 SQA 配置实例 107
1.14 网络层检测 108
1.14.1 配置 ICMP 快速响应 108
1.14.2 配置 IP 源路由选项处理 110
1.14.3 配置 ICMP 不可达报文有效 112
1.14.4 配置接口发送报文不可达有效 113
1.14.5 配置 IP Ping 114
1.14.6 配置 IP Trace 116
1.14.7 配置 LSP Ping 118
1.14.8 配置 LSP Trace 123
1.14.9 配置组播 Ping 126
1.14.10 配置组播 Trace 128
1.14.11 配置 IP 调试命令 129
1.15 LLDP 129
1.15.1 配置 LLDP 129
1.15.2 LLDP 邻居配置实例 131
1.15.3 LLDP 常用属性配置实例 132
2 接口配置 134

2.1 接口基础.....134
2.1.1 配置 IP 地址.....134
2.1.2 配置 IP MTU.....135
2.1.3 配置接口 MTU.....135
2.1.4 启动或关闭接口.....136
2.1.5 配置接口别名和描述信息.....137
2.1.6 配置接口 VRF 绑定.....137
2.1.7 接口信息查看命令.....138
2.1.8 IP 主地址配置实例.....139
2.1.9 IP 辅地址配置实例.....140
2.1.10 IP MTU 配置实例.....142
2.1.11 接口 MTU 配置实例.....143
2.2 以太网接口.....144
2.2.1 配置以太网接口.....144
2.2.2 以太网接口配置实例.....145
2.3 VLAN.....146
2.3.1 配置 VLAN 子接口.....147
2.3.2 配置 VLAN Range 子接口.....147
2.3.3 配置 VLAN TPID.....148
2.3.4 VLAN 子接口配置实例.....148
2.3.5 VLAN Range 子接口配置实例.....150
2.3.6 VLAN TPID 配置实例.....152
2.4 QinQ.....153
2.4.1 配置 QinQ 子接口.....153
2.4.2 配置 QinQ Range 子接口.....154
2.4.3 QinQ 子接口配置实例.....155
2.4.4 QinQ Range 子接口配置实例.....156
2.5 SuperVLAN.....158
2.5.1 配置 SuperVLAN.....158
2.5.2 SuperVLAN 综合配置实例.....159
2.5.3 VLAN 绑定 IP 配置实例.....161
2.5.4 MAC 绑定 IP 配置实例.....162
2.6 SmartGroup.....163
2.6.1 配置 SmartGroup.....164
2.6.2 SmartGroup 802.3ad 模式配置实例.....166
2.6.3 SmartGroup On 模式配置实例.....169
2.7 POS 接口.....170
2.7.1 配置 POS 接口.....171
2.7.2 POS 接口基本配置实例.....173
2.7.3 POS 口延时 Down 配置实例.....174
2.8 CPOS 接口.....175
2.8.1 配置 CPOS 接口属性.....175
2.8.2 配置 CPOS 接口段属性.....176
2.8.3 配置 CPOS 低阶通道.....177
2.8.4 配置 CPOS 高阶通道.....178
2.8.5 验证 CPOS 配置.....179

2.8.6 CPOS 配置实例 180
2.9 E1 接口 181
2.9.1 配置 E1 接口 182
2.9.2 通道化 E1 接口配置实例 183
2.9.3 非通道化 E1 接口配置实例 184
2.10 PPP 185
2.10.1 配置 PPP 185
2.10.2 PPP 配置实例 187
2.11 FR 189
2.11.1 配置 FR 189
2.11.2 FR 物理接口配置实例 191
2.11.3 FR 子链路配置实例 192
2.12 HDLC 194
2.12.1 配置 HDLC 194
2.12.2 HDLC 基本配置实例 195
2.12.3 POSGROUP 配置实例 196
2.13 Multilink 198
2.13.1 配置 Multilink 198
2.13.2 Multilink 配置实例 200
2.14 端口切换 202
2.14.1 配置端口切换 202
2.14.2 端口模式切换配置实例 203
2.15 端口抑制 203
2.15.1 配置端口抑制 204
2.15.2 端口抑制配置实例 205
2.16 接口关联检测 206
2.16.1 配置接口关联检测 206
2.17 其它逻辑接口 207
2.17.1 配置 Loopback 接口 207
2.17.2 配置 NULL 接口 208
2.17.3 配置 ULEI 接口 208
2.17.4 配置 Tunnel 209
2.17.5 用 Loopback 接口构造黑洞路由配置实例 210
2.17.6 将 Loopback 接口作为 Router-ID 配置实例 211
2.17.7 NULL 接口配置实例 211
2.17.8 Tunnel 配置实例 212
3 IPv4 业务 214
3.1 ARP 214
3.1.1 配置 ARP 214
3.1.2 永久 ARP 配置实例 218
3.1.3 ARP 常规属性配置实例 219
3.1.4 ARP 代理配置实例 220
3.1.5 ARP 源过滤配置实例 222
3.1.6 ARP 抑制配置实例 223
3.2 DHCP 223
3.2.1 配置 DHCP Server 224

3.2.2 配置 DHCP Relay 226
3.2.3 配置 DHCP Proxy 228
3.2.4 配置 DHCP Client 231
3.2.5 配置限制 Relay 发包 232
3.2.6 配置 Option82 改写功能 232
3.2.7 DHCP Server 配置实例 233
3.2.8 DHCP Relay 配置实例 235
3.2.9 DHCP Proxy 配置实例 237
3.2.10 DHCP Client 配置实例 239
3.3 TCPv4 与 UDPv4 241
3.3.1 配置 TCPv4 241
3.3.2 维护 UDPv4 243
3.4 DNS 243
3.4.1 配置 DNS 244
3.4.2 DNS 配置实例 245
3.5 反向 TELNET/TCP 和串口终端接入 246
3.5.1 配置反向 TELNET/TCP 和串口终端接入 247
3.5.2 反向 TELNET 配置实例 250
3.5.3 反向 TCP 配置实例 251
3.5.4 串口终端接入配置实例 253
3.6 DDNS Client 254
3.6.1 配置 DDNS Client 254
3.6.2 DDNS Server 为 Oray 的 DDNS Client 配置实例 256
3.6.3 DDNS Server 为 3322 的 DDNS Client 配置实例 257
3.7 UDP Helper 258
3.7.1 配置 UDP Helper 258
3.7.2 UDP Helper 配置实例 260
4 IPv4 路由 262
4.1 路由简介 262
4.2 静态路由 262
4.2.1 配置静态路由 262
4.2.2 下一跳直连的静态路由配置实例 264
4.2.3 下一跳非直连的静态路由配置实例 266
4.2.4 静态路由汇总配置实例 267
4.2.5 默认路由配置实例 268
4.2.6 静态路由负荷分担配置实例 270
4.2.7 公网静态路由 FRR 配置实例 271
4.2.8 VRF 的静态路由 FRR 配置实例 273
4.2.9 静态路由 BFD 配置实例 274
4.2.10 Loopback 提供静态多跳 BFD 的 local 地址配置实例 276
4.3 RIP 277
4.3.1 配置 RIP 基本功能 277
4.3.2 配置 RIP 增强功能 279
4.3.3 配置 RIP 版本 281
4.3.4 配置 RIP 路由负荷分担 282
4.3.5 验证及维护 RIP 283

4.3.6 RIP 基本配置实例 284
4.3.7 RIP 路由汇总配置实例 286
4.3.8 RIP 路由负荷分担配置实例 287
4.3.9 RIP BFD 配置实例 289
4.4 OSPF 291
4.4.1 配置 OSPF 基本功能 292
4.4.2 配置 OSPF 接口属性 295
4.4.3 配置 OSPF 认证 297
4.4.4 配置 OSPF STUB 区域 300
4.4.5 配置 NSSA 区域 302
4.4.6 配置区域间路由聚合 304
4.4.7 配置路由重分布时的路由聚合 308
4.4.8 配置重分布其他路由协议 310
4.4.9 配置 OSPF 缺省路由 312
4.4.10 配置 OSPF 虚链路 313
4.4.11 配置 Sham-link 315
4.4.12 配置 max-metric 316
4.4.13 配置 OSPF 路由负荷分担 317
4.4.14 配置 OSPF FRR 319
4.4.15 配置 OSPF Graceful Restart 320
4.4.16 配置 OSPF 路由过滤 321
4.4.17 验证及维护 OSPF 322
4.4.18 OSPF 建链功能配置实例 324
4.4.19 OSPF NSSA 区域配置实例 326
4.4.20 OSPF 多实例配置实例 328
4.4.21 OSPF FRR 配置实例 331
4.4.22 OSPF 区域间路由聚合配置实例 332
4.4.23 OSPF 路由负荷分担配置实例 334
4.4.24 OSPF Graceful Restart 配置实例 335
4.4.25 OSPF BFD 配置实例 337
4.5 IS-IS 338
4.5.1 配置 IS-IS 基本信息 339
4.5.2 配置 IS-IS 全局参数 340
4.5.3 配置 IS-IS 接口参数 341
4.5.4 配置 IS-IS 认证 343
4.5.5 配置 IS-IS Hostname 344
4.5.6 配置 IS-IS mesh-group 344
4.5.7 配置 IS-IS 重分发 345
4.5.8 配置 IS-IS 负荷分担 346
4.5.9 配置 IS-IS 流量工程 347
4.5.10 配置 IS-IS FRR 347
4.5.11 配置 IS-IS Graceful Restart 348
4.5.12 配置 IS-IS LSP 报文 Buffer 大小 349
4.5.13 验证及维护 IS-IS 350
4.5.14 单区域 IS-IS 配置实例 351
4.5.15 多区域 IS-IS 配置实例 354

4.5.16 IS-IS 多实例配置实例.....359
4.5.17 IS-IS FRR 配置实例.....360
4.5.18 IS-IS 重分发配置实例.....362
4.5.19 IS-IS 认证配置实例.....363
4.5.20 IS-IS 路由负荷分担配置实例.....364
4.5.21 IS-IS Graceful Restart 配置实例.....366
4.5.22 IS-IS BFD 配置实例.....367
4.6 BGP.....369
4.6.1 建立 BGP 邻居.....369
4.6.2 配置 BGP 路由通告.....378
4.6.3 配置 BGP 可靠性.....385
4.6.4 配置 BGP 属性和路由过滤.....388
4.6.5 配置大型网络中 BGP 的应用功能.....405
4.6.6 配置 BGP 动态组.....417
4.6.7 验证及维护 BGP.....419
4.6.8 BGP 综合配置实例一（Loopback 接口创建 BGP）.....420
4.6.9 BGP 综合配置实例二（物理接口创建 BGP）.....427
4.6.10 BGP FRR 配置实例.....430
4.6.11 BGP 路由反射器配置实例.....431
4.6.12 BGP 与 VRRP 联动配置实例.....432
4.6.13 BGP 路由负荷分担配置实例.....434
4.6.14 BGP Graceful Restart 配置实例.....436
4.6.15 BGP 单跳 BFD 配置实例.....437
4.6.16 BGP 多跳 BFD 配置实例.....438
4.6.17 BGP 动态组配置实例.....440
5 IPv4 组播.....444
5.1 组播.....444
5.1.1 配置组播.....444
5.1.2 配置静态组播.....448
5.1.3 静态组播配置实例.....449
5.2 IGMP.....450
5.2.1 配置 IGMP.....450
5.2.2 IGMP 查询路由器选举配置实例.....454
5.2.3 IGMP 动态组、静态组加入配置实例.....455
5.2.4 IGMP 对所有组的快速离开配置实例.....457
5.2.5 IGMP 对指定组的快速离开配置实例.....459
5.2.6 组播接口限制配置实例.....461
5.2.7 IP-Source-Check 功能配置实例.....462
5.3 PIM-DM.....463
5.3.1 配置 PIM-DM.....463
5.3.2 PIM-DM 邻居建立配置实例.....464
5.3.3 PIM-DM 组播负荷分担配置实例.....465
5.4 PIM-SM.....468
5.4.1 配置 PIM-SM.....468
5.4.2 PIM-SM 转发组播流（使用动态 RP）配置实例.....470
5.4.3 PIM-SM 转发组播流（使用静态 RP）配置实例.....472

5.4.4 非法组播源控制配置实例 475
5.4.5 anycast-rp 配置实例 478
5.4.6 RPT-SPT 切换配置实例 480
5.4.7 PIM-SM 与 PIM-DM 混合运行配置实例 482
5.4.8 PIM-SM 组播负荷分担配置实例 485
5.4.9 PIM-SM BFD 配置实例 487
5.5 PIM-SSM 490
5.5.1 配置 PIM-SSM 491
5.5.2 PIM-SSM 配置实例 491
5.5.3 SSM-Mapping 配置实例 493
5.6 组播负荷分担 494
5.6.1 配置组播负荷分担 494
5.6.2 组播负荷分担配置实例 495
5.7 MSDP 495
5.7.1 配置 MSDP 495
5.7.2 MSDP 基本配置实例 497
5.7.3 MSDP 实现 anycast-rp 配置实例 500
6 MPLS 503
6.1 MPLS 简介 503
6.2 MPLS 基础配置 503
6.2.1 配置 MPLS 503
6.2.2 基本的 LDP 邻居会话配置实例 511
6.2.3 LDP 远端会话配置实例 513
6.2.4 分配标签策略配置实例 515
6.2.5 LDP 多实例配置实例 517
6.2.6 LDP FRR 配置实例 520
6.2.7 LDP Graceful Restart 配置实例 525
6.2.8 LDP 标签负荷分担配置实例 530
6.2.9 LDP BFD 配置实例 533
6.2.10 PEER BFD 配置实例 536
6.2.11 GTSM 配置实例 538
6.2.12 IGP 同步配置实例（OSPF） 541
6.2.13 IGP 同步配置实例（IS-IS） 543
6.2.14 报文过滤配置实例 547
6.2.15 Label-distribution 配置实例 549
6.2.16 Label-retention 配置实例 551
6.2.17 Label-advertise 配置实例 553
6.2.18 Label-request 配置实例 556
6.2.19 Lsp-control 配置实例 558
6.2.20 Longest-match 配置实例 561
6.3 MPLS TE 配置 564
6.3.1 RSVP 564
6.3.2 TE-FRR 578
6.3.3 MPLS TE 端到端路径保护 591
6.3.4 MPLS TE 跨 AS 域 596
6.3.5 TE 认证 608

6.3.6 TE 消息确认与重传 612
6.3.7 TE 摘要刷新 615
6.3.8 RESV CONFIRM 618
6.3.9 GR 621
6.3.10 FRR HELLO 625
6.3.11 FRR 提升 630
6.3.12 TE 的共路径双向隧道 637
6.3.13 2.3.13TE 隧道 FA 641
6.3.14 TE 隧道 AR 644
6.3.15 TE Metric 648
6.3.16 TE SRLG 651
6.3.17 TE 隧道重优化 655
7 VPN 659
7.1 VPN 简介 659
7.2 MPLS L2VPN 660
7.2.1 VPLS 660
7.2.2 配置 VPLS 660
7.2.3 VPWS 673
7.2.4 MSPW 681
7.2.5 VLSS 688
7.2.6 MC-ELAM 690
7.2.7 L2VPN 与 L3VPN 桥接 696
7.2.8 L2VPN FRR 702
7.2.9 VPLS 跨域 Option C 709
7.3 MPLS L3VPN 714
7.3.1 MPLS L3VPN 基本功能 714
7.3.2 MPLS L3VPN 路由聚合 739
7.3.3 L3VPN 路由限制和告警 744
7.3.4 Global 静态路由 749
7.3.5 L3VPN FRR 753
7.3.6 MPLS L3VPN 负荷分担 762
7.3.7 MPLS L3VPN 跨域 773
7.3.8 MPLS L3VPN 每 VPN 每标签 792
7.3.9 MPLS L3VPN GR 795
7.3.10 MPLS L3VPN HoPE 801
7.3.11 L3VPN 隧道策略选择 817
7.4 VPN 组播 823
7.4.1 配置 VPN 组播 823
7.4.2 VPN 组播配置实例 826
7.4.3 标签方式 MVPN 配置实例 832
7.4.4 MD 方式 MVPN 配置实例（GRE 方案） 841
7.4.5 MVPN 跨域配置实例 846
7.5 GRE 隧道 854
7.5.1 配置 GRE over IPv4 隧道 854
7.5.2 配置 GRE over IPv6 隧道 855
7.5.3 IPv4 GRE 配置实例 857
7.5.4 GRE 6over4 配置实例 859

7.5.5 IPv6 GRE 配置实例 861
7.6 IPSec VPN 864
7.6.1 配置感兴趣流 864
7.6.2 配置 IKE 阶段 1 864
7.6.3 配置 IKE 阶段 2 867
7.6.4 配置隧道和传输模式 869
7.6.5 验证和维护 IPSec 870
7.6.6 IPSec 基本组网配置实例 872
7.6.7 IPSec 手工 SPI 站点到站点 VPN 配置实例 874
7.6.8 IPSec IKE 协商站点到站点 VPN 配置实例 876
7.6.9 GRE OVER IPSec VPN 配置实例 879
7.6.10 IPSec 动态 NAT 穿越配置实例 882
7.6.11 IPSec 数字证书认证协商配置实例 886
7.6.12 IKEv2 配置实例 889
7.7 IPSec VPN 远程接入 893
7.7.1 配置 IPSec Pool 893
7.7.2 配置远程用户组 894
7.7.3 配置远程接入隧道 895
7.7.4 验证和维护远程接入 895
7.7.5 IPSec VPN 远程接入配置实例 896
7.8 DVMPN 898
7.8.1 配置 MGRE 899
7.8.2 配置 NHRP 899
7.8.3 配置 IPSec 900
7.8.4 验证和维护 DMVPN 900
7.8.5 DMVPN 配置实例 901
7.9 VPDN 908
7.9.1 配置 VPDN 908
7.9.2 LAC 配置实例 912
7.9.3 LNS 配置实例 916
7.10 GET VPN 920
7.10.1 配置 GDOI 组 921
7.10.2 GET VPN 配置实例 922
8 QoS 926
8.1 QoS 简介 926
8.2 CAR 926
8.2.1 配置 CAR 927
8.2.2 CAR 配置实例 928
8.3 流分类 929
8.3.1 配置流分类 929
8.3.2 空规则的流分类配置实例 931
8.3.3 基于 EXP 的流分类配置实例 932
8.3.4 基于 MAC 地址的流分类配置实例 933
8.3.5 基于 IPv4 ACL 的流分类配置实例 934
8.3.6 匹配方式为 match-any 的流分类配置实例 935
8.4 流行为 936

8.4.1 配置流行为 936
8.4.2 报文标记配置实例 938
8.4.3 流量监管配置实例 940
8.4.4 PQ 队列调度配置实例 941
8.4.5 WFQ 调度配置实例 942
8.4.6 CBWFQ 调度配置实例 944
8.4.7 WRED 配置实例 946
8.4.8 流量整形配置实例 947
8.5 H-QoS 948
8.5.1 配置 H-QoS 948
8.5.2 H-QoS 配置实例 949
8.6 优先级继承 950
8.6.1 配置优先级继承 951
8.6.2 802.1P 字段继承配置实例 952
8.6.3 Pipe 模式配置实例 953
8.7 QPPB 957
8.7.1 配置 QPPB 958
8.7.2 QPPB 配置实例 958
9 安全 962
9.1 控制平面安全 962
9.1.1 配置接口上送限速 962
9.1.2 配置路由安全 971
9.1.3 配置 ARP 防攻击 973
9.1.4 配置 IGMP 防攻击 975
9.1.5 控制平面安全基本功能配置实例 976
9.1.6 基于流的控制平面安全功能配置实例 978
9.1.7 黑白名单功能配置实例 979
9.2 URPF 981
9.2.1 配置 URPF 981
9.2.2 严格 URPF 配置实例 982
9.2.3 松散 URPF 配置实例 983
9.3 RADIUS 985
9.3.1 配置 RADIUS 985
9.3.2 RADIUS 配置实例 992
9.4 TACACS+ 994
9.4.1 配置 TACACS+ 994
9.4.2 TACACS+认证授权配置实例 996
9.4.3 TACACS+记账配置实例 997
9.5 镜像 998
9.5.1 配置镜像 999
9.5.2 本地端口镜像配置实例 999
9.5.3 本地流镜像配置实例 1000
9.6 防火墙 1001
9.6.1 配置 IP 源防攻击功能 1002
9.6.2 配置防火墙区域内策略 1002
9.6.3 配置防火墙区域间策略 1006

9.6.4 配置 TCP 拦截功能.....1009
9.6.5 基于协议和端口号设置老化时间.....1010
9.6.6 IP 源防攻击配置实例.....1011
9.6.7 黑名单配置实例.....1012
9.6.8 白名单配置实例.....1013
9.6.9 防攻击配置实例.....1014
9.6.10 0 虚拟分片重组功能配置实例.....1015
9.6.11 区域间策略配置实例.....1016
9.6.12 过滤列表配置实例.....1017
9.6.13 TCP 拦截功能配置实例.....1019
9.6.14 基于协议和端口号的会话老化时间配置实例.....1020
9.7 DPI.....1021
9.7.1 配置 DPI.....1021
9.7.2 DPI 配置实例.....1023
9.8 SSL 和 PKI.....1025
9.8.1 配置 SSL 和 PKI.....1025
9.8.2 SSL 和 PKI 配置实例.....1027
10 可靠性.....1029
10.1 可靠性简介.....1029
10.2 业务可靠性管理.....1029
10.2.1 配置业务可靠性管理.....1029
10.2.2 EFM 联动 VRRP 配置实例.....1031
10.2.3 CFM 联动 VRRP 配置实例.....1033
10.3 VRRP.....1036
10.3.1 配置 VRRP.....1036
10.3.2 基本 VRRP 配置实例.....1039
10.3.3 对称 VRRP 配置实例.....1040
10.3.4 VRRP 心跳线配置实例.....1042
10.3.5 VRRP Track 配置实例.....1044
10.4 Ping Detect.....1046
10.4.1 配置 Ping Detect.....1047
10.4.2 Ping Detect 基本配置实例.....1048
10.4.3 直连路由与 Track Ping 联动配置实例.....1049
10.5 EFM.....1052
10.5.1 配置 EFM.....1052
10.5.2 EFM 连接建立配置实例.....1055
10.5.3 EFM 远端环回配置实例.....1058
10.6 CFM.....1060
10.6.1 配置 CFM.....1060
10.6.2 CFM 快速连续性检测配置实例.....1063
10.6.3 跨越 L2VPN 连通性检测配置实例.....1067
10.7 BFD.....1069
10.7.1 配置 BFD.....1069
10.7.2 PIM BFD 配置实例.....1074
10.7.3 静态单跳 BFD 配置实例.....1077
10.7.4 静态多跳 BFD 配置实例.....1079

10.7.5 单臂 ECHO 配置实例 1082
10.8 主备倒换 1083
10.8.1 配置主备倒换 1084
10.8.2 主备倒换配置实例 1085
11 策略模板 1088
11.1.1 策略模板简介 1088
11.2 AAA 1088
11.2.1 配置 AAA 1089
11.2.2 AAA 配置实例 1091
11.3 Time-range 1093
11.3.1 配置 Time-range 1093
11.3.2 Time-range 列表配置实例 1094
11.3.3 ACL 调用 time-range 配置实例 1097
11.3.4 SQA 调用 time-range 配置实例 1099
11.4 ACL 1100
11.4.1 配置 ACL 1101
11.4.2 配置 Link ACL 1104
11.4.3 ACL 配置实例 1105
11.4.4 Link ACL 配置实例 1107
11.5 Prefix-list 1109
11.5.1 配置 prefix-list 1109
11.5.2 Prefix-list 基本配置实例 1111
11.5.3 组播调用 prefix-list 配置实例 1111
11.5.4 OSPF 调用 prefix-list 配置实例 1113
11.5.5 BGP 调用 prefix-list 配置实例 1115
11.5.6 Route-map 调用 prefix-list 配置实例 1119
11.6 Route-Map 1120
11.6.1 配置路由策略 1120
11.6.2 配置策略路由 1126
11.6.3 RIP 重分配路由策略配置实例 1127
11.6.4 IS-IS 路由策略配置实例 1129
11.6.5 OSPF 路由策略配置实例 1132
11.6.6 BGP 路由策略配置实例 1134
11.6.7 VRF 路由策略配置实例 1137
11.6.8 本地不同接口接入的策略路由配置实例 1142
11.6.9 本地同一个接口接入的策略路由配置实例 1143
11.6.10 远端 VRF 策略路由配置实例 1145
11.7 EEM 1149
11.7.1 配置 EEM 1149
11.7.2 NONE 类型 EEM 配置实例 1150
12 IPv6 1153
12.1 IPv6 基础 1153
12.1.1 配置 IPv6 1153
12.1.2 配置 IPv6 地址 1156
12.1.3 IPv6 地址配置实例 1157
12.2 NDP 1158

12.2.1 配置 NDP 1158
12.2.2 NDP 配置实例 1161
12.3 IPv6 静态路由 1162
12.3.1 配置 IPv6 静态路由 1162
12.3.2 下一跳直连的 IPv6 静态路由配置实例 1163
12.3.3 下一跳非直连的 IPv6 静态路由配置实例 1165
12.3.4 IPv6 默认路由配置实例 1166
12.3.5 IPv6 静态路由公网 FRR 配置实例 1167
12.3.6 IPv6 静态路由私网 FRR 配置实例 1169
12.3.7 IPv6 静态路由负荷分担配置实例 1170
12.3.8 IPv6 静态路由 BFD 源端下一跳配置实例 1172
12.4 RIPng 1174
12.4.1 配置 RIPng 1174
12.4.2 RIPng 基本配置实例 1176
12.4.3 RIPng 路由汇总配置实例 1180
12.5 OSPFv3 1181
12.5.1 配置 OSPFv3 1181
12.5.2 OSPFv3 基本配置实例 1186
12.5.3 OSPFv3 重分发配置实例 1188
12.5.4 OSPFv3 路由负荷分担配置实例 1192
12.6 IS-ISv6 1194
12.6.1 配置 IS-ISv6 1194
12.6.2 单区域 IS-ISv6 配置实例 1199
12.6.3 多区域 IS-ISv6 配置实例 1203
12.7 BGP4+ 1209
12.7.1 配置 BGP4+ 1209
12.7.2 BGP4+路由反射器配置实例 1211
12.7.3 BGP4+路由负荷分担配置实例 1212
12.7.4 BGP4+综合配置实例 1214
12.8 IPv6 Route-Map 策略配置 1216
12.8.1 配置 IPv6 路由策略 1217
12.8.2 配置 IPv6 策略路由 1221
12.8.3 RIPng 重分配路由策略配置实例 1222
12.8.4 IS-ISv6 路由策略配置实例 1224
12.8.5 OSPFv3 路由策略配置实例 1226
12.8.6 BGP4+路由策略配置实例 1229
12.8.7 6VPE 路由策略配置实例 1232
12.8.8 IPv6 策略路由配置实例 1240
12.9 IPv6 组播 1243
12.9.1 配置公共组播 1243
12.9.2 配置 IPv6 静态组播 1244
12.9.3 IPv6 静态组播配置实例 1245
12.10 MLD 1246
12.10.1 配置 MLD 1247
12.10.2 MLD 查询路由器选举配置实例 1250
12.10.3 MLD 动态组、静态组加入配置实例 1251

12.11 PIM-DM 1253
12.11.1 配置 IPv6 PIM-DM 1253
12.11.2 IPv6 PIM-DM 配置实例 1254
12.12 PIM-SM 1256
12.12.1 配置 IPv6 组播 PIM-SM 1256
12.12.2 IPv6 PIM-SM 配置实例 1259
12.13 PIM-SSM 1262
12.13.1 配置 PIM-SSM 1262
12.13.2 IPv6 PIM-SSM 配置实例 1262
12.14 IPv6 隧道 1264
12.14.1 配置 IPv6 隧道 1264
12.14.2 6in4 隧道配置实例 1265
12.14.3 4in6 隧道配置实例 1267
12.14.4 6to4 隧道配置实例 1269
12.15 ISATAP 隧道 1271
12.15.1 配置 ISATAP 隧道 1271
12.15.2 ISATAP 配置实例 1272
12.16 DS-Lite B4 1274
12.16.1 配置 DS-Lite 隧道 1274
12.16.2 手工配置 AFTR 地址配置实例 1275
12.16.3 DNS 获取 AFTR 地址配置实例 1277
12.16.4 DHCPv6 获取 AFTR 地址配置实例 1280
12.17 6RD 1282
12.17.1 配置 6RD 1283
12.17.2 6RD 配置实例 1284
12.18 6PE 1285
12.18.1 配置 6PE 1285
12.18.2 6PE 配置实例 1286
12.19 6VPE 1291
12.19.1 配置 6VPE 1291
12.19.2 6VPE 配置实例 1299
12.20 IPv6 ACL 1304
12.20.1 配置 IPv6 ACL 1304
12.20.2 IPv6 ACL 配置实例 1306
12.21 URPF 1308
12.21.1 配置 IPv6 URPF 1308
12.21.2 严格 IPv6 URPF 配置实例 1309
12.21.3 松散 IPv6 URPF 配置实例 1310
12.22 IPv6 QoS 1312
12.22.1 配置 IPv6 QoS 1312
12.22.2 IPv6 优先级调度配置实例 1312
12.22.3 IPv6 WRED 配置实例 1314
12.22.4 IPv6 CAR 配置实例 1315
12.22.5 IPv6 优先级继承配置实例 1317
12.23 IPv6 VRRP 1318
12.23.1 配置 IPv6 VRRP 1318
12.23.2 基本 VRRP 配置实例 1320

12.23.3 对称 VRRP 配置实例.....1322
12.23.4 VRRP 心跳线配置实例.....1324
12.24 DHCPv6.....1326
12.24.1 配置 DHCPv6 Server.....1326
12.24.2 配置 DHCPv6 Relay.....1329
12.24.3 配置 DHCPv6 Client.....1331
12.24.4 DHCPv6 Server 配置实例.....1332
12.24.5 DHCPv6 Relay 配置实例.....1334
12.24.6 DHCPv6 Client 配置实例.....1337
13 NAT.....1339
13.1 基本 NAT.....1339
13.1.1 配置启用 NAT.....1339
13.1.2 配置地址池.....1339
13.1.3 配置域.....1341
13.1.4 配置策略.....1342
13.1.5 配置高级业务.....1346
13.1.6 配置日志.....1346
13.1.7 配置告警.....1348
13.1.8 配置 NAT 控制面安全.....1348
13.2 SR NAT44.....1349
13.2.1 配置 SR NAT44.....1349
13.2.2 静态 NAT 转换 NAT44 配置实例.....1350
13.2.3 动态 PAT 转换 NAT44 配置实例.....1352
13.2.4 复用出接口 NAT44 配置实例.....1353
13.2.5 动态多出口 NAT44 配置实例.....1354
13.2.6 VPN（私网-公网）NAT44 配置实例.....1356
13.2.7 VPN（私网-相同私网）NAT44 配置实例.....1357
13.2.8 VPN（私网-不同私网）NAT44 配置实例.....1359
13.2.9 VPN（公网-私网）NAT44 配置实例.....1360
13.3 NAT64.....1362
13.3.1 配置 NAT64.....1362
13.3.2 有状态 NAT64 静态 NAT 转换配置实例.....1364
13.3.3 有状态 NAT64 静态 PAT 转换配置实例.....1366
13.3.4 有状态 NAT64 动态 NAT 转换配置实例.....1368
13.3.5 有状态 NAT64 动态 PAT 转换配置实例.....1369
13.3.6 无状态 NAT64 转换配置实例.....1371
13.4 DS-Lite.....1372
13.4.1 配置 DS-Lite.....1373
13.4.2 静态 NAT 转换配置实例.....1375
13.4.3 静态 PAT 转换配置实例.....1377
13.4.4 动态 NAT 转换配置实例.....1380
13.4.5 动态 PAT 转换配置实例.....1382
14 二层交换.....1385
14.1 二层交换功能.....1385
14.1.1 配置二层端口.....1385
14.1.2 切换二层口配置实例.....1386

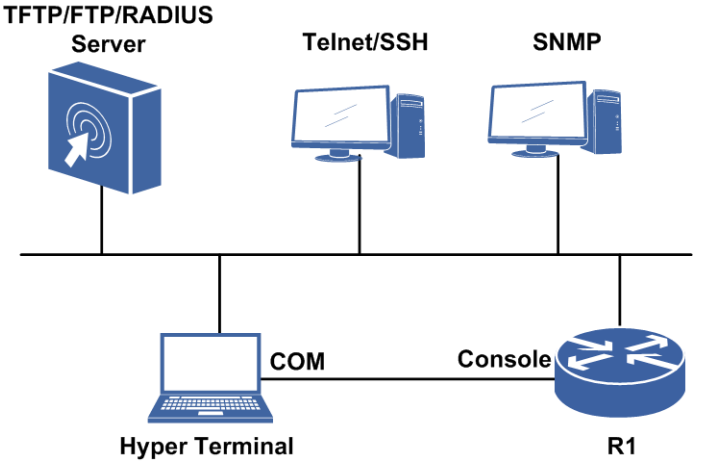
14.2 VLAN 1386
14.2.1 配置 VLAN 1387
14.2.2 VLAN 基本应用配置实例 1388
14.2.3 二层交换汇聚和三层网络接入配置实例 1390
14.3 MAC 1392
14.3.1 配置 MAC 地址表 1392
14.3.2 MAC 地址表配置实例 1394
14.4 STP 1394
14.4.1 配置 STP 1395
14.4.2 MSTP 配置实例一 1398
14.4.3 MSTP 配置实例二 1399

1 系统管理

1.1 设备连接管理

IR12000提供了多种连接配置设备方式，如*图 1-1*所示。

图 1-1 IR12000 配置方式



用户可以根据所连接的网络选用适当的配置方式，下面对各种配置方式进行说明。

- 通过Console口进行配置，这是用户对路由器进行设置的主要方式。
- 通过Telnet/SSH方式进行配置，采用这种方式可以在网络中任何可达位置对路由器进行配置。
- 通过TFTP/FTP/RADIUS服务器下载/上传路由器配置文件，实现对路由器配置的更新。
- 通过网管系统使用SNMP协议进行配置。

1.1.1 配置 Console 口连接

本节介绍通过Console口连接设备的配置步骤和命令。

1.配置超级终端。

超级终端的配置内容，参见*《IR12000 初始配置》*中的“通过Console口连接设备”。

2.（可选）在配置模式下，执行**login authentication**命令开启Console口连接认证功能。

配置示例如下：

```
inspur(config)#login authentication
Warning:
Please make sure local or remote authentication is correctly configured.
Are you sure to configure console authentication?[yes/no]:yes
/*开启Console口连接认证功能*/
```

关于Console口认证使用的用户名和密码的配置，参见"配置用户管理"。

1.1.2 配置 Telnet 连接

本节介绍通过Telnet连接设备的配置步骤和命令。

前提

本地终端与远端路由器网络可达。

相关信息

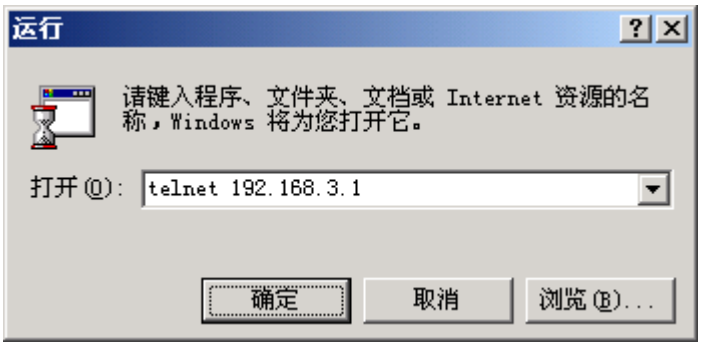
Telnet方式通常在远程配置路由器时使用，为了防止非法用户使用Telnet访问路由器，必须在路由器上设置Telnet访问的用户名和密码，只有使用设置的用户名和密码才能登录到路由器。在IR12000上配置Telnet登录的用户名和密码，参见配置用户管理。

1.通过Telnet连接设备。

假设远端路由器的IP地址为192.168.3.1，本地终端（以Windows XP操作系统终端为例）与远端路由器网络可达，本地终端操作如下：

i.启动本地终端的“运行”程序，输入**telnet 192.168.3.1**，如*图 1-2*所示。

图 1-2 输入 Telnet 命令



ii.单击**确定**按钮，显示**Telnet**登录信息。

显示信息如下：

```
**************************************************************
Welcome to Inspur Intelligent Router 12000 of Inspur networking
**************************************************************

Username:who
Password:
inspur#
```

iii.根据提示输入用户名和密码，即可登录远程路由器。

2.配置Telnet。

在IR12000上用以下命令来配置Telnet可选参数：

命令	功能
inspur(config)#**line console idle-timeout** <*idle-time*>	配置Console口最大空闲超时时间，单位：分钟，取值范围0~1000，默认值30
inspur(config)#**line console absolute-timeout** <*absolute-time*>	配置Console口的最大在线超时时间，单位：分钟，取值范围0~10000，默认值1440
inspur(config)#**line telnet idle-timeout** <*idle-time*>	配置telnet的最大空闲超时时间，单位：分钟，取值范围0~1000，默认值120
inspur(config)#**line telnet absolute-timeout** <*absolute-time*>	配置telnet的最大在线超时时间，单位：分钟，取值范围0~10000，默认值1440
inspur(config)#**line telnet access-class** {**ipv4** | **ipv6**}<*acl-name*>	配置telnet连接绑定的ACL名称
inspur(config)#**line telnet max-link** <*max-number*>	配置telnet连接的最大链接数，取值范围1~15，默认值为15
inspur#**terminal length** <*length*>	配置终端窗口高度，单位：行，取值范围0~512，默认值为24
inspur#**terminal width** <*width*>	配置终端窗口宽度，单位：列，取值范围80~512，默认值为80
inspur(config)#**line telnet dscp** <*dscp-value*>	为IPv4/IPv6 telnet服务端指定控制面报文的DSCP值，范围0~63，默认为48
inspur(config)#**line telnet max-source-connection** <*max-number*>	配置单个源IP地址允许的最大并发连接数，取值范围1~15
inspur(config)#**line telnet server enable** [**listen** {<*23*>|<*49152-65535*>}]	允许终端以telnet方式登录设备，并允许指定端口号
inspur(config)#**line telnet server vrf** <*vrf-name*>	配置telnet服务端支持的VRF名称，默认允许所有与本端建立的telnet连接

3.（可选）在IR12000上执行**telnet**命令，以本设备作为客户端登录其它设备。

命令	功能
inspur#**telnet** {<*dest-address*>[{[<*source-address*>],[<*port-number*>],[{**vrf** <*vrf-name*>| **dcn**}],[**dscp** <*dscp-value*>]}]|<*domain-name*>[{[<*port-number*>],[**vrf** <*vrf-name*>],[**dscp** <*dscp-value*>]}]}	本路由器作为客户端登录其它IPv4类型的telnet服务器 <*domain-name*>：域名，长度1~128个字符

命令	功能
inspur#**telnet6** {<*dest-address*>[{[**interface** <*interface-name*>],[**vrf** <*vrf-name*>],[<*port-number*>],[**dscp** <*dscp-value*>]}]|<*domain-name*>[{[**vrf** <*vrf-name*>],[<*port-number*>],[**dscp** <*dscp-value*>]}]}	本路由器作为客户端登录其它IPv6类型的telnet服务器

4.验证配置结果。

命令	功能
inspur#**show terminal**	显示当前终端信息
inspur#**show history**	显示前十条历史命令
inspur#**show users**	显示登录的用户信息
inspur#**who**	显示登录的用户信息

5.维护Telnet连接。

命令	功能
inspur(config)#**line telnet server disable**	禁止终端以telnet方式登录设备
inspur#**clear line vty** <*vty-number*>	强迫指定vty用户下线 <*vty-number*>：指定终端号，范围0~14

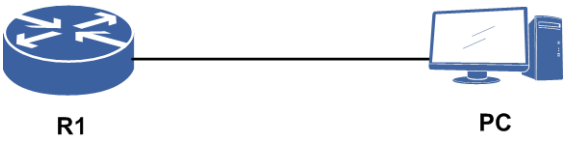
举例

Telnet连接配置实例。

•配置说明

组网环境如*图 1-3*所示，PC通过Telnet方式连接到inspur。

图 1-3 Telnet 连接配置实例



•配置思路

i.PC连接设备

ii.R1上配置Telnet

iii.R1上配置ACL，过滤TCP连接

•配置过程

R1上的配置如下：

```
R1(config)#line telnet idle-timeout 120
R1(config)#line telnet absolute-timeout 1440
R1(config)#line telnet access-class ipv4 wd
R1(config)#ipv4-access-list wd
R1(config-ipv4-acl)#rule permit tcp 169.1.108.82 0.0.0.0 any
R1(config-ipv4-acl)#exit
```

•配置验证

如未配置ACL，则任意同一网段的PC地址均可连接。

如已配置ACL，则PC的IP地址在ACL允许列表内，才可以正常连接。

1.1.3 配置 SSH 连接

本节介绍通过SSH连接设备的配置步骤和命令。

前提

本地终端与远端路由器网络可达。

相关信息

SSH（Secure Shell，安全外壳）由IETF网络工作小组（Network Working Group）制定，是建立在应用层和传输层基础上的安全协议。

传统的网络服务程序，如FTP、POP和Telnet，在网络上用明文传送数据、用户帐号和用户口令，很容易受到中间人（man-in-the-middle）攻击方式的攻击。相比于传统的网络服务程序，SSH是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议，具有以下优点：

•SSH协议可以有效防止远程管理过程中的信息泄露问题。

•SSH协议可以对所有传输的数据进行加密，也能够防止DNS欺骗和IP欺骗。

•SSH协议传输的数据是经过压缩的，可以加快传输的速度。

•SSH常用来代替Telnet，也可以为FTP、POP、甚至为PPP提供一个安全的“通道”。

1.配置SSH。

步骤	命令	功能
1	inspur(config)#**ssh server enable** [**listen** {<*22*>|<*49152-65535*>}]	开启SSH服务器功能，缺省为关闭，并允许指定端口号
2	（可选）inspur(config)#**ssh server access-class** {**ipv4** | **ipv6**}<*acl-name*>	为SSH绑定ACL
3	inspur(config)#**ssh server dscp** <*dscp-value*>	为IPv4/IPv6 ssh server指定控制面报文的DSCP，默认DSCP值为48
	inspur(config)#**ssh server vrf** <*vrf-name*>	配置SSH服务端支持的VRF名称
	inspur(config)#**ssh server version** <*version*>	配置SSH服务器协议版本号

步骤	命令	功能
4	inspur#**ssh** <*dest-address*> **encrypt** {**none** | **aes128** | **blowfish** | **3des**} **compress** {**none** | **zlib**} **mac** {**none** | **sha1** | **md5**}[{[<*source-address*>],[<*port-number*>],[**vrf** <*vrf-name*>],[**dscp** <*dscp-value*>]}]	本路由器作为客户端通过SSH方式登录其他IPv4类型的SSH服务器
5	inspur#**ssh6** <*dest-address*> **encrypt** {**none** | **aes128** | **blowfish** | **3des**} **compress** {**none** | **zlib**} **mac** {**none** | **sha1** | **md5**}[{[<*port-number*>],[**vrf** <*vrf-name*>],[**interface** <*interface-name*>],[**dscp** <*dscp-value*>]}]	本路由器作为客户端通过SSH方式登录其他IPv6类型的SSH服务器

2.维护SSH。

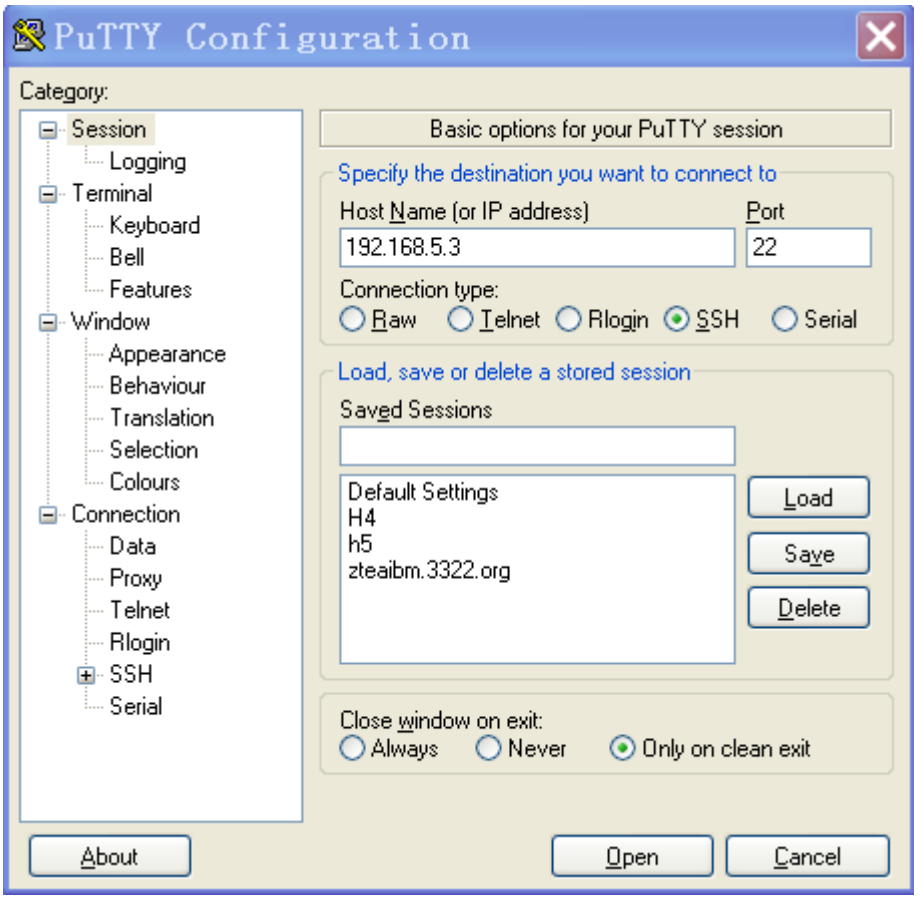
命令	功能
inspur(config)#**ssh server disable**	关闭SSH服务器功能

3.配置SSH客户端。

配置SSH客户端，以Putty为例来说明使用步骤。

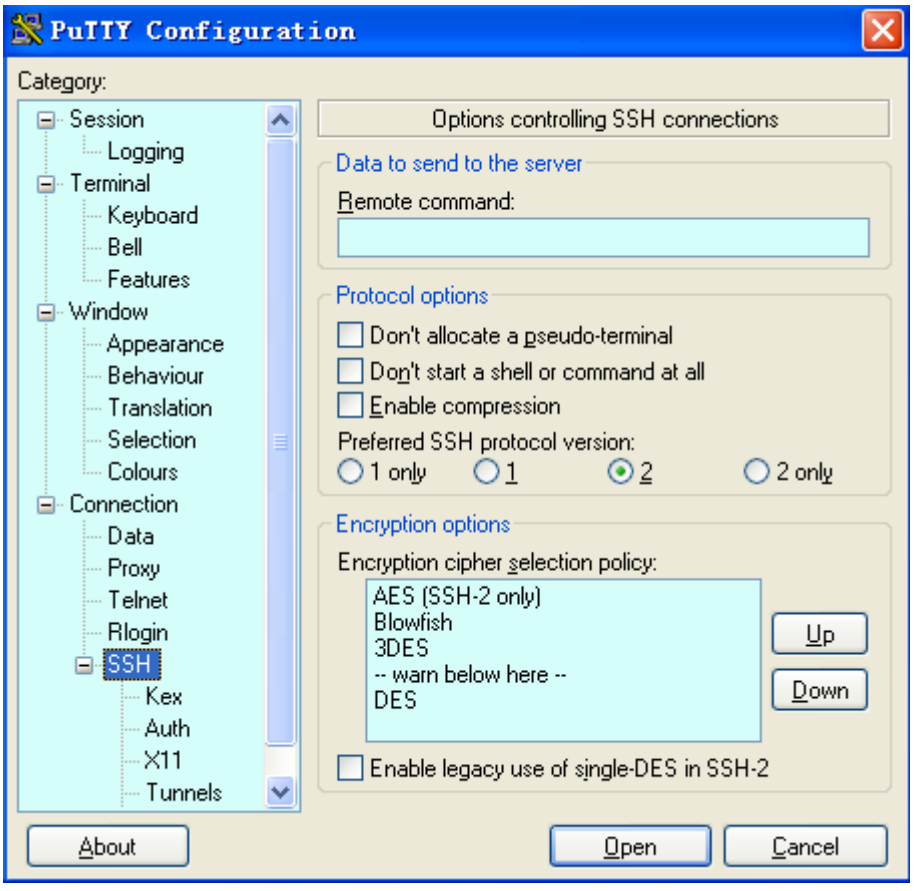
i.在SSH客户端上启用**Putty.exe**，在**Host Name**栏中输入远程路由器IP地址，假设为192.168.5.3，如*图 1-4*所示。

图 1-4 输入登录信息示意图



ii.单击左侧树形目录中的**SSH**，出现如*图 1-5*所示的页面，其中选择SSH版本号为2。

图 1-5 选择 SSH 版本号示意图



iii.单击**Open**按钮，根据界面提示输入正确的用户名和密码。登录成功后，显示路由器的配置界面，即可对路由器进行配置。

```
login as:Inspur
Further authentication required
Inspur@192.168.5.3's password:
************************************************************
Welcome to Inspur Intelligent Router 12000 of Inspur networking
************************************************************
inspur#
```

4.验证配置结果。

命令	功能
inspur#**show ssh**	显示SSH的配置状态

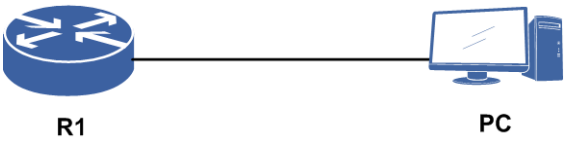
举例

SSH配置实例。

•配置说明

组网环境如*图 1-6*所示，PC通过SSH连接到inspur。

图 1-6 SSH 配置实例



•配置思路

i.PC连接设备

ii.R1上配置SSH

iii.R1上再配置ACL，过滤连接

•配置过程

R1上配置如下：

```
R1(config)#ssh server enable
R1(config)#ssh server access-class ipv4 wd
R1(config)#ipv4-access-list wd
R1(config-ipv4-acl)#rule permit tcp 169.1.108.82 0.0.0.0 any
R1(config-ipv4-acl)#exit
```

•配置验证

如未配置ACL，则任意同一网段的PC地址可以连接。

如已配置ACL，则PC的IP地址在ACL允许列表内，才可以正常连接。

1.1.4 配置设备作为 FTP 服务器

本节介绍IR12000作为FTP服务器的配置步骤和命令。

前提

本地终端与远端路由器网络可达。

1.开启FTP Server功能。

命令	功能
inspur(config)#**ftp-server enable** [**listen** <*port-number*>]	开启FTP Server功能，对指定的端口进行监听，端口的范围为21或2401~2420

2.配置FTP Server其它属性。

命令	功能
inspur(config)#**ftp-server top-directory** <*directory*>[{**read-only** |{[**read-write**],[**copy**]}}]	设置FTP Server允许用户登录的顶级目录。默认情况下，FTP SERVER允许用户通过FTP访问的顶级目录是/datadisk0/
inspur(config)#**ftp-server access-class** [**ipv6**]<*acl-name*>	配置FTP Server绑定ACL

命令	功能
inspur(config)#**ftp-server source-ip ipv4** <*ipv4-address*>	配置FTP Server监听的IPv4地址
inspur(config)#**ftp-server source-ip ipv6** <*ipv6-address*>	配置FTP Server监听的IPv6地址
inspur(config)#**ftp-server source-ip vrf** <*vrf-name*>	配置FTP Server监听的VRF名称
inspur(config)#**ftp-server source-interface** <*interface-name*>	配置FTP Server监听的源接口
inspur(config)#**ftp-server max-login** <*max-number*>	配置FTP Server的最大在线用户数

FTP Server的登录用户名和密码配置，参见配置用户管理。

3.验证配置结果。

命令	功能
inspur#**show ftp-server**	显示FTP服务器的相关配置信息

4.维护FTP Server。

命令	功能
inspur(config)#**ftp-server kick-user** <*user-id*>	将当前的用户从联机状态断开，参数值是联机用户的ID

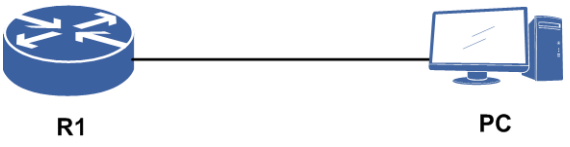
举例

FTP Server配置实例。

•配置说明

如*图 1-7*所示，IR12000与PC相连，IR12000配置FTP Server，PC上FTP client从该Server上传、下载文件。

图 1-7 FTP Server 配置实例拓扑图



•配置思路

i.IR12000开启FTP Server功能，监听端口21

ii.配置FTP Server根目录为“/datadisk0/LOG/”

iii.配置FTP Server的用户名和密码为Inspur

iv.从FTP Server上传、下载文件，验证FTP Server功能

·配置过程

IR12000上的配置过程如下，其中用户名和密码的配置，参见配置用户管理。

```
R1#configure terminal
Enter configuration commands, one per line.End with CTRL/Z.
R1(config)#ftp-server enable
R1(config)#ftp-server top-directory /datadisk0/LOG/
```

1.1.5 配置设备作为 FTP 客户端

本节介绍IR12000作为FTP客户端的配置步骤和命令。

前提

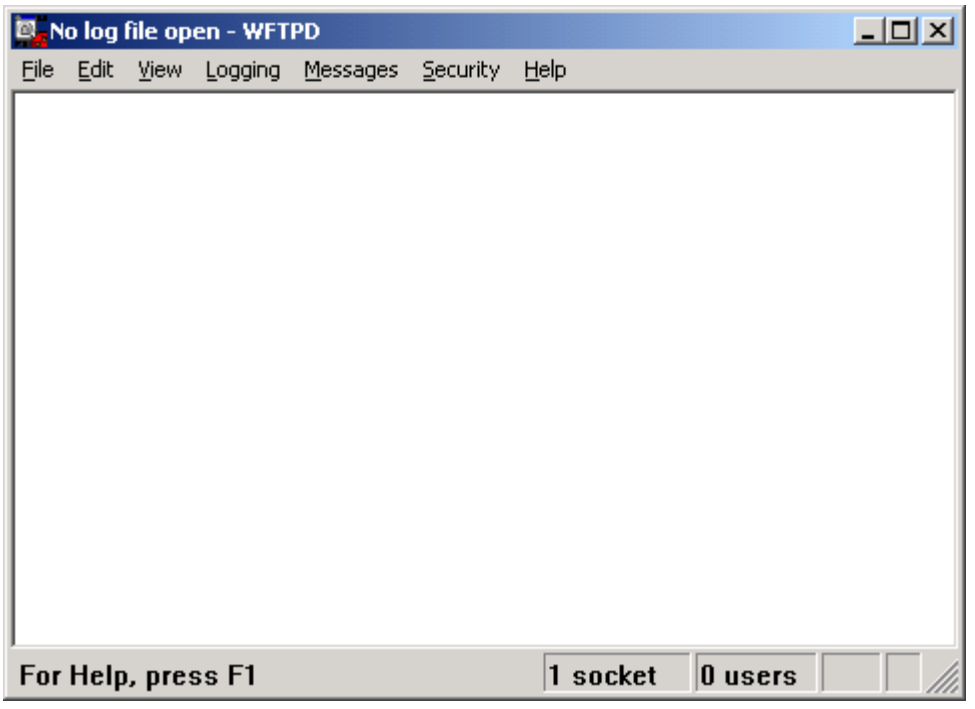
设备与FTP服务器网络可达。

1.配置并启动FTP服务器。

下面以FTP服务器软件**WFTPD**为例说明FTP服务器的配置。

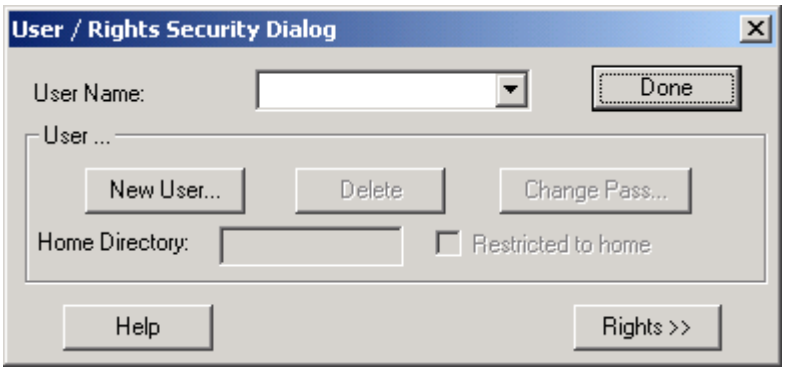
i.执行**wftpd32.exe**，出现如*图 1-8*所示窗口。

图 1-8 WFTPD 窗口



ii.单击*图 1-8*中的菜单项**Security**，选择**User/Rights…**，出现如*图 1-9*所示的对话框。

图 1-9 User/Rights 安全设置对话框



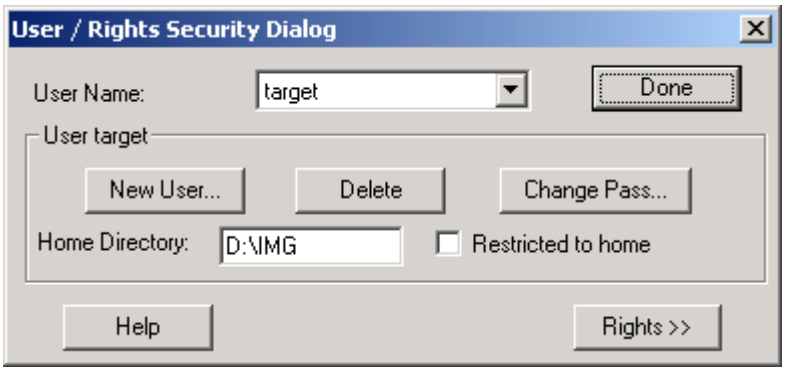
iii.在**User/Rights安全设置**对话框中进行以下操作：

单击**New User…**按钮新建一个用户，如target，并设置密码。

在**User Name**下拉框中选择用户名target。

在**Home Directory**框中输入存放版本文件或配置文件的目录，如D盘的IMG目录。完成设置后对话框显示如*图 1-10*所示。

图 1-10 User/Rights 安全设置对话框



iv.单击*图 1-10*中的**Done**按钮，启动FTP服务器。

2.设备作为FTP客户端上传或下载文件。

命令	功能
inspur#**ftp-client source-ip** {**ipv4** *<ipv4-address>*| **ipv6** *<ipv6-address>*[**interface** *<interface-name>*]}	配置设备作为FTP客户端时的源地址
inspur#**copy ftp** [**vrf** *<vrf-name>*] **//HOST/filename@username:password root: filename or directory&filename** [*<listen_port>*][**ipaddr**][**interface** *<interface-name>*]	FTP客户端下载命令，将FTP服务器上的文件下载到本地
inspur#**copy ftp** [**vrf** *<vrf-name>*] **root: filename or directory&filename //HOST/filename@username:password** [*<listen_port>*][**ipaddr**][**interface** *<interface-name>*]	FTP客户端上传命令，将本地文件上传到FTP服务器上

举例

以下是IR12000作为FTP客户端上传或下载文件的示例。

以用户名为who、密码为who的用户为例，要将设备文件系统/sysdisk0/DATA0目录中的“startrun.dat”文件上传至FTP服务器上，FTP服务器的IP地址为192.168.109.6。

```
inspur#copy ftp root: /sysdisk0/DATA0/startrun.dat
//192.168.109.6/startrun1.dat@who:who
Start copying file

Put file successfully!sent 3492803 bytes!!
```

以用户名为who、密码为who的用户为例，要从IP地址为192.168.109.6的FTP服务器上下载名称为“startrun.dat”的文件，并重命名为“startrun.bak”。

```
inspur#copy ftp //192.168.109.6/startrun.dat@who:who
root: /datadisk0/startrun.bak
Start copying file

Got file successfully!Received 3492803 bytes!!
```

1.1.6 配置 TFTP 连接

通过TFTP，可以对路由器版本文件、配置文件进行备份与恢复。

前提

IR12000作为TFTP客户端与TFTP服务器网络可达。

1.配置并启动TFTP服务器。

下面以TFTP服务器软件**tftpd**为例说明TFTP服务器的配置。

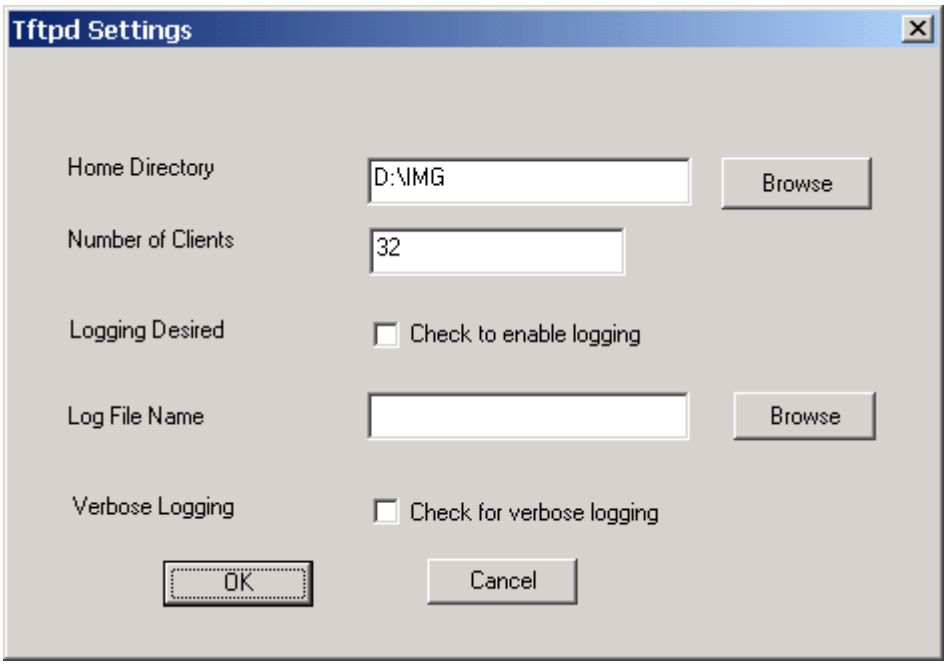
i.运行**tftpd**软件，出现如*图 1-11*所示窗口。

图 1-11 TFTPD 窗口



ii.选择菜单项**Tftpd > Configure**，在弹出的对话框中单击**Browse**按钮，选择存放版本文件或配置文件的目录，如D:\IMG。完成设置后对话框如*图 1-12*所示。

图 1-12 Configure 对话框



iii.单击**OK**按钮完成设置。

2.路由器作为TFTP客户端上传或下载文件。

命令	功能
inspur#**copy tftp** [**ipv6**][**vrf** <*vrf-name*>] **//HOST/filename root: filename or directory** [<*listen_port*>]	TFTP客户端下载命令，将TFTP服务器上的文件下载到本地
inspur#**copy tftp** [**ipv6**][**vrf** <*vrf-name*>] **root: filename or directory //HOST/filename** [<*listen_port*>]	TFTP客户端上传命令，将本地文件上传到TFTP服务器上

举例

将路由器文件系统/datadisk0目录中的“startrun.dat”文件上传至IP地址为192.168.4.244的TFTP服务器：

```
inspur#copy tftp root: /datadisk0/startrun.dat //192.168.4.244/startrun.dat
Starting copying file
.
File copying successfully.
```

到IP地址为192.168.4.244的TFTP服务器上下载名称为“startrun.dat”的文件，并重命名为“startrun.bak”：

```
inspur#copy tftp //192.168.4.244/startrun.dat root: /datadisk0/startrun.bak
Starting copying file
.
File copying successfully.
```

1.1.7 配置设备作为 SFTP 服务器

本节介绍IR12000作为SFTP服务器的配置步骤和命令。

前提

本地终端与远端路由器网络可达。

1.配置SFTP Server。

命令	功能
inspur(config)#**sftp-server top-directory** <*directory*>	设置SFTP Server允许用户登录的顶级目录
inspur(config)#**sftp-server access-class**{**ipv4** | **ipv6**}<*acl-name*>	配置SFTP Server绑定ACL
inspur(config)#**sftp-server idle-timeout** <*idle-time*>	配置SFTP Server的最大空闲超时时间，单位：分钟，取值范围0~1440，默认值0，表示不超时

SFTP Server的登录用户名和密码配置，参见配置用户管理。

2.验证配置结果。

命令	功能
inspur#**show sftp-server**	显示SFTP服务器的相关配置信息

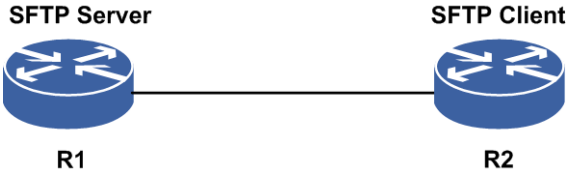
举例

SFTP Server配置实例。

•配置说明

IR12000作为SFTP Server时，Client可以是PC，也可以是其他支持SFTP Client的设备。如*图 1-13*所示，两台IR12000设备相连，一台作为SFTP Server，另一台作为SFTP client从Server上下载文件。

图 1-13 SFTP Server 配置实例拓扑图



•配置思路

i.在SFTP Server上开启SSH功能，配置监听端口。

ii.在SFTP Server上设置SFTP根目录为"/datadisk0/BAK/"。

iii.在SFTP Server上配置用户名和密码为"Inspur"。

iv.从SFTP Server下载文件，验证SFTP Server功能。

·配置过程

IR12000的配置过程如下，其中用户名和密码的配置，参见配置用户管理。

```
/*SFTP server上的配置如下*/
R1#configure terminal
R1(config)#ssh server enable listen 49152
R1(config)#sftp-server top-directory /datadisk0/BAK/

R1#dir BAK
Directory of MPFU-8/0: /datadisk0/BAK
1036288 KB total (560256 KB free)

       attribute   size      date       time        name
1      <DIR>       4096      03-04-2013  15:08       .
2      <DIR>       4096      03-04-2013  15:08       ..
3      ----        615       03-04-2013  15:08       0130.txt

/*SFTP client上下载文件*/
R1#copy sftp vrf mng //169.1.219.14/0130.txt@Inspur:Inspur
root: /datadisk0/0130.txt encrypt 3des compress zlib mac md5 49152
Start copying file
.
Got file successfully!
```

1.1.8 配置设备作为 SFTP 客户端

本节介绍IR12000作为SFTP客户端的配置步骤和命令。

前提

设备与SFTP服务器网络可达。

1.配置SFTP服务器。

先启动SFTP服务器应用软件，路由器作为SFTP客户端与SFTP服务器进行通信。

2.配置设备作为SFTP客户端上传或下载文件。

命令	功能
inspur#**copy sftp** [**vrf** <*vrf-name*>] **//HOST/filename@username:password root: filename or directory&filename encrypt** {**none** | **aes128** | **blowfish** | **3des**} **compress** {**none** | **zlib**} **mac** {**none** | **sha1** | **md5**}[<*listen_port*>][**ipaddr**][**interface** <*interface-name*>]	SFTP客户端下载命令，将SFTP服务器上的文件下载到本地
inspur#**copy sftp** [**vrf** <*vrf-name*>] **root: filename or directory&filename //HOST/filename@username:password encrypt** {**none** | **aes128** | **blowfish** | **3des**} **compress** {**none** | **zlib**} **mac** {**none** | **sha1** | **md5**}[<*listen_port*>][**ipaddr**][**interface** <*interface-name*>]	SFTP客户端上传命令，将本地文件上传到SFTP服务器上

举例

以用户名为who、密码为who的用户为例，将设备文件系统/sysdisk0/DATA0目录

中的"startrun.dat"文件上传至SFTP服务器上，SFTP服务器的IP地址为192.168.109.6，加密算法为aes128，压缩算法为zlib，MAC校验为sha1。

```
inspur#copy sftp root: /sysdisk0/DATA0/startrun.dat
 //192.168.109.6/startrun1.dat @who:who encrypt aes128 compress zlib mac sha1
Start copying file
...
Put file successfully!
```

以用户名为who、密码为who的用户为例，要从IP地址为192.168.109.6的SFTP服务器上下载名称为"startrun.dat"的文件，并重命名为"startrun.bak"，加密算法为aes128，压缩算法为zlib，MAC校验为sha1。

```
inspur#copy sftp //192.168.109.6/startrun.dat@who:who root: /
datadisk0/startrun.bak encrypt aes128 compress zlib mac sha1
Start copying file
...
Got file successfully!
```

1.2 缺省配置

对于路由器设备，往往需要客户找来串口线，连接上后通过串口服务器对设备进行管理配置。但有时在特定的环境中，串口线并未随时就可以取到，此时，通过管理口缺省登录就是一种很好的解决办法。

设备缺省配置主要包括三方面的内容：

•缺省用户名和密码

缺省用户名和密码主要用于用户通过管理口Telnet登录后，进行设备配置前的验证授权。

•管理口缺省IP

管理口缺省IP是指设备出厂时统一配置的一个管理口IP地址，方便用户进行Telnet登录，后续在设备进行组网使用后，客户最好对管理口缺省IP进行修改。

•设备恢复出厂配置

当用户进行了不当操作或忘记用户名、密码等情况下，可以通过设备恢复出厂配置命令恢复设备的初始状态。

1.2.1 缺省用户名和密码配置

概述

缺省用户名和密码是指设备在出厂后，允许客户登录的默认用户名和密码，以便客户对设备进行配置管理，客户在初次登录后可以根据需要自行修改。

缺省用户名、密码

设备在出厂前，系统已经配置了缺省的用户名和密码，其缺省值参见*表 1-1*。

表 1-1 IR12000 缺省用户名和密码

用户名	密码
inspur	inspurinspur

关于缺省用户名和密码说明如下：

•缺省用户名和密码区分大小写。

•缺省用户名由设备出厂时设置，后期不可进行修改，但密码可以修改。

•客户用缺省用户名和密码登录时，如果缺省用户名输入错误，设备会提示“Information incomplete”；如果缺省用户名输入正确，而缺省密码输入错误，设备则会提示“Authentication failed”。

登录方式

缺省用户名和密码的登录方式目前支持Telnet、WEB-GUI、SSH登录，其中SSH登录前需要通过**ssh server enable**命令开启该服务；其他常见的登录方式，如FTP等暂时不支持。

缺省用户名、密码修改

用户名和密码修改主要分为两个部分：

•初始登录的密码修改

客户在初次登录设备后，出于安全考虑，建议客户进行密码修改，密码长度要求为6-32个字符。

初始登录过程如下：

```
Login at: 08:01:57 07-29-2016
Username:inspur
Password:
inspur#
```

用**show rootuser**命令查看配置结果：

```
inspur#show rootuser
Rootuser: inspur
Password:
5adbcc63c132f10ef277543832106d2cfe0d0216042d7eda8e2ab62d1693fe49
Password set-time:
```

修改初始密码步骤如下：

```
inspur(config)#system-user
inspur(config-system-user)#rootuser password
Please enter old password:********
Please enter new password:******
```

```
%Info 59973: New password is configured successfully!
```

用**show rootuser**命令查看配置结果：

```
inspur(config-system-user)#show rootuser
Rootuser: inspur
Password:
6b8d5a67ab470c6bd131a6f350d67f0ba56d6183b66dbd5850465d31084d74c7
Password set-time: 2016-07-29
```

客户修改初始登录密码后，如果后期客户不自行配置普通用户，修改的密码会一直生效。

·后期自行的密码修改

设备运行过程中，客户如果觉得密码使用周期太长或密码已被外界获悉等情况下，可以进行密码的修改，密码长度要求为6-32个字符，配置步骤如下。

```
inspur(config)#system-user
inspur(config-system-user)#rootuser password
Please enter old password:*******
Please enter new password:*******
%Info 59973: New password is configured successfully!
```

用**show rootuser**命令查看配置结果：

```
inspur(config-system-user)#show rootuser
Rootuser: inspur
Password:
a07441c5d3bc4296c596d22a65b71e1edbf39932b1347a22a19063692ce25afe
Password set-time: 2016-07-29
```

自行修改的密码是经过加密的，密码是否修改正确用户可以通过比较前后加密字符串的不同来粗略判断，也可以通过登录和密码修改命令进行精准判断。

注意：

若配置了普通用户名密码后rootuser账号被注销且无法通过配置恢复。

如果后期遇到自行修改的密码丢失或遗忘等，可以通过后面的恢复设备出厂配置命令进行缺省用户名，密码的重置。

缺省用户名与load-mode以及普通用户的关系

Load-mode分两种方式：**load-mode null**加载和**no load-mode加载**（即**txt**加载）。二者的区别就在于是否加载startrun.dat文件。**load-mode null**不进行startrun.dat文件的加载，而**no load-mode**则进行startrun.dat文件的加载。

·**load-mode null**加载

设备**load-mode null**加载，不管存在不存在startrun.dat文件，也不管先前是否进行**write**操作，此时缺省用户名和密码自动生成，客户只需用缺省用户名和密码进行登录即可。具体的对应关系参见*表 1-2*。

表 1-2 load-mode null 方式加载时用户名和密码生效类型

是否存在普通用户	是否进行write操作	用户名和密码生效类型
是	是	缺省的用户名、密码
是	否	缺省的用户名、密码
否	是	缺省的用户名、密码
否	否	缺省的用户名、密码

提示：

如果客户对缺省密码进行过修改，此时缺省密码按新修改的密码生效。

·**no load-mode**加载（即txt加载）

设备**no load-mode**加载，此时缺省用户名和密码是否生效，与startrun.dat文件中是否存在普通用户有着直接的关系。此时需要进一步判断是否存在普通用户，具体的对应关系参考*表 1-3*。

表 1-3 no load-mode 方式加载时用户名和密码生效类型

是否存在普通用户	是否进行write操作	用户名和密码生效类型
否	是	缺省的用户名、密码
否	否	缺省的用户名、密码
是	否	缺省的用户名、密码
是	是	普通的用户名、密码

提示：

如果客户对缺省用户名的密码进行过修改，此时缺省密码按新修改的密码生效。

如果客户对普通用名户的密码进行过修改，此时普通密码按新修改的密码生效。

在缺省用户名、密码失效，普通用户名、密码生效的情况下，客户可以通过**show rootuser**和**show username**进行查看。

注意：

no load-mode配置下，要注意startrun.dat文件的内容是前期保存的，还是后期重新配置再保存的，客户可以通过**show startup-config**命令查看startrun.dat的内容。

1.2.2 管理口缺省 IP 配置

管理口缺省IP与load-mode加载设置以及是否存在startrun.dat文件有直接的关系。

·如果设备为**load-mode null**加载，此时自动生成的缺省管理口IP不生效，而是按

照客户设置的管理口IP进行生效。

- 如果设备为**no load-mode**加载，管理口缺省IP仅在设备不存在`startrun.dat`文件时生效，生效的管理口缺省IP地址为：192.168.1.1/24。

1.2.3 设备恢复出厂配置

在某种紧急情况或客户忘记了修改的密码情况下，客户可以通过设备恢复出厂配置来进行初始化后的设备登录，设备会主动删除startrun.dat文件，此时缺省用户名、密码、缺省管理口IP则生效。

恢复设备出厂配置过程如下：

```
inspur#startrun restore default
This operation will clear startrun.dat and reload system,continue?
[yes/no]:y
```

1.3 文件系统管理

文件系统包含Harddisk、Flash、NVRAM三个部分。除此之外，在MPFU主控板面板上有两个USB接口，从而能够快速方便地备份或添加配置文件、版本文件、日志文件。

1.3.1 配置文件系统管理

本节介绍IR12000上管理文件和目录、硬盘用户区格式化和配置信息存盘的操作命令。

1.管理文件和目录。

命令	功能
inspur#**dir** [<*filename-or-directory*>|[<*cpu-name*>]]	显示文件信息列表： ▸如果不输入参数，则显示当前目录下的文件信息列表 ▸如果输入，则显示指定目录下的文件信息列表或者指定文件
inspur#**pwd**	显示该终端当前的文件路径
inspur#**cd** <*directory*>[<*cpu-name*>]	切换文件目录路径
inspur#**mkdir** <*directory*>[<*cpu-name*>]	创建目录，如果目录已存在则返回目录存在的错误提示
inspur#**rmdir** <*directory*>[<*cpu-name*>]	删除指定目录，如果目录下还存在文件，则删除不成功
inspur#**delete** <*filename*>[<*cpu-name*>]	删除指定文件
inspur#**cp** <*source-file*>[<*cpu-name*>]<*destination-file*>[<*cpu-name*>]	复制文件从源目录到目的目录

命令	功能
inspur#**umount** {**usb1** | **usb2**}	卸载U盘存储设备
inspur#**mount** {**usb1** | **usb2**}	加载U盘存储设备
inspur#**more** <*filename*>[<*cpu-name*>][|{**begin** | **exclude** | **include**}<*line*>]	显示指定文件内容，"|"为输出标志

<*filename-or-directory*>：文件名称（长度为1~79个字符）或路径/文件名称（长度为1~159个字符）或者目录名称（长度为1~79个字符）或路径/目录名称（长度为1~159个字符）。

<*cpu-name*>：CPU名称，不输入默认为当前单板，具体格式为：[MPFU-<slot>/<cpu>|PIU-<slot>/<cpu>]；其中<slot>/<cpu>分别为槽、cpu编号。

<*directory*>：目录名称（长度为1~79个字符）或路径/目录名称（长度为1~159个字符）。

<*filename*>：文件名称（长度为1~79个字符）或路径/文件名称（长度为1~159个字符）。

<*source-file*>：源文件名（长度为1~79个字符）或路径/文件名（长度为1~159个字符）。

<*destination-file*>：目的文件名（长度为1~79个字符）或路径/文件名（长度为1~159个字符）。

{**begin** | **exclude** | **include**}<*line*>：正则表达式。

- **begin**：显示以输入字符串行开头的配置信息。
- **exclude**：显示去除字符串行相关配置信息之后的其它信息。
- **include**：显示包含字符串行的相关配置信息。
- <*line*>：用于匹配筛选的字符串行。

2.格式化硬盘用户区。

命令	功能
inspur#**format** {**/datadisk0**}[<*cpu-name*>]	格式化硬盘的用户区，目前不支持对其他分区进行格式化，该命令采用交互式命令方式，给出提示说明将使该分区上的所有文件丢失 /datadisk0是硬盘的用户区名

3.修改设备启动时的配置加载方式。

命令	功能
inspur(config)#**load-mode null**	配置上电加载方式，以空配置启动

4.存盘配置信息。

命令	功能

命令	功能
inspur#**write**	配置信息存盘

1.3.2 文件系统基本配置实例

文件系统常用操作举例如下。

•进入/datadisk0文件目录：

```
inspur#cd /datadisk0
```

•显示当前工作路径：

```
inspur#pwd
MPFU-8/0: /datadisk0
```

•列出当前目录下的文件信息：

```
inspur#dir
Directory of MPFU-8/0: /datadisk0
1036288 KB total (560256 KB free)

       attribute  size      date       time        name
1 <DIR> 8192 03-12-2013 00:17 .
2 <DIR> 8192 03-12-2013 00:17 ..
3 <DIR> 8192 05-23-2012 14:30 performance
4 <DIR> 8192 12-03-2012 09:49 LOG
5 ---- 463946367 02-27-2013 05:23 2013_Feb_28_10_52_22_AXM
 PFUA_base_B13.set
6 <DIR> 8192 03-12-2013 00:17 techspt
7 ---- 4172191 03-02-2013 04:32 cmdlog_20130128174408_4.
 cmd.log
8 <DIR> 8192 02-04-2013 07:41 license
inspur#
```

•删除目录下文件：

```
inspur#delete /datadisk0/techspt/techspt_cpu-info.txt
Are you sure to delete file(s)?[yes/no]:y
Delete file(s) successfully.
```

在/datadisk0/techspt目录下删除techspt_cpu-info.txt文件：

```
inspur#delete techspt_cpu-info.txt
Are you sure to delete file(s)?[yes/no]:y
Delete file(s) successfully.
```

•修改目录名，将目录test改名为test_new：

```
inspur#rename test test_new
Rename successfully.
```

1.3.3 将配置文件备份到 USB 的配置实例

1.将USB存储设备插在主用主控板的USB接口上，系统会自动挂载USB存储设备，通过**show filesystem**命令可查看到USB路径：

```
inspur#show filesystem
MPFU-8/0:
    /sysdisk0
    /datadisk0
```

```
    /usb1:1
```

2.查看USB设备中的文件：

```
inspur#dir /usb1:1
Directory of MPFU-8/0: /usb1:1
3739652  KB total (3482228 KB free)

       attribute   size      date       time        name
1      <DIR>      4096      07-25-2012  19:20       .
2      <DIR>      4096      07-25-2012  19:20       ..
3                 ----                  261304          07-23-2012    14:56
techspt_basic-info.txt
4      <DIR>      4096      07-25-2012  19:39       1
```

3.使用**cp**命令将配置文件startrun.dat备份到USB设备中：

```
inspur#cp /sysdisk0/DATA0/startrun.dat /usb1:1/startrun.dat
 Copy file successfully.
```

4.备份工作完成后，执行卸载命令后移除USB设备：

```
inspur#umount usb1
MPFU-8/0: usb1 unmounted successfully!
```

1.4 MIM

MIM（Management Information Model，管理信息模型）是指根据业务配置数据建立的信息模型来存储配置数据，并依据模型定义完成对象操作的校验，以及执行对象操作来修改配置数据。信息模型子系统满足CLI/SNMP等配置终端命令处理接口统一的配置提交、回滚需求。

1.4.1 配置 MIM

本节介绍IR12000上MIM功能的配置命令和配置实例。

1.配置MIM。

命令	功能
inspur#**configure exclusive**	配置独占功能
inspur(config)#**commit-mode** {**automatic** | **manual**}	设置配置命令的提交模式，可设置为自动提交模式和手动提交模式，默认自动提交模式
inspur#**commit**	提交配置
inspur#**rollback**	回滚未提交或提交失败的配置
inspur#**rollback-configuration** {{**enable** | **disable**}|{**last** <*last-num*>| **to** <*to-id*>}}	回退功能的开启，关闭以及执行回退
inspur#**lock configuration**	锁定所有终端的配置权限
inspur#**unlock configuration**	解除所有终端的配置权限

提示：

如果某个终端配置为手动提交模式，且有配置未能提交，则可能会影响到其他终端的正常配置。

2.验证配置结果。

命令	功能
inspur#**show commit-mode**	显示提交模式
inspur#**show uncommitted-command**	显示当前配置终端所有未最终提交生效的配置命令
inspur#**show commit-failed**	显示手动提交模式下当前配置终端提交失败的配置命令
inspur#**show configure exclusive**	显示独占信息

1.4.2 MIM 配置实例

配置说明

通过脚本批量输入配置命令，注意需要避免配置冲突。

配置思路

1.配置终端独占，避免配置冲突。

2.修改命令提交方式为手动。

3.通过脚本输入配置命令。

4.提交命令。

配置过程

配置过程如下：

```
inspur#configure exclusive
inspur(config)#mu c

%Info 140359: Allow others to configure, must avoid conflict.
inspur(config)#commit-mode manual

/* 通过脚本输入配置命令，过程略 */
inspur(config)#commit
```

配置验证

通过相关的**show**命令检查脚本输入的命令已经全部提交且生效。

1.5 用户管理

在对设备进行维护和管理时，用户需要通过SSH、Telnet或FTP方式登录设备，用户管理管理用于实现对登录设备的用户进行配置、认证和授权。

1.5.1 配置用户管理

本节介绍用户管理功能的配置步骤和命令。

1.进入用户管理配置模式，配置用户管理参数。

步骤	命令	功能
1	inspur(config)#**system-user**	进入用户管理配置模式
2	inspur(config-system-user)#**default-privilege-level** <*0-15*>	配置缺省权限等级
3	inspur(config-system-user)#**strong-password length** <*length*> **character** {[**capital**][**lowercase**][**number**][**special-character**]}	配置强密码，长度范围6-32字符，密码需包含大写字母、小写字母、数字、特殊字符中的任意一个或几个
4	inspur(config-system-user)#**user-authen-restriction fail-time** <*times*> **lock-minute** <*time*>	配置连续认证失败后锁定用户，失败次数范围3-6，锁定时间范围1-1440分钟
5	inspur(config-system-user)#**global-enable-type** {**aaa**|**local**} **authentication-template** <*1-128*>	配置全局的enable认证方式
6	inspur(config-system-user)#**account-switch** {**off**	**on accounting-template**<*2001-2128*>}	配置全局的记账方式
7	inspur(config-system-user)#**user-default**	进入defaul用户配置模式
8	inspur(config-system-user)#**user-group special** <*usergroup-name*><*username*>{<*password*>| **encrypted** <*password*>}	配置用户组信息
9	inspur(config-system-user)#**login ascii authentication-template** <*1-128*> **authorization-template** <*1-128*>	配置ASCII认证方式模板

2.配置认证模板。

步骤	命令	功能
1	inspur(config)#**aaa-authentication-template** <*1-2128*>	配置AAA认证模板，进入该模板的配置模式
2	inspur(config-aaa-authen-template)#**aaa-authentication-type** {**none** | **local** | **radius** | **local-radius** | **radius-local** | **radius-none** | **local-tacacs** | **tacacs** | **tacacs-local** | **tacac-none**| **diameter**}	在AAA认证模板下，配置认证类型
3	inspur(config)#**system-user**	进入用户管理配置模式
4	inspur(config-system-user)#**authentication-template** <*1-128*>	配置用户管理认证模板，进入该模板的配置模式
5	inspur(config-system-user-authen-temp)#**bind aaa-authentication-template** <*2001-2128*>	在用户管理认证模板配置模式下，绑定AAA的认证模板
6	inspur(config-system-user-authen-temp)#**bind access-list** {**ipv4** |**ipv6**}<*acl-name*>	在用户管理认证模板配置模式下，绑定ACL模板
7	inspur(config-system-user-authen-temp)#**description** <*description*>	在用户管理认证模板配置模式下，增加对该用户管理认证模板的描述信息

3.配置授权模板。

步骤	命令	功能
1	inspur(config)#**aaa-authorization-template** <*1-2128*>	配置AAA授权模板，进入该模板的配置模式
2	inspur(config-aaa-author-template)#**aaa-authorization-type** {**none** | **local-radius** | **local-tacacs** | **local** | **radius** | **tacacs** | **tacacs-local** | **radius-local** }	在AAA授权模板下，配置授权类型
3	inspur(config)#**system-user**	进入用户管理配置模式
4	inspur(config-system-user)#**authorization-template** <*1-128*>	配置用户管理授权模板，进入该模板的配置模式
5	inspur(config-system-user-author-temp)#**bind aaa-authorization-template** <*2001-2128*>	在用户管理授权模板配置模式下，绑定AAA的授权模板
6	inspur(config-system-user-author-temp)#**local-privilege-level** <*0-15*>	在用户管理授权模板配置模式下，配置本地授权等级
7	inspur(config-system-user-author-temp)#**description** <*description*>	在用户管理授权模板配置模式下，增加对该用户管理授权模板的描述信息
8	inspur(config-system-user-author-temp)#**local-cmdgroup** <*group*>	为授权模板绑定本地命令组
9	inspur(config-system-user-author-temp)#**local-cmdgroup-mode exclusive**	定义命令组使用方式为独享方式，缺省为追加方式

步骤	命令	功能
10	inspur(config-system-user-author-temp)#**logfile-allowed** {**cmd-log** | **alarm-log** | **nat-log** | **li-log** | **service-log**}[{**read-only** | **none** |{[**read-write**],[**copy**]}}]	配置授权模板允许访问的日志类型和权限
11	inspur(config-system-user-author-temp)#**ftp top-directory** <*directory*>[{**read-only** |{[**read-write**],[**copy**]}}]	配置授权模板允许通过FTP访问的顶级目录和访问权限
12	inspur(config-system-user-author-temp)#**sftp top-directory** <*directory*>[{**read-only** |{[**read-write**],[**copy**]}}]	配置授权模板允许通过SFTP访问的顶级目录和访问权限

4.创建用户，绑定认证模板和授权模板。

步骤	命令	功能
1	inspur(config-system-user)#**user-name** <*name*>	配置用户名，并进入用户名配置模式
2	inspur(config-system-user-username)#**bind authentication-template** <*1-128*>	绑定用户管理认证模板
3	inspur(config-system-user-username)#**bind authorization-template** <*1-128*>	绑定用户管理授权模板
4	inspur(config-system-user-username)#**password** {<*pwd*>|**encrypted** <*pwd*>}	配置密码
5	inspur(config-system-user-username)#**password-recover-remind**	配置用户名密码恢复相关信息
6	inspur(config-system-user-username)#**password-duration** <*days*>	配置密码有效期，参数0表示永不过期，范围90~60天
7	inspur(config-system-user-username)#**once-password**	配置用户首次登录修改密码功能

5.全局模式下配置其它参数。

命令	功能
inspur(config)#**enable secret level** <*1-18*>{**0** <*unencrypted-password*>| **5** <*encrypted-password*>|<*unencrypted-password*>}	设置登录各级权限的密码
inspur(config)#**login block** <*block-seconds*> **attempts** <*tries*> **within** <*seconds*>	配置和激活远程登录防攻击监测功能
inspur(config)#**login quiet-mode** < *ipv4-access-list* | **ipv6-access-list** ><*access-list-name*>	用于配置安静期的访问控制列表
inspur(config)#**login on-failure alarm** [**every** <*failure-tries*>]	用于配置在有登录尝试失败时生成日志信息或TRAP信息

6.验证配置结果。

命令	功能
inspur#**show running-config adm-mgr** [**all**]	查看用户管理的配置信息
inspur#**show user-group** [**special** <*usergroup-name*>]	显示配置的user-group信息
inspur#**show authen-restriction userinfo**	进行锁定用户和认证失败用户的信息查询，包括用户名、认证失败次数、状态（锁定或未锁定）、剩余锁定的时间
inspur#**show login**	用于查询防攻击监测功能的配置信息
inspur#**show login state** [{[**telnet**][**ssh**][**ftp**]}]	用于查询防攻击监测功能的状态和统计信息
inspur#**show login failure** [{[**telnet**][**ssh**][**ftp**]}]	用于查询防攻击监测功能的登录尝试失败的信息

举例

配置用户名密码恢复的命令**password-recover-remind**为动态交互命令，示例如下。

密码恢复问题设置成功：

```
inspur(config-system-user-username)#password-recover-remind
password is:***
question:what is your name
answer:Inspur
inspur(config-system-user-username)#
```

密码输入错误：

```
inspur(config-system-user-username)#password-recover-remind
password is:***
%Error 59958: Password is wrong!
inspur(config-system-user-username)#
```

密码恢复问题设置失败：

```
inspur(config-system-user-username)#password-recover-remind
password is:***
question:question is 012345678901234567890124567890123456789
%Error 59959: Question has been to upper limit!The limit is 50 characters!
inspur(config-system-user-username)#
```

密码恢复问题的答案设置失败：

```
inspur(config-system-user-username)#password-recover-remind
password is:***
question:what is your name
answer:Inspur 012345678901234567890123456789012345678901234567890123456
%Error 59960: Answer has been to upper limit!The limit is 50 characters!
inspur(config-system-user-username)#
```

user-password recover-remind <*name*>命令的输出说明：

命令输出	描述
password is:	要求输入对应用户名在username配置时设置的password。密码的明文，长度为3~32个字符，界面显示为***，如密码正确，则命令继续执行，

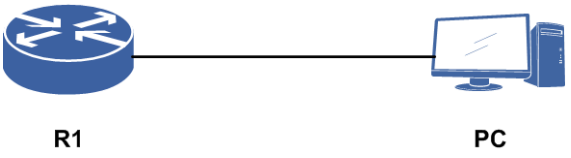
命令输出	描述
	如密码错，则报错，命令结束
question:	输入密码恢复时提示问题，长度为50个字符，包括空格，question不可以全部为空格，也不能包括字符“？”。如长度超过50个字符，则报错，命令结束。正常则命令继续执行
answer:	answer要求同question的输入。长度为50个字符，包括空格，answer不可以全部为空格，也不能包括字符“？”。如长度超过50个字符，则报错，命令结束。正常则命令继续执行

1.5.2 本地认证授权用户配置实例

配置说明

如*图 1-14*所示，PC通过串口或者Telnet等方式登录路由器，进入配置模式，创建一个本地认证方式的用户。

图 1-14 配置本地认证授权



配置思路

1.配置认证模板。

2.配置授权模板。

3.创建用户，绑定认证模板和授权模板。

配置过程

```
R1(config)#aaa-authentication-template 2001
R1(config-aaa-authen-template)#aaa-authentication-type local
R1(config-aaa-authen-template)#exit

R1(config)#aaa-authorization-template 2001
R1(config-aaa-author-template)#aaa-authorization-type local
R1(config-aaa-author-template)#exit

R1(config)#system-user
R1(config-system-user)#authentication-template 1
R1(config-system-user-authen-temp)#bind aaa-authentication-template 2001
R1(config-system-user-authen-temp)#exit

R1(config-system-user)#authorization-template 1
R1(config-system-user-author-temp)#bind aaa-authorization-template 2001
R1(config-system-user-author-temp)#local-privilege-level 15
```

```
R1(config-system-user-author-temp)#exit

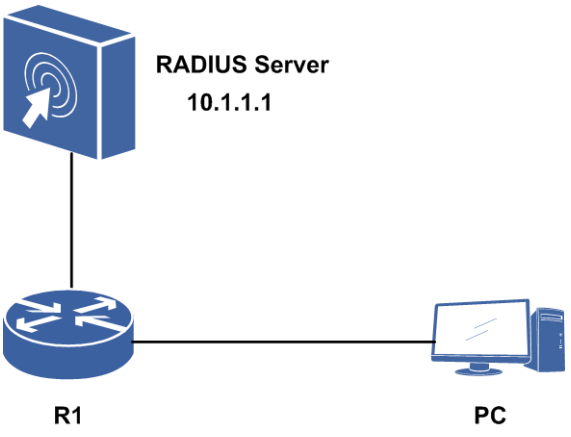
R1(config-system-user)#user-name Inspur
R1(config-system-user-username)#bind authentication-template 1
R1(config-system-user-username)#bind authorization-templat 1
R1(config-system-user-username)#password Inspur
R1(config-system-user-username)#exit
R1(config-system-user)#exit
```

1.5.3 RADIUS-LOCAL 认证授权用户配置实例

配置说明

如*图 1-15*所示，PC通过串口或者telnet等方式登录路由器，进入配置模式，创建一个RADIUS-LOCAL认证方式的用户。

图 1-15 配置 RADIUS-LOCAL 认证授权



配置思路

1.配置RADIUS组。

2.配置认证模板。

3.配置授权模板。

4.创建用户，绑定认证模板和授权模板。

配置过程

```
/*配置RADIUS*/
R1(config)#radius authentication-group 1
R1(config-authgrp-1)#server 1 10.1.1.1 master key Inspur
R1(config-authgrp-1)#nas-ip-address 10.1.1.100
R1(config-authgrp-1)#algorithm round-robin
R1(config-authgrp-1)#max-retries 3
R1(config-authgrp-1)#timeout 30
R1(config-authgrp-1)#deadtime 0
R1(config-authgrp-1)#exit
```

```
/*配置认证模板*/
R1(config)#aaa-authentication-template 2001
R1(config-aaa-authen-template)#aaa-authentication-type radius-local
R1(config-aaa-authen-template)#authentication-radius-group 1
R1(config-aaa-authen-template)#exit

/*配置授权模板*/
R1(config)#aaa-authorization-template 2001
R1(config-aaa-author-template)#aaa-authorization-type radius-local
R1(config-aaa-author-template)#authorization-radius-group 1
R1(config-aaa-author-template)#exit

R1(config)#system-user
/*绑定认证模板*/
R1(config-system-user)#authentication-template 1
R1(config-system-user-authen-temp)#bind aaa-authentication-template 2001
R1(config-system-user-authen-temp)#exit

/*绑定授权模板*/
R1(config-system-user)#authorization-template 1
R1(config-system-user-author-temp)#bind aaa-authorization-template 2001
R1(config-system-user-author-temp)#local-privilege-level 15
R1(config-system-user-author-temp)#exit

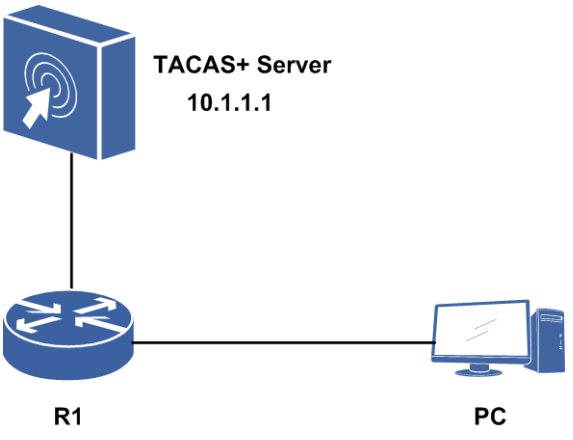
/*创建用户*/
R1(config-system-user)#user-name Inspur
R1(config-system-user-username)#bind authentication-template 1
R1(config-system-user-username)#bind authorization-templat 1
R1(config-system-user-username)#password Inspur
R1(config-system-user-username)#exit
R1(config-system-user)#exit
```

1.5.4 TACACS+认证授权用户配置实例

配置说明

如*图 1-16*所示，PC通过串口或者telnet等方式登录路由器，进入配置模式，创建一个TACACS+认证方式的用户。

图 1-16 配置 TACACS+认证授权



配置思路

1.配置TACACS+。

2.配置认证模板。

3.配置授权模板。

4.创建用户，绑定认证模板和授权模板。

配置过程

```
R1(config)#tacacs enable
R1(config)#tacacs-server host 10.1.1.1 key Inspur
R1(config)#tacplus group-server Inspurgroup
R1(config-sg)#server 10.1.1.1
R1(config-sg)#exit

R1(config)#aaa-authentication-template 2001
R1(config-aaa-authen-template)#aaa-authentication-type tacacs
R1(config-aaa-authen-template)#authentication-tacacs-group Inspurgroup
R1(config-aaa-authen-template)#exit

R1(config)#aaa-authorization-template 2001
R1(config-aaa-author-template)#aaa-authorization-type tacacs
R1(config-aaa-author-template)#authorization-tacacs-group Inspurgroup
R1(config-aaa-author-template)#exit

R1(config)#system-user
R1(config-system-user)#authentication-template 1
R1(config-system-user-authen-temp)#bind aaa-authentication-template 2001
R1(config-system-user-authen-temp)#exit

R1(config-system-user)#authorization-template 1
R1(config-system-user-author-temp)#bind aaa-authorization-template 2001
R1(config-system-user-author-temp)#local-privilege-level 15
R1(config-system-user-author-temp)#exit

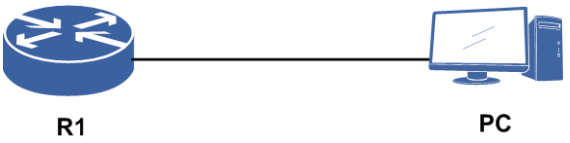
R1(config-system-user)#user-name Inspur
R1(config-system-user-username)#bind authentication-template 1
R1(config-system-user-username)#bind authorization-templat 1
R1(config-system-user-username)#password Inspur
R1(config-system-user-username)#exit
R1(config-system-user)#exit
```

1.5.5 密码恢复配置实例

配置说明

如*图 1-17*所示，PC通过串口或者telnet等方式登录路由器，进入配置模式，创建一个认证用户。配置密码恢复信息时，任意认证方式的用户均可以配置，但密码恢复生效，仅本地认证用户生效。

图 1-17 密码恢复配置实例组网图



配置思路

1.配置认证模板。

2.配置授权模板。

3.创建用户。

4.设置密码提示问题和答案。

5.登录时，恢复密码。

配置过程

路由器上配置如下：

```
R1(config)#aaa-authentication-template 2001
R1(config-aaa-authen-template)#aaa-authentication-type local
R1(config-aaa-authen-template)#exit
R1(config)#aaa-authorization-template 2001
R1(config-aaa-author-template)#aaa-authorization-type none
R1(config-aaa-author-template)#exit

R1(config)#system-user
R1(config-system-user)#authentication-template 1
R1(config-system-user-authen-temp)#bind aaa-authentication-template 2001
R1(config-system-user-authen-temp)#exit
R1(config-system-user)#authorization-template 1
R1(config-system-user-author-temp)#bind aaa-authorization-template 2001
R1(config-system-user-author-temp)#local-privilege-level 15
R1(config-system-user-author-temp)#exit

R1(config-system-user)#user-name who
R1(config-system-user-username)#bind authentication-template 1
R1(config-system-user-username)#bind authorization-templat 1
R1(config-system-user-username)#password who
R1(config-system-user-username)#password-recover-remind
password is:***
question: who are you
answer:who
R1(config-system-user-username)#

/*Telnet登录设备，使用密码提示问题，重设密码*/
R1#login
Username:recover-user who
question: who are you
answer:   /*输入的答案不显示在屏幕上*/
Please input your new password:
Re-enter New password:
The password has been changed successfully,
please remember your new password!
Username:who
Password:
R1#
```

提示：

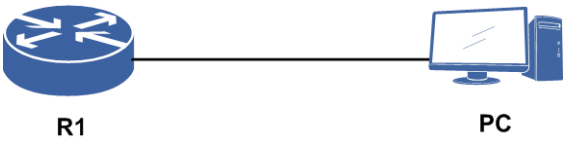
输入密码提示问题正确后，用户who的密码重新配置为新的密码。

1.5.6 OAM 安全管理配置实例

配置说明

如*图 1-18*所示，PC通过串口或者telnet等方式登录路由器，进入配置模式，创建一个认证用户。为了防止用户密码被破解或盗用，IR12000支持对密码强度进行设定，增强密码的安全性。对于连续认证失败的用户进行锁定，在一定时间范围内不再允许其进行登录认证，防止登录者进行多次密码破解尝试。

图 1-18 配置 OAM 安全管理组网图



配置思路

1.配置密码强度。

2.创建用户，密码强度符合要求才能创建成功。

3.配置认证模板。

4.配置授权模板。

5.配置用户连续认证失败次数和锁定时间值。

6.用户登录时连续认证失败，达到设定的次数后用户被锁定。

配置过程

路由器上配置如下：

```
R1(config)#system-user
R1(config-system-user)#strong-password length 6 character special-character
/*配置密码最小长度为6字符，密码强度的字符组合方式中需包含特殊符号*/
R1(config-system-user)#user-name Inspur
R1(config-system-user-username)#bind authentication-template 1
R1(config-system-user-username)#bind authorization-templat 1
R1(config-system-user-username)#password Inspur123*
R1(config-system-user-username)#exit

R1(config-system-user)#authentication-template 1
R1(config-system-user-authen-temp)#bind aaa-authentication-template 2001
R1(config-system-user-authen-temp)#exit
R1(config-system-user)#authorization-template 1
R1(config-system-user-author-temp)#bind aaa-authorization-template 2001
R1(config-system-user-author-temp)#local-privilege-level 15
R1(config-system-user-author-temp)#exit
```

```
R1(config-system-user)#user-authen-restriction fail-time 3 lock-minute 2
/*配置用户连续认证失败次数3将锁定2分钟*/
R1(config-system-user)#exit

R1(config)#aaa-authentication-template 2001
R1(config-aaa-authen-template)#aaa-authentication-type local
R1(config-aaa-authen-template)#exit
R1(config)#aaa-authorization-template 2001
R1(config-aaa-author-template)#aaa-authorization-type none
R1(config-aaa-author-template)#exit

/*Telnet登录设备，连续认证失败达到设定的次数，用户被锁定*/
R1#login
Username:Inspur
Password:
% Local password error!

Username:Inspur
Password:
% Local password error!

Username:Inspur
Password:
% Local password error!
Still logged in as "who"   /*原先登录的用户为who*/
R1#login
Username:Inspur
Password:
% User is locked

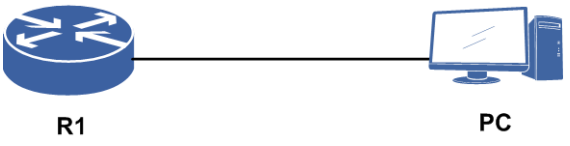
R1#show authen-restriction  userinfo
Username        Failed-time          State        Remain (minute)
Inspur             3                  locked           1
```

1.5.7 密码有效期配置实例

配置说明

如*图 1-19*所示，PC通过串口或者telnet等方式登录路由器，进入配置模式，创建一个用户，默认该账户密码是不会过期的。可以通过配置命令指定该账户的有效期，设备允许的配置是90-360天，通过修改系统时间来测试有效期是否有效。

图 1-19 配置密码有效期组网图



配置思路

1.创建用户。

2.配置认证模板。

3.配置授权模板。

4.设置密码的有效期。

5.修改系统时间，测试有效期是否有效。

配置过程

路由器上配置如下：

```
R1(config)#system-user
R1(config-system-user)#authentication-template 1
R1(config-system-user-authen-temp)#bind aaa-authentication-template 2001
R1(config-system-user-authen-temp)#exit
R1(config-system-user)#authorization-template 1
R1(config-system-user-author-temp)#bind aaa-authorization-template 2001
R1(config-system-user-author-temp)#local-privilege-level 15
R1(config-system-user-author-temp)#exit
R1(config-system-user)#user-name Inspur
R1(config-system-user-username)#bind authentication-template 1
R1(config-system-user-username)#bind authorization-templat 1
R1(config-system-user-username)#password Inspur
R1(config-system-user-username)#password-duration 90  /*配置用户密码有效期*/
R1(config-system-user-username)#exit
R1(config-system-user)#exit

R1(config)#aaa-authentication-template 2001
R1(config-aaa-authen-template)#aaa-authentication-type local
R1(config-aaa-authen-template)#exit
R1(config)#aaa-authorization-template 2001
R1(config-aaa-author-template)#aaa-authorization-type none
R1(config-aaa-author-template)#end
```

配置验证

```
R1#show username
Username    Encrypted-Password      AuthenNo. AuthorNo. AgingTime Set-Time
Inspur        ce7c04930c52bfe1669f6c22 1        1         89      2012-6-28
           9ef61b761ec847e5b3052bdb
           51456385bb2a9a57

/*修改系统时间至密码超过有效期*/
R1#show clock
17:37:48 UTC Thu Jun 28 2012   /*当前时间*/
R1#clock set 15:10:39 9-20-2013  /*修改系统时间至密码超过有效期*/

R1#show username  /*修改系统时间后显示密码过期expired*/
Username    Encrypted-Password      AuthenNo. AuthorNo. AgingTime Set-Time
Inspur        ce7c04930c52bfe1669f6c22 1        1         expired   2012-6-28
           9ef61b761ec847e5b3052bdb
           51456385bb2a9a57

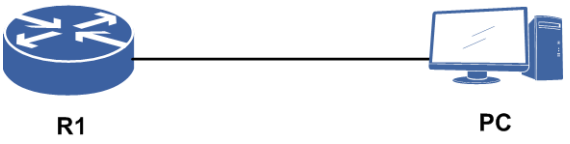
R1#login
Username:Inspur
Password:
% User password expired   /*密码过期，用户无法登录设备*/
```

1.5.8 首次登录修改密码配置实例

配置说明

如*图 1-20*所示，PC通过串口或者telnet等方式登录路由器，进入配置模式，创建一个用户，配置once-password（只对本地认证的用户有效），该用户下次登录时可以使用自己配置的密码，新密码默认长度为3-32个字符。

图 1-20 配置首次登录修改密码组网图



配置思路

1.创建用户。

2.配置认证模板。

3.配置授权模板。

4.配置首次登录修改密码功能。

5.用户登录，可以自己设置密码；下次登录时，可以使用自己配置的新密码登录成功。

配置过程

路由器上配置如下：

```
R1(config)#system-user
R1(config-system-user)#authentication-template 1
R1(config-system-user-authen-temp)#bind aaa-authentication-template 2001
R1(config-system-user-authen-temp)#exit
R1(config-system-user)#authorization-template 1
R1(config-system-user-author-temp)#bind aaa-authorization-template 2001
R1(config-system-user-author-temp)#local-privilege-level 15
R1(config-system-user-author-temp)#exit
R1(config-system-user)#user-name Inspur
R1(config-system-user-username)#bind authentication-template 1
R1(config-system-user-username)#bind authorization-template 1
R1(config-system-user-username)#password Inspur
R1(config-system-user-username)#once-password  /*配置首次登录修改密码*/
R1(config-system-user-username)#exit
R1(config-system-user)#exit

R1(config)#aaa-authentication-template 2001
R1(config-aaa-authen-template)#aaa-authentication-type local
R1(config-aaa-authen-template)#exit
R1(config)#aaa-authorization-template 2001
R1(config-aaa-author-template)#aaa-authorization-type none
R1(config-aaa-author-template)#end
```

配置验证

```
R1#login
Username:Inspur
Password:
Your password has expired.
Enter a new one now.
New password:    /*配置新密码，密码不会显示在屏幕上*/
Re-enter new password:    /*确认新密码，密码不会显示在屏幕上*/
The password has been changed successfully,
Please remember your new password!

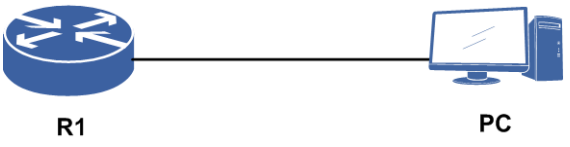
R1#login
Username:Inspur
Password:   /*输入新密码*/
R1#    /*用户登录成功*/
R1#who
   Line      User        Host(s)            Idle       Location
   66 vty 0  who         idle               00:01:17    169.1.1.13
 * 67 vty 1  Inspur         idle               00:00:00    169.1.1.13
   68 vty 2  who         idle               00:00:00    169.1.1.10
```

1.5.9 用户权限配置实例

配置说明

如*图 1-21*所示，PC通过串口或者telnet等方式登录路由器，进入配置模式，创建一个用户，授予一个权限级别。当授予的权限级别较低，想要提升至最高级别时，就需要使用**enable**命令。默认enable认证方式为本地，默认的密码为"inspur"。

图 1-21 用户权限配置实例组网图



配置思路

1.创建用户。

2.配置认证模板。

3.配置授权模板。

4.设置enable密码提升用户权限。

配置过程

路由器上配置如下：

```
R1(config)#tacacs enable
R1(config)#tacacs-server host 10.1.1.1 key Inspur
```

```
R1(config)#tacplus group-server Inspurgroup
R1(config-sg)#server 10.1.1.1
R1(config-sg)#exit

R1(config)#system-user
R1(config-system-user)#authentication-template 1
R1(config-system-user-authen-temp)#bind aaa-authentication-template 2001
R1(config-system-user-authen-temp)#exit
R1(config-system-user)#authorization-template 1
R1(config-system-user-author-temp)#bind aaa-authorization-template 2001
R1(config-system-user-author-temp)#local-privilege-level 5
R1(config-system-user-author-temp)#exit
R1(config-system-user)#user-name Inspur
R1(config-system-user-username)#bind authentication-template 1
R1(config-system-user-username)#bind authorization-template 1
R1(config-system-user-username)#password Inspur
R1(config-system-user-username)#exit
R1(config-system-user)#exit

R1(config)#aaa-authentication-template 2001
R1(config-aaa-authen-template)#aaa-authentication-type tacacs-local
R1(config-aaa-authen-template)#authentication-tacacs-group Inspurgroup
R1(config-aaa-authen-template)#exit

R1(config)#aaa-authorization-template 2001
R1(config-aaa-author-template)#aaa-authorization-type none
R1(config-aaa-author-template)#exit
```

本例中介绍一种全局的enable认证配置方式，可以指定为aaa方式或者local方式，aaa方式就是使用服务器设置的enable密码。

```
R1(config)#system-user
R1(config-system-user)#global-enable-type aaa authentication-template 1
/*配置用户的enable命令认证方式*/
R1(config-system-user)#exit
```

配置enable密码提升用户权限至最高级别，还有以下方式：

- 在全局配置模式下，通过**enable secret level** 命令，具体参见配置命令权限。
- 在全局配置模式下，通过**nvram enable-password** 命令，具体参见*《IR12000初始配置》*中的“设置NVRAM中保存的配置信息”。

对于NVRAM下配置的enable密码，可以配置密码恢复功能：

```
R1(config)#enable secret recover-remind
password:*****
question:Inspur
answer:Inspur
/*当忘记enable的本地密码时，可在1级权限下使用recover-enable命令恢复成默认密码*/
R1>recover-enable
question:Inspur
answer:***
%Info 40449: Recover-enable ok! New enable password is: inspur.
```

配置验证

AAA服务器上配置相应的enable密码，用户正常登录，通过验证即可提升权限级别。

1.6 命令权限分级

IR12000支持命令权限分级功能，命令权限分级管理主要是对命令的权限进行配置，对不同的命令可以设置不同的权限级别。

用户登录后，根据用户的不同权限显示不同的命令视图，低级别的用户不能使用高级别的命令。

1.6.1 配置命令权限

本节介绍命令权限功能的配置步骤和命令。

1.配置命令权限。

命令	功能
inspur(config)#**privilege** <*logic-mode*>[**all**] **level** {<*level*>| **default**}<*command-keywords*>	配置命令的权限级别
inspur(config)#**no privilege** <*logic-mode*>[**all**] **node** <*command-keywords*>	恢复默认的权限级别

[**all**]：支持该命令关键字打头的所有后续命令。

level <*level*>：权限等级，范围1~15。

default：命令的默认权限级别。

<*command-keywords*>：命令关键字，范围为1~200个字符。

2.验证配置结果。

命令	功能
inspur#**show privilege** [{**cur-mode**	**show-mode**}{**detail**	**level** < *level*>| **node** <*command-keywords*>}]	查看当前终端的权限级别或命令权限的配置信息

cur-mode ：显示当前命令模式的权限信息。

show-mode：显示show命令模式的权限信息。

detail：显示所有命令的权限级别。

level <*level*>：显示指定权限级别的命令，范围1~18。

<*command-keywords*>：显示指定命令的权限级别，范围为1~200个字符。

用户模式下的**show privilege**命令不带参数，用于查看当前终端的权限级别。

1.6.2 命令权限分级配置实例

配置说明

给操作设备的A类和B类用户设置不同的使用权限：A类用户的权限级别为15级，能够进行查看、配置等所有操作；B类用户的权限级别为5级。

修改**show clock**命令的权限级别，使B类用户需要能够使用**show clock**命令来查看设备系统时钟。通过**enable**命令提高B类用户权限级别至8级，从而可以进行时区设置。

配置思路

1.修改设备上**show clock**命令的权限级别，使其低于或者等于5级。本例中将**show clock**命令的权限级别设置为5级。

2.修改设备上**clock timezone**命令的权限级别，使其低于或者等于8级，但高于5级。本例中将**clock timezone**命令的权限级别设置为7级。

3.创建A、B类两用户，用户名分别为Inspur_A、Inspur_B，用户权限级别分别为15级和5级。

4.设置将用户权限级别提高到8级时的enable密码。

配置过程

IR12000设备上的配置如下：

```
inspur(config)#privilege show all level 5 show clock
/*show clock命令权限级别的配置信息*/

inspur(config)#privilege configure level 7 clock
inspur(config)#privilege configure level 7 clock timezone
/*clock timezone命令权限级别的配置信息*/

inspur(config)#system-user
inspur(config-system-user)#authentication-template 1
inspur(config-system-user-authen-temp)#bind     aaa-authentication-template
2001
inspur(config-system-user-authen-temp)#exit
inspur(config-system-user)#authorization-template 1
inspur(config-system-user-author-temp)#bind aaa-authorization-template 2001
inspur(config-system-user-author-temp)#local-privilege-level 15
inspur(config-system-user-author-temp)#exit
inspur(config-system-user)#user-name Inspur_A
inspur(config-system-user-username)#bind authentication-template 1
inspur(config-system-user-username)#bind authorization-templat 1
inspur(config-system-user-username)#password Inspur_A_15
inspur(config-system-user-username)#exit
/*用户Inspur_A用户创建、权限级别的配置信息*/

inspur(config-system-user)#authentication-template 2
inspur(config-system-user-authen-temp)#bind     aaa-authentication-template
2002
inspur(config-system-user-authen-temp)#exit
inspur(config-system-user)#authorization-template 2
inspur(config-system-user-author-temp)#bind aaa-authorization-template 2002
inspur(config-system-user-author-temp)#local-privilege-level 5
```

```
inspur(config-system-user-author-temp)#exit
inspur(config-system-user)#user-name Inspur_B
inspur(config-system-user-username)#bind authentication-template 2
inspur(config-system-user-username)#bind authorization-templat 2
inspur(config-system-user-username)#password Inspur_B_5
inspur(config-system-user-username)#exit
inspur(config-system-user)#exit
/*用户Inspur_B用户创建、权限级别的配置信息*/

inspur(config)#aaa-authentication-template 2001
inspur(config-aaa-authen-template)#aaa-authentication-type local
inspur(config-aaa-authen-template)#exit
inspur(config)#aaa-authorization-template 2001
inspur(config-aaa-author-template)#aaa-authorization-type radius-local
inspur(config-aaa-author-template)#exit
/*用户Inspur_A对应的认证、授权模板配置信息*/

inspur(config)#aaa-authentication-template 2002
inspur(config-aaa-authen-template)#aaa-authentication-type local
inspur(config-aaa-authen-template)#exit
inspur(config)#aaa-authorization-template 2002
inspur(config-aaa-author-template)#aaa-authorization-type radius-local
inspur(config-aaa-author-template)#exit
/*用户Inspur_B对应的认证、授权模板配置信息*/

inspur(config)#enable secret level 8 level-8
/*设置用户登录权限级别为8的密码*/
```

配置验证

查看用户名Inspur_A的使用权限：

```
Username:Inspur_A
Password:
inspur#show privilege
Current privilege level is 15
/*表明用户Inspur_A权限级别为15级*/

inspur#?
/*显示用户Inspur_A在特权配置模式下能够操作的命令*/
Exec commands:
  alarm-confirm  Confirm the alarm by flowid
  cd             Change current directory
  cfm            Executing CFM detecting functions
  clear          Reset functions
  clock          Manage the system clock
  commit         Commit the configuration
  configure      Enter configuration mode
  copy           Copy from one file to another by ftp/tftp
  cp             Copy from one file to another locally
  debug          Debugging functions
  delete         Delete a file
--More—

inspur#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
inspur(config)#?
/*显示用户Inspur_A在全局配置模式下能够操作的命令*/
Configure commands:
  aaa-accounting-template     AAA accounting template configurations
  aaa-authentication-template  AAA authentication template configurations
  aaa-authorization-template   AAA authorization template configurations
  alarm                       Configure the alarm parameters
  alarm-mask                   Configure the alarm-mask parameters
  aps                         Configure APS instance
  arp                         Enter ARP configuration mode
```

```
  banner                    Terminal line banner
  bfd                       Configure bfd
  cfm                       Enter CFM configuration mode
  check                     Configure intervals of check
  class-map                  Configure H-QoS class map
  clock                     Configure board clock
--More—
```

查看用户名Inspur_B的使用权限：

```
Username:Inspur_B
Password:
inspur#show privilege
Current privilege level is 5
/*表明用户Inspur_B权限级别为5级*/

inspur#?
/*显示用户Inspur_B在特权配置模式下能够操作的命令*/
Exec commands:
  cd          Change current directory
 cfm Executing CFM detecting functions
  clock       Manage the system clock
  configure    Enter configuration mode
  debug       Debugging functions
  dir         List files on a filesystem
  disable      Turn off privileged commands
  enable       Turn on privileged commands
  exit        Exit from the EXEC
--More—

inspur#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
inspur(config)#?
/*显示用户Inspur_B在全局配置模式下能够操作的命令*/
Configure commands:
  end    Exit from configure mode
  exit   Exit from configure mode
  ping    Send echo messages
  ping6   Send IPv6 echo messages
  show   Show running system information
  trace   Trace route to destination
  trace6  Trace route to destination using IPv6
inspur(config)#
inspur(config)#show ?
  clock     Show current system clock
  privilege  Show current privilege level
```

将用户名Inspur_B的权限级别提升至8级：

```
Username:Inspur_B
Password:
inspur#show privilege
Current privilege level is 5
/*表明用户Inspur_B权限级别为5级*/

inspur#enable 8
Password:
inspur#show privilege
Current privilege level is 8
/*表明用户Inspur_B权限级别已提升至8级*/

inspur#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
inspur(config)#?
Configure commands:
  clock  Configure board clock
  /*表明用户Inspur_B能够操作的命令中增加了clock*/
  end    Exit from configure mode
```

```
  exit   Exit from configure mode
  ping    Send echo messages
  ping6   Send IPv6 echo messages
  show   Show running system information
  trace   Trace route to destination
  trace6  Trace route to destination using IPv6
inspur(config)#clock ?
  timezone  Configure time zone
```

查看设备上的配置情况：

```
inspur#enable  /*将用户的权限级别提高到默认级别15级*/
Password:    /*输入密码不会显示在屏幕上*/
inspur#show running-config adm-mgr
!<adm-mgr>
enable secret level 8 5 52ZJX4aBmmYKbWdVFpSvwg==
system-user
  authentication-template 1
    bind aaa-authentication-template 2001
  $
  authentication-template 2
    bind aaa-authentication-template 2002
  $
  authorization-template 1
    bind aaa-authorization-template 2001
    local-privilege-level 15
  $
  authorization-template 2
    bind aaa-authorization-template 2002
    local-privilege-level 5
  $
  username Inspur_A
    bind authentication-template 1
    bind authorization-template 1
    password encrypted 51213031a28daa4a18e939b9cc83732043f467d88315721af06
6dc4f1c385a28
  $
  username Inspur_B
    bind authentication-template 2
    bind authorization-template 2
    password encrypted a5e686cd3e6778917691bb099a4da1d79768a6b9752b942fe5b
431ec3fff8468
  $
$
!</adm-mgr>
inspur#show running-config aaa
!<aaa>
aaa-authentication-template 2001
  aaa-authentication-type local
$
aaa-authentication-template 2002
  aaa-authentication-type local
$
aaa-authorization-template 2001
  aaa-authorization-type radius-local
$
aaa-authorization-template 2002
  aaa-authorization-type radius-local
$
!</aaa>
inspur#show running-config oam
!<oam>
privilege show all level 5 show clock
privilege configure level 7 clock
privilege configure level 7 clock timezone
!</oam>
```

1.7 SNMP

SNMP协议处于整个路由器系统的最高层，属于TCP/IP协议栈的应用层范围，是管理员操作、控制、维护路由器的主要途径之一。用户可以利用NMS软件在管理站和被管网元间通过发送和接收SNMP报文进行网络管理。

SNMPv1/v2协议定义的安全策略比较简单，使用明文传送团体串。团体串是SNMP协议管理进程和代理进程之间的口令，攻击者采用暴力攻击的方法能破解该口令。SNMP的防暴力攻击功能就是用来防御DoS攻击和暴力破解攻击的。

1.7.1 配置 SNMP

本节介绍通过SNMP协议管理设备时，SNMP的配置步骤和命令。

1.使能SNMP的v1、v2c、v3版本。

命令	功能
inspur(config)#**snmp-server version** {**v1** | **v2c** | **v3**} **enable**	分别打开v1、v2c和v3版本SNMP与client端收发报文的开关，有两种状态：**enable**与**disable**，默认状态为**disable**

2.设置SNMP报文共同体。

命令	功能
inspur(config)#**snmp-server community** {**encrypted** <*encrypted-para*>|<*unencrypted-para*>[**showclear**]}[**view** <*view-name*>][{**ro** | **rw**}][{[**ipv4-access-list** <*ipv4_acl_name*>],[**ipv6-access-list** <*ipv6_acl_name*>]}]	设置SNMP报文团体串

<*encrypted-para*>：密文团体串，64个字符长度。

<*unencrypted-para*>： 明文团体串，1~32个字符。

showclear：配置该字段，显示团体串时用明文显示，不配置该字段为密文显示。

<*view-name*>：视图名，1~32个字符。

ro | **rw**：**ro**表明对MIB对象进行只读访问，**rw**表明对MIB对象进行读写访问。

3.定义SNMP视图。

命令	功能
inspur(config)#**snmp-server view** <*view-name*><*subtree-id*>{**included** | **excluded**}	定义SNMP的视图

<*subtree-id*>：为视图名指定MIB子树ID或MIB子树的节点名，长度为1~79个字符 。

included | **excluded**：指定包括或排除该子树。

4.设置MIB对象的信息。

命令	功能
inspur(config)#**contact** <*mib-syscontact-text*>	设置MIB对象的系统负责人联系方式，长度不超过200个字符
inspur(config)#**location** <*mib-syslocation-text*>	设置MIB对象的系统所在位置的描述信息，长度不超过200个字符

5.设置允许发送的TRAP/INFORM的类型。

命令	功能
inspur(config)#**snmp-server enable inform** [<*notification-type*>]	打开代理发送通知的开关并设置代理能发送的通知类型，类型可以是bgp，ospf，rmon，snmp，stalarm，vpn全部或者其中之一
inspur(config)#**snmp-server enable trap** [<*trap-type*>]	打开代理发送trap的开关并设置代理能发送的trap类型，类型可以是bgp，ospf，rmon，snmp，stalarm，vpn全部或者其中之一

6.设置TRAP的目的主机。

命令	功能
inspur(config)#**snmp-server host** [**vrf** <*vrf-name*>]<*ip-address*>[**trap** | **inform**] **version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}<*community-name/user*>[**udp-port** <*udp-port*>][<*trap-type*>]	设置接收SNMP通知的目的地，**snmp-server host**命令需要与**snmp-server enable**命令协同使用

vrf <*vrf-name*>：VRF名称，长度为1~32个字符。

<*ip-address*>：指定主机的IP地址，支持IPv4和IPv6 。

trap | **inform**：指定发送陷阱/通知到主机。

version 1 | **2c** | **3** ：SNMP版本号为v1、或v2c、或v3。

auth：对发送的报文进行认证但不加密。

noauth：发送的报文不进行认证和加密。

priv：发送的报文进行认证和加密。

<*community-name/user-name*>：v1/v2的团体串名或SNMPv3用户名，长度为1~32个字符。

udp-port <*udp-port*>：指定发送trap或inform的UDP端口号，1~65535。

<*trap-type*>：陷阱或通知类型，可以是bgp，ospf，rmon，snmp，stalarm，vpn等全部或者其中之一。

7.打开系统日志功能。

命令	功能
inspur(config)#**logging on**	打开系统日志功能

8.设置告警消息发送到TRAP服务器的告警消息严重级别。

命令	功能
inspur(config)#**logging trap-enable** <*alarmlevel*>	设置发送到trap服务器的告警消息的严重级别

9.配置SNMP其它参数。

命令	功能
inspur(config)#**snmp-server engine-id** <*engine-id*>	设置SNMP的本地引擎ID。SNMP引擎是SNMP实体中的核心部分，完成SNMP消息的收发验证，提取PDU组装消息，与SNMP 应用程序通信等功能 本地引擎ID长度为1~24个字符，缺省为830900020300010289d64401，必须用16进制数字表示
inspur(config)#**snmp-server input-limit** <*packets*>	设置SNMP接收报文速率，参数范围：100~1000，默认是200包/秒
inspur(config)#**snmp-server packetsize** <*snmp-packet-max-size*>	设置SNMP最大报文长度，单位：字节，取值范围484~8192，默认值8192
inspur(config)#**snmp-server trap-source** <*ip-address*>	配置所有TRAPS的源IP地址
inspur(config)#**snmp-server access-list** {**ipv4**| **ipv6**}< *acl-name*>	应用已配置的ACL来控制通过SNMP协议访问系统的主机地址

10.配置SNMPv3。

步骤	命令	功能
1	inspur(config)#**snmp-server context** <*context-name*>	定义SNMPv3上下文名称，长度为1~30个字符
2	inspur(config)#**snmp-server group** <*groupname*> **v3** {**auth** | **noauth**|**priv**}[**context** <*context-name*>{**match-prefix** | **match-exact**}][**read** <*readview*>][**write** <*writeview*>][**notify** <*notifyview*>]	配置一个新的SNMP组，即将SNMP用户映射到SNMP视图
3	inspur(config)#**snmp-server user** <*user-name*><*group-name*> **v3** {**encrypted** **auth** {**md5** | **sha**}<*auth-key*>[**priv des56** |<*privacy-key*>][**auth** {**md5** | **sha**}|<*auth-password*>|[**priv des56** |<*privacy-password*>]]}	配置SNMPv3用户

group <*groupname*>：配置的SNMPv3组名，长度为1~32个字符。

v3：指定该组用于SNMPv3版本。

auth：指明对报文进行认证但不加密。

noauth：指明对报文不进行认证和加密。

priv：指明对报文进行认证和加密。

<*context-name*>：指定该组所属的上下文，长度为1~30字符。

match-prefix：指明上下文匹配模式为前缀匹配。

match-exact：指明上下文匹配模式为精确匹配。

read <*readview*>：指定读视图，长度为1~32个字符。

write <*writeview*>：指定写视图，长度为1~32个字符。

notify <*notifyview*>：指定通知视图，长度为1~32个字符。

user <*username*>：SNMP用户名，长度为1~32个字符。

<*groupname*>：用户关联的组名，长度为1~32个字符。

v3：指定该用户用于SNMPv3版本。

encrypted：指定后面输入的不是口令原文而是经过处理的密钥，建议用户不要随便使用该选项。

md5 | sha：使用HMAC-MD5-96或HMAC-SHA-96作为认证方式。

<*auth-key*>：认证口令或认证密钥，长度为1~32字符，如果是加密口令，长度是32~40字符。

des56：使用CBC-DES作为加密方式。

<*privacy-key*>：密文加密口令，长度为1~32字符。

<*auth-password*>：认证口令（或认证密钥），长度为1~32字符，如果是加密口令，长度是32~40字符。

<*privacy-password*>：明文加密口令，长度为1~32字符。

11.验证配置结果。

命令	功能
inspur#**show snmp**	查看SNMP的状态属性值
inspur#**show snmp config**	查看能配置的SNMP的状态属性值
inspur#**show snmp engine-id**	显示SNMP的本地引擎ID
inspur#**sshow snmp group**	显示SNMP配置的组
inspur#**show snmp security**	显示SNMP当前安全性的相关配置信息
inspur#**show snmp security failures**	显示SNMP检测模式下错误的community尝试登录的IP以及尝试次数
inspur#**show snmp security trust-users**	显示SNMP学习到的动态信任用户以及手工配置的静态信任用户

命令	功能
inspur#**show snmp user**	显示SNMP配置的用户
inspur#**show running-config snmp** [|{**begin** | **exclude** | **include**}<*line*>]	显示SNMP的配置

1.7.2 配置 SNMP 防暴力攻击

本节介绍实现SNMP的防暴力攻击功能的配置步骤和命令。

1.激活SNMP安全功能。

命令	功能
inspur(config)#**snmp-server security block** < *block-seconds*><*detect-tries*>< *detect-seconds*>[**when** <*tries*><*startup-seconds*>]	SNMP安全防护功能默认是不启用的，该命令用来激活SNMP安全功能

block <*block-seconds*>：阻塞时间（安静期的时长），单位：秒，范围1~65535。

<*detect-tries*>：监测模式的最大失败尝试次数，单位：次数，范围1~65535。

<*detect-seconds*>：监测模式的最大检测时间，单位：秒，范围1~65535。

<*tries*>：正常模式的最大失败尝试次数，单位：次数，范围1~65535，默认为50。

<*startup-seconds*>：正常模式的最大检测时间，单位：秒，范围1~65535，默认60。

2.配置通过SNMP协议访问主机的ACL。

命令	功能
inspur(config)#**snmp-server access-list** { **ipv4**| **ipv6**}<*acl-name*>	应用已配置的ACL来控制通过SNMP协议访问系统的主机地址

3.配置动态信任用户的老化时间以及手工配置静态信任用户。

步骤	命令	功能
1	inspur(config)#**snmp-server security dynamic-trust-user idle-timeout** <*timeout-seconds*>	配置动态信任用户的老化时间，单位：秒，范围1~65535，默认值是1800秒
2	inspur(config)#**snmp-server security static-trust-user** <*static-ip-addr*>	手工配置静态信任用户

4.配置团体串尝试失败或状态转换时生成日志信息和trap消息。

命令	功能

命令	功能
inspur(config)#**snmp-server security on-failure log** [**and trap**]	配置在有团体串尝试失败或状态转换时生成日志信息和trap消息

5.验证配置结果。

命令	功能
inspur#**show snmp security** [**failures** | **trust-users**]	查询SNMP安全功能参数。该命令主要以自然语言的方式显示SNMP安全的状态、配置信息和当前的状态信息、统计信息
inspur#**show running-config snmp** [|{**begin** | **exclude** | **include**}<*line*>]	显示SNMP的配置

failures为可选项，选择该参数时，命令功能为查询失败尝试的详细信息。

trust-users为可选项，选择该参数时，命令功能为查询信任用户的详细信息，包括动态学习和手工配置的。

begin：显示以输入字符串行开头的配置信息。

include：显示包含字符串行的相关配置信息。

exclude：显示去除字符串行相关配置信息之后的其它信息

<*line*>：用于匹配筛选的字符串行。

6.维护SNMP防暴力攻击。

命令	功能
inspur(config)#**snmp-server security dynamic-trust-user clear** <*dyn-ip-addr*>	手工清除动态信任用户

1.7.3 SNMP 配置实例

配置说明

通过配置SNMP功能，用户可以使用一台网管服务器来管理网络中的设备，如*图 1-22*所示。

图 1-22 SNMP 配置实例拓扑图



配置思路

1.设置SNMP报文团体串，SNMPv1/v2c采用团体串认证方式，SNMP团体串由字符串命名，不同的团体串具有只读（read-only）或读写（read-write）访问权限。

2.为配置的团体串指定视图名。当不配置**view**时，将为团体串指定默认视图（DefaultView）；当不配置**ro | rw**时，将为团体串指定默认权限ro。无论是只读还是读写，其范围都受到视图**view**的限制，只能在允许的视图范围内进行操作。

3.设置告警trap，设置允许发送的trap类型和发送的目的主机，trap是被管理设备主动向NMS上报的信息，用于报告一些紧急的重要事件。缺省配置是能发送所有类型的trap。

配置过程

路由器上的配置如下：

```
R1(config)#snmp-server version v2c enable
R1(config)#location No.1036,Langchao Road,High Technology Zone,Jinan,Shandong
R1(config)#contact +86-25-52870000
R1(config)#snmp-server packetsize 1400
R1(config)#snmp-server engine-id 830900020300010289d64401
R1(config)#snmp-server community public view AllView ro
R1(config)#snmp-server host 61.139.48.18 inform version 2c public udp-port 162
snmp
R1(config)#snmp-server host 61.139.48.18 trap version 2c public udp-port 162
R1(config)#snmp-server enable trap
R1(config)#snmp-server enable inform
R1(config)#logging on
R1(config)#logging trap-enable warnings
```

配置验证

配置完成后用**show**命令检验配置：

```
R1(config)#show snmp config

snmp-server community encrypted
d6ddeaa4dab74523b246fe346c94c31ae58b79ad4776396438ea1e9bb01a9ef3
 view AllView ro
snmp-server enable inform snmp
snmp-server enable inform bgp
snmp-server enable inform mac
snmp-server enable inform ospf
snmp-server enable inform stp
snmp-server enable inform ppp
snmp-server enable inform arp
snmp-server enable inform rmon
snmp-server enable inform udld
snmp-server enable inform cfm
snmp-server enable inform efm
snmp-server enable inform lacp
snmp-server enable inform mc-elam
snmp-server enable inform tcp
snmp-server enable inform sctp
snmp-server enable inform stalarm
snmp-server enable inform cps
snmp-server enable inform interface
snmp-server enable inform acl
snmp-server enable inform fib
```

```
snmp-server enable inform pim
snmp-server enable inform isis
snmp-server enable inform rip
snmp-server enable inform msdp
snmp-server enable inform aps
snmp-server enable inform config
snmp-server enable inform am
snmp-server enable inform um
snmp-server enable inform system
snmp-server enable inform ldp
snmp-server enable inform pwe3
snmp-server enable inform vpn
snmp-server enable inform mpls-oam
snmp-server enable inform ptp
snmp-server enable inform tunnel-te
snmp-server enable inform radius
snmp-server enable inform dhcp
snmp-server enable inform bfd
snmp-server enable inform ippool
snmp-server enable inform ntp
snmp-server enable inform ssm
snmp-server enable inform sqa
snmp-server enable inform ipsec
snmp-server enable inform cgn
snmp-server enable inform vrrp
snmp-server enable inform ftp_tftp
snmp-server enable inform ping-trace
snmp-server enable inform gm
snmp-server enable trap snmp
snmp-server enable trap bgp
snmp-server enable trap mac
snmp-server enable trap ospf
snmp-server enable trap stp
snmp-server enable trap ppp
snmp-server enable trap arp
snmp-server enable trap rmon
snmp-server enable trap udld
snmp-server enable trap cfm
snmp-server enable trap efm
snmp-server enable trap lacp
snmp-server enable trap mc-elam
snmp-server enable trap tcp
snmp-server enable trap sctp
snmp-server enable trap stalarm
snmp-server enable trap cps
snmp-server enable trap interface
snmp-server enable trap acl
snmp-server enable trap fib
snmp-server enable trap pim
snmp-server enable trap isis
snmp-server enable trap rip
snmp-server enable trap msdp
snmp-server enable trap aps
snmp-server enable trap config
snmp-server enable trap am
snmp-server enable trap um
snmp-server enable trap system
snmp-server enable trap ldp
snmp-server enable trap pwe3
snmp-server enable trap vpn
snmp-server enable trap mpls-oam
snmp-server enable trap ptp
snmp-server enable trap tunnel-te
snmp-server enable trap radius
snmp-server enable trap dhcp
snmp-server enable trap bfd
snmp-server enable trap ippool
snmp-server enable trap ntp
snmp-server enable trap ssm
snmp-server enable trap sqa
```

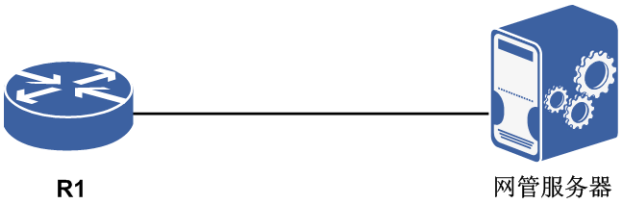
```
snmp-server enable trap ipsec
snmp-server enable trap cgn
snmp-server enable trap vrrp
snmp-server enable trap ftp_tftp
snmp-server enable trap ping-trace
snmp-server enable trap gm
snmp-server engine-id is 830900020300010289d64401
snmp-server host 61.139.48.18 trap version 2c public udp-port 162 snmp bgp mac
ospf stp ppp arp rmon udld cfm efm lacp mc-elam tcp sctp stalarm cps interface
 acl fib pim isis rip msdp aps config am um system ldp pwe3 vpn mpls-oam ptp
 tunnel-te radius dhcp bfd ippool ntp ssm sqa ipsec cgn vrrp ftp_tftp ping-trace
gm
snmp-server host 61.139.48.18 inform version 2c public udp-port 162 snmp
snmp-server packetsize is 1400
snmp-server view AllView internet included
snmp-server view DefaultView system included
snmp-server security dynamic-trust-user idle-timeout 1800
snmp-server version v2c enable
```

1.7.4 SNMP 防暴力攻击配置实例

配置说明

如*图 1-23*所示的配置实例为在路由器上配置SNMP防暴力攻击功能。

图 1-23 SNMP 防暴力攻击配置实例



配置思路

1.打开SNMP防暴力攻击功能开关。

2.配置动态信任用户的老化时间。

3.配置允许访问的静态信任用户。

4.配置用户尝试失败时以及状态切换时生成的trap消息和日志消息。

配置过程

R1上的配置如下：

```
R1(config)#snmp-server security block 180 3 180 when 50 60
R1(config)#snmp-server security dynamic-trust-user idle-timeout 100
R1(config)#snmp-server security static-trust-user 169.1.110.6
R1(config)#snmp-server security on-failure log and trap
```

配置验证

查看SNMP相关配置信息：

```
R1(config)#show running-config snmp
!<snmp>
snmp-server security block 180 3 180 when 50 60
snmp-server security dynamic-trust-user idle-timeout 100
snmp-server security on-failure log and trap
snmp-server security static-trust-user 169.1.110.6
!</snmp>
```

1.8 告警

告警模块在各个单板上都驻留有告警代理进程，在主控板上驻留有告警服务端进程。一旦硬件或者程序运行时发生了故障，那么各种业务应用就会向自己的告警代理上报告警消息，告警代理再将告警消息上报给告警服务端，告警服务端会对告警消息进行记录便于查询。

1.8.1 配置告警

本节介绍设备告警功能的配置步骤和命令。

1.配置告警基本功能。

步骤	命令	功能
1	inspur(config)#**logging on**	打开告警记录总开关，相应级别的告警可以上报给日志、控制终端、SNMP和SYSLOG
2	inspur(config)#**logging buffer** <*buffer-size*>	设置告警日志缓冲区的大小，单位是千字节，默认值是200，取值范围为100~1000
3	inspur(config)#**logging timestamps** [**datetime localtime** | **precisetime** | **uptime**]	设置告警的时间显示方式，默认是**datetime localtime**
4	inspur(config)#**logging level** <*level*>	设置记录告警日志的级别，告警级别高于或等于设定值的告警都会被记录日志，默认是INFORMATIONAL（7级）告警
5	inspur(config)#**logging console** <*level*>	设置console或telnet终端显示的告警级别，告警级别高于或等于设定值的告警都会被console或telnet终端显示 ，默认是NOTIFICATIONS（6级）告警
6	inspur(config)#**logging trap-enable** <*level*>	使能并设置以TRAP方式上报给SNMP的告警级别，告警级别高于或等于设定值的告警都会被以TRAP方式上报给SNMP，默认不上报
7	inspur(config)#**logging alarmlog-interval** <*minute*>	设置告警记录从缓冲区中写入文件的时间间隔，单位为分钟，取值范围是10~30000，

步骤	命令	功能
		默认值是10
8	inspur(config)#**logging cmdlog-interval** <*second*>	设置命令日志从缓冲区中写入日志文件的时间间隔，单位为秒，取值范围是2~30000，默认值是2
9	inspur(config)#**logging ftp** <*level*>[**vrf** <*vrf-name*>]<*ip-address*><*username*><*password*>[<*filename*>]	设置告警上报FTP的级别、FTP服务器的IP地址、用户名、密码和保存的文件名，默认不上报
10	inspur(config)#**logging filesavetime** {**interval** <*time1*>| **everyday** <*time2*>| **week** <*weekday*><*time3*>| **month** <*mothday*><*time4*>}[**vrf** <*vrf-name*>]<*ftp-server*><*username*><*password*>[<*filename*>]	设置将告警日志写成文件后发送到FTP服务器上的时间、FTP服务器的IP地址、用户名、密码和文件名前缀，默认不上报
11	inspur(config)#**logging mode** {**fullclear** | **fullcycle** | **fullend**}	设置告警缓存区满了后的清除缓存方式，默认是**fullcycle**
12	inspur(config)#**alarm heartbeat-send** {**all**| **console**| **ftp**| **snmp**| **syslog**}	立即向配置的目的地发送一个告警心跳保活报文
13	inspur(config)#**alarm heartbeat-period** < *minute*>< *type*>	配置告警心跳报文发送的时间间隔，单位为分钟，配置范围为0~30000，默认值为0，不发送
14	inspur(config)#**alarm level-change** <*alarm-code*><*level*>	修改相应告警码的告警级别，每个告警码有默认级别，告警码范围1~4294967294

<*level*>：告警上报的最低级别，可以设置为DEBUGGING（8级），INFORMATIONAL（7级），NOTIFICATIONS（6级），WARNINGS（5级），ERRORS（4级），CRITICAL（3级），ALERTS（2级），EMERGENCIES（1级）。

<*time1*>：上报FTP的间隔时间，范围是1:00:00~23:59:59。

<*time2*>：每天上报FTP的时间，范围是00:00:00~23:59:59。

<*weekday*>：每周上报FTP的某日，可设置为Monday，Tuesday，Thursday，Wednesday，Friday，Saturday，Sunday。

<*time3*>：每周上报FTP当天上报的具体时间，范围是00:00:00~23:59:59。

<*mothday*>：每月上报FTP的日期，范围是1~31。

<*time4*>：每月上报FTP当前上报的具体时间，范围是00:00:00~23:59:59。

<*filename*>：FTP服务器上保存的文件名的前缀，长度是1~31个字符。

2.配置CPU、内存、存储设备告警门限。

步骤	命令	功能
1	inspur(config)#**logging on**	打开告警记录总开关，使告警能够根据不同

步骤	命令	功能
		的级别上报给不同的目的地 执行了该命令，CPU负荷、内存利用率、存储介质利用率、电压值等会根据相应值产生相应告警。电压模块可以根据电压值的范围告警
2	inspur(config)#**cpuload-threshold** *<percent>*[**level**{**low** | **middle** | **high**}]	配置CPU负荷告警阈值，范围为50~100，单位：%，缺省值95% CPU告警门限值对应的告警级别，共支持三个级别：**low**、**middle**和**high**，缺省为**low**
	inspur(config)#**check cpu interval** *<interval>*	配置CPU负荷的告警检查时间间隔，范围1~20，单位：10s
3	inspur(config)#**memory-threshold** *<percent>*[**level** {**low** | **middle** | **high**}]	配置内存利用率告警阈值，范围为1~100，单位：%，缺省值60% 内存利用率告警门限值对应的告警级别，共支持三个级别：**low**、**middle**和**high**，缺省为**low**
	inspur(config)#**check memory interval** *<interval>*	配置内存负荷的告警检查时间间隔
4	inspur(config)#**storage-threshold** *<percent>*[**level** {**low** | **middle** | **high**}]	配置存储介质利用率告警阈值，范围为50~100，单位：%，缺省值90% 存储设备告警门限值对应的告警级别，共支持三个级别：**low**、**middle**和**high**，缺省为**low**
5	inspur(config)#**cpualarm** {**granularity-10s** | **granularity-20s** | **granularity-30s** | **granularity-40s** | **granularity-50s** | **granularity-60s**}	配置CPU占有率告警粒度，默认是**granularity-10s**

3.验证告警基本配置结果。

命令	功能
inspur#**show logging alarm** [[**level** *<level>*][**start-time** *<date><time>*][**end-time** *<date><time>*][**typeid** *<type>*]]	显示告警日志缓冲区中的告警信息记录，可以根据级别**level**，时间**start-time**和**end-time**或者**typeid**来筛选告警信息
inspur#**show logfile** [[**username** *<username>*][**start-time** *<date><time>*][**end-time** *<date><time>*][**vtyno** *<number>*][**ip-address** *<ip-address>*]]	显示保存于命令日志缓存中的历史配置操作命令记录，可以根据时间**start-time**和**end-time**或者**ip-address**，**username**，**vtyno**来筛选日志信息
inspur#**show logging configuration**	显示告警模块当前的各项配置信息
inspur#**show running-config alarm** [**all** |{**begin** | **exclude** | **include**}*<line>*]	显示告警的配置

level *<level>*：告警级别，可以设置为DEBUGGING（8级），INFORMATIONAL（7级），NOTIFICATIONS（6级），WARNINGS（5级），ERRORS（4级），CRITICAL

（3级），ALERTS（2级），EMERGENCIES（1级）。

start-time <*date*><*time*>：告警开始时间，<date>格式为mm-dd-yyyy，可以设置为01-01-2001到12-31-2037之间，<time>格式为hh:mm:ss，可以设置00:00:00到23:59:59。

end-time <*date*><*time*>：告警结束时间，<date>格式为mm-dd-yyyy，可以设置为01-01-2001到12-31-2037之间，<time>格式为hh:mm:ss，可以设置00:00:00到23:59:59。

typeid <*type*>：告警类型，可以设置为ACL，BFD，BGP，LDP等六十多种类型进行筛选。

username <*username*>：用户的登录名称，1~32字符。

start-time <*date*><*time*>：命令操作的开始时间，<date>格式为mm-dd-yyyy，可以设置为01-01-2001到12-31-2037之间，<time>格式为hh:mm:ss，可以设置00:00:00到23:59:59。

end-time <*date*><*time*>：命令操作的结束时间，<date>格式为mm-dd-yyyy，可以设置为01-01-2001到12-31-2037之间，<time>格式为hh:mm:ss，可以设置00:00:00到23:59:59。

vtyno <*number*>：用户的终端号，范围0~15。

{begin | **exclude** | **include}**<*line*>：正则表达式，**begin**显示以输入字符串行开头的配置信息；**include**显示包含字符串行的相关配置信息；**exclude**显示去除字符串行相关配置信息之后的其它信息。<line> 用于匹配筛选的字符串行。

4.验证CPU、内存、存储设备告警配置结果。

命令	功能
inspur#**show cpuload-threshold**	显示CPU负荷告警阈值
inspur#**show check cpu interval**	显示CPU负荷的告警检查时间间隔
inspur#**show memory-threshold**	显示内存利用率告警阈值
inspur#**show check memory interval**	显示内存负荷的告警检查时间间隔
inspur#**show storage-threshold**	显示存储介质利用率告警阈值
inspur#**show cpualarm**	显示CPU占有率告警粒度

5.查看机框管理温度及电源电压告警信息。

温度告警及电源电压告警目前不能够对阈值进行配置，仅通过命令进行查询。在IR12000上提供了以下命令来查看机框管理温度及电源电压告警功能：

命令	功能
inspur#**show temperature detail** [<*shelf*>][<*slot*>]	显示各个单板的测温点温度信息
inspur#**show logging alarm typeid TEMPERATURE**	显示温度相关的告警信息

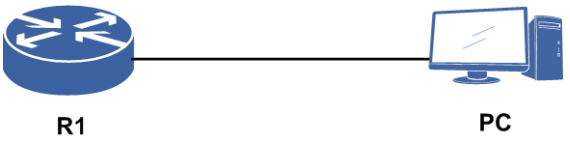
命令	功能
inspur#**show power** [<*shelf*>][<*slot*>]	查看电源信息
inspur#**show logging alarm typeid POWER**	显示电源相关的告警信息

1.8.2 告警配置实例

配置说明

如*图 1-24*所示，PC连接设备R1，可以查看到R1上报的告警信息。

图 1-24 告警配置实例拓扑图



配置思路

1.打开告警开关。

2.配置告警级别，终端告警打印级别，告警缓存，告警缓存满后清除方式，日志写盘时间间隔，时间显示方式，告警上传的服务器地址。

3.配置告警trap，以及trap类型和上送的服务器地址。

配置过程

R1上配置如下：

```
R1(config)#logging on
R1(config)#logging level warnings
R1(config)#logging console warnings
R1(config)#logging buffer 200
R1(config)#logging mode fullcycle
R1(config)#logging cmdlog-interval 2880
R1(config)#logging ftp warnings 192.168.154.253 Inspur Inspur Inspurlog
R1(config)#logging timestamps datetime localtime
R1(config)#logging trap-enable notifications
R1(config)#snmp-server enable trap
R1(config)#snmp-server version v2c enable
R1(config)#snmp-server host 192.168.154.253 trap version 2c Inspur
```

配置验证

告警配置验证如下：

```
R1(config)#show logging configuration
logging on
logging level warnings
logging console warnings
logging trap-enable notifications
logging buffer 200
logging mode fullcycle
logging alarmlog-interval 10
logging cmdlog-interval 2880
logging timestamps datetime localtime
syslog level notifications
syslog-server facility local0
logging ftp warnings 192.168.154.253 Inspur Inspur Inspurlog
alarm heartbeat-period 0 snmp
alarm heartbeat-period 0 syslog
alarm heartbeat-period 0 ftp
alarm heartbeat-period 0 console
alarm heartbeat-period 0 all
logging nat buffer 1000
logging nat password encrypted
 5f942ecb8d1bf9ff5104c77b19c73cb9c14f151612fef1ac1ca09c19fb98ab8d
logging nat file-size 50 file-num 300
logging nat encrypt off
logging nat description-type basemac
logging nat zip on
logging nat terminal local

R1(config)#show snmp config

snmp-server enable trap snmp
snmp-server enable trap bgp
snmp-server enable trap mac
snmp-server enable trap ospf
snmp-server enable trap stp
snmp-server enable trap ppp
snmp-server enable trap arp
snmp-server enable trap rmon
snmp-server enable trap udld
snmp-server enable trap cfm
snmp-server enable trap efm
snmp-server enable trap lacp
snmp-server enable trap mc-elam
snmp-server enable trap tcp
snmp-server enable trap sctp
snmp-server enable trap stalarm
snmp-server enable trap cps
snmp-server enable trap interface
snmp-server enable trap acl
snmp-server enable trap fib
snmp-server enable trap pim
snmp-server enable trap isis
snmp-server enable trap rip
snmp-server enable trap msdp
snmp-server enable trap aps
snmp-server enable trap config
snmp-server enable trap am
snmp-server enable trap um
snmp-server enable trap system
snmp-server enable trap ldp
snmp-server enable trap pwe3
snmp-server enable trap vpn
snmp-server enable trap mpls-oam
snmp-server enable trap ptp
snmp-server enable trap tunnel-te
snmp-server enable trap radius
snmp-server enable trap dhcp
snmp-server enable trap bfd
snmp-server enable trap ippool
snmp-server enable trap ntp
snmp-server enable trap ssm
```

```
snmp-server enable trap sqa
snmp-server enable trap ipsec
snmp-server enable trap cgn
snmp-server enable trap vrrp
snmp-server enable trap ftp_tftp
snmp-server enable trap ping-trace
snmp-server enable trap gm
snmp-server engine-id is 830900020300010289d64401
snmp-server host 192.168.154.253 trap version 2c Inspur udp-port 162 snmp bgp
 mac ospf stp ppp arp rmon udld cfm efm lacp mc-elam tcp sctp stalarm cps
 interface acl fib pim isis rip msdp aps config am um system ldp pwe3 vpn
 mpls-oam ptp tunnel-te radius dhcp bfd ippool ntp ssm sqa ipsec cgn vrrp
 ftp_tftp ping-trace gm
snmp-server packetsize is 8192
snmp-server view AllView internet included
snmp-server view DefaultView system included
snmp-server security dynamic-trust-user idle-timeout 1800
snmp-server version v2c enable
snmp-server input-limit 200

R1(config)#show logging alarm
An alarm 100401 ID 100 level 5 cleared at 06:37:35 03-10-2000 sent
by R1 MPFU-8/0
%CPS% The upsend packet flow of control plane reached quota limit!
Interface = gei-4/5, flowtype = multi-hop-access, current value = 0,
quota value = 100
An alarm 100401 ID 100 level 5 occurred at 06:36:55 03-10-2000
sent by R1 MPFU-8/0
%CPS% The upsend packet flow of control plane reached quota limit!
Interface = gei-4/5, flowtype = multi-hop-access,
current value = 12867, quota value = 100
An alarm 50901 ID 99 level 5 cleared at 06:36:44 03-10-2000 sent
by R1 MPFU-8/0 %LACP% LACP interface active status The interface
(index = 66, name = gei-4/6) turns into ACTIVE
An alarm 150101 ID 96 level 5 cleared at 06:36:44 03-10-2000
sent by R1 MPFU-8/0
%IP% Interface status The interface(index=75,name='smartgroup1')
turned into protocol UP
An alarm 50901 ID 99 level 5 occurred at 06:36:26 03-10-2000
sent by R1 MPFU-8/0
%LACP% LACP interface active status
The interface (index = 66, name = gei-4/6) turns into INACTIVE
An alarm 400123 ID 98 level 2 cleared at 06:36:25 03-10-2000 sent
by R1 MPFU-8/0
%BOARD% Slot offline The slot = 4 is online
 --More--
```

执行命令**terminal monitor**后，可以实时看到产生的告警信息，执行命令**show logging alarm**可看到缓存中的告警。

1.9 SYSLOG

SYSLOG是一种日志格式，记录可打印字符文本内容。SYSLOG起源于UNIX操作系统，用来记录系统日志。

当有告警消息上报时，如果上报SYSLOG的开关打开，系统会根据告警消息的级别决定是否将告警消息上报给SYSLOG服务器。

1.9.1 配置 SYSLOG

本节介绍设备上报SYSLOG功能的配置步骤和命令。

1.配置SYSLOG。

步骤	命令	功能
1	inspur(config)#**syslog level** *<level>*	在全局配置模式下设置告警上报给SYSLOG Server的级别 告警级别高于或等于设定级别的告警都会被上报到SYSLOG Server
2	inspur(config)#**syslog-server facility** *<facility>*	配置SYSLOG报文的上报源，可以设置为ftp，ntp，user等多种源，默认是local0
3	inspur(config)#**syslog-server source** {**ipv4**|**ipv6**}*<source-ip>*	配置上报SYSLOG报文的源地址，支持IPv4和IPv6
4	inspur(config)#**syslog-server host** [**vrf** *<vrf-name>*]*<server-ip>*[**fport** *<fport>*][**lport** *<lport>*][**alarmlog**][**cmdlog**][**debugmsg**][**servicelog**][**braslog**][**natlog**]	设置SYSLOG的参数，包括SYSLOG Server的IP地址、端口号、客户端的端口号以及上送的日志类型

<level>：告警上报给SYSLOG Server的级别，可以设置为DEBUGGING（8级），INFORMATIONAL（7级），NOTIFICATIONS（6级），WARNINGS（5级），ERRORS（4级），CRITICAL（3级），ALERTS（2级），EMERGENCIES（1级），默认值是NOTIFICATIONS。

<server-ip>：报文上报的SYSLOG服务器的IP地址，支持IPv4和IPv6。

<fport>：远端端口号，取值范围是1~65535，默认值是514。

<lport>：本地端口号，取值范围是514或者1024~65535，默认值是514。

[alarmlog][cmdlog][debugmsg][servicelog][braslog][natlog]: 上报SYSLOG服务器的日志类型。

2.验证配置结果。

命令	功能
inspur#**show logging configuration**	查看SYSLOG的所有配置
inspur#**show running-config alarm** [**all** ||{**begin** | **exclude** | **include**}*<line>*]	使用正则表达式查看SYSLOG的配置

1.9.2 SYSLOG 配置实例

配置说明

SYSLOG的作用是将告警信息按一定格式发送给SYSLOG服务器。如*图 1-25*所示，设备上配置好SYSLOG功能后，将告警信息发送给SYSLOG服务器。

图 1-25 SYSLOG 配置实例拓扑图



配置思路

1.将SYSLOG服务器与路由器相连接。

2.将SYSLOG服务器与路由器直连接口配置在同一网段。

3.配置上报SYSLOG服务器的告警级别。

4.配置SYSLOG的类别。

5.指定SYSLOG服务器的地址。

配置过程

路由器R1上的配置如下：

```
R1(config)#interface gei-2/1
R1(config-if-gei-2/1)#no shutdown
R1(config-if-gei-2/1)#ip address 1.1.1.2 255.255.255.0
R1(config-if-gei-2/1)#exit

R1(config)#syslog level warnings
/*配置SYSLOG的告警级别为WARNINGS*/
R1(config)#syslog-server facility syslog
/*配置SYSLOG的类别为SYSLOG*/
R1(config)#syslog-server host 1.1.1.1
/*配置SYSLOG服务器的IP地址*/
```

配置验证

配置完成后用show命令检验配置：

```
R1(config)#show running-config alarm
!<alarm>
syslog level warnings
syslog-server facility syslog
syslog-server host 1.1.1.1 alarmlog cmdlog debugmsg servicelog
 braslog natlog
```

```
!</alarm>
```

1.10 时钟与时钟同步

IR12000系列设备支持NTP协议。

1.10.1 配置 NTP

本节介绍NTP Server和NTP Client功能的配置步骤和命令。

1.配置NTP Server。

步骤	命令	功能
1	inspur(config)#**ntp enable**	启用NTP功能
2	inspur(config)#**ntp master** <*stratum*>	配置NTP服务器等级，取值范围1~15，值越小则服务器发布的NTP时间越可靠
3	inspur(config)#**interface** <*interface-name*>	进入接口配置模式
4	inspur(config-if-interface-name)#**ntp broadcast-server** [**version** <*version-number*>][**key** <*key-number*>]	可选配置，开启设备NTP广播服务器功能
5	inspur(config-if-interface-name)#**ntp multicast-server** {<*ipv4-address*>|<*ipv6-address*>}[**version** <*version-number*>][**ttl** <*ttl-value*>][**key** <*key-number*>]	可选配置，开启设备NTP组播服务器功能

version <*version-number*>：NTP的版本号，范围1~4，在IPv4中版本号默认为3。

key <*key-number*>：设置有效的密钥号，范围1~4294967295。

ttl <*ttl-value*>：设置生存时间TTL值，可选。

2.配置NTP Client。

步骤	命令	功能
1	inspur(config)#**ntp enable**	启用NTP功能
2	inspur(config)#**ntp server** [{**vrf** <*vrf-name*>| **mng**]<*ip-address*> **priority** <*lever*>[**version** <*number*>][**key** <*key-number*>][**lock** | **unlock**]	在客户端定义NTP服务器，其中IP地址和优先级是必配选项，其它为可选项
3	inspur(config)#**ntp source ipv4**	配置客户端NTP协议发出报文的

步骤	命令	功能
	<*ip-address*>	源IP地址
4	inspur(config)#**ntp poll-interval** <*interval*>	配置客户端NTP请求报文发送的时间间隔，范围4~14，指的是2的幂，比如配置了4，则时间间隔为16秒
5	inspur(config)#**interface** < *interface-name*>	进入接口配置模式
6	inspur(config-if-interface-name)#**ntp broadcast-client**	可选配置，开启设备NTP广播客户端功能
7	inspur(config-if-interface-name)#**ntp multicast-client** {<*ipv4-address*>|<*ipv6-address*>}	可选配置，开启设备NTP组播客户端功能

version <*number*>：NTP的版本号，范围1~4，在IPv4中版本号默认为3。

key <*key-number*>：设置有效的密钥号，范围1~4294967295。

priority<*level*>：优先级，每一个Server的优先级不同，范围1~5。

[**lock** | **unlock**]：配置服务器是否锁定，默认值是unlock。

3.配置NTP认证功能。

步骤	命令	功能
1	inspur(config)#**ntp authenticate**	启用NTP认证功能。只有当NTP Server指定的key已成功配置时，NTP认证功能才生效
2	inspur(config)#**ntp authentication-key** <*key-number*> **md5** {**clear** <*clear-word*>|**encrypted** <*encrypted-word*>}	设置NTP认证密钥号和对应的验证码
3	inspur(config)#**ntp trusted-key** <*key-number*>	设置NTP认证可信的密钥号

<*key-number*>：NTP的密钥号，范围1~4294967295。

<*clear-word*>：MD5明文认证码，1~16个字符。

<*encrypted-word*>：MD5密文认证码，1~24个字符。

配置NTP认证功能包括配置客户端和服务器两部分，在配置该功能时，应遵循以下原则：

- 如果开启了NTP认证功能，应同时配置NTP的MD5密钥，并将密钥设为可信密钥。否则，无法正常启用NTP认证功能。
- 如果客户端没有开启NTP验证功能，在其他配置无误的情况下，不论服务器端是否开启NTP验证，客户端都可以与服务器端同步；如果客户端开启了NTP认证功能，客户端只会同步到提供可信密钥的服务器。
- 服务器和客户端的配置应保持一致。

4.验证配置结果。

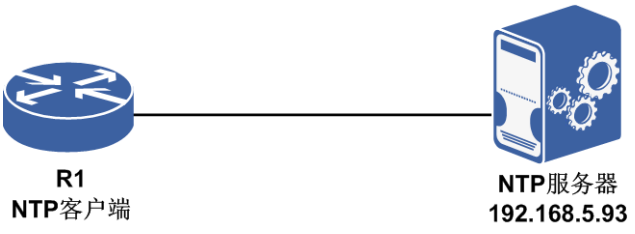
命令	功能
inspur#**show running-config ntp**	查看NTP的配置信息
inspur#**show ntp status**	查看NTP的状态属性值
inspur#**show clock**	查看系统时钟信息

1.10.2 IR12000 作为 NTP 客户端配置实例

配置说明

NTP的作用是将不同网络成员之间时间进行同步。如*图 1-26*所示，IR12000作为NTP客户端同步NTP服务器的时间。

图 1-26 IR12000 作为 NTP 客户端配置实例



配置思路

1.将NTP服务器与路由器相连接。

2.开启NTP功能。

3.指定NTP服务器的地址。

配置过程

路由器R1上的配置如下：

```
R1(config)#ntp enable
R1(config)#ntp server 192.168.5.93 priority 1
```

配置验证

配置完成后用show命令检验配置：

```
R1#show running-config ntp
!<ntp>
```

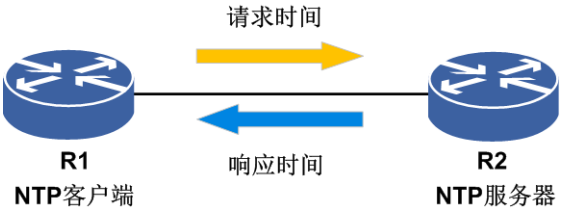
```
ntp server 192.168.5.93 priority 1
ntp enable
!</ntp>
```

1.10.3 IR12000 作为 NTP 服务器端配置实例

配置说明

NTP的作用是将不同网络成员之间的时间进行同步。如*图 1-27*所示，IR12000作为NTP服务器端提供同步信息给客户端。

图 1-27 IR12000 作为 NTP 服务器端配置实例



配置思路

1.在R1（客户端）开启NTP功能，配置NTP服务器的地址。

2.在R2（服务器端）开启NTP功能，配置NTP服务器等级。

配置过程

R1（客户端）上配置如下：

```
R1(config)#ntp enable
R1(config)#ntp server 192.168.5.93 priority 1
```

R2（服务器端）上配置如下：

```
R2(config)#ntp enable
R2(config)#ntp master 1
```

配置验证

在客户端和服务器端**show running-config ntp**可以看到相应配置，在客户端**show ntp status**可以看到客户端参考时钟（R2）的IP地址和时间。在客户端**show clock**可以看到时间同步为服务器时间。

1.11 性能统计

性能统计主要提供以下功能：

·接口性能统计

·TCP/IP层流量、参数等统计

·QoS相关统计

·VPN相关统计

1.11.1 配置性能统计

本节介绍性能统计功能的配置步骤和命令。

1.配置性能统计。

步骤	命令	功能
1	inspur(config)#**intf-statistics**	进入接口统计配置模式
2	inspur(config-intf-statistics)#**one_minute_peak_value** {**disable** | **enable**}{<*interface-name*>| **default**}	一分钟峰值开关，对指定以太口或者所有以太口一分钟峰值是否计数进行控制
	inspur(config-intf-statistics)#**one_minute_peak_value_clear** [<*interface-name*>]	一分钟峰值清零，对指定以太口或者所有以太口一分钟峰值的计数进行清零
3	inspur(config-intf-statistics)#**traffic-statistics** {**enable** | **disable**}	开启或关闭接口性能统计功能，默认开启
4	inspur(config)#**performance data-save-interval** {**15min,5min**}	设定保存数据周期，单位：分钟，默认是15分钟
5	inspur(config)#**performance update-interval** <*periodreport*><*interface-checkPtType*>	配置PMServer向PMAgent采样数据时间间隔，默认为10秒；可以设置具体检测点类型或使用default设置所有检测点类型
6	inspur#**clear statistics interface** [<*interface-name*>]	将指定的某一接口或所有接口持续累计的性能值清零

2.查看性能统计。

命令	功能
inspur#**show running-config performance**	显示性能统计配置信息
inspur#**show interface** < *interface-name*>	查看所有接口或某个接口的状态信息
inspur#**show one_minute_peak_value** [< *interface-name*>]	显示接口一分钟峰值

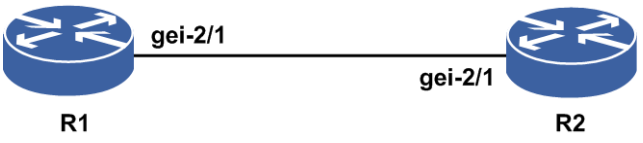
命令	功能
inspur#**show performance data-save-interval**	查询应用性能历史数据保存周期
inspur#**show ip traffic**	流量统计
inspur#**show tcp statistics**	显示TCP层的统计参数
inspur#**show qos-statistics interface** <*interface-name*>{**input**|**output**}	显示某接口指定方向的HQoS统计情况
inspur#**show l2vpn-statistics perfvalue** {**access-point** <*acl-name*>| **pwname pw** <*1-115986*>| **vpnname** <*instance-name*>}	显示L2VPN实例的流量统计值
inspur#**show l2vpn-statistics status** [<*instance-name*>]	显示L2VPN实例的流量统计状态是否使能
inspur#**show l3vpn-statistics perfvalue** <*vrf-name*>	显示L3VPN具体某一业务实例的统计数据信息
inspur#**show l3vpn-statistics status** [<*vrf-name*>]	显示L3VPN业务类型下具体某一业务实例（若没指定，则为L3VPN全部业务）的统计状态

1.11.2 性能统计配置实例

配置说明

性能统计可以根据用户的需要，更改接口计数更新时间或者设置计数开关等功能。如*图 1-28*所示，流量从R1的gei-2/1流出后进入R2的gei-2/1端口。

图 1-28 性能统计配置实例拓扑图



配置思路

1.查看接口gei-2/1的计数，如果要查看新计数统计，先清除之前统计值。

2.修改PMServer向PMAgent采样数据的时间间隔，来控制gei-2/1的计数更新时间间隔。

配置过程

1.清除gei-2/1接口计数：

```
inspur#clear statistics interface gei-2/1
```

2.设置gei-2/1等实接口的计数更新时间为30秒：

```
inspur(config)#performance update-interval 30s ethernet
```

配置验证

检查配置是否已经生效：

```
inspur(config)#show running-config performance
!<performance>
performance update-interval 30s ethernet
!</performance>
```

1.12 NetFlow

NetFlow是用于统计网络流量信息的协议，可以单独对每条流量进行跟踪和计量。统计的流量信息可以带来以下几个应用：

- 网络规划：NetFlow可以长时间地统计网络流量信息，因此可以跟踪和估计网络流量的增长（减少）趋势，从而在需要的地方增加（减少）路由设备或者升级（降级）路由设备的带宽，从而使网络的运营更加合理。
- 分析新的应用：NetFlow可以收集一个新的应用协议的网络使用信息，分析这些信息可以合理地分配网络资源给这些新的应用。
- 网络监测：NetFlow提供近乎实时的网络监测能力。当网络出现问题时，NetFlow提供的信息可以帮助快速地定位问题或者可以发现潜在的网络问题。

1.12.1 配置 NetFlow

本节介绍NetFlow功能的配置步骤和命令。

1.创建并配置NetFlow输出策略。

步骤	命令	功能
1	inspur(config)#**flow exporter** <*exporter-name*>	建立一个flow exporter策略，并为之命名，名字可配范围1-32个字符，可以配置200个不同的flow exporter策略
2	inspur(config-flow-exporter)#**destination** {**ipv4-address** <*ip-address*>| **ipv6-address** <*ip-address*>|[**vrf** <*name*>]}	配置NetFlow服务器的IP地址，为IPv4或IPv6地址
3	inspur(config-flow-exporter)#**export-protocol** {**netflow-v5** | **netflow-v8** | **netflow-v9** | **ipfix**}	设置NetFlow的输出报文格式 可以使用NetFlow v5、v8、v9或者IPFIX的的报文格式进行输出，默认使用v9 当使用v5时，配置的模板必须为**netflow-original**

步骤	命令	功能
		当使用v8时，配置的模板为**netflow protocol-port**
4	inspur(config-flow-exporter)#**template data** {**refresh** <*packets*>| **timeout** <*seconds*>}	将模板按照报文数或者时间重发
5	inspur(config-flow-exporter)#**transport udp** <*port*>	设置NetFlow输出的协议为UDP以及使用的端口号，范围1-65535，默认值是2055
6	inspur(config-flow-exporter)#**source** {**ipv4-address** <*ip-address*>| **ipv6-address** <*ip-address*>| **interface** <*interface-name*>}	设置发送的Netflow报文的源IP地址
7	inspur(config-flow-exporter)#**dscp** <*value*>	设置发送Netflow报文时IP头中的TOS字段，范围0~63，默认值是0

refresh <*packets*>：将模板按照输出的netflow报文个数进行重复发送，范围1~600，默认值为20。

timeout <*seconds*>：将模板按照时间重发，范围1~86400，默认值是600秒。

interface <*interface-name*>：指定源接口名称。

2.创建NetFlow记录策略，并设置关键字段和非关键字段。

步骤	命令	功能
1	inspur(config)#**flow record** <*record-name*>	建立一个flow record策略，并为之命名，名字可配范围1~32字符，可以配置60个不同的flow record策略
2	inspur(config-flow-record)#**match datalink mac** {**destination-address**	**source-address**}	配置源MAC地址或者目的MAC地址为关键字段
	inspur(config-flow-record)#**match flow** {**direction**|**sample-rate**}	设置流的方向\采样速率为关键字段
	inspur(config-flow-record)#**match interface** {**input**	**output**}	设置入接口索引或者出接口索引为关键字段
	inspur(config-flow-record)#**match ipv4** {**destination**[**address**	**address-mask**	**address-prefix minimum-mask** <*len*>]|**source**[**address**	**address-mask**	**address-prefix minimum-mask** <*len*>]}	设置IPv4的相关信息为关键字段
	inspur(config-flow-record)#**match mpls label stack section** <*1-5*>	设置MPLS相关信息为关键字段<*1-5*>：设置采集的标签为1|2|3|4|5层标签
	inspur(config-flow-record)#**match**	设置相关的路由下一跳信息为

步骤	命令	功能
	routing {**bgp as-number** {**destination** | **source** | **next-adjacent** | **prev-adjacent**}| **next-hop-address** {**ipv4** | **ipv6**}}	关键字段
	inspur(config-flow-record)#**match transport** {**destination-port** |**icmp** {**ipv4** | **ipv6**}{**type** | **code**}| **source-port** | **tcp flags**}	设置传输层的信息为关键字段 **icmp {ipv4 | ipv6} {type | code}**：设置ICMP报文的type字段为采集字段，该字段的值填充为**ICMP Type * 256 + ICMP code**
	inspur(config-flow-record)#**match ip** {**cos** | **protocol** | **version**}	设置IP相关信息为关键字段
	inspur(config-flow-record)#**match ipv6** {**destination** [**address** | **address-mask** | **address-prefix minimum-mask** <*len*>]|**source** [**address** | **address-mask** | **address-prefix minimum-mask** <*len*>]| **flow-label**}	设置IPv6的相关信息为关键字段，len范围1~128
3	inspur(config-flow-record)#**collect counter** {**bytes** [**long**]| **packets** [**long**]}	设置流的报文个数和字节数为非关键字段 **bytes**：存储该字段的大小为4字节 **bytes long**：存储该字段的大小为8字节 **packets** ：存储该字段的大小为4字节 **packets long**：存储该字段的大小为8字节
	inspur(config-flow-record)#**collect datalink mac** {**destination-address** | **source-address**}	配置源MAC地址或者目的MAC地址为非关键字段
	inspur(config-flow-record)#**collect flow** {**direction**|**sample-rate**}	设置流的方向/采样速率为非关键字段
	inspur(config-flow-record)#**collect interface** {**input** | **output**}	设置入接口索引或者出接口索引为非关键字段
	inspur(config-flow-record)#**collect ipv4** {**destination** [**address** | **address-mask** | **address-prefix minimum-mask** <*len*>]|**source**[**address** | **address-mask** | **address-prefix minimum-mask** <*len*>]}	设置IPv4的相关信息为非关键字段
	inspur(config-flow-record)#**collect mpls label stack section** <*1-5*>	设置MPLS相关信息为非关键字段
	inspur(config-flow-record)#**collect routing** {**bgp as-number** {**destination** | **source** | **next-adjacent** | **prev-adjacent**}| **next-hop-address** {**ipv4** | **ipv6**}}	设置相关的路由下一跳信息为非关键字段
	inspur(config-flow-record)#**collect timestamp** {**sys-uptime** {**first** | **last**}| **absolute** {**first-millisec** | **last-millisec**}}	设置流的第一次被交换或者最后一次被交换的时间或绝对时

步骤	命令	功能
		间为非关键字段 **sys-uptime first**：设置流第一次进入cache的系统上电时间为采集的非关键字段，单位：毫秒 **sys-uptime last**：设置流最后一次在cache中被更新的系统上电时间为采集的非关键字段，单位：毫秒
	inspur(config-flow-record)#**collect transport** {**destination-port** | **icmp** {**ipv4** | **ipv6**}{**code** | **type**}| **source-port** | **tcp flags**}	设置传输层的信息为非关键字段
	inspur(config-flow-record)#**collect ip** {**cos**| **protocol** | **version**}	设置IP相关信息为非关键字段
	inspur(config-flow-record)#**collect ipv6** {**destination** [**address** | **address-mask** | **address-prefix minimum-mask** <*len*>]|**source** [**address** | **address-mask** | **address-prefix minimum-mask** <*len*>]| **flow-label**}	设置IPv6的相关信息为非关键字段，len范围1~128

3.配置NetFlow采样策略。

步骤	命令	功能
1	inspur(config)#**sampler** <*sampler-name*>	建立一个sampler策略，并为之命名，名字可配范围1–32字符，可以配置200个不同的sampler策略
2	inspur(config-sampler)#**mode deterministic 1-out-of**<*rate*>	配置采样方式与采样速率

deterministic：设置采样方式为非随机采样，即如果采样率为N，则每N个报文采样1个。

<*rate*>：设置采样速率，设置范围为1~65535，默认值为1000。

4.配置NetFlow监测策略。

步骤	命令	功能
1	inspur(config)#**flow monitor** <*monitor-name*>	建立一个flow monitor策略，并为之命名，名字可匹配范围1–32字符，可以配置60个不同的flow monitor策略
2	inspur(config-flow-monitor)#**cache** {**entries** <*num*>| **timeout** {**active** | **inactive**}<*seconds*>}	配置cache相关信息
3	inspur(config-flow-monitor)#**exporter**	关联flow exporter策略

步骤	命令	功能
	<exporter-name>	关联一个之前已经配置好的flow exporter策略，则该flow monitor策略使用这个flow exporter策略输出netflow报文，如果该flow exporter策略使用v5输出格式，则该flow monitor使用的模板必须是预定好的netflow-original
4	inspur(config-flow-monitor)#**record** {**netflow** {**protocol-port** | **ipv4** {**original-input** | **original-output**}}| **netflow-original** |<*record-name*>}	使用一个之前已经配置好的flow record策略

entries <*num*>：设置缓存的大小为<*num*>，<*num*>代表该缓存能够存储的流的个数，可以设置的范围为16~131072，默认值为4096。

timeout active <*seconds*>：设置活跃老化时间，单位：秒，可以设置的范围为10~604800，默认值为1800。

timeout inactive <*seconds*>：设置非活跃老化时间，单位：秒，可以设置的范围为10~604800，默认值为600。

protocol-port：预定义netflow-v8模板。

original-input：预定义netflow-v5模板，采集的关键字段和非关键字段与netflow v5保持一致。

original-output：与**original-input**的区别在于，**original-output**使用出方向的接口索引作为采集的关键字段，入方向的接口索引为非关键字段。

netflow-original：预定义netflow-v5模板，采集的关键字段和非关键字段与netflow v5保持一致。

<*record-name*>：使用一个之前已经配置好的flow record策略作为模板

5.配置NetFlow接口。

步骤	命令	功能
1	inspur(config)#**interface** <*interface-name*>	进入接口配置模式
2	inspur(config-if-interface-name)#**ip flow monitor** <*monitor-name*>[**sampler** <*sampler-name*>][**unicast**|**multicast**|**ipv4–access-list** <*name*>]{**input**|**output**}	在接口上设置对IPv4报文的采样
	inspur(config-if-interface-name)#**ipv6 flow monitor** <*monitor-name*>[**sampler** <*sampler-name*>][**unicast** | **multicast** | **ipv6–access-list** <*name*>]{**input** | **output**}	在接口上设置对IPv6报文的采样
	inspur(config-if-interface-name)#**mpls flow monitor** <*monitor-name*>[**sampler** <*sampler-name*>] **unicast** {**input** | **output**}	在接口上设置对MPLS报文的采样

ip flow monitor <*monitor-name*>：在接口下使用一个之前已经配置好的netflow监测策略（flow monitor策略）。配置完成后，与该监测策略相关的、涉及到缓存大小的配置都不能更改，如cache的大小、使用的模板以及模板的采集字段。只有将该flow monitor策略从接口上删除后才可以更改。而流的活跃、非活跃老化时间

以及输出策略则可以更改。

sampler *<sampler-name>*：在接口下使用一个之前已经配置好的采样策略（sampler策略）。

unicast | **multicast**| **ipv4-access-list** *<acl-name>*：配置采样报文的类型，默认对单播和组播报文同时采样。**unicast**表述对单播报文进行采样；**multicast**表示对组播报文进行采样；对被ACL规则过滤的报文进行采样，最多可以使用6个不同的ACL规则。

在一个方向上可以同时对单播、组播、MPLS报文或者ACL规则的报文进行采样。两个方向上的采样并不互斥。但是如果在一个方向上使用了ACL规则的报文，则不能再对单播和组播报文进行采样，反之亦然。

6.验证配置结果。

命令	功能
inspur#**show ip flow exporter** [*<exporter-name>*]	查看指定名字的flow exporter策略或者查看所有的flow exporter策略
inspur#**show ip flow interface** [*<interface-name>*]	查看指定接口下的配置或者查看所有的接口配置
inspur#**show ip flow monitor** [*<monitor-name>*]	查看指定名字的flow monitor策略或者查看所有的flow monitor策略
inspur#**show ip flow record** [**netflow-original** | **netflow** {**protocol-port** | **ipv4** {**original-input** | **original-output**}}|*<record-name>*]	查看指定名字的flow record策略或者查看预定义的v5策略（v5模板：netflow-original），或者查看所有的flow record策略
inspur#**show ip flow sampler** [*<sampler-name>*]	查看指定名字的sampler策略或者查看所有的sampler策略
inspur#**show running-config ipflow** [**all**][|{**begin** | **exclude** | **include**}*<line>*]	显示NetFlow的配置，带**all**表示显示所有配置，包括NetFlow其他未配置的参数默认值
inspur#**show running-config-interface** *<interface-name>*[**all**][|{**begin** | **exclude** | **include**}*<line>*]	显示NetFlow相关接口的配置
inspur#**show ip flow service-cpu**	显示启动了NetFlow功能的业务CPU信息

1.12.2 NetFlow V5 版本采集配置实例

配置说明

如*图 1-29*所示，在IR12000上配置NetFlow，将服务器端与路由器相连，配置IP地址，如有需要还需配置到达服务器端的路由，使NetFlow报文可以发送到服务器端。

图 1-29 NetFlow V5 版本采集配置拓扑图



配置思路

1.启用NetFlow业务功能。

2.配置flow exporter中的相关输出项，包括服务器地址、端口号、协议类型。

3.配置sampler设置采集率及采集方式。

4.配置flow monitor中缓冲区大小，超时活跃时间和超时非活跃时间，绑定配置的flow exporter及系统自带的v5模板。

5.将flow monitor绑定在接口下，配置采集类型及采集方向。

配置过程

在IR12000上的配置如下：

```
R1#configure terminal

R1(config)#flow exporter exp
R1(config-flow-exporter)#destination ipv4-address 169.1.109.60
R1(config-flow-exporter)#transport udp 2055
R1(config-flow-exporter)#export-protocol netflow-v5
R1(config-flow-exporter)#exit

R1(config)#sampler sam
R1(config-sampler)#mode deterministic 1-out-of 1024
R1(config-sampler)#exit

R1(config)#flow monitor mo
R1(config-flow-monitor)#cache entries 4096
R1(config-flow-monitor)#exporter exp
R1(config-flow-monitor)#record netflow-original
R1(config-flow-monitor)#cache timeout inactive 60
R1(config-flow-monitor)#cache timeout active 10
R1(config-flow-monitor)#exit

R1(config)#interface gei-0/8
R1(config-if-gei-0/8)#no shutdown
R1(config-if-gei-0/8)#ip flow monitor mo sampler sam unicast input
R1(config-if-gei-0/8)#exit
```

配置验证

在IR12000上查看配置结果：

```
R1#show running-config ipflow
!<ipflow>
flow exporter exp
```

```
  destination ipv4-address 169.1.109.60
  export-protocol netflow-v5
$
flow monitor mo
  cache timeout active 10
  cache timeout inactive 60
  record netflow-original
  exporter exp
$
sampler sam
  mode deterministic 1-out-of 1024
$
interface  gei-0/8
  ip flow monitor mo sampler sam unicast input
$
!</ipflow>
```

1.12.3 NetFlow V8 版本采集配置实例

配置说明

如*图 1-30*所示，在IR12000上配置NetFlow，将服务器端与路由器相连，配置IP地址。如有需要还需配置到达服务器端的路由，使NetFlow报文可以发送到服务器端。

图 1-30 NetFlow V8 版本采集配置拓扑图



配置思路

1.启用NetFlow业务功能。

2.配置flow exporter中的相关输出项，包括服务器地址、端口号、协议类型。

3.配置sampler设置采集率及采集方式。

4.配置flow monitor中缓冲区大小，超时活跃时间和超时非活跃时间，绑定配置的flow exporter及系统自带的v8模板。

5.将flow monitor绑定在接口下，配置采集类型及采集方向。

配置过程

在IR12000上的配置如下：

```
R1(config)#flow exporter exp
R1(config-flow-exporter)#destination ipv4-address 169.1.109.60
R1(config-flow-exporter)#transport udp 2055
R1(config-flow-exporter)#export-protocol netflow-v8
R1(config-flow-exporter)#exit
```

```
R1(config)#sampler sam
R1(config-sampler)#mode deterministic 1-out-of 1024
R1(config-sampler)#exit

R1(config)#flow monitor mo
R1(config-flow-monitor)#cache entries 4096
R1(config-flow-monitor)#exporter exp
R1(config-flow-monitor)#record netflow protocol-port
R1(config-flow-monitor)#cache timeout inactive 60
R1(config-flow-monitor)#cache timeout active 10
R1(config-flow-monitor)#exit

R1(config)#interface gei-0/8
R1(config-if-gei-0/8)#no shutdown
R1(config-if-gei-0/8)#ip flow monitor mo sampler sam unicast input
R1(config-if-gei-0/8)#exit
```

配置验证

在IR12000上查看配置结果：

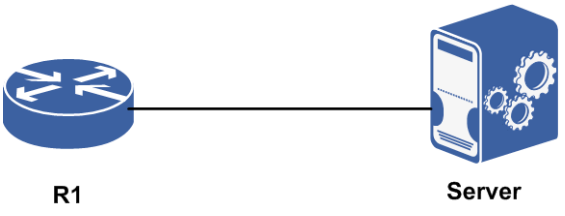
```
R1#show running-config ipflow
!<ipflow>
sampler sam
  mode deterministic 1-out-of 1024
$
flow exporter exp
  destination ipv4-address 169.1.109.60
  export-protocol netflow-v8
$
flow monitor mo
  cache timeout active 10
  cache timeout inactive 60
  record netflow protocol-port
  exporter exp
$
interface gei-0/8
  ip flow monitor mo sampler sam unicast input
$
!</ipflow>
```

1.12.4 NetFlow V9 版本采集配置实例

配置说明

如*图 1-31*所示，在IR12000上配置NetFlow，将服务器端与路由器相连，配置IP地址，如有需要还需配置到达服务器端的路由，使NetFlow报文可以发送到服务器端。

图 1-31 NetFlow V9 版本采集配置拓扑图



配置思路

1.启用NetFlow业务功能。

2.配置flow exporter中的相关输出项，包括服务器地址、端口号、协议类型、模板刷新时间及刷新率。

3.配置flow record中的match项与collect项。

4.配置flow monitor中缓冲区大小，超时活跃时间和超时非活跃时间，绑定配置的flow exporter及配置的flow record。

5.配置sampler设置采集率及采集方式。

6.将flow monitor绑定在接口下，配置采集类型及采集方向。

配置过程

在IR12000上的配置如下：

```
R1(config)#flow exporter exp
R1(config-flow-exporter)#destination ipv4-address 169.1.109.60
R1(config-flow-exporter)#transport udp 2055
R1(config-flow-exporter)#export-protocol netflow-v9
R1(config-flow-exporter)#template data refresh 20
R1(config-flow-exporter)#template data timeout 60
R1(config-flow-exporter)#exit

R1(config)#sampler sam
R1(config-sampler)#mode deterministic 1-out-of 1024
R1(config-sampler)#exit

R1(config)#flow record rec
R1(config-flow-record)#match ipv4 source address
R1(config-flow-record)#match ipv4 destination address
R1(config-flow-record)#match transport source-port
R1(config-flow-record)#match transport destination-port
R1(config-flow-record)#collect counter bytes
R1(config-flow-record)#collect counter packets
R1(config-flow-record)#exit

R1(config)#flow monitor mo
R1(config-flow-monitor)#cache entries 4096
R1(config-flow-monitor)#cache timeout active 60
R1(config-flow-monitor)#cache timeout inactive 10
R1(config-flow-monitor)#exporter exp
R1(config-flow-monitor)#record rec
R1(config-flow-monitor)#exit

R1(config)#interface gei-0/8
R1(config-if-gei-0/8)#no shutdown
R1(config-if-gei-0/8)#ip flow monitor mo sampler sam unicast input
R1(config-if-gei-0/8)#end
```

配置验证

在IR12000上查看配置结果：

```
R1#show running-config ipflow
!<ipflow>
sampler sam
```

```
  mode deterministic 1-out-of 1024
$
flow exporter exp
  destination ipv4-address 169.1.109.60
  #export-protocol netflow-v9
$
flow record rec
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  collect counter bytes
  collect counter packets
$
flow monitor mo
  cache timeout active 60
  cache timeout inactive 10
  record rec
  exporter exp
$
interface  gei-0/8
  ip flow monitor mo sampler sam unicast input
$
!</ipflow>
```

1.12.5 NetFlow IPFIX 版本采集配置实例

配置说明

如*图 1-32*所示，在IR12000上配置NetFlow，将服务器端与路由器相连，配置IP地址，如有需要还需配置到达服务器端的路由，使NetFlow报文可以发送到服务器端。

图 1-32 NetFlow IPFIX 版本采集配置拓扑图



配置思路

1.启用NetFlow业务功能。

2.配置flow exporter中的相关输出项，包括服务器地址、端口号、协议类型、模板刷新时间及刷新率。

3.配置flow record中的match项与collect项。

4.配置flow monitor中缓冲区大小，超时活跃时间和超时非活跃时间，绑定配置的flow exporter及配置的flow record。

5.配置sampler设置采集率及采集方式。

6.将flow monitor绑定在接口下，配置采集类型及采集方向。

配置过程

在IR12000上的配置如下：

```
inspur(config)#flow exporter exp
inspur(config-flow-exporter)#destination ipv4-address 169.1.109.60
inspur(config-flow-exporter)#transport udp 2055
inspur(config-flow-exporter)#export-protocol ipfix
inspur(config-flow-exporter)#template data refresh 20
inspur(config-flow-exporter)#template data timeout 60
inspur(config-flow-exporter)#exit

inspur(config)#sampler sam
inspur(config-sampler)#mode deterministic 1-out-of 1024
inspur(config-sampler)#exit

inspur(config)#flow record rec
inspur(config-flow-record)#match ipv4 source address
inspur(config-flow-record)#match ipv4 destination address
inspur(config-flow-record)#match transport source-port
inspur(config-flow-record)#match transport destination-port
inspur(config-flow-record)#collect counter bytes
inspur(config-flow-record)#collect counter packets
inspur(config-flow-record)#exit

inspur(config)#flow monitor mo
inspur(config-flow-monitor)#cache entries 4096
inspur(config-flow-monitor)#cache timeout active 60
inspur(config-flow-monitor)#cache timeout inactive 10
inspur(config-flow-monitor)#exporter exp
inspur(config-flow-monitor)#record rec
inspur(config-flow-monitor)#exit

inspur(config)#interface gei-0/8
inspur(config-if-gei-0/8)#no shutdown
inspur(config-if-gei-0/8)#ip flow monitor mo sampler sam unicast input
inspur(config-if-gei-0/8)#end
```

配置验证

在IR12000上查看配置结果：

```
inspur#show running-config ipflow
!<ipflow>
sampler sam
  mode deterministic 1-out-of 1024
$
flow exporter exp
  destination ipv4-address 169.1.109.60
  #export-protocol ipfix
$
flow record rec
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  collect counter bytes
  collect counter packets
$
flow monitor mo
  cache timeout active 60
  cache timeout inactive 10
  record rec
  exporter exp
$
interface  gei-0/8
```

```
  ip flow monitor mo sampler sam unicast input
$
!</ipflow>
```

1.12.6 NetFlow 采样信息支持 IPv6 配置实例

配置说明

如*图 1-33*所示，在IR12000上配置NetFlow采样信息支持封装在IPv6发送给服务器。

图 1-33 NetFlow 采样信息支持封装在 IPv6 发送给服务器配置拓扑图



配置思路

1.启用NetFlow业务功能。

2.配置flow exporter中的相关输出项。

3.配置flow record中的match项与collect项。

4.配置flow monitor，绑定配置的flow exporter及flow record。

5.接口下绑定flow monitor。

配置过程

在IR12000上的配置如下：

```
inspur(config)#flow exporter exporter
inspur(config-flow-exporter)#destination ipv6-address 192:168::12:12
inspur(config-flow-exporter)#export-protocol netflow-v9
inspur(config-flow-exporter)#exit

inspur(config)#flow record record
inspur(config-flow-record)#match ipv6 source address
inspur(config-flow-record)#match ipv6 destination address
inspur(config-flow-record)#match transport source-port
inspur(config-flow-record)#match transport destination-port
inspur(config-flow-record)#collect counter bytes
inspur(config-flow-record)#collect counter packets
inspur(config-flow-record)#exit

inspur(config)#flow monitor monitor
inspur(config-flow-monitor)#exporter exporter
inspur(config-flow-monitor)#record record
inspur(config-flow-monitor)#exit

inspur(config)#interface gei-0/1
```

```
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#ipv6 flow monitor monitor unicast input
inspur(config-if-gei-0/1)#ipv6 flow monitor monitor unicast output
inspur(config-if-gei-0/1)#exit
```

配置验证

在IR12000上查看配置结果：

```
inspur#show running-config ipflow
!<ipflow>
flow exporter exporter
  destination ipv6-address 192:168::12:12
  export-protocol netflow-v9
$
flow record record
  match ipv6 destination address
  match ipv6 source address
  match transport destination-port
  match transport source-port
  collect counter packets
  collect counter bytes
$
flow monitor monitor
  record record
  exporter exporter
$
interface gei-0/1
  ipv6 flow monitor monitor unicast input
  ipv6 flow monitor monitor unicast output
$
!</ipflow>
```

1.13 SQA

SQA是一种量化探测技术，通过SQA的量化测量技术分析，不但可以获取更为详细的IP层网络质量分析，还可以分析具体业务的网络质量是否达到SLA的要求。

SQA一般用于网络故障诊断。

1.13.1 配置 SQA

本节介绍SQA功能的配置步骤和命令。

1.配置SQA测试实例。

步骤	命令	功能
1	inspur(config)#**sqa-test** <*number*>	选择测试实例号，并进入SQA模式下，实例号范围为1-150
2	inspur(config-sqa)#**type-icmp** [**vrf** <*vrf-name*>]<*destination-address*>[**source** <*source-address*>][**repeat** < *repeat-number*>][**tos** <*tos-value*>][**ttl** < *ttl-value*>][**size** < *size-value*>][**interval**	在SQA模式下，配置ICMP测试实例

	<*interval-value*>]	
	inspur(config-sqa)#**type-udp** [**vrf** <*vrf-name*>]<*destination-address*><*destination-port*>[**size** <*size-value*>][**interval** <*interval-value*>][**repeat** <*repeat-number*>]	在SQA模式下，配置UDP测试实例
	inspur(config-sqa)#**type-tcp** [**vrf** <*vrf-name*>]<*destination-address*><*destination-port*>[**interval** <*interval-value*>][**repeat** <*repeat-number*>]	在SQA模式下，配置TCP测试实例
	inspur(config-sqa)#**type-ftp copy** <*destination-address*> **uesr-name** <*user-name*> **password** {**encrypted** <*ftp-server-encrypted-password*>|<*ftp-server-password*>} **file-name** <*file-name*> **root** <*local-path*>**/**<*file-name*>	在SQA模式下，配置FTP测试实例
	inspur(config-sqa)#**type-dns** [**vrf** <*vrf-name*>] **destination-url** <*destination-url*> **dns-ip** <*dns-ip-address*>[**repeat** <*repeat-number*>]	在SQA模式下，配置DNS测试实例
	inspur(config-sqa)#**type-http** [**vrf** <*vrf-name*>]{**http-ip**<*http-ip-address*>|**http-url**<*http-url*> **dns-ip** <*dns-ip-address*>}[**repeat** <*repeat-number*>]	在SQA模式下，配置HTTP测试实例
	inspur(config-sqa)#**type-snmp** [**vrf** <*vrf-name*>]<*specify-destination-ip-address*>	在SQA模式下，配置SNMP测试实例
	inspur(config-sqa)#**type-udp-jitter** [**vrf** <*vrf-name*>]<*specify-destination-ip-address*> <*specify-destination-port*>[**interval**<*interval-time*>][**repeat**< *repeat-number*> **size**<*size-number*>| **interval**<*interval-time*>][**size**<*size-number*> **interval**<*interval-time*>|**repeat**< *repeat-number*>]	在SQA模式下，配置UDP-JITTER测试实例
	inspur(config-sqa)#**type-icmp-jitter** [**vrf** <*vrf-name*>]<*destination-address*>[**source** <*source-address*>][**repeat** < *repeat-number*>][**tos** <*tos-value*>][**ttl** < *ttl-value*>][**size** < *size-value*>][**interval** <*interval-value*>]	在SQA模式下，配置ICMP jitter测试实例

<*repeat-number*>：重复次数，ICMP检测类型范围1~65535，默认值1；UDP检测类型范围1~1000，默认值1；TCP检测类型范围1~200，默认值1；DNS检测类型范围1~10，默认值1；ICMP jitter检测类型范围1~65535，默认值1。

<*tos-value*>：ToS值，范围0~255，默认值0。

<*ttl-value*>：TTL值，范围1~255，默认值255。

<*size-value*>：报文大小，ICMP检测类型范围36~8192bytes，默认值36bytes；UDP检测类型范围50~1500bytes，默认值50bytes；ICMP jitter检测类型范围40~8192bytes，默认值40bytes。

<*interval-value*>：包间隔时间，单位：ms，ICMP检测类型范围50~65535，默认值100；UDP检测类型范围50~2000，默认值100；TCP检测类型范围1000~4000，默认值1000；ICMP jitter检测类型范围50~65535，默认值100。

<*destination-port*>：目的端口号，范围1025~65535。

<*user-name*>：FTP Server的用户名，可配范围1~31字符。

<*ftp-server-password*>：FTP Server的明文密码，可配范围1~31字符。

<*ftp-server-encrypted-password*>：FTP Server的密文密码，可配64字符。

<*file-name*>：FTP源文件名，可配范围1~79字符。

<*local-path*>/<*file-name*>：FTP目的路径以及目的文件名，可配范围1~151字符。

<*destination-url*>：要解析的域名，可配范围1~128字符。

<*dns-ip-address*>：域名服务器的IP地址。

2.启动SQA测试，开启TRAP告警。

步骤	命令	功能
1	inspur(config-sqa)#**sqa-begin** {**now** | **timerange** <*timerange-name*>}	在SQA模式下，启动测试，用**sqa-stop**暂停测试；**now**表示立即启动测试
2	inspur(config-sqa)#**send-trap** { **enable** <*percent*>}	在SQA模式下，开启TRAP告警，参数<*percent*>为告警阈值，取值范围1~100

3.配置SQA TCP或UDP服务器。

命令	功能
inspur(config)#**sqa-tcp-server** <*ip-address*><*port*>	在配置模式下，配置SQA TCP服务器（选择TCP测试实例时需要配置）
inspur(config)#**sqa-udp-server** <*ip-address*><*port*>	在配置模式下，配置SQA UDP服务器（选择UDP测试实例时需要配置）

4.验证配置结果。

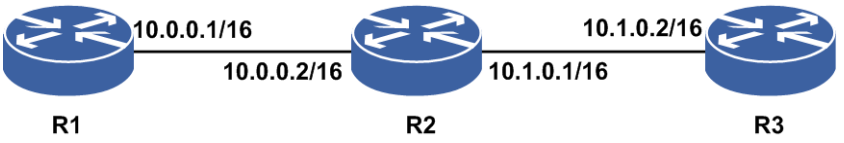
命令	功能
inspur#**show running-config sqa** [**all**][|**begin** | **exclude** | **include**}<*line*>	查看SQA配置
inspur#**show sqa-test** <*number*>	显示SQA Test配置信息
inspur#**show sqa-server** {**upd**|**tcp**}	显示SQA Server配置信息
inspur#**show sqa-result** {**udp** | **tcp** | **icmp** | **ftp** | **dns** | **http** | **snmp** | **udpjitter** | **icmpjitter**}	显示SQA各类型检测的结果

1.13.2 ICMP 类型的 SQA 配置实例

配置说明

如*图 1-34*所示，R1与R3之间存在一个链路，配置ICMP测试实例，测试R1与R3之间的报文转发。

图 1-34 ICMP 类型的 SQA 配置实例



配置思路

1.创建一个SQA实例。

2.进入该SQA实例后，为该实例配置ICMP测试的目的地址，并设定ICMP测试属性。

3.设置SQA测试开始时间，立即开始执行或者定时开始执行。

4.查看测试结果。

配置过程

R1上的配置如下：

```
R1(config)#sqa-test 1
R1(config-sqa-1)#type-icmp 10.1.0.2
R1(config-sqa-1)#sqa-begin now
%Info 757: The sqa test is starting now, please wait a moment for test result......
R1(config-sqa-1)#
```

配置验证

使用显示命令查看配置信息以及测试结果。

```
R1#show sqa-test 1
test number:1
test type: ICMP
destination IP: 10.1.0.2
repeat:1
tos:0
ttl: 255
size: 36
interval time:100
send trap:disable

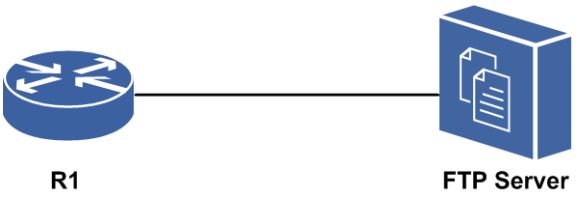
R1#show sqa-result icmp
icmp test[1] result
SendPackets:1  ResponsePackets:1
Completion:success  Destination IP Address: 10.1.0.2
Min/Max/Avg/Sum RTT:29/99/39/787ms
Min/Max/Avg/Sum Positive Jitter:1/7/3/9ms
Min/Max/Avg/Sum Negative Jitter:1/70/35/71ms
Min/Max/Avg/Sum Jitter:1/70/16/80ms
Packet loss rate:0%
Last Probe Time:2012-11-18 01:57:38
```

1.13.3 FTP 类型的 SQA 配置实例

配置说明

如*图 1-35*所示，FTP Server与路由器之间存在一个链路，之间的报文能正常转发。FTP Server上开启FTP-SERVER功能，并设置相应的用户名和密码。在路由器上配置ICMP测试实例，测试FTP服务。

图 1-35 FTP 类型的 SQA 配置实例



配置思路

1.创建一个SQA实例。

2.进入该SQA实例后，配置FTP测试属性，包括FTP服务器地址、用户名、密码、源文件名，目的路径以及目的文件名。

3.设置SQA测试开始时间，立即开始执行或者定时开始执行。

4.查看测试结果。

配置过程

路由器上的配置如下：

```
R1(config)#sqa-test 2
R1(config)#type-ftp copy 1.1.1.1 filename abc.txt root /datadisk0/abc.txt
R1(config)#type-ftp  username who  password who
R1(config-sqa-2)#sqa-begin now
%Info 757: The sqa test is starting now，please wait a moment for test result......
R1(config-sqa-2)#
```

配置验证

使用显示命令查看配置信息以及测试结果。

```
R1#show sqa-test 2
test number:2
test type: FTP
ftp IP:10.1.0.2
username:who
password: 9654d35c7f907ad5c1a1f803d1e4a21c667d8939cade03478bad7db48099d0e4
/*被加密的*/
filename:abc.txt
root:/datadisk0/abc.txt
send trap:disable
```

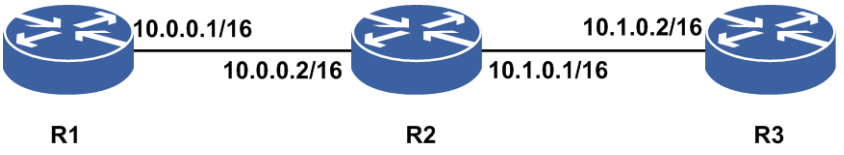
```
R1#show sqa-result ftp
ftp test[2] result
Completion:success
Last RTT:127s   Bytes read:4817497
Last Probe Time:2012-07-29 09:22:58
```

1.13.4 TCP 类型的 SQA 配置实例

配置说明

如*图 1-36*所示，R1与R3之间存在一个链路，R1与R3之间的报文也能正常转发。R3上开启SQA-TCP-SERVER监听端口。在R1上配置TCP测试实例。

图 1-36 TCP 类型的 SQA 配置实例



配置思路

1.创建一个SQA实例。

2.进入该SQA实例后配置TCP测试的目的地址和目的端口，并为该实例设定TCP测试属性。

3.设置SQA测试开始时间，立即开始执行或者定时开始执行。

4.查看测试结果。

配置过程

R3上的配置如下：

```
R3(config)#sqa-tcp-server 10.1.0.2 10000
```

R1上的配置如下：

```
R1(config)#sqa-test 3
R1(config-sqa-3)#type-tcp 10.1.0.2 10000
R1(config-sqa-3)#sqa-begin now
%Info 757: The sqa test is starting now, please wait a moment for test result......
R1(config-sqa-3)#
```

配置验证

使用显示命令查看配置信息以及测试结果。

```
R1#show sqa-test 3
test number:1
```

```
test type: TCP
destination IP:10.1.0.2
desitnation port:10000
interval time:1000
repeat:1
send trap:disable

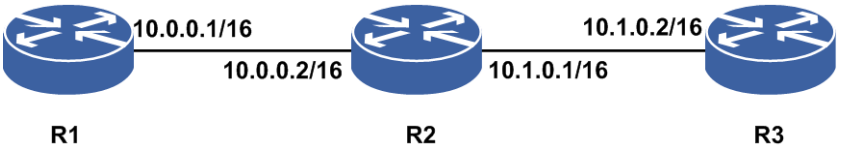
R1#show sqa-result tcp
tcp test[3] result
SendPackets:1    ResponsePackets:1
Completion:success    Destination Ip Address:10.1.0.2
Min/Max/Avg/Sum RTT:5/5/5/5ms
Last Probe Time:2012-07-29 09:45:49
```

1.13.5 UDP 类型的 SQA 配置实例

配置说明

如*图 1-37*所示，R1与R3之间存在一个链路，R1与R3之间的报文也能正常转发。R3上开启SQA-UDP-SERVER监听端口。在R1上配置UDP测试实例。

图 1-37 UDP 类型的 SQA 配置实例



配置思路

1.创建一个SQA实例。

2.进入该SQA实例后配置UDP测试的目的地址和目的端口号，并为该实例设定UDP测试属性。

3.设置SQA测试开始时间，立即开始执行或者定时开始执行。

4.查看测试结果。

配置过程

R3上的配置如下：

```
R3(config)#sqa-udp-server 10.1.0.2 10000
```

R1上的配置如下：

```
R1(config)#sqa-test 4
R1(config-sqa-4)#type-udp 10.1.0.2 10000
R1(config-sqa-4)#sqa-begin now
%Info 757: The sqa test is starting now, please wait a moment for test result......
R1(config-sqa-4)#
```

配置验证

使用显示命令查看配置信息以及测试结果。

```
R1#show sqa-test 4
test number:1
test type: UDP
destination IP:10.1.0.2
desitnation port:10000
size: 50
interval time:100
repeat:1
send trap:disable

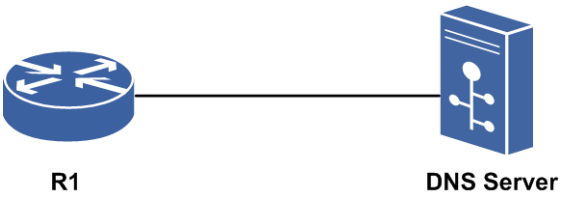
R1#show sqa-result udp
udp test[4] result
SendPackets:1  ResponsePackets:1
Completion:success  Destination IP Address: 10.1.0.2
Min/Max/Avg/Sum RTT:61/63/62/622ms
Min/Max/Avg/Sum Positive Jitter:0/0/0/0ms
Min/Max/Avg/Sum Negative Jitter:1/1/1/2ms
Min/Max/Avg/Sum Jitter:1/1/1/2ms
Packet loss rate:0%
Last Probe Time:2012-09-01 23:52:35
```

1.13.6 DNS 类型的 SQA 配置实例

配置说明

如*图 1-38*所示，在IR12000上配置SQA测试实例，将服务器端与路由器相连，配置IP地址。如有需要还需配置到达服务器端的路由，使DNS报文可以发送到服务器端。

图 1-38 DNS 类型的 SQA 配置实例



配置思路

1.创建一个SQA实例。

2.进入该SQA实例后，配置DNS测试需要解析的域名以及DNS服务器的IP地址，并设置解析次数。

3.设置SQA测试开始时间，立即开始执行或者定时开始执行。

4.查看测试结果。

配置过程

路由器上的配置如下：

```
R1(config)#ip domain lookup
R1(config)#ip domain name-server ipv4-address 10.1.0.1
R1(config)#sqa-test 5
R1(config-sqa-5)#type-dns destination-url abc.cn dns-ip 10.1.0.1
R1(config-sqa-5)#sqa-begin now
%Info 757: The sqa test is starting now, please wait a moment for test result......
R1(config-sqa-5)#
```

配置验证

使用显示命令查看配置信息以及测试结果。

```
R1#show sqa-test 5
test number:1
test type: DNS
destination-url:abc.cn
dns-ip:10.1.0.1
repeat:1
send trap:disable

R1#show sqa-result dns
dns test[5] result
SendPackets:1  ResponsePackets:1
Completion:success
Destination-url:abc.cn
DNS Interpret IP Address:192.0.0.100
Min/Max/Avg/Sum RTT:1010/1010/1010/1010ms
Last Probe Time:2012-07-29 09:49:36
```

1.14 网络层检测

在网络层，通过配置网络层检测协议或者检测命令，对网络中的主机和流量进行检测，探查远端是否可达、网络是否通畅等。

1.14.1 配置 ICMP 快速响应

ICMP快速响应功能是相对于ICMP慢速响应而言的。为了改善Ping包的时延和时延抖动，快速ICMP响应功能缩短了时延，提高网络时延达标率。

1.配置ICMP快速响应。

命令	功能
inspur(config)#**ip icmp-fast-reply**	开启ICMP的快速响应（ping）功能，该功能默认是开启的

2.维护ICMP快速响应。

对于网络层检测，有时需要用到debug调试命令，可以用来查看报文收发的具体信

息以及报文包个数统计，主要有以下几种：

命令	功能
inspur#**debug ip icmp**	打开ICMP协议的debug功能，显示ICMP协议处理的调试信息，同时关闭ICMP快ping功能
inspur#**debug ip icmp detail**	打开ICMP协议的debug功能，显示ICMP协议处理的详细调试信息，同时关闭ICMP快速响应功能
inspur#**debug ip interface**<*interface-name*>	打开配置接口上发出和接收到的IP协议的debug功能，显示IP协议处理的调试信息，同时关闭ICMP快速响应功能
inspur#**debug ip**	打开IP协议的debug功能，显示协议栈IP层处理的调试信息，同时关闭ICMP快速响应功能
inspur#**show debug icmp**	显示已经打开的ICMP协议debug功能相关开关
inspur#**show debug ip**	显示已经打开的IP协议debug功能相关开关
inspur#**show ip traffic**	查看IP/ICMP/UDP/TCP层报文收发统计
inspur#**clear ip traffic**	清除IP/ICMP/UDP/TCP层报文收发统计

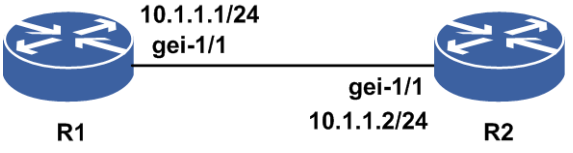
举例

ICMP快速响应配置实例如下。

•配置说明

如*图 1-39*所示，R1接口gei-1/1和R2接口gei-1/1直接连接，要求R1与R2能够互相快速ICMP响应（ping）。

图 1-39 ICMP 快速响应配置实例拓扑图



•配置思路

i.配置R1和R2接口的IP地址。

ii.测试配置结果，确认R1和R2能够快速ICMP响应（ping）。

•配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
```

```
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ip address 10.1.1.1 255.255.255.0
R1(config-if-gei-1/1)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 10.1.1.2 255.255.255.0
R2(config-if-gei-1/1)#exit
```

•配置验证

在R1上验证结果：

```
R1#ping 10.1.1.2
sending 5,100-byte ICMP echoes to 10.1.1.2,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/21 ms.
```

在R2上验证结果：

```
R2#ping 10.1.1.1
sending 5,100-byte ICMP echoes to 10.1.1.2,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/21 ms.
```

提示：

默认情况下ICMP快速响应功能是使能的。如打开相应的debug命令，再进行ping操作，则关闭了ICMP快速响应（ping）功能。

1.14.2 配置 IP 源路由选项处理

IP允许源主机通过网络预先指定一个路径，称为源路由。如果指定了源路由，系统就按照指定的源路径转发信息包。当需要强制一个包采用指定的路径通过网络时，就可以使用源路由指定功能进行处理。

IP数据报文中有选项字段，选项字段是变长的，主要用于网络测试和调试。

1.配置IP源路由选项的处理。

命令	功能
inspur(config)#**ip source-route**	使能路由器处理带IP源路由选项的数据报文

2.查看IP源路由选项的配置。

命令	功能
inspur#**show running-config ip all**	显示是否配置了**ip source-route**

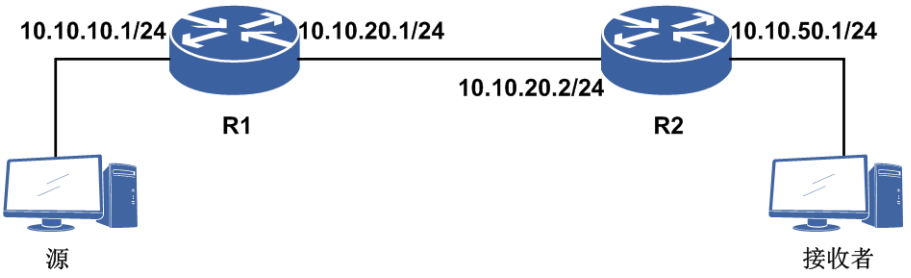
举例

IP源路由选项的处理的配置实例如下。

•配置说明

如*图 1-40*所示，配置路由器对IP源路由进行选择处理。

图 1-40 IP 源路由选项处理配置实例



•配置思路

i.配置IGP路由、单播路由互通。

ii.R1上配置源路由选项。

iii.源发送带有正确IP选项的IP报文。

iv.源发送带有错误IP选项的IP报文。

•配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ip address 10.10.20.1 255.255.255.0
R1(config-if-gei-1/1)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 10.10.10.0 0.0.0.255
R1(config-ospf-1-area-0)#network 10.10.20.0 0.0.0.255
R1(config-ospf-1-area-0)#exit
R1(config-ospf-1)#exit
R1(config)#ip source-route
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 10.10.20.2 255.255.255.0
R2(config-if-gei-1/1)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 10.10.20.0 0.0.0.255
R2(config-ospf-1-area-0)#network 10.10.50.0 0.0.0.255
R2(config-ospf-1-area-0)#exit
```

•配置验证

源发送带有正确IP选项的IP报文时，流量正常转发。

源发送带有错误IP选项的IP报文时，报文被丢弃。

1.14.3 配置 ICMP 不可达报文有效

在ICMP接口配置模式下，配置接口发送报文不可达的功能有效。

1.配置ICMP不可达报文有效。

命令	功能
inspur(config)#**icmp-config**	进入ICMP配置模式
inspur(config-icmp)#**interface**<*interface-name*>	进入ICMP接口配置模式
inspur(config-icmp-if-interface-name)#**ip unreachable**	使接口发送报文不可达的功能有效

2.查看配置ICMP不可达报文有效。

命令	功能
inspur#**debug ip icmp detail**	查看ICMP报文打印信息

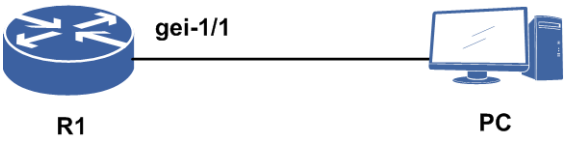
举例

ICMP不可达报文有效配置实例如下。

•配置说明

收到未知协议报文，ICMP不可达报文有效的拓扑，如*图 1-41*所示。

图 1-41 ICMP 不可达报文有效配置实例



•配置思路

i.进入ICMP配置模式。

ii.到指定的接口，配置ICMP不可达报文。

iii.配置接口ICMP不可达报文有效。

•配置过程

R1上配置如下：

```
R1(config)#icmp-config
R1(config-icmp)#interface gei-1/1
R1(config-icmp-if-gei-1/1)#ip unreachable
R1(config-icmp-if-gei-1/1)#exit
R1(config-icmp)#exit

R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 60.0.0.1 255.255.255.0
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ip forward unreachable
```

```
R1(config-if-gei-1/1)#exit
```

•配置验证

PC上发送未知协议报文，发给设备，设备上发送ICMP不可达报文给PC。

1.14.4 配置接口发送报文不可达有效

配置接口发送报文不可达有效命令后，转发平面会把未知协议的报文或者查不到路由的报文上送控制平面，由控制平面给源节点回复一个ICMP不可达报文。缺省情况下功能未开启时，对于该类报文转发平面会进行丢弃处理。

1.配置接口发送ICMP不可达报文有效。

命令	功能
inspur(config)#**interface**<*interface-name*>	进入接口配置模式
inspur(config-if-interface-name)#**ip forward unreachable**	开启接口发送报文不可达的功能，目前支持以太接口、POS接口

2.查看ICMP报文打印信息。

命令	功能
inspur#**debug ip icmp detail**	查看ICMP报文打印信息

举例

接口发送报文不可达有效功能的配置实例如下。

•配置说明

对未知目的路由的报文，接口发送ICMP不可达报文的拓扑，如*图 1-42*所示。

图 1-42 接口发送 ICMP 不可达报文配置实例



•配置思路

i.配置设备的接口地址。

ii.配置到达非直连设备的静态路由。

iii.配置接口ICMP不可达报文有效。

•配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 10.1.1.1 255.255.255.0
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit

R1(config)#ip route 1.2.3.4 255.255.255.255 10.1.1.2
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 10.1.1.2 255.255.255.0
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip forward unreachable
R2(config-if-gei-1/1)#exit

R2(config)#icmp-config
R2(config-icmp)#interface gei-1/1
R2(config-icmp-if-gei-1/1)#ip unreachable
R2(config-icmp-if-gei-1/1)#exit
```

•配置验证

R2并无达到1.2.3.4/32的路由。

在R2上打开**debug ip icmp detail**，在R1上**ping 1.2.3.4**，可以看到R2发送主机不可达的报文给R1。

1.14.5 配置 IP Ping

Ping命令发送ICMP Echo报文，如果目的地收到一个ICMP Echo回显报文，就发送一个ICMP Echo Reply响应报文到发送Echo报文的源地址。因此，可以用Ping命令来诊断网络的连通问题。

一般来说，如果不能Ping到某台主机，那么就不能Telnet或者FTP到那台主机。反过来，如果不能Telnet到某台主机，那么通常可以用Ping程序来确定问题出在哪里。Ping程序还能测出到这台主机的往返时间，以表明该主机有“多远”。

1.配置IP Ping功能。

命令	功能
inspur>**ping** [**vrf** <*vrf-name*>]{<*ip-address*>|**domain** <*domain-name*>}	在用户模式下的Ping命令
inspur#**ping** [{**dcn**|**vrf** <*vrf-name*>}]{<*ip-address*>|**domain** <*domain-name*>}[**df-bit** <*don't-frag*>][**pattern** <*string*>][**speed** {**limit** {**0** |<*limit-num*>}| **interval** <*interval-number*>}][**repeat** <*repeat-count*>][**size** <*datagram-size*>][**source** <*source-address*>][**timeout** <*timeout*>][**tos** <*tos*>][**ttl** <*ttl*>][**option** {[{**loose** | **strict**}<*source-route-address*>][**record** <*record-hops*>][**timestamp** <*record-timestamps*>][**none**]}][**interface** <*interface-name*>]	在特权模式下的Ping命令
inspur#**ping vrf** <*vrf-name*><*ip-address*>	Ping IP地址所属的VRF名称，长度

命令	功能
	为1~32个字符
inspur#**ping dcn** <*ip-address*>	Ping DCN的IP地址
inspur#**ping domain** <*domain-name*>	Ping DNS域名

domain <*domain-name*>：DNS域名，长度为1~128个字符。

repeat<*repeat-count*>：需要重复测试的次数，范围1~65535，缺省为5次。

size <*datagram-size*>：Ping信息包的大小，范围36~8192，缺省为100字节。

timeout <*timeout*>：超时时间，单位：秒，范围1~20。

tos <*tos*>：设置发送包的服务类型，范围0~255，缺省为0。

ttl <*ttl*>：设置TTL值，范围1~255。

df-bit <*don't-frag*>：设置不分片标志，取值为0或1，缺省为0，表示允许分片。

pattern <*pad*>：报文中带的pad填充字段值。

option：是否需要配置IP选项，取值为1时，表示可以配置IP选项。

speed limite <*limite-num*>：1秒中发出的ping包个数。

speed interval<*interval-seconds*>：两个数据请求包之间的时间间隔，单位：秒，范围2~10。

loose | **strict** <*source-route-address*>：指定的源站路由路径，为十进制点分形式。

record <*record-hops*>：所需的记录的最大路由数，范围1~9。

timestamp <*record-timestamps*>：所须记录的最大时间戳数，范围1~9。

2.维护IP Ping。

命令	功能
inspur#**debug ip icmp**	打印ping时，发送和接收ICMP报文的情况

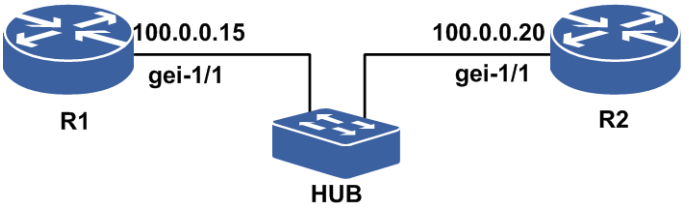
举例

IP Ping功能的配置实例如下。

·配置说明

如*图 1-43*所示，两台设备同一网段的接口使用Ping检测连通性。

图 1-43 IP Ping 配置实例拓扑图



•配置思路

i.进入接口模式下，为需要进行通讯的接口配置IP地址。

ii.在特权模式下，执行ping命令。

•配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ip address 100.0.0.15 255.255.255.0
R1(config-if-gei-1/1)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 100.0.0.20 255.255.255.0
R2(config-if-gei-1/1)#exit
```

•配置验证

在R1上用Ping命令验证连通性：

```
R1#ping 100.0.0.20
sending 5,100-byte ICMP echoes to 100.0.0.20,timeout is 2 seconds.
!!!!!      /*打印结果，表示能够Ping通，链路通畅*/
Success rate is 100 percent(5/5),round-trip min/avg/max= 17/18/20 ms.

R1#ping 100.0.0.21
sending 5,100-byte ICMP echoes to 100.0.0.21,timeout is 2 seconds.
.....      /*打印结果，表示不能Ping通，链路有问题*/
Success rate is 0 percent(0/5).
```

1.14.6 配置 IP Trace

Trace主要用于调测，其功能是打印IP数据包，显示从一台主机到另一台主机所经过的路由。由于IP包的首部中留给选项的空间有限，因此不能使用路由记录选项。IP Trace使用ICMP报文和IP首部中的TTL字段来实现其功能。

1.配置IP Trace。

命令	功能
inspur>**trace** [**vrf** <*vrf-name*>]<*ip-address*>	在用户模式下的Trace命令
inspur#**trace** [{**dcn**|**vrf** <*vrf-name*>}]{<*ip-address*>|**domain**	在特权模式下的Trace命令

命令	功能
<*domain-name*>}[**source** <*source-address*>][**maxttl** <*ttl*>][**timeout** <*timeout*>]	

Trace命令使用ICMP出错报文工作，这是在数据包超过TTL值时产生的。Trace命令通过发送TTL值为1的报文启动，引起第一个路由器丢弃该数据报文并发送一个错误报文。TTL超时报文表示一个中间路由器收到了该报文并放弃了探测；目标不可达出错报文表示目标节点收到该报文，但无法提交该报文。如果定时器在应答到来之前已经停止，Trace则输出打印一个“*”号。

2.查看IP Trace。

以下是一个在特权模式下使用**trace**命令的实例，跟踪到168.1.10.100的路径。

```
inspur#trace 168.1.10.100
tracing the route to 168.1.10.100
1    168.1.10.100    2 ms  3 ms  5 ms
[finished]
```

以上命令的输出示例说明如下。

命令输出	描述
1	表示到目标的路由中的路由器的顺序号
168.1.10.100	路由中某一跳路由器的IP，最后一个为目的IP
2 ms 3 ms 5 ms	要发送的三个探测中每一个的环绕时间

举例

IP Trace的配置实例如下。

•配置说明

如*图 1-44*所示，inspur上通过Trace命令检测到达Router所经过的路径。

图 1-44 IP Trace 配置实例拓扑图



•配置思路

i.配置接口地址和路由。

ii.在特权模式下，执行**trace**命令。

•配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
```

```
R1(config-if-gei-1/1)#ip address 100.0.0.15 255.255.255.0
R1(config-if-gei-1/1)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 100.0.0.0 0.0.0.255
R1(config-ospf-1-area-0)#end
```

•配置验证

R1上执行Trace命令的结果如下：

```
R1#trace 175.103.59.110
tracing the route to 175.103.59.110  over a maximum of 30 hops:
1   100.0.0.22 55 ms 2 ms 2 ms       /*第一跳设备IP地址和时延信息*/
2   10.17.94.81 176 ms 143 ms 333 ms
3   10.28.5.61 131 ms 133 ms 134 ms
4    *  *  *                        /*第四跳设备没有返回报文，打*号*/
5   202.70.62.169 151 ms 149 ms 146 ms
6   202.43.177.81 176 ms 162 ms 165 ms
7   218.100.27.30 142 ms 134 ms 159 ms
8   175.103.59.110 140 ms 166 ms 138 ms
 [finished]
```

1.14.7 配置 LSP Ping

在MPLS网络中，使用IP Ping时，Ping报文会被打上标签，并在MPLS网络中进行标签交换。但是IP Ping只能检查IP层面的连通性，无法检测MPLS LSP链路是否存在问题。因为在MPLS网络环境中，如果两台LSR之间的LDP会话断开，标签无法进行标记转发，但此时IP Ping是可达的，而LSP却存在故障。

LSP存在故障的因素较多，包括LDP会话中断、某些LSR上LDP协议未启用、LDP标签转发表异常等，这就需要一个不同于IP Ping的机制来检测端到端的LSP是否正常，即LSP Ping。

1.配置LSP Ping。

命令	功能
inspur#**ping mpls ipv4** <*ip-address*><*mask-length*>[**output-interface** <*interface-name*>][**destination** <*start-ipv4-address*>[<*end-ipv4-address*>][<*increment*>]][**repeat** <*repeat-count*>| **size** <*datagrame-size*>| **timeout** <*timeout*>| **source** {<*source-ipv4-address*>|<*source-ipv6-address*>}| **ttl** <*ttl*>]	IPv4 LDP LSP的PING检测
inspur#**ping mpls traffic-eng te_tunnel**<*id*>[{**master**|**slave**}][**repeat** <*repeat-count*>| **size** <*datagrame-size*>| **timeout** <*timeout*>| **source** {<*source-ipv4-address*>|<*source-ipv6-address*>}| **ttl** <*ttl*>]	RSVP LSP的PING检测
inspur#**ping mpls pseudowire** [**multisegment**]<*pw-name*>[**repeat** <*repeat-count*>| **size** <*datagrame-size*>| **timeout** <*timeout*>| **source** {<*source-ipv4-address*>|<*source-ipv6-address*>}| **ttl** <*ttl*>]	PWE3 LSP的PING检测

<*repeat-count*>：需要重复的次数，范围：1~65535，缺省为5。

<*datagram-size*>：LSP Ping信息包的大小，范围：100~1500，单位：byte，缺省为120bytes。

<*timeout*>：超时时间，单位：秒，范围：1~20，缺省为2。

master ：指定主LSP发送LSP Ping报文。

slave ：指定备LSP发送LSP Ping报文。

multisegment：使能Ping多段伪线功能。

2.维护LSP Ping。

命令	功能
inspur#**debug lspv** {**error** | **event** | **packet** | **tlv** | **all**}	LSP Ping时，发送的UDP echo request报文和接收的UDP echo reply报文等信息

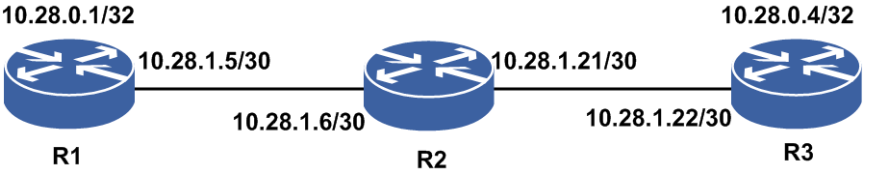
LSP Ping的配置实例如下。

LDP LSP Ping配置实例

•配置说明

如*图 1-45*所示，三台路由器R1、R2、R3，启用LDP协议，R1上进行LSP Ping检测连通性。

图 1-45 LDP LSP Ping 的配置实例



•配置思路

i.搭建LDP环境

ii.在R1上执行LDP LSP Ping

•配置过程

LDP的配置省略，可参考MPLS配置实例。

•配置验证

R1上ping对端结果如下：

```
R1#ping mpls ipv4 10.28.0.4 32
sending 5,120-byte MPLS echo(es) to 10.28.0.4,timeout is 2 second(s).
Codes: '!' - success,              'Q' - request not sent,      '.' - timeo
ut,
      'L' - labeled output interface, 'B' - unlabeled output interface,
      'D' - DS Map mismatch,         'F' - no FEC mapping,        'f' - FEC
```

```
m
ismatch,
      'M' - malformed request,       'm' - unsupported tlvs,      'N' - no
rx
 label,
      'P' - no rx intf label prot,    'p' - premature termination of LSP,
      'R' - transit router,          'I' - unknown upstream index, 'X' - unkno
wn return code, 'x' - return code 0
      'd' - DDMAP
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 5/38/151 ms.
```

R1上ping对端（不匹配的FEC）结果如下：

```
R1#ping mpls ipv4 10.28.0.4 30
sending 5,120-byte MPLS echo(es) to 10.28.0.4,timeout is 2 second(s).
Codes: '!' - success,               'Q' - request not sent,      '.' - timeo
ut,
      'L' - labeled output interface, 'B' - unlabeled output interface,
      'D' - DS Map mismatch,         'F' - no FEC mapping,        'f' - FEC
m
ismatch,
      'M' - malformed request,       'm' - unsupported tlvs,      'N' - no
rx
 label,
      'P' - no rx intf label prot,    'p' - premature termination of LSP,
      'R' - transit router,          'I' - unknown upstream index, 'X' - unkno
wn return code, 'x' - return code 0
      'd' - DDMAP
QQQQQ
Success rate is 0 percent(0/5).
```

从此次ping不成功可以看出，LSP Ping会检查<FEC目的地址+掩码>信息是否正确，否则LSP ping会不成功。

R1上ping对端（不存在的FEC）结果如下：

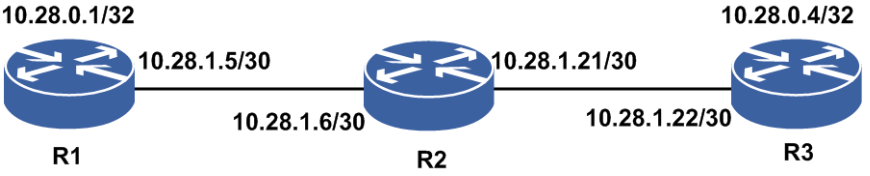
```
R1#ping mpls ipv4 9.9.9.8 32
sending 5,120-byte MPLS echo(es) to 9.9.9.8,timeout is 2 second(s).
Codes: '!' - success,               'Q' - request not sent,      '.' - timeo
ut,
      'L' - labeled output interface, 'B' - unlabeled output interface,
      'D' - DS Map mismatch,         'F' - no FEC mapping,        'f' - FEC
m
ismatch,
      'M' - malformed request,       'm' - unsupported tlvs,      'N' - no
rx
label,
      'P' - no rx intf label prot,    'p' - premature termination of LSP,
      'R' - transit router,          'I' - unknown upstream index, 'X' - unkno
wn return code, 'x' - return code 0
      'd' - DDMAP
QQQQQ
Success rate is 0 percent(0/5).
```

RSVP LSP Ping配置实例

·配置说明

如*图 1-46*所示，三台路由器R1、R2、R3，启用RSVP协议，搭建OSPF-TE的环境，R1上进行LSP Ping检测连通性。

图 1-46 RSVP LSP Ping 配置实例



•配置思路

i.搭建OSPF-TE环境

ii.在R1上执行RSVP LSP Ping

•配置过程

RSVP的配置省略，可参考OSPF-TE配置实例。

•配置验证

R1上查看配置情况：

```
R1#show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:          running
    RSVP Process:                 running
    Forwarding:                   enabled
TUNNEL NAME          DESTINATION     UP IF DOWN IF     STATE/PROT
tunnel_4000          10.28.0.5       -     unknown     up/down
tunnel_1             10.28.0.4       -     gei-1/2     up/up
```

R1上测试隧道连通性：

```
R1#ping mpls traffic-eng te_tunnel1   /*R1上LSP Ping UP的TE隧道*/
sending 5,120-byte MPLS echo(es) to te_tunnel1,timeout is 2 second(s).

Codes: '!' - success,                'Q' - request not sent,       '.' - timeo
ut,
      'L' - labeled output interface, 'B' - unlabeled output interface,
      'D' - DS Map mismatch,         'F' - no FEC mapping,         'f' - FEC
m
ismatch,
      'M' - malformed request,       'm' - unsupported tlvs,       'N' - no
rx
 label,
      'P' - no rx intf label prot,    'p' - premature termination of LSP,
      'R' - transit router,          'I' - unknown upstream index, 'X' - unkno
wn return code, 'x' - return code 0
      'd' - DDMAP
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 2/3/6 ms.

R1#ping mpls traffic-eng te_tunnel4000   /*R1上LSP Ping Down的TE隧道*/
sending 5,120-byte MPLS echos to te_tunnel4000,timeout is 2 seconds.

Codes: '!' - success,                'Q' - request not sent,       '.' - timeo
ut,
      'L' - labeled output interface, 'B' - unlabeled output interface,
      'D' - DS Map mismatch,         'F' - no FEC mapping,         'f' - FEC
m
ismatch,
      'M' - malformed request,       'm' - unsupported tlvs,       'N' - no
rx
 label,
      'P' - no rx intf label prot,    'p' - premature termination of LSP,
```

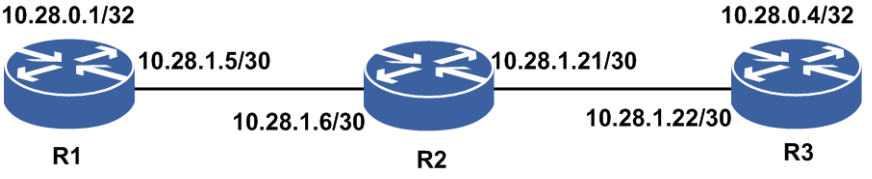
```
      'R' - transit router,          'I' - unknown upstream index, 'X' - unkno
wn return code, 'x' - return code 0
      'd' - DDMAP
QQQQQ
Success rate is 0 percent(0/5).
```

PWE3 LSP Ping的配置实例

·配置说明

如*图 1-47*所示，三台路由器R1、R2、R3，搭建L2VPN的环境，R1上进行LSP Ping检测连通性。

图 1-47 PWE3 LSP Ping 的配置实例



·配置思路

i.搭建L2VPN环境。

ii.在R1上执行PWE3 LSP Ping。

·配置过程

LDP的基本配置这里省略。

·配置验证

R1上查看配置情况：

```
R1#show l2vpn forwardinfo vpnname Inspur
Hearders: PWType - Pseudowire type and Pseudowire connection mode
        Llabel - Local label, Rlabel - Remote label
        VPNowner - owner type and instance name
Codes:   H - HUB mode, S - SPOKE mode, L - VPLS, W - VPWS, M - MSPW, MO -
MONITOR
       $pw - auto_
PWName   PeerIP         FEC PWType     State Llabel  Rlabel  VPNowner
pw1      10.28.0.4    128 Ethernet  H UP    81938   82241   L:Inspur
```

R1上测试连通性：

```
R1#ping mpls pseudowire pw1
sending 5,120-byte MPLS echo(es) to 10.28.0.4,timeout is 2 second(s).
Codes: '!' - success,               'Q' - request not sent,      '.' - timeo
ut,
      'L' - labeled output interface, 'B' - unlabeled output interface,
      'D' - DS Map mismatch,         'F' - no FEC mapping,        'f' - FEC
m
ismatch,
      'M' - malformed request,       'm' - unsupported tlvs,      'N' - no
rx
 label,
      'P' - no rx intf label prot,    'p' - premature termination of LSP,
      'R' - transit router,          'I' - unknown upstream index, 'X' - unkno
wn return code, 'x' - return code 0
      'd' - DDMAP
!!!!!
```

```
Success rate is 100 percent(5/5),round-trip min/avg/max= 2/2/2 ms.
```

1.14.8 配置 LSP Trace

MPLS Trace是一种检测MPLS LSP数据平面故障的方法，这个方法简单有效可以发现一些控制平面无法发现的故障，为用户提供了一种在短时间内发现和隔离路由黑洞或者路由丢失等故障的方法。

1.配置LSP Trace。

命令	功能
inspur#**trace mpls ipv4** <*ip-address*><*mask-length*>[**output-interface** <*interface-name*>][**destination** <*start-ipv4-address*>[<*end-ipv4-address*>][<*increment*>]][**ttl** <*ttl*>| **timeout** <*timeout*>| **source** {<*source-ipv4-address*>|<*source-ipv6-address*>}|[{**ddmap**|**dsmap**}]]	启用IPv4 LDP LSP Trace功能
inspur#**trace mpls traffic-eng te_tunnel** <*id*>[{**master**|**slave**}][**ttl** <*ttl*>| **timeout** <*timeout*>| **source** {<*source-ipv4-address*>|<*source-ipv6-address*>}|[{**ddmap**|**dsmap**}]]	启用RSVP LSP Trace功能
inspur#**trace mpls pseudowire** [**multisegment**]<*pw-name*>[**ttl** <*ttl*>| **timeout** <*timeout*>| **source** {<*source-ipv4-address*>|<*source-ipv6-address*>}|[{**ddmap**|**dsmap**}]]	启用PWE3 LSP Trace功能

master ：指定主LSP发送LSP Ping报文。

slave ：指定备LSP发送LSP Ping报文。

multisegment：使能Ping多段伪线功能。

2.维护LSP Trace。

命令	功能
inspur#**debug lspv** {**error** | **event** | **packet** | **tlv** | **all**}	LSP Trace时，发送的UDP echo request报文和接收的UDP echo reply报文等信息

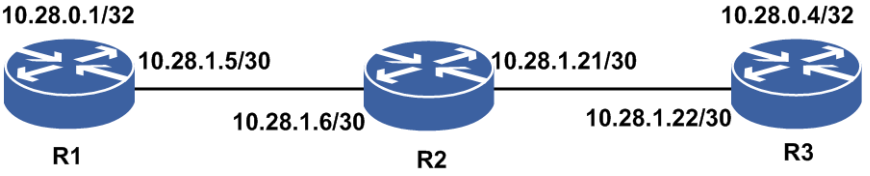
LSP Trace的配置实例如下。

LDP LSP Trace配置实例

·配置说明

如*图 1-48*所示，三台路由器R1、R2、R3，启用LDP协议，R1上进行LSP Trace检测连通性。

图 1-48 LDP LSP Trace 配置实例



•配置思路

i.搭建LDP环境。

ii.在R1上执行LDPLSP Trace。

•配置过程

LDP的配置这个省略，可参考MPLS配置实例。

•配置验证

R1上查看配置情况：

```
R1#show mpls forwarding-table
Local     Outgoing  Prefix or         Outgoing       Next Hop       M/S
label     label     Lspname           interface
20        Pop tag   10.28.0.3/32      gei-0/2        10.28.1.6      M
57        49        10.28.0.4/32      gei-0/2        10.28.1.6      M

R1#trace mpls ipv4 10.28.0.3 32
Tracing MPLS Lable Switched to 10.28.0.3,timeout is 3 second(s).
 Codes:'!' - success,               'Q' - request not sent,      '*' - timeo
ut,
      'L' - labeled output interface, 'B' - unlabeled output interface,
      'D' - DS Map mismatch,         'F' - no FEC mapping,        'f' - FEC
m
ismatch,
      'M' - malformed request,       'm' - unsupported tlvs,      'N' - no
rx
 label,
      'P' - no rx intf label prot,    'p' - premature termination of LSP,
      'R' - transit router,          'I' - unknown upstream index, 'X' - unkno
wn return code, 'x' - return code 0
      'd' - DDMAP
   0   10.28.1.5 MTU 1500 [label 3 ]
!  1   10.28.1.6  10 ms
[finished]
```

R1上测试trace：

```
R1#trace mpls ipv4 10.28.0.4 32
  Tracing MPLS Lable Switched to 10.28.0.4,timeout is 3 second(s).
 Codes:'!' - success,               'Q' - request not sent,      '*' - timeo
ut,
      'L' - labeled output interface, 'B' - unlabeled output interface,
      'D' - DS Map mismatch,         'F' - no FEC mapping,        'f' - FEC
m
ismatch,
      'M' - malformed request,       'm' - unsupported tlvs,      'N' - no
rx
 label,
      'P' - no rx intf label prot,    'p' - premature termination of LSP,
      'R' - transit router,          'I' - unknown upstream index, 'X' - unkno
wn return code, 'x' - return code 0
      'd' - DDMAP
   0   10.28.1.5 MTU 1500 [label 49 ]
```

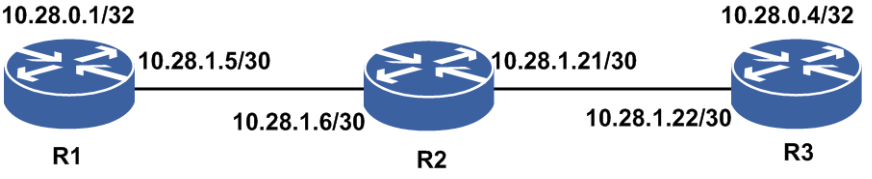
```
R  1   10.28.1.21 MTU 1500 [label 0 ]  8 ms
!  2   10.28.1.22  7 ms
[finished]
```

RSVP LSP Trace配置实例

•配置说明

如*图 1-49*所示，三台路由器R1、R2、R3，启用RSVP协议，搭建OSPF-TE的环境，R1上进行LSP Trace检测连通性。

图 1-49 RSVP LSP Trace 配置实例



•配置思路

i.搭建OSPF-TE环境

ii.在R1上执行RSVP LSP Trace

•配置过程

RSVP的配置省略，可参考OSPF-TE配置实例。

•配置验证

R1上查看配置情况：

```
R1#show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:           running
    RSVP Process:                 running
    Forwarding:                   enabled
TUNNEL NAME         DESTINATION     UP IF DOWN IF     STATE/PROT
tunnel_1            10.28.0.4       -     gei-0/8     up/up
```

R1上测试trace：

```
R1#trace  mpls traffic-eng te_tunnel1
Tracing MPLS Lable Switched to te_tunnel1,timeout is 3 second(s).
 Codes:'!' - success,                'Q' - request not sent,       '*' - timeo
ut,
      'L' - labeled output interface, 'B' - unlabeled output interface,
      'D' - DS Map mismatch,          'F' - no FEC mapping,         'f' - FEC
m
ismatch,
      'M' - malformed request,        'm' - unsupported tlvs,       'N' - no
rx
 label,
      'P' - no rx intf label prot,    'p' - premature termination of LSP,
      'R' - transit router,           'I' - unknown upstream index, 'X' - unkno
wn return code, 'x' - return code 0
      'd' - DDMAP
   0  10.28.1.5 MTU 1500 [label 147457 ]
R  1  10.28.1.6 MTU 1500 [label 3 ]  3 ms
!  2  10.28.1.22 4 ms
[finished]
```

1.14.9 配置组播 Ping

组播Ping通过发送ICMP请求报文到组播组地址，并且等待远端的ICMP回应报文。组播Ping可以从组播分发树上的任意节点（除组播接收者外）发起，目的地址为组播组地址，通过组播转发路径转发到组播接收者节点，通过单播回应ICMP响应报文。

1.配置组播Ping。

命令	功能
inspur#**ping** [**vrf** *<vrf-name>*]*<ip-address>*{[**df-bit** *<don't-frag>*][**repeat** *<repeat-count>*][**size** *<datagram-size>*][**source** *<source-address>*][**timeout** *<timeout>*][**tos** *<tos>*][**ttl** *<ttl>*]**option**{[{**loose** | **strict**}*<source-route-address>*][**record** *<record-hops>*][**timestamp** *<record-timestamps>*][**none**]}][**pattern** *<pad>*][**speed** {**limit** *<limite-num>*| **interval** *<interval-seconds>*}]}	在除用户模式外的其他所有模式下的组播ping命令

<repeat-count>：需要重复测试的次数，范围1~4294967295，缺省为5次。

<datagram-size>：Ping信息包的大小，范围36~8192，缺省为100字节。

<timeout>：超时时间，单位：秒，范围1~20。

<tos>：设置发送包的服务类型，范围0~255，缺省为0。

<ttl>：设置TTL值，范围1~255。

<don't-frag>：设置不分片标志，取值为0或1，缺省为0，表示允许分片。

<pad>：报文中带的pad填充字段值。

option：是否需要配置IP选项，取值为1时，表示可以配置IP选项。

<limite-num>：1秒中发出的ping包个数。

<interval-seconds>：两个数据请求包之间的时间间隔，单位：秒，范围2~10。

loose | **strict** *<source-route-address>*：指定的源站路由路径，为十进制点分形式。

<record-hops>：所需的记录的最大路由数，范围1~9。

<record-timestamps>：所须记录的最大时间戳数，范围1~9。

2.维护组播Ping。

命令	功能
inspur#**debug ip icmp**	打印执行组播ping的时候发送和接收到的ICMP报文

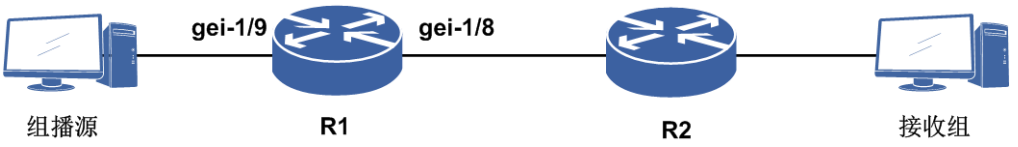
举例

组播Ping的配置实例如下。

·配置说明

如*图 1-50*所示，检查组播最后一跳是否可达。

图 1-50 组播 Ping 的配置实例



•配置思路

i.按图搭建环境。

ii.R1和R2上启动PIM-SM协议。

iii.接收者加入组播组。

iv.R1上ping组播组地址。

•配置过程

R1上配置如下：

```
R1(config)#interface gei-1/9
R1(config-if-gei-1/9)#no shutdown
R1(config-if-gei-1/9)#ip address 12.131.1.1 255.255.255.0
R1(config-if-gei-1/9)#exit
R1(config)#interface gei-1/8
R1(config-if-gei-1/8)#no shutdown
R1(config-if-gei-1/8)#ip address 17.1.1.2 255.255.255.0
R1(config-if-gei-1/8)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 3.3.3.3 255.255.255.0
R1(config-if-loopback1)#exit
/*下面配置组播协议*/
R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#rp-candidate loopback1
R1(config-mcast-pim)#bsr-candidate loopback1
R1(config-mcast-pim)#interface gei-1/9
R1(config-mcast-pim-if-gei-1/9)#pimsm
R1(config-mcast-pim-if-gei-1/9)#exit
R1(config-mcast-pim)#interface gei-1/8
R1(config-mcast-pim-if-gei-1/8)#pimsm
R1(config-mcast-pim-if-gei-1/8)#end
```

R2上配置类似R1，配置IP地址和组播协议。

R2上增加一条到RP的静态路由：

```
R2(config)#ip route 3.3.3.3 255.255.255.255 17.1.1.2
```

•配置验证

接收组加入组播组225.0.0.1，在R1上操作：

```
R1#ping 225.0.0.1
sending 5,100-byte ICMP echoes to 225.0.0.1,timeout is 2 seconds.
Reply to request 1 received from 17.1.1.1, 2 ms
Reply to request 2 received from 17.1.1.1, 2 ms
Reply to request 3 received from 17.1.1.1, 2 ms
Reply to request 4 received from 17.1.1.1, 2 ms
Reply to request 5 received from 17.1.1.1, 2 ms

Success rate is 100 percent(5/5),round-trip min/avg/max= 2/2/2 ms.
```

1.14.10 配置组播 Trace

组播Trace为组播路由监测和RPF检测提供了方法，通过发送和接收IGMP协议报文来判断组播路径的连通性。

配置组播Trace。

命令	功能
inspur#**mtrace** <*source-address*>[<*destination-address*>][<*group-address*>]	显示从目的地址到反向组播路径源的路径

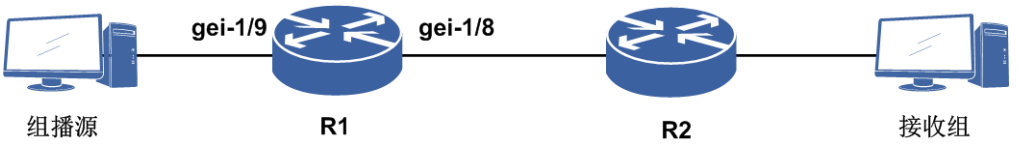
举例

组播Trace的配置实例如下。

•配置说明

配置举例通过（S,G）或者（*,G）路由条目查找下一跳路由，组网如*图 1-51*所示。

图 1-51 组播 Trace 配置实例



•配置思路

i.R1和R2启动PIM-SM协议。

ii.接收组加入组播组，源发送组播流。

iii.R2上进行mtrace。

•配置过程

R1上配置如下：

```
R1(config)#interface gei-1/9
R1(config-if-gei-1/9)#no shutdown
R1(config-if-gei-1/9)#ip address 12.131.1.1 255.255.255.0
R1(config-if-gei-1/9)#exit
R1(config)#interface gei-1/8
R1(config-if-gei-1/8)#no shutdown
R1(config-if-gei-1/8)#ip address 17.1.1.2 255.255.255.0
R1(config-if-gei-1/8)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 3.3.3.3 255.255.255.0
R1(config-if-loopback1)#exit
/*下面配置组播协议*/
R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#rp-candidate loopback1
R1(config-mcast-pim)#bsr-candidate loopback1
R1(config-mcast-pim)#interface gei-1/9
```

```
R1(config-mcast-pim-if-gei-1/9)#pimsm
R1(config-mcast-pim-if-gei-1/9)#exit
R1(config-mcast-pim)#interface gei-1/8
R1(config-mcast-pim-if-gei-1/8)#pimsm
R1(config-mcast-pim-if-gei-1/8)#end
```

R2上配置类似R1，配置IP地址和组播协议。

R2上增加一条到RP的静态路由：

```
R2(config)#ip route 3.3.3.3 255.255.255.255 17.1.1.2
```

•配置验证

接收组加入组播组225.0.0.1，源发组播流：

```
R2#mtrace 12.131.1.2  17.1.1.1  225.0.0.1
 Type escape sequence to abort.
Mtrace from 12.131.1.2 to 17.1.1.1 via group 225.0.0.1
0 17.1.1.1 PIM  21 ms
-1 17.1.1.2 PIM  76 ms
-2 12.131.1.1 PIM  76 ms
[finished]
```

1.14.11 配置 IP 调试命令

对于IP相关功能复杂故障的处理，有时需要用到debug调试命令。

IP debug调试命令，主要有以下几种。

命令	功能
inspur#**debug ip**	打开IP协议的debug功能，显示IP协议处理的调试信息，显示路由器是否在发送IP报文，以及是否在接受IP报文
inspur#**debug ip interface** <*interface-name*>	打开从指定接口上发出和接收到的IP协议的debug功能，显示IP协议处理的调试信息
inspur#**show debug ip**	显示已经打开的IP协议debug功能相关开关

1.15 LLDP

LLDP是一种链路层发现协议，网络管理系统可以通过LLDP协议快速掌握二层网络的拓扑及其变化情况。LLDP 将本地设备的信息组织成TLV封装在LLD PDU中发送给直连的邻居，同时将邻居发来的LLD PDU以标准MIB的形式保存起来，供网络管理系统查询及判断链路的通信状况。

1.15.1 配置 LLDP

本节介绍LLDP功能的配置步骤和命令。

1.配置LLDP。

步骤	命令	功能
1	inspur(config)#**lldp**	从配置模式下进入LLDP配置模式
2	inspur(config-lldp)#**hellotime** <*time*>	配置LLDP邻居发现报文发送时间间隔，单位：秒，范围：5~32768，默认30
	inspur(config-lldp)#**holdtime** <*time*>	配置LLDP邻居保持时间，<*times*>为邻居发现报文时间间隔的倍数，范围：2~10，默认为4倍
	inspur(config-lldp)#**maxneighbor** <*num*>	配置LLDP可以发现的最大邻居数，范围1~128，默认128
3	inspur(config-lldp)#**lldp** {**enable** | **disable**}	打开或关闭LLDP功能
4	inspur(config-lldp)#**lldp-rx** {**enable** | **disable**}	打开或关闭LLDP接收功能
5	inspur(config-lldp)#**lldp-tx** {**enable** | **disable**}	打开或关闭LLDP发送功能
6	inspur(config-lldp)#**txcreditmax** <*credit*>	配置最大信誉数，范围1~10，默认5
	inspur(config-lldp)#**txfastinit** <*num*>	配置快速发送报文的个数，范围1~8，默认4
	inspur(config-lldp)#**msgfasttx** <*interval*>	配置快速发送报文的间隔，范围1~3600秒，默认1秒

2.接口模式下配置LLDP。

步骤	命令	功能
1	inspur(config-lldp-if-interface-name)#**lldp** {**enable** | **disable**}	接口上打开或关闭接口LLDP功能
2	inspur(config-lldp-if-interface-name)#**lldp-rx** {**enable** | **disable**}	接口上打开或关闭接口LLDP接收功能
3	inspur(config-lldp-if-interface-name)#**lldp-tx** {**enable** | **disable**}	接口上打开或关闭接口LLDP发送功能
4	inspur(config-lldp-if-interface-name)#**maxneighbor** <*num*>	配置LLDP接口可以发现的最大邻居数，范围1~8，默认8

3.验证配置结果。

命令	功能
inspur#**show lldp** {**config** [**interface** <*interface-name*>]| **entry** [**interface** <*interface-name*>]| **neighbor** [**interface** <*interface-name*>]| **statistic** [**interface**	显示LLDP的配置信息，邻居详细信息，邻居概要信息，统计信息

命令	功能
<*interface-name*>]}	

4.维护LLDP。

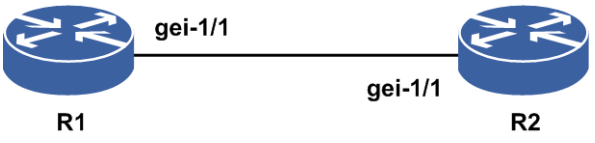
命令	功能
inspur#**debug lldp** { **adjacency** | **event** | **packets** [**receive** | **send**]| **all** }	显示LLDP相关的普通信息，事件信息，所有收发报文信息
inspur(config-lldp)#**clearneighbor**	清除已经建立的LLDP邻居
inspur(config-lldp)#**clearstatistic**	清除LLDP统计信息
inspur(config-if-interface-name)#**clearneighbor**	清除接口下已经建立的LLDP邻居
inspur(config-if-interface-name)#**clearstatistic**	清除接口下的LLDP统计信息

1.15.2 LLDP 邻居配置实例

配置说明

如*图 1-52*所示，要在R1的gei-1/1接口下使能LLDP。

图 1-52 LLDP 邻居配置实例



配置思路

1.进入LLDP的配置模式。

2.再进入某一个接口。

3.开启LLDP功能。

配置过程

在LLDP模式下进入某一接口进行配置。

```
R1(config)#lldp
R1(config-lldp)#interface gei-1/1
R1(config-lldp-if-gei-1/1)#lldp enable
R1(config-lldp-if-gei-1/1)#end
```

配置验证

用**show lldp neighbor**命令来查看配置结果：

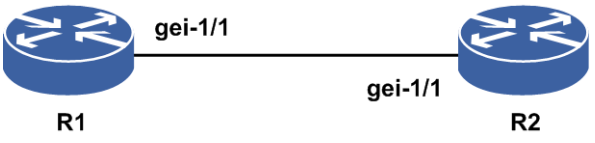
```
R1(config)#show lldp neighbor
Capability Codes:
            N - Other, r - Repeater, B - Bridge, W - WLAN Access Point,
            R - Router, T - Telephone, D - DOCSIS Cable Device,
            S - Station Only
Local-Port  Chassis-ID   Holdtime Capability  Platform         Peer-Port
-------------------------------------------------------------------------
-
gei-1/1     0023e4221134  103      B R       IR12000 V2.00.20    gei-1/1
```

1.15.3 LLDP 常用属性配置实例

配置说明

如*图 1-53*所示，在R1上配置LLDP常用属性。

图 1-53 LLDP 常用属性配置实例



配置思路

1.进入LLDP配置模式。

2.配置LLDP常用属性。

配置过程

R1上的配置如下：

```
R1(config)#lldp
R1(config-lldp)#maxneighbor 3   /*配置系统最大邻居数*/
R1(config-lldp)#hellotime 30000 /*配置LLDP邻居发现报文发送时间间隔*/
R1(config-lldp)#holdtime 8     /*配置LLDP邻居保持时间*/
R1(config-lldp)#lldp enable    /*开启DP全局功能*/
R1(config-lldp)#lldp-rx enable  /*开启DP接收功能
R1(config-lldp)#lldp-tx enable  /*开启DP发送功能*/
R1(config-lldp)#clearneighbor   /*清除已经建立的LLDP邻居*/
R1(config-lldp)#clearstatistic  /*清除LLDP统计信息*/
```

配置验证

用**show running-config lldp**命令来查看配置结果：

```
R1(config-lldp)#show running-config lldp
!<lldp>
lldp
  hellotime 30000
  holdtime 8
  maxneighbor 3
$
!</lldp>
```

2 接口配置

2.1 接口基础

IR12000系列设备上的接口可以分为两大类：物理接口和逻辑接口。接口需要正常工作必须配置有IP地址和MAC地址2个属性：

- IP地址是指给连接在因特网上的网络设备分配的一个在全世界范围内唯一的32bit标识符，应用于网络层。
- MAC地址是网络设备的硬件标识，应用于物理链路层，设备根据MAC地址进行报文转发。MAC地址具有唯一性，保证报文的正确转发。

以太网和802.3对数据帧的长度都有一个限制，其最大值分别是1500字节和1476字节。链路层的这个特性称作IP MTU。

MTU是指一种通信协议的某一层上面所能通过的最大数据报大小（以字节为单位）。

路由设备的每个接口必须具有二层MTU（L2 MTU）属性，这个属性在执行转发的过程中，对从接口发送出去的报文发生作用。路由设备在转发时，对超过接口L2 MTU的报文不能够直接发出去，需要对数据报进行分片，以使得从接口转发出去的报文不会超过接口MTU值。

设备在转发标签报文的时候，通过MPLS MTU来检查标签报文的长度，工作机制和L2 MTU类似。

2.1.1 配置 IP 地址

本节介绍接口IP地址的配置步骤和命令。

1.配置接口IP地址。

步骤	命令	功能
1	inspur(config)#**interface** <*interface-name*>	进入接口配置模式
2	inspur(config-if-interface-name)#**ip address** {<*ip-address*><*net-mask*>|<*A.B.C.D/X*>}[<*broadcast-address*>| **secondary**]	配置IP地址

secondary：配置接口的辅地址。

2.验证配置结果。

命令	功能

命令	功能
inspur#**show ip interface** [**brief** [**phy** |<*interface-name* >|[{ **exclude** | **include**}<*line*>]]]	查看当前接口下配置的IP地址信息

brief ： 显示接口的简短信息。

phy ： 显示物理接口的状态 。

exclude | include是正则表达式，**exclude**是不包括，**include**是包括。

2.1.2 配置 IP MTU

本节介绍IP MTU的配置步骤和命令。

1.配置IP MTU。

步骤	命令	功能
1	inspur(config)#**interface** {<*interface-name*>| **byname** <*byname*>}	进入需要配置IP MTU的接口下
2	inspur(config-if-interface-name)#**ip mtu** <*bytes*>	配置接口的IP MTU，单位：字节

以太口的IP MTU范围68~9202，默认值为1500，子接口的IP MTU范围68-9194，默认值为1500。

POS口的IP MTU取值范围为：68~9212， 默认值为4470。

2.验证配置结果。

命令	功能
inspur#**show ip interface** <*interface-name*>	查看接口的IP MTU值

2.1.3 配置接口 MTU

本节介绍接口MTU的配置步骤和命令。

1.配置接口MTU。

步骤	命令	功能
1	inspur(config)#**interface** {<*interface-name*>| **byname** <*byname*>}	进入接口配置模式
2	inspur(config-if-interface-name)#**mtu**	配置接口的MTU

步骤	命令	功能
	<*bytes*>	

以太接口的配置范围：1514~9216，缺省值为1600字节。

以太子接口的配置范围都是1522~9216，默认不配置的情况下继承父接口的MTU值。

POS接口的配置范围：1504~9216，缺省值为4600字节。

2.验证配置结果。

命令	功能
inspur#**show interface** [<*interface-name*>]	显示接口基本信息

<*interface-name*>为指定接口的接口名，不输入该参数显示所有接口基本信息，输入该参数显示指定接口基本信息。

2.1.4 启动或关闭接口

本节介绍启动或者关闭接口的配置步骤和命令。

1.启动接口。

步骤	命令	功能
1	inspur(config)#**interface** {<*interface-name*>| **byname** <*byname*>}	进入接口配置模式
2	inspur(config-if-interface-name)#**no shutdown**	启动接口

2.关闭接口。

步骤	命令	功能
1	inspur(config)#**interface** {<*interface-name*>| **byname** <*byname*>}	进入接口配置模式
2	inspur(config-if-interface-name)#**shutdown**	关闭接口

3.验证配置结果。

命令	功能
inspur#**show ip interface** [**brief** [**phy** |<*interface-name* >|[{ **exclude** | **include**}<*line*>]]]	查看当前接口的管理状态

brief ： 显示接口的简短信息。

phy ： 显示物理接口的状态。

exclude | include是正则表达式，**exclude**是不包括，**include**是包括。

<*interface-name*>为指定接口的接口名，不输入该参数显示所有接口基本信息，输入该参数显示指定接口基本信息。

2.1.5 配置接口别名和描述信息

本节介绍接口别名和描述信息的配置步骤和命令。

1.配置接口别名和描述信息。

步骤	命令	功能
1	inspur(config)#**interface** <*interface-name*>	进入接口配置模式
2	inspur(config-if-interface-name)#**byname** <*WORD*>	配置接口别名，长度为1~31的字符串
3	inspur(config-if-interface-name)#**description** <*line*>	配置接口描述信息，长度为1~104的字符串

接口别名可唯一标识一个接口。配置接口别名后，可以通过接口别名进入接口配置模式。

2.验证配置结果。

步骤	命令	功能
1	inspur#**show ip interface** [**brief** |[|<*interface-name* >|[{ **exclude** | **include**}<*line*>]]]	查看当前接口下配置的别名
2	inspur#**show interface description** |<*interface-name* >]	查看当前接口下配置的描述信息

brief ： 显示接口的简短信息。

phy ： 显示物理接口的状态 。

exclude | include是正则表达式，**exclude**是不包括，**include**是包括。

2.1.6 配置接口 VRF 绑定

本节介绍接口VRF绑定的配置步骤和命令。

1.配置接口VRF绑定。

步骤	命令	功能
1	inspur(config)#**ip vrf** <*vrf-name*>	创建VRF。VRF名称范围：长度为1~32的字符串
2	inspur(config-vrf-vrf-name)#**rd** {<*0-65535*>**:**<*0-4294967295*>|**A.B.C.D:**<*0-65535*>|<*1-65535*>**.**<*0-65535*>**:**<*0-65535*>}	配置路由标识
3	inspur(config-vrf-vrf-name)#**address family ipv4**	激活VRF的IPv4地址族能力
4	inspur(config-vrf-vrf-name)#**address family ipv6**	激活VRF的IPv6地址族能力
5	inspur(config-vrf-vrf-name)#**exit**	返回全局配置模式
6	inspur(config)#**interface** <*interface-name*>	进入接口配置模式
7	inspur(config-if-interface-name)#**ip vrf forwarding** <*vrf-name*>	配置接口VRF绑定

2.验证配置结果。

命令	功能
inspur#**show running-config-interface** <*interface-name*>	查看当前接口下的配置信息

2.1.7 接口信息查看命令

查看IP相关状态和配置

IR12000中提供了以下命令来查看IP相关信息：

命令	功能
inspur#**show ip interface**	显示所有的接口信息
inspur#**show ip interface** [<*interface-name*>]	显示指定的接口信息
inspur#**show ip interface brief**	显示所有接口的简短信息
inspur#**show ip interface brief** [<*interface-name*>]	显示指定接口的简短信息
inspur#**show ip interface brief phy**	显示物理接口的简短信息
inspur#**show ip interface brief include** <*line*>	显示接口名匹配<*line*>中所写字符

命令	功能
	的简短信息
inspur#**show ip interface brief exclude** <*line*>	显示接口名不匹配<*line*>中所写字符的简短信息

查看接口描述信息

IR12000中提供了如下命令来查看接口描述信息：

命令	功能
inspur#**show interface description** [<*interface-name*>]	查看接口的状态和描述信息

查看接口配置信息

IR12000中提供了如下命令来查看接口配置信息：

命令	功能
inspur#**show running-config-interface** <*interface-name*>[**all**]	查看接口的配置信息

查看接口其他相关信息

IR12000中提供了如下命令来查看接口其他相关信息：

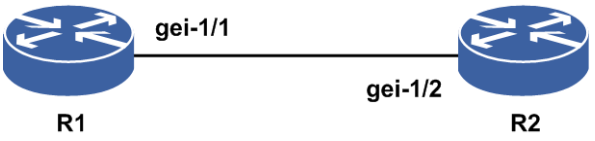
命令	功能
inspur#**show interface** [<*interface-name*>]	查看接口的其他相关信息，如IP地址、MAC地址、接口计数、带宽、利用率、MTU等

2.1.8 IP 主地址配置实例

配置说明

如*图 2-1*所示，R1接口gei-1/1和R2接口gei-1/2直接连接，要求R1与R2的主地址能够互相ping通。

图 2-1 IP 主地址配置实例拓扑图



配置思路

1.配置R1和R2接口的IP主地址。

2.测试配置结果，确认R1和R2能够ping通。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 10.1.1.1 255.255.255.0
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 10.1.1.2 255.255.255.0
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#exit
```

配置验证

在R1上验证：

```
R1#ping 10.1.1.2
sending 5,100-byte ICMP echoes to 10.1.1.2,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 129/185/200 ms.
```

在R2上验证：

```
R2#ping 10.1.1.1
sending 5,100-byte ICMP echoes to 10.1.1.2,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 129/185/200 ms.
```

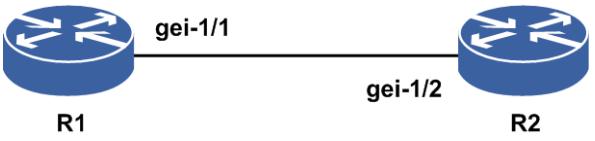
以上结果说明地址配置正确，R1与R2通信正常。

2.1.9 IP 辅地址配置实例

配置说明

如*图 2-2*所示，R1接口gei-1/1和R2接口gei-1/2直接连接，要求R1与R2的辅地址能够互相ping通。

图 2-2 IP 辅地址配置实例拓扑图



配置思路

1.配置R1和R2接口的IP辅地址（配置辅地址前必须保证接口已经配置主地址）。

2.测试配置结果，确认R1和R2能够ping通。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 11.1.1.1 255.255.255.0
R1(config-if-gei-1/1)#ip address 10.1.1.1 255.255.255.0 secondary
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 11.1.1.2 255.255.255.0
R2(config-if-gei-1/2)#ip address 10.1.1.2 255.255.255.0 secondary
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#exit
```

配置验证

在R1上进行验证：

```
R1#ping 10.1.1.2
sending 5,100-byte ICMP echoes to 10.1.1.2,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 129/185/200ms.
```

在R2上进行验证：

```
R2#ping 10.1.1.1
sending 5,100-byte ICMP echoes to 10.1.1.2,timeout is 2 seconds.

!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 129/185/200ms.
```

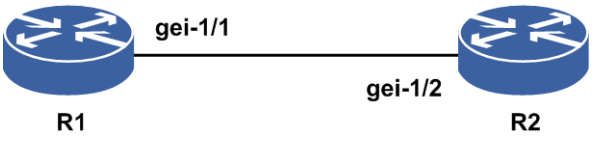
以上结果说明地址配置正确，R1与R2通信正常。

2.1.10 IP MTU 配置实例

配置说明

通过设置IP MTU值控制转发流量的最大包长，*图 2-3*简单描述了IP MTU的应用实例。路由器R1的接口gei-1/1与路由器R2的接口gei-1/2相连。二层流量的包长小于接口gei-1/1的MTU值，流量能按原包长正常转发；如果大于接口gei-1/1的MTU值，流量直接丢弃（不分片）。

图 2-3 IP MTU 配置实例拓扑图



配置思路

1.进入接口模式。

2.配置接口的IP MTU值。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip mtu 1300
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
```

配置验证

查看接口gei-1/1的IP MTU配置信息：

```
R1(config)#show running-config-interface gei-1/1
!<if-intf>
interface gei-1/1
  no shutdown
  ip mtu 1300
$
!</if-intf>
```

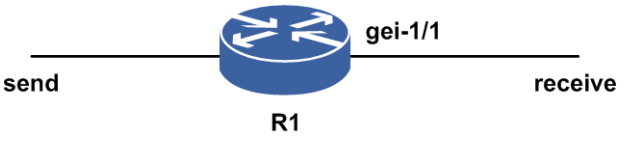
可以看到，接口gei-1/1的IP MTU值已经更改为1300字节了。

2.1.11 接口 MTU 配置实例

配置说明

如*图 2-4*所示，流量转发时，通过设置出接口MTU，超过MTU选择丢弃。

图 2-4 接口 MTU 配置实例拓扑图



配置思路

1.配置接口的MTU。

2.发送流量，R1转发流量。

配置过程

配置gei-1/1接口MTU值为2000：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#mtu 2000
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
```

配置验证

查看配置结果信息：

```
R1(config)#show interface gei-1/1
gei-1/1 is administratively down, line protocol is down
 Hardware is Gigabit Ethernet, address is 0000.12aa.aabb
 Internet address is unassigned
 BW 1000000 Kbits
 IP MTU 1500 bytes
 MTU 2000 bytes
 IPv6 MTU 1500 bytes
 MPLS MTU 1500 bytes
 Holdtime is 10 sec(s)
 The port is electric
 The MDIMode of the port is reserved
 Loopback cancel
 Duplex full
 Negotiation auto
 ARP type ARP
 ARP Timeout 04:00:00
 Last Clear Time : 2013-07-04 09:14:59 Last Refresh Time: 2013-07-04 09:14:59
 120s input rate : 0Bps 0Pps
 120s output rate: 0Bps 0Pps
 Peak rate:
 input 0Bps peak time N/A
 output 0Bps peak time N/A
```

```
 Intf utilization: input 0% output 0%
 HardWareCounters:
 In_Bytes 0 In_Packets 0
 In_CRC_ERROR 0 In_Unicasts 0
 In_Broadcasts 0 In_Multicasts 0
 In_Undersize 0 In_Oversize 0
 In_64B 0 In_65_127B 0
 In_128_255B 0 In_256_511B 0
 In_512_1023B 0 In_1024_1518B 0
 In_1519_MaxB N/A
 E_Bytes 0 E_Packets 0
 E_CRC_ERROR N/A E_Unicasts 0
 E_Broadcasts 0 E_Multicasts 0
 E_Undersize N/A E_Oversize N/A
 E_64B N/A E_65_127B N/A
 E_128_255B N/A E_256_511B N/A
 E_512_1023B N/A E_1024_1518B N/A
 E_1519_MaxB N/A
 StreamCounters :
 In_Bytes 0 In_Packets 0
 In_Discards 0 In_V4Bytes 0
 In_V4Pkts 0 In_V6Bytes 0
 In_V6Pkts 0 In_UpsendCar_Drop 0
 E_Bytes 0 E_Packets 0
 E_Discards 0 E_V4Bytes 0
 E_V4Pkts 0 E_V6Bytes 0
 E_V6Pkts 0
R1(config)#
```

发送大于2000bytes的报文，流量转发丢弃。

2.2 以太网接口

IR12000系列设备支持的LAN接口为以太网接口，包括快速以太网FE（Fast Ethernet）接口、千兆以太网GE（Gigabit Ethernet）接口等。

2.2.1 配置以太网接口

本节介绍以太网接口的配置步骤和命令。

1.配置以太网接口IP地址。

步骤	命令	功能
1	inspur(config)#**interface** {*<interface-name>*| **byname** *<byname>*}	进入接口配置模式或逻辑接口配置模式，如果为不存在的逻辑接口，则创建并进入逻辑接口配置模式
2	inspur(config-if-interface-name)#**ip address** {*<ip-address><net-mask>*|*<A.B.C.D/X>*}[*<broadcast-address>*| **secondary**]	配置接口的IP地址和子网掩码

byname *<byname>*：配置接口别名。

secondary：配置接口的辅地址。

提示：

使用说明：要先对接口配置了接口别名，才能使用**byname**参数进入该接口的配置模式。

2.配置接口的MAC地址偏移。

命令	功能
inspur(config-if-interface-name)#**interface mac-address** {<mac-address>|**offset** <*mac-offset*>}	配置接口的MAC地址偏移，范围1~64，设备启动时可以更改配置MAC偏移的范围，默认范围根据这个值做动态提示，缺省为0

3.（可选）配置接口的模式及工作速率。

步骤	命令	功能
1	inspur(config-if-interface-name)#**duplex** {**duplex-full** |**duplex-half**}	设置端口的工作模式，**duplex-full** 为全双工模式，**duplex-half** 为半双工模式
2	inspur(config-if-interface-name)#**negotiation** {**negotiation-auto** | **negotiation-force**}	配置以太网接口的协商模式，**negotiation-auto**是自动协商模式，**negotiation-force**是强制协商模式
3	inspur(config-if-interface-name)#**speed** {**speed-100M** | **speed-10G** | **speed-10M** | **speed-1G**}	配置以太网接口的工作速率

4.验证配置结果。

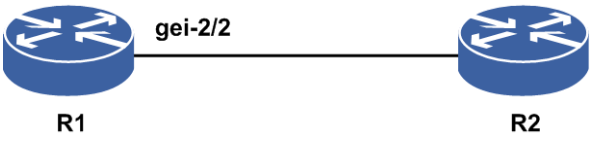
命令	功能
inspur#**show interface** [<*interface-name*>]	显示接口基本信息
inspur#**show ip interface** [**brief** [**phy** |<*interface-name*>|[{**exclude** | **include**}<*line*>]]]	显示接口的三层信息
inspur#**show running-config-interface** <*interface-name*>	显示接口的配置信息

2.2.2 以太网接口配置实例

配置说明

如*图 2-5*所示是以太网接口的配置拓扑图，为了实现两台路由器互联。

图 2-5 以太网接口配置实例拓扑图



配置思路

1.进入全局配置模式。

2.进入要配置的接口。

3.接口下进行相应的配置。

配置过程

在R1上的配置如下：

```
R1(config)#interface gei-2/2
R1(config-if-gei-2/2)#ip address 168.2.1.1 255.255.255.0
R1(config-if-gei-2/2)#no shutdown
R1(config-if-gei-2/2)#mtu 1700
R1(config-if-gei-2/2)#ip mtu 1000
R1(config-if-gei-2/2)#exit
```

配置验证

用**show**命令验证配置结果：

```
R1(config)#show running-config-interface gei-2/2
!<if-intf>
interface gei-2/2
  description TO-236-M320
  mtu 1700
  ip mtu 1000
  ip address 168.2.1.1 255.255.255.0
  no shutdown
$
!</if-intf>
```

2.3 VLAN

以太网采用CSMA/CD技术，一个二层网络属于一个广播域。为了减少对带宽资源的消耗，802.1Q引入了VLAN技术，将一个物理的LAN划分为逻辑上的多个广播域。不同VLAN的用户之间限制访问，同时广播报文限制在逻辑广播域内。

VLAN报文结构中VLAN TAG包含四个字段，分别是TPID（标签协议标识），Priority（用户优先级），CFI（标准格式指示）和VLAN ID（VLAN值）。其中TPID用来标识本数据帧是带有VLAN TAG的数据，长度为16 bit。

为了实现VLAN终结，路由设备必须在物理接口上划分VLAN子接口，每个VLAN子

接口可配置VLAN用于终结报文中的VLAN-ID。由于子接口的数目有限，因此允许一个子接口上面配置多个VLAN，称为VLAN Range。

2.3.1 配置 VLAN 子接口

本节介绍VLAN子接口的配置步骤和命令。

1.配置VLAN子接口。

步骤	命令	功能
1	inspur(config)#**vlan-configuration**	进入VLAN配置模式
2	inspur(config-vlan)#**interface** <*interface-name*>	进入VLAN子接口业务配置模式
3	inspur(config-vlan-if-interface-name)#**encapsulation-dot1q** <*vlan-id*>	为新创建的子接口封装VLAN-ID号，范围1~4094

2.验证配置结果。

命令	功能
inspur(config)#**show interface-vlan dot1q** [<*interface-name*>]	显示所有端口/某个端口的DOT1Q的配置信息

2.3.2 配置 VLAN Range 子接口

本节介绍VLAN Range子接口的配置步骤和命令。

1.配置VLAN Range子接口。

步骤	命令	功能
1	inspur(config)#**vlan-configuration**	进入VLAN配置模式
2	inspur(config-vlan)#**interface** <*interface-name*>	进入VLAN子接口业务配置模式
3	inspur(config-vlan-if-interface-name)#**encapsulation-dot1q range**<*vlan-id*>**-**<*vlan-id*>	为新创建的子接口封装多段VLAN-ID号，范围1~4094
4	inspur(config-vlan-if-interface-name)#**vlan-range-broadcast** {**enable** | **disable** | **single-layer enable**}	开启和关闭vlan range广播

2.验证配置结果。

命令	功能

命令	功能
inspur(config)#**show interface-vlan dot1q** [<*interface-name*>]	显示所有端口/某个端口的VLAN配置

2.3.3 配置 VLAN TPID

本节介绍VLAN TPID的配置步骤和命令。

1.配置VLAN TPID。

步骤	命令	功能
1	inspur(config)#**vlan-configuration**	进入VLAN配置模式
2	inspur(config-vlan)#**interface** <*interface-name*>	进入VLAN子接口业务配置模式
3	inspur(config-vlan-if-interface-name)#**pi d-tag external** <*tpid*>[**internal** <*tpid*>]	为新创建的子接口封装TPID <*tpid*>：子接口支持的TPID封装类型，分为88a8、8100、9100、9200、9300
	inspur(config-vlan-if-interface-name)#**pi d-tag internal** <*tpid*>[**external** <*tpid*>]	

2.验证配置结果。

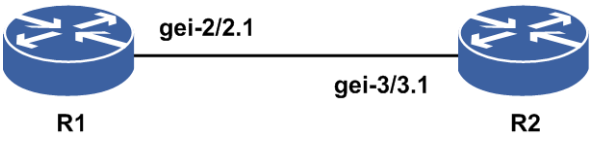
命令	功能
inspur#**show interface-vlan qinq** [<*interface-name*>]	显示配置了双层VLAN的接口上的TPID配置信息
inspur#**show interface-vlan dot1q** [<*interface-name*>]	显示配置了单层VLAN的接口上的TPID配置信息

2.3.4 VLAN 子接口配置实例

配置说明

如*图 2-6*所示，利用VLAN子接口技术，实现同一物理以太网接口上不同VLAN用户的接入和路由。

图 2-6 VLAN 子接口配置实例拓扑图



配置思路

1.创建子接口。

2.进入子接口VLAN配置模式。

3.配置VLAN-ID。

4.为子接口配置IP地址，并且R1、R2可以互相ping通。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/2.1
R1(config-if-gei-2/2.1)#exit
R1(config)#vlan-configuration
R1(config-vlan)#interface gei-2/2.1
R1(config-vlan-if-gei-2/2.1)#encapsulation-dot1q 100
R1(config-vlan-if-gei-2/2.1)#exit
R1(config-vlan)#exit
R1(config)#interface gei-2/2.1
R1(config-if-gei-2/2.1)#ip address 192.2.1.1 255.255.255.0
R1(config-if-gei-2/2.1)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-3/3.1
R2(config-if-gei-3/3.1)#exit
R2(config)#vlan-configuration
R2(config-vlan)#interface gei-3/3.1
R2(config-vlan-if-gei-3/3.1)#encapsulation-dot1q 100
R2(config-vlan-if-gei-3/3.1)#exit
R2(config-vlan)#exit
R2(config)#interface gei-3/3.1
R2(config-if-gei-3/3.1)#ip address 192.2.1.2 255.255.255.0
R2(config-if-gei-3/3.1)#exit
```

配置验证

用**show**命令验证配置结果：

R1上验证配置：

```
R1#show running-config vlan
!<vlan>
vlan-configuration
  interface gei-2/2.1
    encapsulation-dot1q 100
  $
$
!</vlan>
```

R2上验证配置：

```
R2#show running-config-interface gei-3/3.1
!<if-intf>
interface gei-3/3.1
  ip address 192.2.1.2 255.255.255.0
$
!</if-intf>
!<vlan>
vlan-configuration
```

```
  interface gei-3/3.1
    encapsulation-dot1q 100
  $
$
!</vlan>
```

检查结果是可以互相ping通：

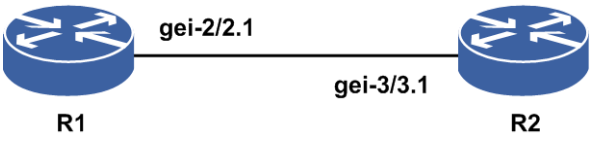
```
R2#ping 192.2.1.1
sending5, 100-byte ICMP echoes to 192.2.1.1, timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max=157/190/199 ms.
R1#ping 192.2.1.2
sending5, 100-byte ICMP echoes to 192.2.1.2, timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max=157/190/199 ms.
```

2.3.5 VLAN Range 子接口配置实例

配置说明

要在如*图 2-7*所示的网络中配置VLAN Range子接口功能：R1上配置封装子接口gei-2/2.1的vlan range 1-10，打开广播开关；R2上在子接口gei-3/3.1配置单个VLAN-ID为5。

图 2-7 VLAN Range 子接口配置实例拓扑图



配置思路

1.在R1上配置VLAN Range，并打开广播开关。

2.在R2上配置单层VLAN-ID。

3.R1和R2可以相互通信。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/2.1
R1(config-if-gei-2/2.1)#exit
R1(config)#vlan-configuration
R1(config-vlan)#interface gei-2/2.1
R1(config-vlan-if-gei-2/2.1)#encapsulation-dot1q range 1-10
R1(config-vlan-if-gei-2/2.1)#vlan-range-broadcast enable
R1(config-vlan-if-gei-2/2.1)#exit
R1(config-vlan)#exit
R1(config)#interface gei-2/2.1
R1(config-if-gei-2/2.1)#ip address 192.2.1.1 255.255.255.0
R1(config-if-gei-2/2.1)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-3/3.1
R2(config-if-gei-3/3.1)#exit
R2(config)#vlan-configuration
R2(config-vlan)#interface gei-3/3.1
R2(config-vlan-if-gei-3/3.1)#encapsulation-dot1q 5
R2(config-vlan-if-gei-3/3.1)#exit
R2(config-vlan)#exit
R2(config)#interface gei-3/3.1
R2(config-if-gei-3/3.1)#ip address 192.2.1.2 255.255.255.0
R2(config-if-gei-3/3.1)#exit
```

配置验证

R1上显示配置结果：

```
R1#show running-config-interface gei-2/2.1
!<if-intf>
interface gei-2/2.1
  ip address 192.2.1.1 255.255.255.0
$
!</if-intf>
!<vlan>
vlan-configuration
  interface gei-2/2.1
    encapsulation-dot1q range 1-10
    vlan-range-broadcast enable
  $
$
!</vlan>
```

R2上显示配置结果：

```
R2#show running-config-interface gei-3/3.1
!<if-intf>
interface gei-3/3.1
  ip address 192.2.1.2 255.255.255.0
$
!</if-intf>
!<vlan>
vlan-configuration
  interface gei-3/3.1
    encapsulation-dot1q 5
  $
$
!</vlan>
```

检查结果是可以互相ping通：

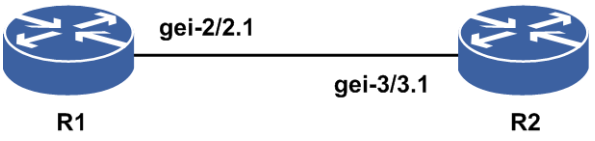
```
R2#ping 192.2.1.1
sending 5,100-byte ICMP echoes to 192.2.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 157/190/199 ms.
R1#ping 192.2.1.2
sending 5,100-byte ICMP echoes to 192.2.1.2,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 157/190/199 ms.
```

2.3.6 VLAN TPID 配置实例

配置说明

如*图 2-8*所示是VLAN TPID配置实例拓扑图，R1和R2相连接，配置R1接口gei-2/2.1和R2接口gei-3/3.1的VLAN TPID和VLAN ID，使之可以互通。

图 2-8 VLAN TPID 配置实例拓扑图



配置思路

1.进入子接口VLAN配置模式。

2.配置VLAN ID和VLAN TPID。

3.为子接口配置IP地址，并且R1、R2可以互相ping通；如果配置不同的VLAN TPID，也可以互通（pid-tag主要用来控制出的报文，宽进严出）。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/2.1
R1(config-if-gei-2/2.1)#exit
R1(config)#vlan-configuration
R1(config-vlan)#interface gei-2/2.1
R1(config-vlan-if-gei-2/2.1)#encapsulation-dot1q 100
R1(config-vlan-if-gei-2/2.1)#pid-tag external 9100 internal 9300
R1(config-vlan-if-gei-2/2.1)#exit
R1(config-vlan)#exit

R1(config)#interface gei-2/2.1
R1(config-if-gei-2/2.1)#ip address 192.2.1.1 255.255.255.0
R1(config-if-gei-2/2.1)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-3/3.1
R2(config-if-gei-3/3.1)#exit
R2(config)#vlan-configuration
R2(config-vlan)#interface gei-3/3.1
R2(config-vlan-if-gei-3/3.1)#encapsulation-dot1q 100
R2(config-vlan-if-gei-3/3.1)#pid-tag external 9100 internal 9300
R2(config-vlan-if-gei-3/3.1)#exit
R2(config-vlan)#exit

R2(config)#interface gei-3/3.1
R2(config-if-gei-3/3.1)#ip address 192.2.1.2 255.255.255.0
R2(config-if-gei-3/3.1)#exit
```

配置验证

用show命令验证配置结果。

R1上验证配置：

```
R1#show running-config vlan
!<vlan>
vlan-configuration
  interface gei-2/2.1
    pid-tag external 9100 internal 9300
    encapsulation-dot1q 100
  $
$
!</vlan>
```

R2上验证配置：

```
R2#show running-config vlan
!<vlan>
vlan-configuration
  interface gei-3/3.1
    pid-tag external 9100 internal 9300
    encapsulation-dot1q 100
  $
$
!</vlan>
```

检查结果是可以互相ping通：

```
R2#ping 192.2.1.1
sending5, 100-byte ICMP echoes to 192.2.1.1, timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max=157/190/199ms.

R1#ping 192.2.1.2
sending5, 100-byte ICMP echoes to 192.2.1.2, timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max=157/190/199ms.
```

2.4 QinQ

QinQ是802.1Q in 802.1Q的简称，主要是为拓展VLAN的数量空间而产生的，在原有的802.1Q报文的基础上又增加一层802.1Q标签来实现，QinQ使VLAN数量增加到4K×4K。

为了实现VLAN终结，路由设备必须在物理接口上划分VLAN子接口。每个VLAN子接口可配置QinQ，用于终结报文中的QinQ ID。由于子接口的数目有限，因此允许一个子接口上面配置多个QinQ，称为QinQ Range。

2.4.1 配置 QinQ 子接口

本节介绍QinQ子接口的配置步骤和命令。

1.配置QinQ子接口。

步骤	命令	功能

步骤	命令	功能
1	inspur(config)#**vlan-configuration**	进入VLAN配置模式
2	inspur(config-vlan)#**interface** <*interface-name*>	进入VLAN子接口业务配置模式
3	inspur(config-vlan-if-interface-name)#**qinq internal-vlanid** <*vlan-id*> **external-vlanid** <*vlan-id*>	配置内外层VLAN标签，范围1~4094

2.验证配置结果。

命令	功能
inspur(config)#**show interface-vlan qinq** [<*interface-name*>]	显示所有端口或某个端口的QinQ配置信息

2.4.2 配置 QinQ Range 子接口

本节介绍QinQ Range子接口的配置步骤和命令。

1.配置QinQ Range子接口。

在IR12000上使用以下命令配置QinQ Range子接口：

步骤	命令	功能
1	inspur(config)#**vlan-configuration**	进入VLAN配置模式
2	inspur(config-vlan)#**interface** <*interface-name*>	进入VLAN子接口业务配置模式
3	inspur(config-subvlan-if)#**qinq range internal-vlan-range** <*vlan-id*>**-**<*vlan-id*> **external-vlan-range** <*vlan-id*>**-**<*vlan-id*>	配置多段内外层VLAN标签，范围1~4094

2.验证配置结果。

IR12000中提供了以下命令查看QinQ Range子接口配置信息：

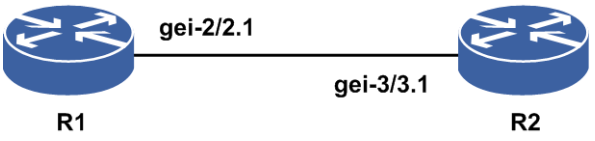
命令	功能
inspur(config)#**show interface-vlan qinq** [<*interface-name*>]	显示所有端口或某个端口的QinQ配置信息

2.4.3 QinQ 子接口配置实例

配置说明

如*图 2-9*所示是QinQ配置实例拓扑图。R1和R2相连接，R1接口gei-2/2.1和R2接口gei-3/3.1分别封装QinQ ID。

图 2-9 QinQ 子接口配置实例拓扑图



配置思路

1.创建子接口。

2.进入子接口VLAN配置模式。

3.配置QinQ ID。

4.为子接口配置IP地址，并且R1、R2可以互相ping通。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/2.1
R1(config-if-gei-2/2.1)#exit
R1(config)#vlan-configuration
R1(config-vlan)#interface gei-2/2.1
R1(config-vlan-if-gei-2/2.1)#qinq  internal-vlanid 1 external-vlanid 2
R1(config-vlan-if-gei-2/2.1)#exit
R1(config-vlan)#exit
R1(config)#interface gei-2/2.1
R1(config-if-gei-2/2.1)#ip address 192.2.1.1 255.255.255.0
R1(config-if-gei-2/2.1)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-3/3.1
R2(config-if-gei-3/3.1)#exit
R2(config)#vlan-configuration
R2(config-vlan)#interface gei-3/3.1
R2(config-vlan-if-gei-3/3.1)#qinq  internal-vlanid 1 external-vlanid 2
R2(config-vlan-if-gei-3/3.1)#exit
R2(config-vlan)#exit
R2(config)#interface gei-3/3.1
R2(config-if-gei-3/3.1)#ip address 192.2.1.2 255.255.255.0
R2(config-if-gei-3/3.1)#exit
```

配置验证

用**show**命令验证配置结果。

R1上的配置结果：

```
R1#show running-config vlan
!<vlan>
vlan-configuration
  interface gei-2/2.1
    qinq internal-vlanid 1 external-vlanid 2
  $
$
!</vlan>
```

R2上的配置结果：

```
R2#show running-config-interface gei-3/3.1
!<if-intf>
interface gei-3/3.1
  ip address 192.2.1.2 255.255.255.0
$
!</if-intf>
!</vlan>
vlan-configuration
  interface gei-3/3.1
    qinq internal-vlanid 1 external-vlanid 2
  $
$
!</vlan>
```

检查结果是可以互相ping通：

```
R2#ping 192.2.1.1
sending5，100-byte ICMP echoes to 192.2.1.1，timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max=157/190/199ms.

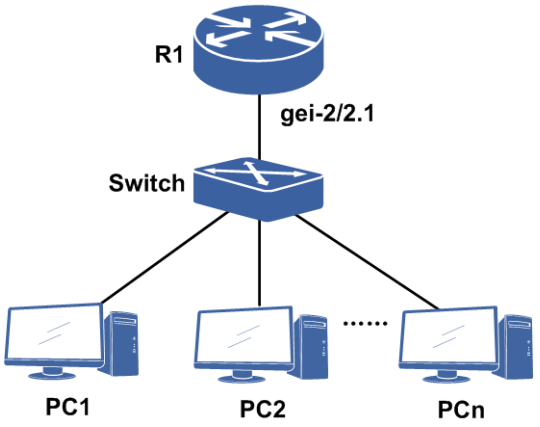
R1#ping 192.2.1.2
sending5，100-byte ICMP echoes to 192.2.1.2，timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max=157/190/199ms.
```

2.4.4 QinQ Range 子接口配置实例

配置说明

如*图 2-10*所示，是QinQ Range子接口配置实例的典型组网图。

图 2-10 子接口配置实例拓扑图



配置思路

1.创建子接口。

2.子接口VLAN配置模式。

3.配置QinQ Range。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/2.1
R1(config-if-gei-2/2.1)#exit
R1(config)#vlan-configuration
R1(config-vlan)#interface gei-2/2.1
R1(config-vlan-if-gei-2/2.1)#qinq range internal-vlan-range 1-10
external-vlan-range 1-10
R1(config-vlan-if-gei-2/2.1)#exit
R1(config-vlan)#exit
```

配置验证

用**show**命令验证配置结果：

```
R1(config)#show running-config vlan
!<vlan>
vlan-configuration
  interface gei-2/2.1
    qinq range internal-vlan-range 1-10 external-vlan-range 1-10
  $
$
!</vlan>
```

2.5 SuperVLAN

SuperVLAN技术是把多个SubVLAN（子VLAN）聚合在一起，这些SubVLAN共同使用一个IP子网和缺省网关。

SuperVLAN接口是由多个接口绑定而成的虚拟接口，可由不同单板的不同VLAN子接口、QinQ子接口或以太网实接口绑定而成。

以太网中不同VLAN间不能通过二层方式进行通讯，要通讯只能通过三层路由进行转发。为此不同VLAN间需要配置不同的IP地址子网，出于节省IP地址考虑，引入了SuperVLAN技术。

2.5.1 配置 SuperVLAN

本节介绍SuperVLAN的配置步骤和命令。

1.配置SuperVLAN开关属性。

步骤	命令	功能
1	inspur(config)#**supervlan**	进入SuperVLAN配置模式
2	inspur(config-supervlan-superif)#**interface supervlan** *<supervlan-id>*	进入SuperVLAN聚合接口配置模式，SuperVLAN的ID号范围：1~255
3	inspur(config-supervlan-superif)#**arp-broadcast** {**enable** | **disable**}	打开或关闭SuperVLAN向所有SubVLAN进行ARP广播功能。缺省情况下，该功能是关闭的
4	inspur(config-supervlan-superif)#**inter-subvlan-routing** {**enable** | **disable**}	打开或关闭SubVLAN之间的路由功能。缺省情况下，该功能是开启的
5	inspur(config-supervlan-superif)#**ip-pool-filter** {**enable** | **disable**}	打开或者关闭SubVLAN的源IP地址过滤功能，缺省情况下，该功能是开启的

2.配置SuperVLAN的成员接口属性。

步骤	命令	功能
1	inspur(config)#**supervlan**	进入SuperVLAN配置模式
2	inspur(config-supervlan)#**interface** *<interface-name>*	进入SuperVLAN子接口配置模式
3	inspur(config-supervlan-subif)#**supervlan** *<supervlan-id>*	将接口绑定到SuperVLAN，参数范围： 1~255
4	inspur(config-supervlan-subif)#**vlanpool** *<ip-address1><ip-address2>*	绑定一段IP地址到某个SubVLAN接口上

3.验证配置结果。

命令	功能
inspur(config)#**show supervlan** [<*supervlan-id*>]	显示SuperVLAN的配置
inspur(config)#**show supervlan-pool** [<*supervlan-id*>]	显示所有绑定在SubVLAN上的IP POOL

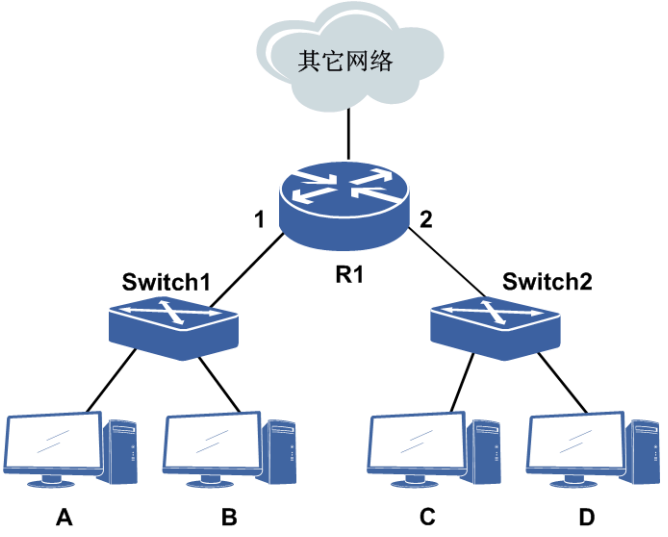
2.5.2 SuperVLAN 综合配置实例

配置说明

SuperVLAN技术是把多个SubVLAN聚合在一起，这些SubVLAN共同使用一个IP子网和缺省网关。在SuperVLAN中，所有的SubVLAN可以灵活地分配SuperVLAN子网中的IP地址和使用SuperVLAN的缺省网关。每个SubVLAN都是独立的广播域，保证了不同用户间的隔离，SubVLAN间的通信通过SuperVLAN进行路由。

在如*图 2-11*所示的网络中配置SuperVLAN。

图 2-11 SuperVLAN 综合配置实例拓扑图



配置思路

先创建SuperVLAN接口，关闭源IP地址过滤开关，之后把SubVLAN接口绑定到指定SuperVLAN接口下，并在SubVLAN接口下配置好IP-POOL。具体配置流程如下：

1.创建SuperVLAN接口。

2.配置SuperVLAN接口IP地址。

3.输入SuperVLAN接口名称，进入SuperVLAN聚合接口配置模式。

4.将ip-pool-filter设置为disable。

5.输入已经封装了VLANID的子接口名称，进入SuperVLAN成员接口配置模式。

6.将该子接口绑定到SuperVLAN。

7.在该子接口下配置IP-POOL。

配置过程

IR12000上的配置如下：

```
R1(config)#interface gei-2/2.1
R1(config-if-gei-2/2.1)#exit
R1(config)#vlan-configuration
R1(config-vlan)#interface gei-2/2.1
R1(config-vlan-if-gei-2/2.1)#encapsulation-dot1q 100
R1(config-vlan-if-gei-2/2.1))#exit
R1(config-vlan)#exit

R1(config)#interface supervlan11
R1(config-if-supervlan11)#ip address 192.11.1.1 255.255.255.0
R1(config-if-supervlan11)#exit
R1(config)#supervlan
R1(config-supervlan)#interface  supervlan11
R1(config-supervlan-superif)#ip-pool-filter disable
R1(config-supervlan-superif)#exit
R1(config-supervlan)#interface gei-2/2.1
R1(config-supervlan-subif)#supervlan 11
R1(config-supervlan-subif)#vlanpool 192.11.1.1 192.11.1.10
R1(config-supervlan-subif)#end
```

配置验证

用show命令验证配置结果：

```
R1#show supervlan
The total supervlan number:1

  SuperVLAN No: 11
    ARP-Broadcast           : Disable
    Gratuitous-ARP-Broadcast  : Enable
    Inter-SubVLAN-Routing-IPv4: Enable
    Inter-SubVLAN-Routing-IPv6: Enable
    IP-POOL-Filter          : Disable
    ND-Broadcast            : Disable
----------------------------------------
     SubIntf  :  gei-2/2.1

R1#show running-config supervlan
!<supervlan>
supervlan
  interface supervlan11
    inter-subvlan-routing enable
    ip-pool-filter disable
  $
  interface gei-2/2.1
    supervlan 11
    vlanpool 192.11.1.1 192.11.1.10
  $
$
!</supervlan>

R1(config)#show supervlan-pool
Addr-Begin      Addr-End        SuperVLAN-Name  SubIntf-Name
```

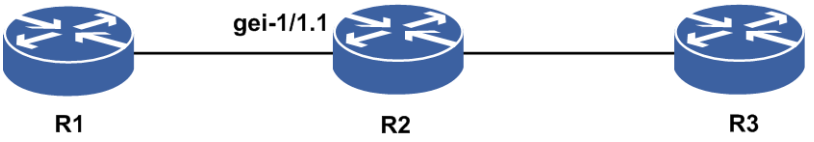
```
192.11.1.1       192.11.1.10       supervlan11     gei-2/2.1
```

2.5.3 VLAN 绑定 IP 配置实例

配置说明

如*图 2-12*所示是一个VLAN绑定IP配置实例的拓扑图。

图 2-12 VLAN 绑定 IP 配置实例拓扑图



配置思路

1.创建子接口并封装VLAN-ID。

2.将子接口绑到SuperVLAN中。

3.在SuperVLAN模式下，配置vlanpool。

配置过程

R2上的配置如下：

```
R2#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
R2(config)#interface gei-1/1.1
R2(config-if-gei-1/1.1)#exit

R2(config)#vlan-configuration
R2(config-vlan)#interface gei-1/1.1
R2(config-vlan-if-gei-1/1.1)#encapsulation-dot1q 1
R2(config-vlan-if-gei-1/1.1)#exit
R2(config-vlan)#exit

R2(config)#interface supervlan11
R2(config-if-supervlan11)#ip address 192.1.1.1 255.255.255.0
R2(config-if-supervlan11)#exit

R2(config)#supervlan
R2(config-supervlan)#interface gei-1/1.1
R2(config-supervlan-subif)#supervlan 11
R2(config-supervlan-subif)#vlanpool 192.1.1.2 192.1.1.10   /*VLAN绑定IP*/
R2(config-supervlan-subif)#exit
R2(config-supervlan)#exit
```

配置验证

R2上查看配置情况：

```
R2#show supervlan11
The total SuperVLAN number:1

  SuperVLAN No: 11
    ARP-Broadcast           : Disable
    Gratuitous-ARP-Broadcast  : Enable
    Inter-SubVLAN-Routing-IPv4: Enable
    Inter-SubVLAN-Routing-IPv6: Enable
    IP-POOL-Filter          : Enable
    ND-Broadcast            : Disable
-----------------------------------------
      SubIntf  :  gei-1/1.1

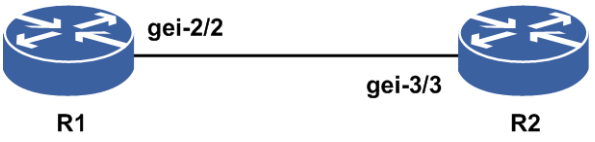
R2(config)#show supervlan-pool 11
Addr-Begin      Addr-End        SuperVLAN-Name  SubIntf-Name
192.1.1.2       192.1.1.10      supervlan11     gei-1/1.1
```

2.5.4 MAC 绑定 IP 配置实例

配置说明

如*图 2-13*所示是一个MAC绑定IP配置实例的拓扑图。

图 2-13 MAC 绑定 IP 配置实例拓扑图



配置思路

1.R1上创建SuperVLAN接口，配置IP地址。

2.将物理接口绑到SuperVLAN中。

3.在SuperVLAN模式下，配置vlanpool。

4.在ARP模式下，进入SuperVLAN的成员接口，配置MAC绑定IP（配置的MAC地址为对端接口的MAC地址）。

5.R2上配置直连接口同网段IP地址，R1可以ping通对端。

6.R2的接口下配置MAC偏移，R1上ping对端不通。

配置过程

R1上的配置如下：

```
R1(config)#interface supervlan255
R1(config-if-supervlan255)#ip address 192.11.1.1 255.255.255.0
R1(config-if-supervlan255)#exit

R1(config)#supervlan
R1(config-supervlan)#interface gei-2/2
R1(config-supervlan-subif)#supervlan 255
```

```
R1(config-supervlan-subif)#vlanpool 192.11.1.2 192.11.1.10
R1(config-supervlan-subif)#exit
R1(config-supervlan)#exit

R1(config)#arp
R1(config-arp)#interface gei-2/2
R1(config-arp-if-gei-2/2)#arp permanent 192.11.1.2 0000.0145.4303  /*MAC绑定
IP*/
R1(config-arp-if-gei-2/2)#exit
R1(config-arp)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-3/3
R2(config-if-gei-3/3)#ip address 192.11.1.2 255.255.255.0
R2(config-if-gei-3/3)#no shutdown
R2(config-if-gei-3/3)#end

R2#show arp interface gei-3/3
Arp protect interface is disabled
The count is 1
IP                   Hardware                Exter  Inter  Sub
Address        Age     Address       Interface    VlanID VlanID Interface
------------------------------------------------------------------------------
--
192.11.1.2     H       0000.0145.4303 gei-3/3     N/A    N/A    N/A
```

配置验证

R1上ping对端，可以ping通：

```
R1#ping 192.11.1.2
sending 5,100-byte ICMP echo(es) to 192.11.1.2,timeout is 2 second(s).
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/2/7 ms.
```

R2的接口配置MAC偏移（配置的MAC地址和绑定IP的MAC不一致），R1上ping对端，ping不通：

```
R2(config)#interface gei-3/3
R2(config-if-gei-3/3)#interface mac-address offset 2
R2(config-if-gei-3/3)#end
R2#show arp interface gei-3/3
Arp protect interface is disabled
The count is 1
IP                   Hardware                Exter  Inter  Sub
Address        Age     Address       Interface    VlanID VlanID Interface
------------------------------------------------------------------------------
--
192.11.1.2     H       0000.0145.4305 gei-3/3     N/A    N/A    N/A

R1#ping 192.11.1.2
sending 5,100-byte ICMP echo(es) to 192.11.1.2,timeout is 2 second(s).
.....
Success rate is 0 percent(0/5).
```

2.6 SmartGroup

SmartGroup技术是指将多个同类型的以太网接口捆绑成一个逻辑接口来使用。

SmartGroup的链路聚合（Link Aggregation，又称端口捆绑、端口聚集或链路聚集）是将多个端口聚合在一起形成一个聚合组，以实现出/入负荷在各成员端口中的分担，

同时也提供了更高的连接可靠性。实际应用时，一个聚合组就象是一个端口。

SmartGroup功能可以为用户提供更加灵活、更加高效的组网解决方案。利用SmartGroup功能进行网络规划、组网设计时，有了更大的灵活性，同时可以大大提高网络的稳定性，尤其是对于以太网组网环境和应用以太网接口的网络环境。

2.6.1 配置 SmartGroup

本节介绍SmartGroup的配置步骤和命令。

1.创建SmartGroup。

步骤	命令	功能
1	inspur(config)#**interface smartgroup** <*smartgroup-id*>	创建链路聚合组SmartGroup，链路聚合组号范围1~64

2.配置LACP接口及参数。

步骤	命令	功能
1	inspur(config)#**lacp**	进入LACP配置模式
2	inspur(config-lacp)#**lacp system-priority** <*priority*>	配置LACP的系统优先级，范围1~65535，缺省为32768，较小的值具有较高优先级 系统优先级和系统MAC唯一标识一个设备，是LACP协商报文中的一个字段，系统优先级高的作为LACP协商的主动端，当系统优先级相同时，系统MAC小的优先
3	inspur(config-lacp)#**lacp minimum-member** < *member-number*>	配置全局的SmartGroup协议UP阈值，范围1~32，缺省为1
4	inspur(config-lacp)#**interface smartgroup** <*smartgroup-id*>	进入LACP接口配置模式
5	inspur(config-lacp-sg-if-smartgroupid) #**lacp mode** {**802.3ad** | **on**}	设置链路聚合组的聚合模式
6	inspur(config-lacp-sg-if-smartgroupid) #**lacp load-balance** {**per-packet** | **per-destination**}	设置链路聚合组的负荷分担方式，缺省模式为**per-destination**
7	inspur(config-lacp-sg-if-smartgroupid) #**lacp minimum-member** < *member-number*>	配置SmartGroup协议UP阈值，范围1~32，缺省为1
8	inspur(config-lacp-sg-if-smartgroupid) #**lacp fast respond**	配置LACP协商快速应答模式
9	inspur(config-lacp-sg-if-smartgroupid)	配置SmartGroup最多可以激活多

步骤	命令	功能
	#**lacp active limitation** < *member-number*>	少成员，范围0-32，缺省值为32
10	inspur(config-lacp-sg-if-smartgroupid) #**lacp sys-priority**<*priority*>	进入SmartGroup接口配置模式，配置LACP的系统优先级，范围1~65535，缺省为32768
11	inspur(config-lacp-sg-if-smartgroupid) #**lacp restore**{ **revertive** <*holdoff-time*>| **immediately** | **non-revertive**}	配置聚合端口备向主回切方式，如果是回切模式，可以指定回切时间，单位秒
12	inspur(config-lacp-sg-if-smartgroupid) #**lacp aggregator timeout** <*10-500*>	SmartGroup接口模式下配置聚合链路组超时时间，单位秒，缺省为30秒。当一个聚合链路组已经选中但是在超时时间内仍然不能使聚合端口协议UP，就要进行聚合链路重新选择
13	inspur(config-lacp-sg-if-smartgroupid) #**lacp force-switch**	SmartGroup接口模式下命令强制切换

802.3ad ：指SmartGroup接口聚合控制方式是采用802.3ad标准的LACP协议。

on：指静态trunk，此时不运行LACP协议，缺省配置是静态trunk模式（on模式）。

3.配置LACP成员接口及参数。

步骤	命令	功能
1	inspur(config-lacp)#**interface** <*interface-name*>	进入LACP成员接口配置模式
2	inspur(config-lacp-member-if-interface -name)#**smartgroup** <*smartgroup-id*> **mode** {**passive** | **active** | **on**}	添加接口到链路聚合组，并设置接口的链路聚合模式
3	inspur(config-lacp-member-if-interface -name)#**lacp timeout** {**long** | **short**}	配置LACP的成员端口长、短超时
4	inspur(config-lacp-member-if-interface -name)#**lacp port-priority** <*priority*>	配置LACP的成员端口优先级，范围1~65535，缺省为32768，较小的值具有较高的优先级，端口优先级高的将优先被选作活动端口
5	inspur(config-lacp-member-if-interface -name)#**track** <*track-name*>	配置LACP的成员关联SAMGR的track name，可以通过track name关联检测机制，来快速感应链路的状态变化

passive：指接口的LACP处于被动协商模式。

active：指接口的LACP处于主动协商模式。

on：指静态trunk，此时不运行LACP，聚合的两端都需要设置成on模式。

4.验证配置结果。

命令	功能
inspur#**show lacp** {[<*smartgroup-id*>]{**counters** | **internal** | **neighbors**}| **sys-id**}	查看LACP当前配置和状态

counters ： 查看端口LACP收发包状态。

internal ： 显示成员端口的聚合状态。

neighbors：查看对端邻居的成员端口状态。

sys-id：查看LACP系统优先级、系统ID。

5.维护SmartGroup。

命令	功能
inspur(config-lacp)#**clear lacp** [<*smartgroup-id*>] **counters**	清除LACP收发包计数
inspur#**debug lacp** {**packets** [**interface** <*interface-name*>]| **fsm** [**interface** <*interface-name*>]| **all**}	LACP的报文收发、状态机转换的debug开关
inspur#**show debug lacp**	显示已打开的LACP调试命令

all ： 打开所有调试开关。

packets ： 显示所有端口报文内容。

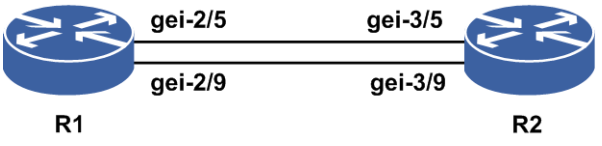
fsm ： 显示所有端口状态机的变化信息。

2.6.2 SmartGroup 802.3ad 模式配置实例

配置说明

如*图 2-14*所示，R1和R2之间运行LACP协议。R1接口gei-2/5与R2接口gei-3/5直连，R1接口gei-2/9与R2接口gei-3/9直连。

图 2-14 802.3ad 模式配置实例拓扑图



配置思路

1.R1上创建smartgroup1，R2上创建smartgroup1。

2.全局模式下进入LACP配置模式，再进入所要配置的SmartGroup接口。

3.将R1，R2上smartgroup1的聚合控制方式配置为采用802.3ad标准的LACP协议，配置负荷分担策略以及最小成员数。

4.全局模式下进入LACP配置模式，再进入所要配置实接口。

5.分别将图中R1，R2的实接口绑入smartgroup1。

6.分别为R1，R2上smartgroup1中成员接口配置LACP协商模式以及超时时长。

配置过程

R1上的配置如下：

```
R1(config)#interface smartgroup1
R1(config-if-smartgroup1)#ip address 196.1.1.27 255.255.255.0
R1(config-if-smartgroup1)#exit
R1(config)#lacp
R1(config-lacp)#interface smartgroup1
R1(config-lacp-sg-if-smartgroup1)#lacp mode 802.3ad
R1(config-lacp-sg-if-smartgroup1)#lacp load-balance  per-destination
R1(config-lacp-sg-if-smartgroup1)#lacp  minimum-member 1
R1(config-lacp-sg-if-smartgroup1)#exit
R1(config-lacp)#interface gei-2/5
R1(config-lacp-member-if-gei-2/5)#smartgroup 1 mode active
R1(config-lacp-member-if-gei-2/5)#lacp timeout short
R1(config-lacp-member-if-gei-2/5)#exit
R1(config-lacp)#interface gei-2/9
R1(config-lacp-member-if-gei-2/9)#smartgroup 1 mode active
R1(config-lacp-member-if-gei-2/9)#lacp timeout short
R1(config-lacp-member-if-gei-2/9)#exit
R1(config-lacp)#exit
```

R2上的配置如下：

```
R2(config)#interface smartgroup1
R2(config-if-smartgroup1)#ip address 196.1.1.28 255.255.255.0
R2(config-if-smartgroup1)#exit
R2(config)#lacp
R2(config-lacp)#interface smartgroup1
R2(config-lacp-sg-if-smartgroup1)#lacp mode 802.3ad
R2(config-lacp-sg-if-smartgroup1)#lacp load-balance  per-destination
R2(config-lacp-sg-if-smartgroup1)#lacp  minimum-member 1
R2(config-lacp-sg-if-smartgroup1)#exit
R2(config-lacp)#interface gei-3/5
R2(config-lacp-member-if-gei-3/5)#smartgroup 1 mode active
R2(config-lacp-member-if-gei-3/5)#lacp timeout short
R2(config-lacp-member-if-gei-3/5)#exit
R2(config-lacp)#interface gei-3/9
R2(config-lacp-member-if-gei-3/9)#smartgroup 1 mode active
R2(config-lacp-member-if-gei-3/9)#lacp timeout short
R2(config-lacp-member-if-gei-3/9)#end
```

配置验证

查看R1的SmartGroup配置和生效情况：

```
R1(config)#show lacp 1 internal
Smartgroup:1
Flags:          * - Port is Active member Port
                S - Port is requested in Slow LACPDUs
                F - Port is requested in Fast LACPDUs
```

```
               A - Port is in Active mode
               P - Port is in Passive mode
Actor           Agg     LACPDUs  Port  Oper   Port  RX       Mux
Port[Flags]      State    Interval Pri   Key    State Machine   Machine
-------------------------------------------------------------------------------
-
gei-2/5     [FA*] ACTIVE    32768 0x111  0x3f  CURRENT   COLL&DIST
gei-2/9     [FA*] ACTIVE   32768 0x111  0x3f  CURRENT   COLL&DIST
/*端口聚合。Active：聚合成功；Inactive：聚合失败*/

R1(config)#show running-config-interface smartgroup1
!<if-intf>
interface smartgroup1
  ip address 196.1.1.27 255.255.255.0
$
!</if-intf>
!<lacp>
lacp
  interface smartgroup1
    lacp mode 802.3ad              /*协商模式*/
    lacp minimum-member 1           /*聚合成功最小成员数，只有聚合成功的链路
大于或等于聚合成功最小成员数，SmartGroup协议才会up*/
  $
$
!</lacp>

R1(config)#show running-config lacp
!<lacp>
lacp
  interface smartgroup1
    lacp mode 802.3ad
    lacp minimum-member 1
  $
  interface gei-2/9
    smartgroup 1 mode active  /*802.3ad模式下，链路的两端必须至少要有一个配置
为active模式，该链路才会聚合成功 */
    lacp timeout short
  $
  interface gei-2/5
    smartgroup 1 mode active
    lacp timeout short
  $
$
!</lacp>

R1(config)#show ip interface smartgroup1
smartgroup1 AdminStatus is up, PhyStatus is up, line protocol is up
  Internet address is 196.1.1.27/24
  Broadcast address is 255.255.255.255
  IP MTU is 1500 bytes

R1(config)#show lacp 1 neighbors     /*查看邻居*/
Smartgroup 1  neighbors
Actor        Partner            Partner   Port     Oper    Port
Port         System ID          Port No.  Priority  Key     State
-------------------------------------------------------------------------
gei-2/9      0x8000,00d0.d012.1127    21      0x8000    0x111   0x3f
gei-2/5      0x8000,00d0.d012.1127    17      0x8000    0x111   0x3f

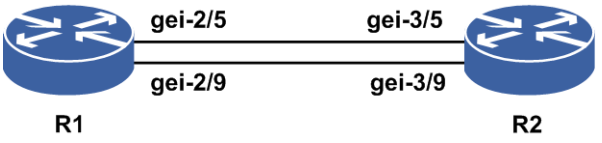
R1(config)#show lacp 1 counters
Smartgroup:1
Actor        LACPDUs             Marker    LACPDUs    Marker
Port         Tx        Rx        Tx  Rx    Err        Err
---------------------------------------------------------------------
gei-2/9      1840      1840      0   0     0          0
/*依据配置的timeout参数，Tx和Rx的数值每30秒或1秒增加1*/
gei-2/5      1840      1840      0   0     0          0
```

2.6.3 SmartGroup On 模式配置实例

配置说明

如*图 2-15*所示，R1接口gei-2/5与R2接口gei-3/5直连，R1接口gei-2/9与R2接口gei-3/9直连，R1和R2采用不协商的on模式建链。

图 2-15 SmartGroup ON 模式配置实例拓扑图



配置思路

1.R1上创建smartgroup1，R2上创建smartgroup1。

2.全局模式下进入LACP配置模式，再进入所要配置的SmartGroup接口。

3.分别为R1，R2上的smartgroup1配置相同的协商模式为on。

4.全局模式下进入LACP配置模式，再进入所要配置实接口。

5.分别配置将图中R1，R2的实接口绑入smartgroup1。

配置过程

R1上的配置如下：

```
R1(config)#interface smartgroup1
R1(config-if-smartgroup1)#ip address 196.1.1.27 255.255.255.0
R1(config-if-smartgroup1)#exit
R1(config)#lacp
R1(config-lacp)#interface smartgroup1
R1(config-lacp-sg-if-smartgroup1)#lacp mode on
R1(config-lacp-sg-if-smartgroup1)#exit
R1(config-lacp)#interface gei-2/5
R1(config-lacp-member-if-gei-2/5)#smartgroup 1 mode on
R1(config-lacp-member-if-gei-2/5)#exit
R1(config-lacp)#interface gei-2/9
R1(config-lacp-member-if-gei-2/9)#smartgroup 1 mode on
R1(config-lacp-member-if-gei-2/9)#exit
R1(config-lacp)#end
```

R2上的配置如下：

```
R2(config)#interface smartgroup1
R2(config-if-smartgroup1)#ip address 196.1.1.28 255.255.255.0
R2(config-if-smartgroup1)#exit
R2(config)#lacp
R2(config-lacp)#interface smartgroup1
R2(config-lacp-sg-if-smartgroup1)#lacp mode on
R2(config-lacp-sg-if-smartgroup1)#exit
R2(config-lacp)#interface gei-3/5
R2(config-lacp-member-if-gei-3/5)#smartgroup 1 mode on
R2(config-lacp-member-if-gei-3/5)#exit
```

```
R2(config-lacp)#interface gei-3/9
R2(config-lacp-member-if-gei-3/9)#smartgroup 1 mode on
R2(config-lacp-member-if-gei-3/9)#end
```

配置验证

查看R1的SmartGroup配置和生效情况：

```
R1#show lacp 1 internal
Smartgroup:1
Flags:          * - Port is Active member Port
               S - Port is requested in Slow LACPDUs
               F - Port is requested in Fast LACPDUs
               A - Port is in Active mode
               P - Port is in Passive mode
Actor           Agg     LACPDUs     Port  Oper   Port  RX        Mux
Port[Flags]      State    Interval    Pri   Key    State Machine    Machine
-------------------------------------------------------------------------------
--
gei-2/9          ACTIVE    30       32768  0x11  0x3d  N/A       N/A
gei-2/5          ACTIVE    30       32768  0x11  0x3d  N/A       N/A

R1#show running-config-interface smartgroup1
!<if-intf>
interface smartgroup1
  ip address 196.1.1.27 255.255.255.0
$
!</if-intf>
!<lacp>
lacp
  interface smartgroup1
    lacp minimum-member 1
  $
$
!</lacp>

R1#show running-config lacp
!<lacp>
lacp
  interface smartgroup1
  $
  interface gei-2/5
    smartgroup 1 mode on
  $
  interface gei-2/9
    smartgroup 1 mode on
  $
$
!</lacp>

R1#show ip interface smartgroup1
smartgroup1 AdminStatus is up, PhyStatus is up, line protocol is up
  Internet address is 196.1.1.27/24
  Broadcast address is 255.255.255.255
  IP MTU is 1500 bytes
```

2.7 POS 接口

POS是Packet over SONET/SDH的缩写，是一种利用SONET/SDH提供的高速传输通道直接传送IP数据包的技术。

POS使用SONET/SDH作为物理层协议，在HDLC帧中封装分组业务，使用PPP作为数据链路层的链路控制，IP分组业务则运行在网络层。

2.7.1 配置 POS 接口

本节介绍POS接口的配置步骤和命令。

1.配置POS接口基本信息。

步骤	命令	功能
1	inspur(config)#**interface** {*<interface-name>*| **byname** *<byname>*}	配置接口或子接口
2	inspur(config-if-interface-name)#**ip address** {*<ip-address><net-mask>*|*<A.B.C.D/X>*}[*<broadcast-address>*| **secondary**]	配置POS口IP地址
3	inspur(config-if-interface-name)#**mtu** *<bytes>*	设置接口能处理的IP包的MTU值，单位：字节，POS接口的MTU范围1504~9216，缺省为4600字节
4	inspur(config-if-interface-name)#**ip mtu** *<bytes>*	设置接口能处理的IP包的IP MTU值，单位：字节，POS接口的IP MTU范围68~9212，缺省为4470字节
5	inspur(config-if-interface-name)#**encapsulation** {**ppp** | **hdlc** | **frame-relay**}| {**rx**|**tx**}	配置接口封装格式，默认封装PPP

2.配置POS接口时钟。

POS接口工作时为获得更好的通信质量，需要选择工作的时钟模式，通信两端的POS接口时钟有两个选择：选择线路提取时钟或选择内部时钟。

配置POS接口的时钟模式时，请注意以下情况：

- 当两个POS接口直接相连或通过WDM（Wavelength Division Multiplexing）相连时，应配置一端使用内部时钟，另一端使用线路提取时钟。
- 当POS接口与交换设备连接时，交换设备为DCE（Data Circuit-terminating Equipment），使用内部时钟，IR12000的POS接口为DTE（Data Terminal Equipment），时钟设为线路提取时钟。
- 缺省情况下，POS接口的时钟模式为内部时钟。

POS接口选择的时钟模式参见*表 2-4*。

{表 2-4 本端和对端POS口时钟选择表

本端POS端口	对接端POS端口	可行性	备注
线路提取时钟	线路提取时钟	X	—
线路提取时钟	内部时钟	√	—

本端POS端口	对接端POS端口	可行性	备注
内部时钟	线路提取时钟	√	—
内部时钟	内部时钟	√	对接两端POS端口的内部时钟必须是同步的

IR12000中提供了以下命令来配置接口时钟：

步骤	命令	功能
1	`inspur(config)#`**interface** *<interface-name>*	进入接口配置模式
2	`inspur(config-if-interface-name)#`**clock mode** {**internal**| **line**}	配置时钟模式 internal：内部时钟，默认配置为internal，即内部时钟 line：线路提取时钟

3.配置POS口延时Down功能。

当物理层发生闪断的时候，不应该影响业务，而原来在物理层发生LOS（Lost of Signal）的时候，立即判定端口Down，并将端口Down状态上报，影响路由的更新和收敛。

通过增加延时Down命令，依据设置的延时时间判断物理层是否为闪断。当物理层状态发生瞬时Down时，启动一个定时器，在设置的时延时间后再去检查端口状态：

- 如果检测到端口状态正常了，则不去触发端口Down
- 如果此时端口仍然是Down的，那么此时触发端口Down

目前光路只有LOS（Lost of Signal）告警会触发Down，通道没有告警触发Down。

- 如果使能了延时触发，且延时触发时间不为0，则等待延时时间后检查是否还有LOS，如果有LOS则触发Down，否则返回并恢复LOS告警。
- 如果没有使能延时触发，或者延时触发时间为0，则立即触发Down。

IR12000上提供了以下命令来配置POS口延时Down功能：

步骤	命令	功能
1	`inspur(config)#`**interface** *<interface-name>*	进入接口配置模式
2	`inspur(config-if-interface-name)#`**port delay-trigger enable**	激活POS端口的延时Down功能
3	`inspur(config-if-interface-name)#`**port delay-trigger** *<time>*	该值为配置的时延时间，范围0~1000，单位：ms，默认值：100ms

提示：

如果配置port delay的值为x后，先关闭延时Down功能，再激活延时Down功能，那么此时的延时值仍为x。

4.验证配置结果。

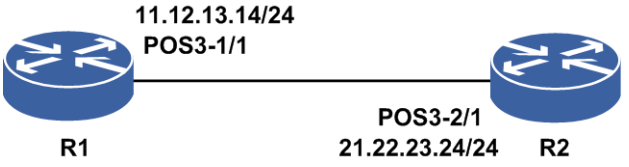
命令	功能
inspur#**show ip interface** [**brief** [**phy** |<*interface-name*>|[{**exclude** | **include**}<*line*>]]]	查看接口信息
inspur#**show interface description**	查看接口的描述信息
inspur#**show running-config-interface** <*interface-name*>	显示接口配置，包括时钟模式、POS口延时Down的配置信息

2.7.2 POS 接口基本配置实例

配置说明

如*图 2-16*所示，R1接口POS3-1/1和R2接口POS3-2/1连接，要求R1与R2能够互相ping通。

图 2-16 POS 接口配置实例拓扑图



配置思路

1.配置R1和R2上POS3接口的IP地址。

2.测试配置结果，确认R1和R2之间能相互Ping通。

配置过程

R1的配置如下：

```
R1(config)#interface pos3-1/1
R1(config-if-pos3-1/1)#clock mode line
R1(config-if-pos3-1/1)#exit
R1(config)#interface pos3-1/1
R1(config-if-pos3-1/1)#no shutdown
R1(config-if-pos3-1/1)#ip address 11.12.13.14  255.255.255.0
R1(config-if-pos3-1/1)#exit
```

R2的配置如下：

```
R2(config)#interface pos3-2/1
R2(config-if-pos3-2/1)#clock mode internal
R2(config-if-pos3-2/1)#exit
R2(config)#interface pos3-2/1
R2(config-if-pos3-2/1)#no shutdown
R2(config-if-pos3-2/1)#ip address 21.22.23.24 255.255.255.0
```

```
R2(config-if-pos3-2/1)#exit
```

配置验证

在R1上验证结果：

```
R1#ping 21.22.23.24
sending 5,100-byte ICMP echoes to 21.22.23.24,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 12/18/20 ms.
```

在R2上验证结果：

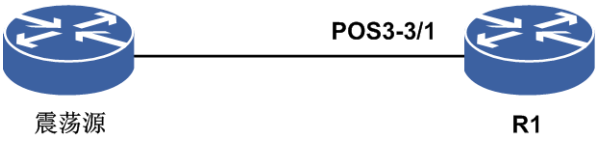
```
R2#ping 11.12.13.14
sending 5,100-byte ICMP echoes to 11.12.13.14,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 12/18/20ms.
```

2.7.3 POS 口延时 Down 配置实例

配置说明

如*图 2-17*所示，由于信号丢失，导致R1的接口硬件频繁地up/down，这时需要在R1的POS口上启用接口延时Down功能。

图 2-17 POS 延时 Down 配置实例拓扑图



配置思路

1.进入接口配置模式。

2.将R1的POS延时Down功能激活。

3.设置已处于激活状态的POS口延时Down属性值。

配置过程

R1上的配置如下：

```
R1(config)#interface pos3-3/1
R1(config-if-pos3-3/1)#port delay-trigger enable
R1(config-if-pos3-3/1)#port delay-trigger 1000
R1(config-if-pos3-3/1)#exit
```

配置验证

单板的ACT灯在配置的时间（1000ms）内没有变化，在R1上用**show**命令查看的结果如下：

```
R1#show running-config-interface pos3-3/1
!<if-intf>
interface pos3-3/1
  no shutdown
$
!</if-intf>
!<pm_if>
interface pos3-3/1
  port delay-trigger enable
  port delay-trigger 1000
$
!</pm_if>
```

2.8 CPOS 接口

CPOS接口是指通道化的POS（Channelized POS）接口，其充分利用了SDH制式的特点，提供对带宽精细划分的能力，可减少组网中对路由设备低速物理接口的数量要求，增强路由设备的低速接口汇聚能力，并提高路由设备的专线接入能力。

2.8.1 配置 CPOS 接口属性

本节介绍COPS接口属性的配置步骤和命令。

1.进入CPOS接口的controller配置模式。

命令	功能
inspur(config)#**controller** <*interface-name*>	全局配置模式下，进入CPOS接口的controller配置模式

2.配置CPOS接口属性。

命令	功能
inspur(config-ctrl-interface-name)#**loopback** { **loopback-cancel** | **loopback-inner** | **loopback-outer** }	配置CPOS接口的环回方式
inspur(config-ctrl-interface-name)#**clock mode** { **internal** |**line**}	配置CPOS接口时钟源
inspur(config-ctrl-interface-name)#**damping** {<*maxsuptime*><*suppress*><*reuse*><*halflife*>|**enable** |**disable**}	配置CPOS接口振荡抑制参数
inspur(config-ctrl-interface-name)#**holdtime** <*holdtime*>	配置CPOS接口保持时间，默认值120，范围：0~1200，单位：秒

{ **loopback-cancel** | **loopback-inner** | **loopback-outer** }：接口的环回方式，包括取消

环回loopback-cancel、内环loopback-inner、外环loopback-outer，默认值是loopback-cancel。

{ **internal** |**line**}：接口时钟源模式，本地时钟internal（默认值）、线路时钟line。

<*maxsuptime*>：最大抑制时间，默认值为20，范围：2~600，单位：秒。

<*suppress*>：抑制门限值，默认值为2000，范围：2~10000。

<*reuse*>：重用门限值，默认值1000，范围：1~2000。

<*halflife*>：半衰期，由当前惩罚值衰减到一半所用的时间，默认值5，范围：1~100，单位：秒。

2.8.2 配置 CPOS 接口段属性

本节介绍CPOS接口段属性的配置步骤和命令。

1.配置CPOS接口帧格式为SDH帧格式。

步骤	命令	功能
1	inspur(config)#**controller** <*interface-name*>	进入CPOS接口的controller配置模式
2	inspur(config-ctrl-interface-name)#**framing sdh**	配置CPOS接口帧格式为SDH帧格式

2.配置CPOS接口段属性。

命令	功能
inspur(config-ctrl-interface-name-sdh)#**flag j0** {**1-trace-byte** |**16-trace-byte** |**64-trace-byte** }<*j0*>	设置CPOS接口段（section）跟踪标记字节J0
inspur(config-ctrl-interface-name-sdh)#**flag j0ex** {**1-trace-byte** |**16-trace-byte** |**64-trace-byte** }<*j0ex*>	设置CPOS接口段（section）期望的对端跟踪标记字节J0
inspur(config-ctrl-interface-name-sdh)#**threshold sd-ber** <*sd*>	配置信号下降BER门限，范围：5~8
inspur(config-ctrl-interface-name-sdh)#**threshold sf-ber** <*sf*>	配置信号失败BER门限，范围：4~8
inspur(config-ctrl-interface-name-sdh)#**aug mapping** {**au3**|**au4**}	设置SDH帧格式下CPOS物理口复用路径的映射模式

1-trace-byte：开销字节1字节模式，字符串长度为1。

16-trace-byte：开销字节16字节模式，字符串长度1~15。

64-trace-byte：开销字节64字节模式，字符串长度1~62。

<*j0*>：段（section）跟踪标记字节，取值范围为0x0~0xff。

<*j0ex*>：期望的对端段（section）跟踪标记字节，取值范围为0x0~0xff。

au3：映射au3复用路径模式。

au4：映射au4复用路径模式。

2.8.3 配置 CPOS 低阶通道

本节介绍CPOS接口复用路径低阶通道的配置步骤和命令。

1.配置CPOS接口帧格式为SDH帧格式。

步骤	命令	功能
1	inspur(config)#**controller** *<interface-name>*	进入CPOS接口的controller配置模式
2	inspur(config-ctrl-interface-name)#**framing sdh**	配置CPOS接口帧格式为sdh帧格式

2.配置映射模式和复用路径。

步骤	命令	功能
1	inspur(config-ctrl-interface-name-sdh)#**aug mapping au4**	选择映射au4（cops只支持au4模式）
2	inspur(config-ctrl-interface-name-sdh)#**au4** *<au4-num>* **tug3** *<tug3-num>*	复用路径配置

<au4-num>：复用路径au4取值1。

<tug3-num>：复用路径tug3取值1~3。

3.配置E1和低阶通道。

步骤	命令	功能
1	inspur(config-ctrl-interface-name-sdh-tug3)#**mode e1**	选择e1模式（cpos支持e1）
2	inspur(config-ctrl-interface-name-sdh-tug3)#**tug2** *<tug2-num>* **e1** *<e1-num>*	创建e1
3	inspur(config-ctrl-interface-name-sdh-tug3-e1)#**clock mode** {**internal**|**line**|**ces-domain**}	配置e1时钟源或恢复时钟
4	inspur(config-ctrl-interface-name-sdh-tug3-e1)#**framing** { **crc4**|**no-crc4**}	配置e1帧格式
5	inspur(config-ctrl-interface-name-sdh-tug3-e1)#**loopback** { **loopback-cancel** | **loopback-inner** | **loopback-outer** }	配置e1环回模式
6	inspur(config-ctrl-interface-name-sdh-tug3-e1)#**flag j2** {**16-trace-byte** | **64-trace-byte** |	设置低阶通道的开销字节j2，取值范围0x0~0xff

步骤	命令	功能
	1-trace-byte-hex}<*j2*>	
7	inspur(config-ctrl-interface-name-sdh-tug3-e1)#**flag j2ex** {**16-trace-byte** | **64-trace-byte** | **1-trace-byte-hex** }<*j2ex*>	设置低阶通道期望的对端开销字节j2，取值范围0x0~0xff
8	inspur(config-ctrl-interface-name-sdh-tug3-e1)#**flag v5** <*v5*>	设置低阶通道的v5值（000、001、010、011、100、101、110、111）
9	inspur(config-ctrl-interface-name-sdh-tug3-e1)#**channelgroup** <*channel-num*> **timeslot** <*timeslot*>	创建成帧通道
10	inspur(config-ctrl-interface-name-sdh-tug3-e1)#**unframe**	创建非成帧通道

<*tug2-num*>：e1对应tug2层取值：1~7。

<*e1-num*>：e1取值1~3。

<*channel-num*>：生成的成帧通道在当前的e1内的通道编号。

<*timeslot*>：成帧通道占用当前e1内时隙（按位使用，范围1~31）。

2.8.4 配置 CPOS 高阶通道

本节介绍CPOS接口复用路径高阶通道的配置步骤和命令。

1.配置CPOS接口帧格式为SDH帧格式。

步骤	命令	功能
1	inspur(config)#**controller** <*interface-name*>	进入CPOS接口的controller配置模式
2	inspur(config-ctrl-interface-name)#**framing sdh**	配置CPOS接口帧格式为sdh帧格式

2.配置映射模式和复用路径。

步骤	命令	功能
1	inspur(config-ctrl-interface-name-sdh)#**aug mapping au4**	选择映射au4（cpos只支持au4模式）
2	inspur(config-ctrl-interface-name-sdh)#**au4** <*au4-num*> **tug3** <*tug3-num*>	复用路径配置

3.配置高阶通道路径的模式和高阶通道参数。

步骤	命令	功能
1	inspur(config-ctrl-interface-name-sdh-tug3)#**mode e1**	选择e1模式（cpos只支持e1）
2	inspur(config-ctrl-interface-name-sdh-tug3)#**flag j1** { **1-trace-byte-hex** | **16-trace-byte** | **64-trace-byte**}<*j1*>	设置高阶通道跟踪标记字节J1值
3	inspur(config-ctrl-interface-name-sdh-tug3)#**flag j1ex** { **1-trace-byte-hex** | **16-trace-byte** | **64-trace-byte**}<*j1ex*>	设置期望的对端高阶通道跟踪标记字节j1值
4	inspur(config-ctrl-interface-name-sdh-tug3)#**flag c2** <*c2*>	信号标记字节，表明可以支持的上层业务
5	inspur(config-ctrl-interface-name-sdh-tug3)#**flag c2ex** <*c2ex*>	期望的对端信号标记字节

<*j1*>：高阶通道跟踪标记字节J1，取值范围0x0~0xff。

- 16–trace-byte：J1描述允许输入1~15个字符
- 64–trace-byte：J1描述允许输入1~62个字符
- 1–trace-byte-hex：J1描述允许输入十六进制的0x0~0xff范围内的任意数值

<*j1ex*>：期望的对端高阶通道跟踪标记字节J1，取值范围0x0~0xff。

<*c2*>：信号标记字节，用来指示VC帧的复接结构和信息净负荷的性质，例如通道是否已装载、所载业务种类和映射方式。可以配置为000，001，002，003，004，018，019，020，021，022，023，024，025，026，027，207和254。例如C2=00H表示这个VC4通道未装载信号，这时要往这个VC4通道的净负荷TUG3中插全“1”码---TU-AIS，设备出现高阶通道未装载告警：HP-UNEQ。C2=02H，表示VC4所装载的净负荷是按TUG结构的复用路线复用来的，中国的2Mbit/s复用进VC4采用的是TUG结构，C2=15H表示VC4的负荷是FDDI（光纤分布式数据接口 ）格式的信号，2M信号的复用，C2要选择TUG结构。C2字节的设置一定要使收/发两端相一致，收发匹配，否则在收端设备出现HP-SLM （高阶通道信号标记字节失配），该告警会使设备向该VC4的下级结构TUG3插全“ 1”码---TU-AIS告警指示信号。

2.8.5 验证 CPOS 配置

IR12000上提供以下命令查看CPOS属性和通道化功能的配置结果：

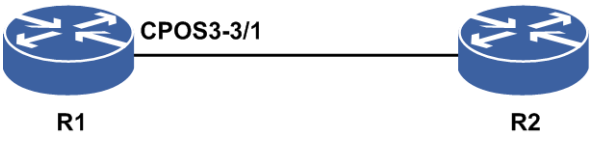
命令	功能
inspur#**show controller** <*interface-name*>	显示当前生效的CPOS接口相关的接口、通道配置和告警、误码等信息
inspur#**show running-config-controller** <*interface-name*>[**all**]	显示指定的CPOS口的配置相关信息

2.8.6 CPOS 配置实例

配置说明

如*图 2-18*所示，E1接口，对接的两个CPOS口能够正常工作。

图 2-18 CPOS 配置实例拓扑图



配置思路

1.进入CPOS controller配置模式。

2.Frame类别选择。

3.择映射模式，选择AU4配置E1通道化接口。

4.SDH E1配置AU（管理单位）序号。

5.选择接口模式。

6.进入E1配置模式。

7.配置通道化接口。

配置过程

R1上配置如下：

```
R1(config)#controller cpos3-3/1
R1(config-ctrl-cpos3-3/1)#framing sdh
R1(config-ctrl-cpos3-3/1-sdh)#aug mapping au4
R1(config-ctrl-cpos3-3/1-sdh)#au4 1 tug3 1
R1(config-ctrl-cpos3-3/1-sdh-tug3)#mode e1
R1(config-ctrl-cpos3-3/1-sdh-tug3)#tug2 2 e1 1
R1(config-ctrl-cpos3-3/1-sdh-tug3-e1)#unframe
R1(config-ctrl-cpos3-3/1-sdh-tug3-e1)#!
R1(config)#interface cpos3_e1-3/1.1/2/1:1
R1(config-if-cpos3_e1-3/1.1/2/1:1)#no shutdown
```

对端接口配置类似。

配置验证

R1上查看CPOS口运行状态：

```
R1#show ip interface brief include cpos:
Interface                  IP-Address      Mask          Admin Phy  Prot
cpos3_e1-3/1.1/2/1:1         unassigned      unassigned      up    up   up
/*两端对接成功后，协议状态up */
```

```
R1#show controller cpos3-3/1
cpos3-3/1 is up
Physical layer is Packet over (SDH)
Clock source: internal
Clock(Tx) grade: S1=00 Quality unknown
Clock(Rx) grade: S1=00 Quality unknown
SPE scrambling : enable
Loopback is not set
BER thresholds
 SD: 10e-6 SF: 10e-4
SECTION
 Active Alarm: LOS
 History Alarm: LOF = 0 LOS = 1
 AIS = 0 RDI = 0
 SD = 0 SF = 0
 TIM = 0 TU = 0
 SEF = 0
 Error : BIP(B1) = 0
 BIP(B2) = 0 REI(M1) = 0
 J0(TX) : "Inspur inspur IR12000"
 CRC-7 : 0x0
 5a 54 45 20 5a 58 52 31 30 20 36 38 30 30 00
 J0(RX) : ""
 CRC-7 : 0x0
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 J0(EX) : "Inspur inspur IR12000"
 CRC-7 : 0x0
 5a 54 45 20 5a 58 52 31 30 20 36 38 30 30 00
Higher order Path 1: STM1/AU4 1/1 is up
 Active Alarm: AIS TU SLU
 History Alarm: AIS = 1 RDI = 0 LOP = 0
 TIM = 0 TU = 1
 SLM = 0 SLU = 1
 UNEQP = 0
 Error : BIP(B3) = 0 REI(G1) = 0
 NEWPTR = 0 PSE = 0 NSE = 0
 C2(TX) : 0x2 TUG structure
 C2(RX) : 0x0 Unequipped or supervisory-unequipped
 C2(EX) : 0x2 TUG structure
 J1(TX) : "Inspur inspur IR12000"
 CRC-7 : 0x0
 5a 54 45 20 5a 58 52 31 30 20 36 38 30 30 00
 J1(RX) : ""
 CRC-7 : 0x0
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 J1(EX) : "Inspur inspur IR12000"
 CRC-7 : 0x0
 5a 54 45 20 5a 58 52 31 30 20 36 38 30 30 00
```

2.9 E1 接口

E1属于ITU-T建议的数字通信体系，数据传输速率为2.048 Mbit/s。CE1是指可通道化的E1，即Channelized E1。

CE1接口工作时分为E1工作模式（clear channel）和 CE1工作模式（channelized）。

- 当工作在E1模式时，相当于一个不分时隙、数据带宽为2.048 Mbit/s的接口，其逻辑特性与同步串口相同，支持PPP、HDLC、帧中继等链路层协议，支持IP网络协议。
- 当工作在CE1模式时，在物理上分为32个时隙，对应编号为0～31。其中的 31个时隙可以被任意地分成若干组（时隙0用于传送帧同步信号，不能被捆绑），每组时隙捆绑以后作为一个接口（channel-set）使用，其逻辑特性与同步串口相同，支持PPP、

HDLC、帧中继等链路层协议，支持IP等网络协议。

2.9.1 配置 E1 接口

本节介绍E1接口的配置步骤和命令。

配置E1接口。

步骤	命令	功能
1	inspur(config)#**controller** <*interface-name*>	进入E1接口的controller配置模式
2	inspur(config-ctrl-interface-name)#**unframe**	配置非通道化E1接口
3	inspur(config-ctrl-interface-name)#**channelgroup**<*channel-num*> **timeslots** <*timeslots*>	配置通道化E1接口（包括通道和时隙）
4	inspur(config-ctrl-interface-name)#**clock mode**{**internal** | **line**|**ces-domain**}	配置E1接口的时钟模式，默认为internal，其中ces-domain只支持TDM模式的E1接口
5	inspur(config-ctrl-interface-name)#**framing**{**crc4**|**no-crc4** }	配置通道化方式E1接口的帧格式，默认为no-crc4
6	inspur(config-ctrl-interface-name)#**linecode** {**hdb3** | **ami**}	配置E1接口的线路编码格式，默认为hdb3
7	inspur(config-ctrl-interface-name)#**exit**	退出E1接口的controller配置模式
8	inspur(config)#**interface** <*interface-name*>	进入E1接口配置模式
9	inspur(config-if-interface-name)#**encapsulation**{**ppp**|**hdlc** | **frame-relay** }	配置E1接口二层协议封装，默认为ppp
10	inspur(config-if-interface-name)#**crc** {**crc16** | **crc32**}	配置E1接口校验模式，默认为crc16
11	inspur(config-if-interface-name)#**ip address**{<*ip-address*>*<net-mask*>}[<*broadcast-addr*>|**secondary**]	配置E1接口IP地址

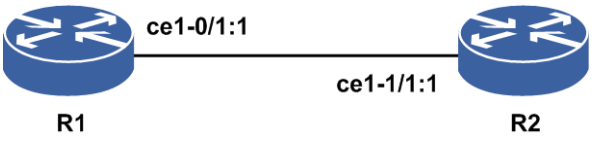
在配置采用E1接口连接的两端路由器时，E1接口的下面几个参数必须保持一致：时隙、framing、linecode（默认是hdb3）、CRC（默认是16）、二层封装协议，另外还要注意时钟保持同步。

2.9.2 通道化 E1 接口配置实例

配置说明

如*图 2-19*所示，R1接口ce1-0/1:1和R2接口ce1-1/1:1连接，要求R1与R2能够互相ping通。采用通道化配置，使用1~10时隙，二层广域网封装协议为PPP，默认线路编解码为hdb3，帧格式为crc16，时钟方式为internal。

图 2-19 通道化 E1 配置实例拓扑图



配置思路

1.配置R1和R2上E1接口的通道和时隙。

2.配置E1接口的封装协议和IP地址。

3.测试配置结果，确认R1和R2之间能相互ping通。

配置过程

R1的配置如下：

```
R1(config)#controller ce1-0/1
R1(config-ctrl-ce1-0/1)#channel-group 1 timeslots 1-10
R1(config-ctrl-ce1-0/1)#no shutdown
R1(config-ctrl-ce1-0/1)#exit
R1(config)#interface ce1-0/1:1
R1(config-if-ce1-0/1:1)#no shutdown
R1(config-if-ce1-0/1:1)#encapsulation ppp
R1(config-if-ce1-0/1:1)#ip address 10.10.1.1 255.255.255.0
```

R2的配置如下：

```
R2(config)#controller ce1-1/1
R2(config-ctrl-ce1-1/1)#channel-group 1 timeslots 1-10
R2(config-ctrl-ce1-1/1)#no shutdown
R2(config-ctrl-ce1-1/1)#exit
R2(config)#interface ce1-1/1:1
R2(config-if-ce1-1/1:1)#no shutdown
R2(config-if-ce1-1/1:1)#encapsulation ppp
R2(config-if-ce1-1/1:1)#ip address 10.10.1.2 255.255.255.0
```

配置验证

在R1上验证结果：

```
R1#ping 10.10.1.2
sending 5,100-byte ICMP echoes to 10.10.1.2,timeout is 2 seconds.
```

```
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 12/18/20 ms.
```

在R2上验证结果：

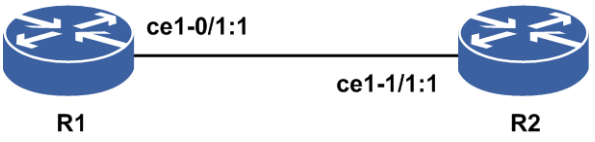
```
R2#ping 10.10.1.1
sending 5,100-byte ICMP echoes to 10.10.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 12/18/20 ms.
```

2.9.3 非通道化 E1 接口配置实例

配置说明

如*图 2-20*所示，R1接口ce1-0/1:1和R2接口ce1-1/1:1连接，要求R1与R2能够互相ping通。采用非通道化配置，二层广域网封装协议采用PPP。

图 2-20 非通道化 E1 配置实例拓扑图



配置思路

1.配置R1和R2上E1接口为非通道化方式。

2.配置E1接口的封装协议和IP地址。

3.测试配置结果，确认R1和R2之间能相互ping通。

配置过程

R1的配置如下：

```
R1(config)#controller ce1-0/1
R1(config-ctrl-ce1-0/1)#unframe
R1(config-ctrl-ce1-0/1)#no shutdown
R1(config-ctrl-ce1-0/1)#exit
R1(config)#interface ce1-0/1:1
R1(config-if-ce1-0/1:1)#no shutdown
R1(config-if-ce1-0/1:1)#encapsulation ppp
R1(config-if-ce1-0/1:1)#ip address 10.10.1.1 255.255.255.0
```

R2的配置如下：

```
R2(config)#controller ce1-1/1
R2(config-ctrl-ce1-1/1)#unframe
R2(config-ctrl-ce1-1/1)#no shutdown
R2(config-ctrl-ce1-1/1)#exit
R2(config)#interface ce1-1/1:1
R2(config-if-ce1-1/1:1)#no shutdown
R2(config-if-ce1-1/1:1)#encapsulation ppp
R2(config-if-ce1-1/1:1)#ip address 10.10.1.2 255.255.255.0
```

配置验证

在R1上验证结果：

```
R1#ping 10.10.1.2
sending 5,100-byte ICMP echoes to 10.10.1.2,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 12/18/20 ms.
```

在R2上验证结果：

```
R2#ping 10.10.1.1
sending 5,100-byte ICMP echoes to 10.10.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 12/18/20 ms.
```

2.10 PPP

PPP是一个被广泛使用的广域网协议，协议跨同步电路和异步电路实现路由设备到路由设备（router-to-router）和主机到网络（host-to-network）的点对点连接。

PPP协议包括LCP和NCP两个部分，用于点到点接口（如E1/T1/E3/T3/POS）链路的协商建链和链路维护，并为上层提供不同于以太网协议的报文封装格式。

2.10.1 配置 PPP

本节介绍PPP协议的配置步骤和命令。

1.配置POS接口的封装模式为**ppp**。

步骤	命令	功能
1	inspur(config)#**interface** <*interface-name*>	进入POS接口配置模式
2	inspur(config-if-interface-name)#**encapsulation** {**hdlc** | **ppp** | **frame-relay**}[**tx** |**rx**]	配置POS接口封装模式，这里选择**ppp**模式

2.配置PPP协议。

步骤	命令	功能
1	inspur(config)#**ppp**	进入PPP配置模式
2	inspur(config-ppp)#**interface** <*interface-name* >	进入PPP接口配置模式
3	inspur(config-ppp-if-interface-name)#**ppp authentication** {**pap** | **chap**}	配置PPP的认证方式，是CHAP和PAP的一种
4	inspur(config-ppp-if-interface-name)#**ppp chap hostname** <*hostname*>	配置本地路由器域名，默认情况下未配置本地路由器域名，允许配置1~159个字符
5	inspur(config-ppp-if-interface-name)#**pp**	配置本地路由器密钥。默认情

步骤	命令	功能
	p chap password {<*password*>| **encrypted** <*password*>}	况下未配置本地路由器密钥，允许配置1~31个字符；加密后的密钥允许配置1~200字符
6	inspur(config-ppp-if-interface-name)#**pp p open**	主动和对方路由器建立PPP链路
7	inspur(config-ppp-if-interface-name)#**pp p pap sent-username** <*username*> **password** {<*password*>| **encrypted** <*password*>}	配置本地路由器被对端路由器以PAP方式验证时发送的PAP用户名和口令。默认情况下未配置用户名（1~159个字符）和口令（1~31个字符）；加密后的口令范围1~120个字符
8	inspur(config-ppp-if-interface-name)#**pp p timeout negotiation** [<*timeout*>]	配置PPP链路协商超时间隔，默认情况下协商超时间隔都为5秒，范围1~30秒
9	inspur(config-ppp-if-interface-name)#**pp p timeout authentication** [<*timeout*>]	配置PPP链路认证超时间隔，默认情况下认证超时间隔都为5秒，范围1~30秒
10	inspur(config-ppp-if-interface-name)#**kee palive** [<*timeout*>| **disable**]	配置PPP链路保活报文的发送间隔时间，默认情况下保活报文发送时间间隔为10秒，范围1~32767秒
11	inspur(config-ppp-if-interface-name)#**pp p max-echo** <*max-count*>	配置PPP链路在没有收到对端的echo应答时，发送的最大echo请求报文数目，默认情况下重发保活报文最大次数5次，范围1~10
12	inspur(config-ppp-if-interface-name)#**pp p ipcp** <*enable*| **disable**>	配置PPP链路NCP协商选项IPCP的开启和关闭
13	inspur(config-ppp-if-interface-name)#**pp p bcp** <*enable*| **management-inline**| **packet-indicator**| **tagged-frame**>	配置PPP链路NCP协商选项BCP的开启
14	inspur(config-ppp-if-interface-name)#**pp p mplscp** <*enable*| **disable**>	配置PPP链路NCP协商选项MPLSCP的开启和关闭
15	inspur(config-ppp-if-interface-name)#**bin d-ip-pool** <*poolname*>	配置IP Pool地址池绑定，给对端分配IP地址
16	inspur(config-ppp-if-interface-name)#**ip-access-type** <*dual*| **ipv4**| **ipv6**>	配置PPP链路IPCP的接入类型：IPv4接入和IPv6接入，默认为dual两个都支持
17	inspur(config-ppp-if-interface-name)#**pp p ipcp neighbor-route** <*enable*	**disable**>	开启或关闭PPP链路主机路由功能
18	inspur(config-ppp-if-interface-name)#**pp p protocol-compress** <*enable*	**disable**>	开启或关闭PPP链路协议域压缩功能
19	inspur(config-ppp-if-interface-name)#**pp**	配置PPP链路给对端分配IP地

步骤	命令	功能
	p ipcp peer-address <*ip*>	址

3.验证配置结果。

命令	功能
inspur#**show ip interface** [**brief** [**phy** |<*interface-name*>|[{**exclude** | **include**}<*line*>]]]	查看接口信息

4.维护PPP。

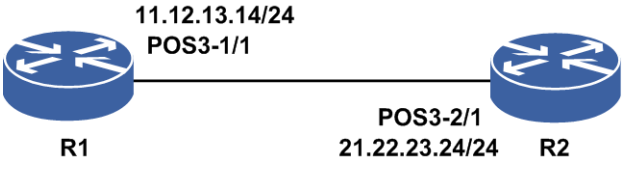
命令	功能
inspur#**debug ppp all**	打开PPP功能所有调试开关
inspur#**debug ppp authentication** [**interface** <*interface-name*>]	打开PPP认证信息调试开关
inspur#**debug ppp error** [**interface** <*interface-name*>]	打开PPP错误信息调试开关
inspur#**debug ppp events** [**interface** <*interface-name*>]	打开PPP事件调试开关
inspur#**debug ppp lcp** [**interface** <*interface-name*>]	打开PPP LCP报文解析输出调试开关
inspur#**debug ppp ncp** [**interface** <*interface-num*>]	打开PPP NCP报文解析输出调试开关
inspur#**debug ppp packet** [**interface** <*interface-name*>]	打开PPP控制报文输出调试开关
inspur#**show debug ppp**	查看所有已开启PPP的debug

2.10.2 PPP 配置实例

配置说明

如*图 2-21*所示，R1接口POS3-1/1和R2接口POS3-2/1组网连接。R1和R2应用PPP协议的认证方式，要求R1和R2之间能够互相Ping通。

图 2-21 PPP 配置实例拓扑图



配置思路

1.配置R1和R2上POS3接口的IP地址。

2.配置R1和R2上的POS3的认证方式。

3.测试配置结果，确认R1和R2之间能相互ping通。

配置过程

R1上的配置如下：

```
R1(config)#interface pos3-1/1
R1(config-if-pos3-1/1)#ip address 11.12.13.14 255.255.255.0
R1(config-if-pos3-1/1)#exit
R1(config)#ppp
R1(config-ppp)#interface pos3-1/1
R1(config-ppp-if-pos3-1/1)#ppp authentication pap
R1(config-ppp-if-pos3-1/1)#ppp pap sent-username Inspur password Inspur
R1(config-ppp-if-pos3-1/1)#end
```

R2上的配置如下：

```
R2(config)#interface pos3-2/1
R2(config-if-pos3-2/1)#ip address 21.22.23.24 255.255.255.0
R2(config-if-pos3-2/1)#exit
R2(config)#ppp
R2(config-ppp)#interface pos3-2/1
R2(config-ppp-if-pos3-2/1)#ppp authentication pap
R2(config-ppp-if-pos3-2/1)#ppp pap sent-username Inspur password Inspur
R2(config-ppp-if-pos3-2/1)#end
```

配置验证

在R1上验证结果：

```
R1#ping 21.22.23.24
sending 5,100-byte ICMP echoes to 21.22.23.24,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),
round-trip min/avg/max= 129/185/200ms.

R1#show running-config-interface pos3-1/1
!<if-intf>
interface pos3-1/1
  ip address 11.12.13.14 255.255.255.0
  no shutdown
$
!</if-intf>
!<ppp>
ppp
  interface pos3-1/1
    ppp authentication pap
    ppp pap sent-username Inspur password encrypted QYOXzHFY98jEIFmivoT6mA==
  $
$
!</ppp>
```

在R2上验证结果：

```
R2#ping 11.12.13.14
sending 5,100-byte ICMP echoes to 21.22.23.24,timeout is 2 seconds.
!!!!!
```

```
Success rate is 100 percent(5/5),
round-trip min/avg/max= 129/185/200ms.

R2#show running-config-interface pos3-2/1
!<if-intf>
interface pos3-2/1
  ip address 21.22.23.24 255.255.255.0
  no shutdown
$
!</if-intf>
!<ppp>
ppp
  interface pos3-2/1
    ppp authentication pap
    ppp pap sent-username Inspur password encrypted QYOXzHFY98jEIFmivoT6mA==
  $
$
!</ppp>
```

2.11 FR

帧中继FR是一种高性能的广域网协议，运行在OSI参考模型的物理层和数据链路层。

2.11.1 配置 FR

本节介绍FR协议的配置步骤和命令。

1.配置POS接口的封装模式为**frame-relay**。

步骤	命令	功能
1	inspur(config)#**interface** <*interface-name*>	进入POS接口配置模式
2	inspur(config-if-interface-name)#**encapsulation** { **frame-relay** | **hdlc** | **ppp** }[**tx** |**rx**]	配置POS接口封装模式，这里选择**frame-relay**模式

2.配置FR协议。

步骤	命令	功能
1	inspur(config)#**frame-relay**	进入FR配置模式
2	inspur(config-fr)#**interface** <*interface-name*>	进入FR接口配置模式，<*interface-name*>为指定的接口名
3	inspur(config-fr-if-interface-name)#**keepalive** [<*period*>| **disable**]	设置指定接口的保活时间间隔，<*period*>为保活时间间隔，单位：秒，默认为10秒，范围1-29
4	inspur(config-fr-if-interface-name)#**frame-relay interface-type** { **dte** | **dce** }	设置指定接口的FR类型，默认为DTE

步骤	命令	功能
5	inspur(config-fr-if-interface-name)#**frame-relay interface-mode** { **point-to-point** | **point-to-multipoint** }	设置指定接口的FR传输类型，默认为点到点传输
6	inspur(config-fr-if-interface-name)#**frame-relay lmi-type** {**ansi** | **cisco** | **q933a**}	设置指定接口的LMI类型，默认为Q933A
7	inspur(config-fr-if-interface-name)#**frame-relay lmi-n391dte** <*events*>	设置FR DTE设备的全状态查询报文计数器，<*events*>为间隔设置，范围为1~255，默认为6
8	inspur(config-fr-if-interface-name)#**frame-relay lmi-n392dte** <*events*>	设置FR DTE设备的LMI错误门限值，<*events*>为间隔设置，范围为1~10，默认为3
9	inspur(config-fr-if-interface-name)#**frame-relay lmi-n392dce** <*events*>	设置FR DCE设备LMI错误门限值，<*events*>为间隔设置，范围为1~10，默认为3
10	inspur(config-fr-if-interface-name)#**frame-relay lmi-n393dte** <*events*>	设置FR DTE设备成功事件计数，<*events*>为间隔设置，范围为1~10，默认为5
11	inspur(config-fr-if-interface-name)#**frame-relay lmi-n393dce** <*events*>	设置FR DCE设备成功事件计数，<*events*>为间隔设置，范围为1~10，默认为5
12	inspur(config-fr-if-interface-name)#**frame-relay interface-dlci** <*dlci-value*>[**cisco**][**broadcast**]	设置点到点模式的DLCI值 <*dlci-value*>：可配置的DLCI值范围为16~1007 [**cisco**]：采用CISCO封装格式 [**broadcast**]：支持广播包
13	inspur(config-fr-if-interface-name)#**frame-relay map** {**ip**}<*ip-address*><*dlci-value*>[{**cisco**}][**broadcast**]	设置点到多点模式的map映射关系 <*dlci-value*>：MAP映射的本端的DLCI值，范围16~1007

3.验证配置结果。

命令	功能
inspur#**show ip interface** [**brief** [**phy** |<*interface-name*>|[{**exclude** | **include**}<*line*>]]]	查看接口信息
inspur#**show frame-relay pvc** [< *dlci-value*>| **interface** [<*interface-name*>][< *dlci-value*>]]	查看PVC状态信息 <*dlci-value*>为PVC对应的DLCI值，范围为16~1007
inspur#**show frame-relay lmi** [**interface** <*interface-name*>]	查看LMI统计信息
inspur#**show frame-relay map**	查看全局MAP条目

4.维护FR。

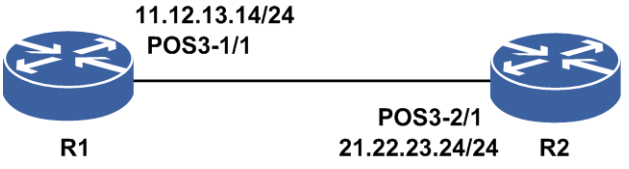
命令	功能
inspur#**debug frame-relay lmi** [**interface** <*interface-name*>]	查看LMI报文信息

2.11.2 FR 物理接口配置实例

配置说明

如*图 2-22*所示，R1接口POS3-1/1和R2接口POS3-2/1直接连接，两个POS接口封装FR协议，要求R1和R2之间能够互相ping通。

图 2-22 FR 的配置实例拓扑图



配置思路

1.配置R1和R2上POS3接口的封装类型为frame-relay。

2.配置R1和R2上的POS3的IP地址，为同网段的不同IP。

3.配置R1上POS3接口类型为DTE，R2上POS3为DCE。

4.配置R1和R2上POS3接口的DLCI，两端为相同的DLCI。

5.测试配置结果，确认R1和R2之间能相互ping通。

配置过程

R1上的配置如下：

```
R1(config)#interface pos3-1/1
R1(config-if-pos3-1/1)#encapsulation frame-relay
R1(config-if-pos3-1/1)#ip address 11.12.13.14 255.255.255.0
R1(config-if-pos3-1/1)#exit
R1(config)#frame-relay
R1(config-fr)#interface pos3-1/1
R1(config-fr-if-pos3-1/1)#frame-relay interface-type dte
R1(config-fr-if-pos3-1/1)#frame-relay interface-dlci 16
R1(config-fr-if-pos3-1/1)#end
```

R2上的配置如下：

```
R2(config)#interface pos3-2/1
R2(config-if-pos3-2/1)#encapsulation frame-relay
R2(config-if-pos3-2/1)#ip address 11.12.13.15 255.255.255.0
R2(config-if-pos3-2/1)#exit
```

```
R2(config)#frame-relay
R2(config-fr)#interface pos3-2/1
R2(config-fr-if-pos3-2/1)#frame-relay interface-type dce
R2(config-fr-if-pos3-2/1)#frame-relay interface-dlci 16
R2(config-fr-if-pos3-2/1)#end
```

配置验证

在R1上验证结果：

```
R1#ping 11.12.13.15
sending 5,100-byte ICMP echoes to 11.12.13.15,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 129/185/200 ms.
```

在R2上验证结果：

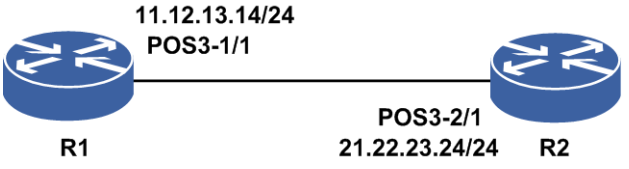
```
R2#ping 11.12.13.14
sending 5,100-byte ICMP echoes to 11.12.13.14,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 129/185/200 ms.
```

2.11.3 FR 子链路配置实例

配置说明

如*图 2-23*所示，R1接口POS3-1/1和R2接口POS3-2/1直接连接，两个POS接口封装FR协议，创建POS的子接口，要求R1和R2之间能够互相Ping通。注：子接口如果采用默认的点对点，那么配置方式与实接口相同，以下示例基于子接口的点对多点模式，需要对IP地址与DLCI进行映射。

图 2-23 FR 子链路配置实例拓扑图



配置思路

1.配置R1和R2上POS接口的封装类型为frame-relay。

2.配置R1上POS接口类型为DTE，R2上POS口为DCE。

3.创建POS接口的子接口。

4.配置R1和R2上的POS的子接口IP地址，为同网段的不同IP。

5.配置R1和R2上POS子接口为point-to-multipoint（点对多点）模式。

6.配置POS子接口与对端IP地址及DLCI的MAP（映射）关系。

7.测试配置结果，确认R1和R2之间能相互ping通。

配置过程

R1上的配置如下：

```
R1(config)#interface pos3-1/1
R1(config-if-pos3-1/1)#encapsulation frame-relay
R1(config-if-pos3-1/1)#exit
R1(config)#frame-relay
R1(config-fr)#interface pos3-1/1
R1(config-fr-if-pos3-1/1)#frame-relay interface-type dte
R1(config-fr-if-pos3-1/1)#exit
R1(config-fr)#exit
R1(config)#interface pos3-1/1.10
R1(config-if-pos3-1/1.10)#ip address 11.12.13.14 255.255.255.0
R1(config-if-pos3-1/1.10)#exit

R1(config)#frame-relay
R1(config-fr)#interface pos3-1/1.10
R1(config-fr-if-pos3-1/1.10)#frame-relay interface-mode point-to-multipoint
R1(config-fr-if-pos3-1/1.10)#frame-relay map ip  11.12.13.15 16
R1(config-fr-if-pos3-1/1.10)#exit
R1(config-fr)#exit
```

R2上的配置如下：

```
R2(config)#interface pos3-2/1
R2(config-if-pos3-2/1)#encapsulation frame-relay
R2(config-if-pos3-2/1)#exit
R2(config)#frame-relay
R2(config-fr)#interface pos3-2/1
R2(config-fr-if-pos3-2/1)#frame-relay interface-type dce
R2(config-fr-if-pos3-2/1)#exit
R2(config-fr)#exit
R2(config)#interface pos3-2/1.10
R2(config-if-pos3-2/1.10)#ip address 11.12.13.15 255.255.255.0
R2(config-if-pos3-2/1.10)#exit

R2(config)#frame-relay
R2(config-fr)#interface pos3-2/1.10
R2(config-fr-if-pos3-2/1.10)#frame-relay interface-mode point-to-multipoint
R2(config-fr-if-pos3-2/1.10)#frame-relay map ip 11.12.13.14 16
R2(config-fr-if-pos3-2/1.10)#exit
R2(config-fr)#exit
```

配置验证

在R1上验证结果：

```
R11#ping 11.12.13.15
sending 5,100-byte ICMP echoes to 11.12.13.15,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 108/181/200 ms.
```

在R2上验证结果：

```
R2#ping 11.12.13.14
sending 5,100-byte ICMP echoes to 11.12.13.14,timeout is 2 seconds.
!!!!
Success rate is 100 percent(4/4),round-trip min/avg/max= 132/183/200 ms.
```

2.12 HDLC

HDLC是链路层协议的一种，与PPP、FR等二层协议平行，为上层协议（IP）提供透明的点到点之间的传输。

HDLC协议提供了一种检测物理链路是否正常工作的机制，为上层协议的数据包提供一种封装方式，支持对IP数据包和IS-IS协议数据包的封装。HDLC还可以将多个HDLC封装的POS口捆绑成一个具有更大带宽的逻辑接口（POSGroup），即实现POS口的链路聚合。

浪潮思科网络科技有限公司路由设备和多数路由设备厂商一样，支持CISCO HDLC。

2.12.1 配置 HDLC

本节介绍HDLC协议的配置步骤和命令。

1.配置POS接口的封装模式为**hdlc**。

步骤	命令	功能
1	inspur(config)#**interface** <*interface-name*>	进入POS接口配置模式
2	inspur(config-if-interface-name)#**encapsulation** { **frame-relay** | **hdlc** | **ppp** }[**tx** |**rx**]	配置POS接口封装模式，这里选择**hdlc**模式

2.配置HDLC协议。

步骤	命令	功能
1	inspur(config)#**hdlc**	进入HDLC配置模式
2	inspur(config-hdlc)#**interface** <*interface-name*>	从HDLC配置模式进入接口配置模式，只能进入HDLC模块关注的POS接口
3	inspur(config-hdlc-if-interface-name)#**keepalive** [<*timeout*>|**disable**]	配置HDLC链路保活报文的发送间隔时间，单位：秒，范围1~32767，默认是10秒
4	inspur(config)#**interface** <*posgroup-name*>	创建聚合组posgroup，进入posgroup接口配置模式
5	inspur(config)#**mhdlc**	进入POS捆绑配置模式
6	inspur(config-mhdlc)#**interface** <*interface-name*>	进入mhdlc接口配置模式
7	inspur(config-mhdlc-member-if-interface-name)#**posgroup** < *posgroup-id* >	添加接口到聚合组，并设置接口的链路聚合模式
8	inspur(config-mhdlc)#**interface** <*posgroup-name* >	从MHDLC配置模式进入聚合组接口配置模式，聚合端口名称的格式为“posgroup＋组号”，组号范

步骤	命令	功能
		围1~64
9	inspur(config-mhdlc-pg-if-posgroup-name)#**mhdlc minimum-member** <*member-number*>	配置posgroup接口up门限，范围1~16，默认是1，即只要有一个成员接口保持up状态，该pos-group接口就是up状态
10	inspur(config-mhdlc-pg-if-posgroup-name)#**mhdlc load-balance** {**per-packet**| **per-destination**}	设置聚合组的负荷分担方式，默认模式为**per-destination**

3.验证配置结果。

命令	功能
inspur#**show ip interface** [**brief** [**phy** |<*interface-name*>|[{**exclude** | **include**}<*line*>]]]	查看接口信息
inspur#**show mhdlc** <*posgroup -id*>	查看posgroup当前配置和状态

4.维护HDLC。

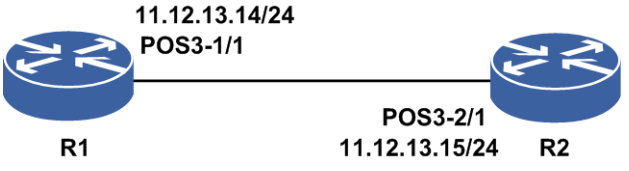
命令	功能
inspur#**debug hdlc** { **packet** [**interface**<*interface-name*>]| **all** }	打开HDLC的报文收发的debug开关
inspur#**show debug hdlc**	显示已打开的HDLC调试命令

2.12.2 HDLC 基本配置实例

配置说明

如*图 2-24*所示，R1接口POS3-1/1和R2接口POS3-2/1直接连接，两个POS接口封装HDLC协议，要求R1和R2之间能够互相ping通。

图 2-24 HDLC 配置实例拓扑图



配置思路

1.配置R1和R2上POS3接口的封装类型为HDLC。

2.配置R1和R2上的POS3的IP地址，该地址为同网段的不同IP。

3.测试配置结果，确认R1和R2之间能相互ping通。

配置过程

R1上的配置如下：

```
R1(config)#interface pos3-1/1
R1(config-if-pos3-1/1)#no shutdown
R1(config-if-pos3-1/1)#encapsulation hdlc
R1(config-if-pos3-1/1)#ip address 11.12.13.14 255.255.255.0
R1(config-if-pos3-1/1)#exit
```

R2上的配置如下：

```
R2(config)#interface pos3-2/1
R2(config-if-pos3-2/1)#no shutdown
R2(config-if-pos3-2/1)#encapsulation hdlc
R2(config-if-pos3-2/1)#ip address 11.12.13.15 255.255.255.0
R2(config-if-pos3-2/1)#exit
```

配置验证

在R1上验证结果：

```
R1#ping 11.12.13.15
sending 5,100-byte ICMP echoes to 11.12.13.15,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 129/185/200 ms.
```

在R2上验证结果：

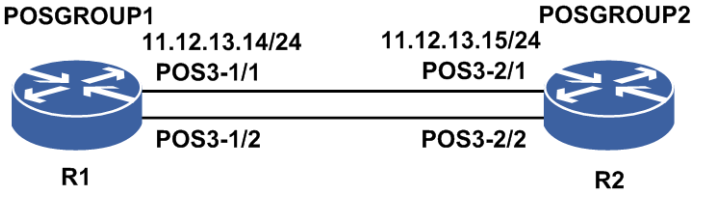
```
R2#ping 11.12.13.14
sending 5,100-byte ICMP echoes to 11.12.13.14,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 129/185/200 ms.
```

2.12.3 POSGROUP 配置实例

配置说明

如*图 2-25*所示，R1上POS3-1/1与POS3-1/2封装HDLC，捆绑到POSGROUP1虚接口中，R2上POS3-2/1与POS3-2/2封装HDLC，捆绑到POSGORUP2虚接口中，要求R1和R2之间能够互相Ping通。

图 2-25 POSGROUP 的配置实例拓扑图



配置思路

1.配置R1和R2上共4个POS接口的封装类型为HDLC。

2.创建POSGROUP接口，配置POSGROUP接口的IP地址，为同网段的不同IP。

3.将POS接口绑入到POSGROUP接口中。

4.测试配置结果，确认R1和R2之间的POSGROUP能相互ping通。

配置过程

R1上的配置如下：

```
R1(config)#interface pos3-1/1
R1(config-if-pos3-1/1)#no shutdown
R1(config-if-pos3-1/1)#encapsulation hdlc
R1(config-if-pos3-1/1)#exit
R1(config)#interface pos3-1/2
R1(config-if-pos3-1/2)#no shutdown
R1(config-if-pos3-1/2)#encapsulation hdlc
R1(config-if-pos3-1/2)#exit
R1(config)#interface  posgroup1
R1(config-if-posgroup1)#ip address 11.12.13.14 255.255.255.0
R1(config-if-posgroup1)#exit

R1(config)#mhdlc
R1(config-mhdlc)#interface  pos3-1/1
R1(config-mhdlc-member-if-pos3-1/1)#posgroup 1
R1(config-mhdlc-member-if-pos3-1/1)#exit
R1(config-mhdlc)#interface  pos3-1/2
R1(config-mhdlc-member-if-pos3-1/2)#posgroup 1
R1(config-mhdlc-member-if-pos3-1/2)#end
```

R2上的配置如下：

```
R2(config)#interface pos3-2/1
R2(config-if-pos3-2/1)#no shutdown
R2(config-if-pos3-2/1)#encapsulation hdlc
R2(config-if-pos3-2/1)#exit
R2(config)#interface pos3-2/2
R2(config-if-pos3-2/2)#no shutdown
R2(config-if-pos3-2/2)#encapsulation hdlc
R2(config-if-pos3-2/2)#exit
R2(config)#interface  posgroup2
R2(config-if-posgroup2)#ip address 11.12.13.15 255.255.255.0
R2(config-if-posgroup2)#exit

R2(config)#mhdlc
R2(config-mhdlc)#interface  pos3-2/1
R2(config-mhdlc-member-if-pos3-2/1)#posgroup 2
R2(config-mhdlc-member-if-pos3-2/1)#exit
R2(config-mhdlc)#interface  pos3-2/2
R2(config-mhdlc-member-if-pos3-2/2)#posgroup 2
R2(config-mhdlc-member-if-pos3-2/2)#end
```

配置验证

在R1上验证结果：

```
R1#ping 11.12.13.15
sending 5,100-byte ICMP echoes to 11.12.13.15,timeout is 2 seconds.
```

```
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 129/185/200 ms.
```

在R2上验证结果：

```
R2#ping 11.12.13.14
sending 5,100-byte ICMP echoes to 11.12.13.14,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 129/185/200 ms.
```

2.13 Multilink

Multilink是PPP的一个可选特性，允许PPP捆绑多条物理链路，并像使用单一的高性能链路一样来使用。Multilink必须在链路配置阶段准备好，设备在运行的时候，会将全部PPP帧分片，再经不同的物理链路发送出去。

Multilink接口是一种虚接口，同样具有普通三层接口的所有功能。多个PPP接口绑定到Multilink接口上，即Multilink虚接口对应多个PPP物理实接口（Multilink对应多条物理链路）。

2.13.1 配置 Multilink

本节介绍Multilink接口的配置步骤和命令。

1.创建Multilink接口。

命令	功能
inspur(config)#**interface multilink**<*multilink-id*>	创建多链接口，multilink接口的范围是1~64

2.配置PPP接口，并将接口绑入Multilink。

步骤	命令	功能
1	inspur(config)#**ppp**	进入PPP配置模式
2	inspur(config-ppp-interface-name)#**interface** <*interface-name*>	进入PPP接口配置模式
3	inspur(config-ppp-if-interface-name)#**multilink-group multilink**<*multilink-id*>	将本链路捆绑入指定的MPPP接口
4	inspur(config-ppp-if-interface-name)#**ppp multilink endpoint** <*endpoint-string*>	设定链路协商时MPPP EPD属性，用于区分子链路属于不同的MPPP链路

endpoint <*string*>：描述符字符串，长度为1~16个字符，默认按照一定规则自动生成，默认方式下，在一个多链中的子链endpoint相同。

3.配置MPPP协议参数。

步骤	命令	功能
1	inspur(config)#**mppp**	进入MPPP配置模式
2	inspur(config-mppp)#**interface** <*interface-name*>	进入MPPP接口配置模式
3	inspur(config-mppp-if-interface-name)#**mppp load-balance** {**per-destination** | **per-packet**}	配置MPPP的负荷分担方式，配此参数时需要解除链路Multilink绑定关系，负荷分担默认是采用逐目的方式
4	inspur(config-mppp-if-interface-name)#**mppp multilink fragmentation**	配置MPPP的分片功能，配此参数时需要解除链路Multilink绑定关系，默认不分片
5	inspur(config-mppp-if-interface-name)#**mppp mplscp** <*enable*| **disable**>	配置MPPP链路NCP协商选项MPLSCP的开启和关闭

per-destination| **per-packet**：Multilink接口负荷分担方式，分别是逐目的和逐包，默认是逐目的。

4.验证配置结果。

命令	功能
inspur#**show ppp multilink** [<*multilink-id*>]	显示多链路内的摘要信息

5.维护Multilink。

命令	功能
inspur#**debug ppp all**	打开PPP功能所有调试开关
inspur#**debug ppp authentication** [**interface** <*interface-name*>]	打开PPP认证信息调试开关
inspur#**debug ppp error** [**interface** <*interface-name*>]	打开PPP错误信息调试开关
inspur#**debug ppp events** [**interface** <*interface-name*>]	打开PPP事件调试开关
inspur#**debug ppp lcp** [**interface** <*interface-name*>]	打开PPP LCP报文解析输出调试开关
inspur#**debug ppp ncp** [**interface** <*interface-num*>]	打开PPP NCP报文解析输出调试开关
inspur#**debug ppp packet** [**interface** <*interface-name*>]	打开PPP控制报文输出调试开关
inspur#**show debug ppp**	查看所有已开启PPP的debug

2.13.2 Multilink 配置实例

配置说明

如*图 2-26*所示，R1接口CE1-0/1:1和R2接口CE1-1/1:1直连连接，R1和R2的CE1接口分别绑入Multilink接口，要求R1和R2之间能够互相Ping通。

图 2-26 Multilink 配置实例拓扑图



配置思路

1.在R1和R2上分别创建Multilink1接口，并配置不同网段的IP地址。

2.配置Multilink接口负荷分担方式为逐包。

3.R1和R2的CE1接口分别绑入Multilink1接口。

4.测试配置结果，确认R1和R2之间的Multilink接口能相互ping通。

配置过程

R1上的配置如下：

```
R1(config)#interface multilink1
R1(config-if-multilink1)#ip address 11.12.13.14 255.255.255.0
R1(config-if-multilink1)#exit

R1(config)#mppp
R1(config-mppp)#interface multilink1
R1(config-mppp-if-multilink1)#mppp load-balance per-packet
R1(config-mppp-if-multilink1)#exit
R1(config-mppp)#exit

R1(config)#interface ce1-0/1:1
R1(config-if-ce1-0/1:1)#no shutdown
R1(config-if-ce1-0/1:1)#exit

R1(config)#ppp
R1(config-ppp)#interface ce1-0/1:1
R1(config-ppp-if-ce1-0/1:1)#multilink-group multilink1
R1(config-ppp-if-ce1-0/1:1)#end
```

R2上的配置如下：

```
R2(config)#interface multilink1
R2(config-if-multilink1)#ip address 21.22.23.24 255.255.255.0
R2(config-if-multilink1)#exit

R2(config)#mppp
R2(config-mppp)#interface multilink1
R2(config-mppp-if-multilink1)#mppp load-balance per-packet
```

```
R2(config-mppp-if-multilink1)#exit
R2(config-mppp)#exit

R2(config)#interface ce1-1/1:1
R2(config-if-ce1-1/1:1)#no shutdown
R2(config-if-ce1-1/1:1)#exit

R2(config)#ppp
R2(config-ppp)#interface ce1-1/1:1
R2(config-ppp-if-ce1-1/1:1)#multilink-group multilink1
R2(config-ppp-if-ce1-1/1:1)#end
```

配置验证

查看R1上的配置：

```
R1#show running-config-interface ce1-0/1:1
!<if-intf>
interface ce1-0/1:1
  no shutdown
$
!</if-intf>
!<ppp>
ppp
  interface ce1-0/1:1
    multilink-group multilink1
  $
$
!</ppp>

R1#show running-config-interface multilink1
!<if-intf>
interface multilink1
ip address 11.12.13.14 255.255.255.0
$
!</if-intf>
!<mppp>
mppp
  interface multilink1
    mppp load-balance per-packet
  $
$
!</mppp>
```

查看R2上的配置：

```
R2#show running-config-interface ce1-1/1:1
!<if-intf>
interface ce1-1/1:1
  no shutdown
$
!</if-intf>
!<ppp>
ppp
  interface ce1-1/1:1
    multilink-group multilink1
  $
$
!</ppp>

R2#show running-config-interface multilink1
!<if-intf>
interface multilink1
  ip address 21.22.23.24 255.255.255.0
$
!</if-intf>
```

```
!<mppp>
mppp
  interface multilink1
    mppp load-balance per-packet
  $
$
!</mppp>
```

在R1上验证结果：

```
R1#ping 21.22.23.24
sending 5,100-byte ICMP echo(es) to 21.22.23.24,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 5/7/10 ms.
```

在R2上验证结果：

```
R2#ping 11.12.13.14
sending 5,100-byte ICMP echo(es) to 11.12.13.14,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 7/7/10 ms.
```

以上结果说明Multilink配置成功。

2.14 端口切换

10G以太网接口可作为LAN接口使用，也可作为WAN接口使用。

提示：

接口板RA-DPIU-01XGE-SFP+支持10G LAN和10G WAN接入。

通过命令，可以手动指定接口板RA-DPIU-01XGE-SFP+对10G LAN和10G WAN接入的两种模式进行互相切换。

2.14.1 配置端口切换

本节介绍端口LAN/WAN切换的配置步骤和命令。

1.配置端口LAN/WAN切换。

步骤	命令	功能
1	inspur(config)#**interface** <*interface-name*>	进入接口配置模式
2	inspur(config-if-interface-name)#**port-mode lan-wan** {**lan** | **wan**}	进行LAN/WAN切换

注意：

如果端口没有配置LAN/WAN属性，RP-02XGE-SFP+-S会以LAN口进行初始化。

LAN/WAN模式切换会清除所有上层配置。在使用中应先确定模式，再进行其它配置；如果在配置后再进行模式切换，会造成接口上的之前的配置全部清除。

2.验证配置结果。

命令	功能
inspur#**show ip interface brief**	显示当前端口状态，xgei为LAN口，xgeiw为WAN口

2.14.2 端口模式切换配置实例

配置说明

在IR12000路由器上，将端口xgei-2/1切换到WAN模式。

配置思路

1.通过**show version**命令来查看当前需要切换的子卡所在槽位。

2.全局模式下进入接口配置模式。

3.使用**port-mode**命令切换LAN/WAN模式。

配置过程

IR12000路由器上的配置如下：

```
inspur(config)#interface xgei-2/1
inspur(config-if-xgei-2/1)#port-mode lan-wan wan
inspur(config)#
```

配置验证

查看R1的切换结果：

```
inspur#show ip interface brief phy
gei-0/1        unassigned      unassigned      up          up        up
gei-0/2        10.2.1.1        255.255.255.0   up          up        up
gei-0/3        unassigned      unassigned      down        down      down
gei-0/4        unassigned      unassigned      up          up        up
gei-0/5        unassigned      unassigned      down        down      down
gei-0/6        172.0.2.1       255.255.255.0   up          up        up
gei-0/7        unassigned      unassigned      up          up        up
gei-0/8        unassigned      unassigned      up          up        up
gei-0/9        unassigned      unassigned      up          up        up
xgeiw-2/1      unassigned      unassigned      down        down      down
```

2.15 端口抑制

网络应用中，设备端口可能会因各种原因（如物理信号干扰、链路层配置错误等）导

致端口频繁交替出现up和down的状态，从而造成路由协议、MPLS功能等不稳定，对设备和网络产生严重影响，甚至可能造成部分设备瘫痪，网络不可用。

端口震荡抑制特性（Damping）对端口频繁up和down事件进行控制，使其小于一定的频率，以减小对设备及网络稳定性的影响。

2.15.1 配置端口抑制

本节介绍端口震荡抑制的配置步骤和命令。

1.配置端口震荡抑制。

IR12000提供以下命令来配置某一端口的震荡抑制激活状态（默认为激活）：

步骤	命令	功能
1	`inspur(config)#`**interface** *<interface-name>*	进入接口配置模式
2	`inspur(config-if-interface-name)#`**damping enable**	配置端口的端口震荡抑制激活状态

2.设置端口抑制属性值。

IR12000提供了以下命令来为处于enable状态的端口设置抑制属性值，其中包括：最大抑制时间，抑制门限值，重用门限值，半衰期。

步骤	命令	功能
1	`inspur(config-if-interface-name)#`**damping** *<maxsuptime><suppress><reuse><halflife>*	设置处于enable状态的端口的振荡抑制属性值

<maxsuptime>：最大抑制时间，单位：秒，范围1~600，默认值为20秒。

<suppress>：抑制门限值，范围1~10000，默认值2000。

<reuse>：重用门限值，范围1~2000，默认值1000。

<halflife>：半衰期，由当前惩罚值衰减到一半所用的时间，单位：秒，范围1~100，默认值5秒。

提示：

配置要求：*<maxsuptime>*大于*<halflife>*，*<suppress>*大于*<reuse>*。

3.验证配置结果。

命令	功能
`inspur#`**show damping** *<interface-name>*	显示端口的振荡抑制属性值

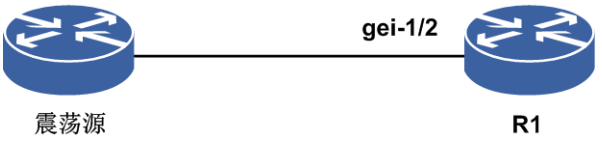
本条命令显示的内容包括：端口类型、端口物理地址，端口震荡次数、端口被抑制次数、当前惩罚值、最大惩罚值、是否处于抑制状态、最大抑制时间，抑制门限值，重用门限值，半衰期。

2.15.2 端口抑制配置实例

配置说明

如*图 2-27*所示，由于震荡源的信号不稳定，导致R1的接口硬件频繁地up/down，这时需要在R1的接口上启用接口震荡抑制功能。

图 2-27 端口 Damping 配置实例拓扑图



配置思路

配置端口抑制功能的思路如下：

1.进入接口配置模式。

2.激活R1的端口震荡抑制功能（默认是激活状态）。

3.设置已处于激活状态的端口抑制属性值。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#damping enable
R1(config-if-gei-1/2)#damping 20 2000 1000 5
R1(config-if-gei-1/2)#end
```

配置验证

在R1上查看配置结果：

```
R1#show damping gei-1/2
================================================================================
Flaps      :Displays the number of times that an interface has flapped.
Penalty    :Displays the accumulated penalty.
MaxSTm     :Displays the maximum suppress.
SuppV      :Displays the suppress threshold.
ReuseV     :Displays the reuse threshold.
HalfL      :Displays the half-life counter.
MaxPenalty :Displays the maximum penalty.
DampNum    :Displays the number of dampening.
Suppress   :Indicates if the interface is dampened(F:FALSE,T:TRUE).
================================================================================
gei-1/2
MaxSTm(s) SuppV ReuseV HalfL(s) MaxPenalty DampNum Suppress Penalty Flaps
```

```
================================================================================
  20      2000   1000      5       16000       0      F          0    0
--------------------------------------------------------------------------------
```

2.16 接口关联检测

在某些典型的组网（如桥接）环境下，接入层、汇聚层、核心层分别采用各自网络内的保护手段，且各部分之间没有映射机制，会造成多点故障下的业务中断。

这主要是因为在多点故障后，接入层、汇聚层、核心层只能在本层提供保护，相关的层无法感知。在这种情况下，会导致无故障层继续沿原有路由发送数据，故障层由于多点故障无法将业务流量继续转发出去。

提供不同层间的接口OAM映射以及联动可以解决上述故障问题。

2.16.1 配置接口关联检测

本节介绍接口关联检测的配置步骤和命令。

1.配置接口二层关联检测。

IR12000提供以下命令来配置某一端口的震荡抑制激活状态（默认为激活）：

步骤	命令	功能
1	inspur(config)#**interface** {<*interface-name*>| **byname** <*byname*>}	进入接口配置模式
2	inspur(config-if-interface-name)#**track** {<*track-name*>| **group** <*track-name*>| **trigger** {<*track-name*>| **group** <*track-name*>}}	配置接口二层关联检测

<*track-name*>：Track名，1~31位字符串。

2.配置接口IPv4关联检测。

命令	功能
inspur(config-if-interface-name)#**ipv4 track** [**group**]<*track-name*>	配置接口IPv4关联检测

3.配置接口IPv6关联检测。

命令	功能
inspur(config-if-interface-name)#**ipv6 track** [**group**]<*track-name*>	配置接口IPv6关联检测

4.验证配置结果。

命令	功能
inspur#**show running-config-interface** [**interface-name**]	显示接口配置

2.17 其它逻辑接口

逻辑接口指用户配置的不是实际存在的接口，IR12000支持的逻辑接口有：Loopback接口、NULL接口、ULEI接口、Tunnel接口、SuperVLAN接口、SmartGroup接口等，逻辑接口有如下几个共同点：

1.不存在与该接口对应的真实物理接口，虽然有时会存在一定的“映射”关系。

2.由于第一条的原因，此类接口（除NULL接口外）不会依据物理接口自动生成，必须根据实际情况需要手工创建。

2.17.1 配置 Loopback 接口

Loopback接口是应用最为广泛的一种虚接口，创建后可一直保持Up状态，并具有环回的特性，Loopback接口常用来提高配置的可靠性。

1.配置Loopback接口。

步骤	命令	功能
1	inspur(config)#**interface** {<*interface-name*>| **byname** <*byname*>}	进入接口配置模式，配置Loopback接口，范围Loopback1到Loopback64
2	inspur(config-if-interface-name)#**ip address** {<*ip-address*><*net-mask*>|<*A.B.C.D/X*>}[<*broadcast-address*>| **secondary**]	配置Loopback接口的IP地址和子网掩码

2.验证配置结果。

命令	功能
inspur#**show ip interface**	显示接口的三层信息
inspur#**show running-config-interface** <*interface-name*>	显示接口的配置信息

2.17.2 配置 NULL 接口

本节介绍NULL接口的应用场景及NULL接口的配置信息查看方法。

1.配置NULL接口。

系统自动创建NULL1接口，不需要配置，不允许删除。

2.查看NULL接口配置信息。

命令	功能
inspur#**show running-config-interface null1**	查看NULL接口配置信息

2.17.3 配置 ULEI 接口

本节介绍ULEI接口的应用场景以及ULEI接口的配置步骤和命令。

1.创建ULEI接口。

步骤	命令	功能
1	inspur(config)#**request interface** <**ulei-name**>	创建ULEI接口
2	inspur(config)#**interface** <**ulei-name**>	进入ULEI接口配置模式

2.将POS接口映射到ULEI接口。

步骤	命令	功能
1	inspur(config)#**ppp**	进入PPP配置模式
2	inspur(config-ppp)#**interface** <**interface-name**>	进入POS接口配置模式，<**interface-name**>为POS接口名
3	inspur(config-ppp-if-interface-name)#**no ppp ipcp enable**	关闭IPCP功能
4	inspur(config-ppp-if-interface-name)#**ppp bcp enable**	激活BCP功能
5	inspur(config)#**interface** <**interface-name**>	进入POS接口配置模式
6	inspur(config-if-interface-name)#**map-to** <**ulei-name**>	POS接口映射到ULEI接口，<**ulei-name**>为ULEI接口名

3.验证配置结果。

命令	功能

命令	功能
inspur(config)#**show running-config portmap**	显示POS接口映射ULEI接口情况，**portmap**为POS映射模块名
inspur(config)#**show running-config–interface** <*ulei-name*>	查看ULEI接口的配置

2.17.4 配置 Tunnel

本节介绍Tunnel的应用场景以及Tunnel的配置步骤和命令。

1.配置Tunnel。

在IR12000上使用以下命令配置GRE隧道：

命令	功能
inspur(config)#**interface gre_tunnel** <*tunnel-id*>	创建GRE隧道，<*tunnel-id*>为GRE隧道号，范围：1~4000

在IR12000上使用以下命令配置TE隧道：

命令	功能
inspur(config)#**interface te_tunnel**<*tunnel-id*>	创建TE隧道，<*tunnel-id*>为TE隧道号，范围：1~16000

在IR12000上使用以下命令配置v6隧道：

命令	功能
inspur(config)#**interface v6_tunnel**<*tunnel-id*>	创建v6隧道，<*tunnel-id*>为v6隧道号，范围：1~12288

2.验证配置结果。

命令	功能
inspur(config)#**show ip interface gre_tunnel**<*tunnel-id*>	显示gre_tunnel的状态信息，<*tunnel_id*>为GRE隧道号，范围：1~4000
inspur(config)#**show ip interface te_tunnel**<*tunnel-id*>	显示te_tunnel的状态信息，<*tunnel_id*>为TE隧道号，范围：1~64511
inspur(config)#**show ip interface v6_tunnel**<*tunnel-id*>	显示v6_tunnel的状态信息，<*tunnel_id*>为v6隧道号，范围：1~3000

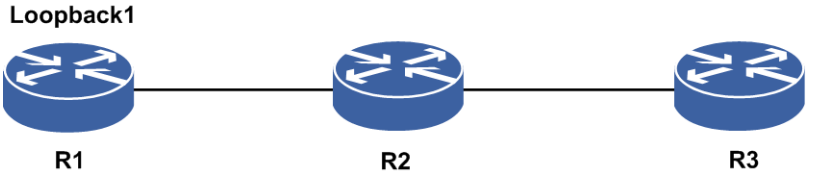
2.17.5 用 Loopback 接口构造黑洞路由配置实例

配置说明

Loopback接口可应用在IP地址借用中和Router-ID中。Loopback接口经常作为路由的下一跳，产生黑洞路由的效果。

如*图 2-28*所示，现在要在R1上构造一条黑洞路由，将到目的地址为192.11.1.2的主机路由导入到黑洞路由中。

图 2-28 用 Loopback 接口构造黑洞路由配置实例拓扑图



配置思路

1.创建Loopback接口并配置IP地址。

2.将Loopback接口作为路由的下一跳。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 192.1.1.2 255.255.255.0
R1(config-if-loopback1)#exit
R1(config)#ip route 192.11.1.2 255.255.255.255 loopback1
```

配置验证

用show命令验证配置结果：

```
R1(config)#show running-config-interface loopback1
!<if-intf>
interface loopback1
  ip address 192.1.1.2 255.255.255.0
$
!</if-intf>
!<static>
ip route 192.11.1.2 255.255.255.255 loopback1
!</static>

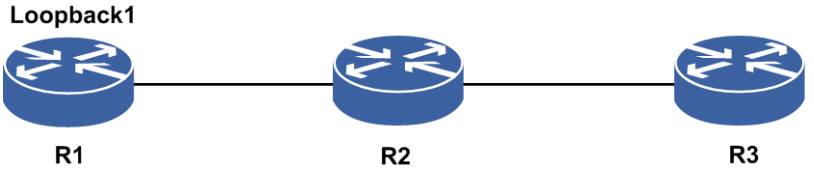
R1(config)#show ip forwarding route 192.11.1.2
IPv4 Routing Table:
status codes: *valid, >best
   Dest            Gw            Interface      Owner      Pri Metric
*> 192.11.1.2/32     192.1.1.2      loopback1      static     1   0
```

2.17.6 将 Loopback 接口作为 Router-ID 配置实例

配置说明

如*图 2-29*所示，在R1上配置Loopback接口在路由协议中作为Router-ID。

图 2-29 Loopback 接口作为 Router-ID 配置实例拓扑图



配置思路

1.创建Loopback接口并配置IP地址。

2.将Loopback接口作为路由协议的Router-ID。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip adderss 1.1.1.2 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 30.0.0.1 255.255.255.252
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip address 30.0.2.1 255.255.255.252
R1(config-if-gei-1/2)#exit
R1(config)#router ospf 10
R1(config-ospf-10)#router-id 1.1.1.2
R1(config-ospf-10)#area 0
R1(config-ospf-10-area-0)#network 30.0.0.0 0.0.0.3
R1(config-ospf-10-area-0)#redistribute connected
R1(config-ospf-10-area-0)#exit
```

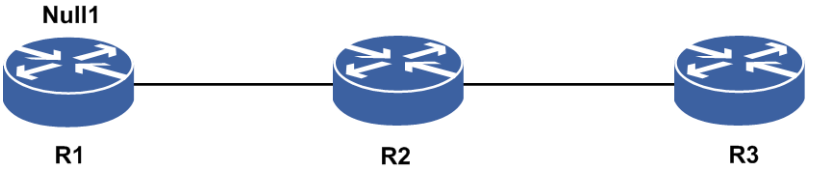
2.17.7 NULL 接口配置实例

配置说明

NULL接口从不转发任何报文，对于所有发到该接口的报文都直接丢弃，由于这个特征，NULL接口主要被用在以下两方面：防止路由环，用于过滤通信量。

NULL接口经常作为路由的下一跳，产生黑洞路由的效果。如*图 2-30*所示，现在要在R1上构造一条黑洞路由，将到目的地址为192.11.1.2的主机路由导入到黑洞路由中。

图 2-30 NULL 接口配置实例拓扑图



配置思路

将NULL接口作为配置静态路由的下一跳。

配置过程

R1上的配置如下：

```
R1(config)#ip route 192.11.1.2 255.255.255.255 null?
<1-1>
R1(config)#ip route 192.11.1.2 255.255.255.255 null1
```

配置验证

用show命令验证配置结果：

```
R1(config)#show running-config-interface null1
!<if-intf>
interface null1
$
!</if-intf>
!<static>
ip route 192.11.1.2 255.255.255.255 null1
!</static>

R1(config)#show ip forwarding route 192.11.1.2
IPv4 Routing Table:
status codes: *valid, >best
   Dest            Gw            Interface      Owner      Pri Metric
*> 192.11.1.2/32     0.0.0.0        null1          static     1   0
```

2.17.8 Tunnel 配置实例

配置说明

单台设备上配置Tunnel接口以及具体Tunnel应用（如MPLS、VPN、IPv6等）。

配置思路

1.进入tunnel接口配置模式。

2.配置相关属性。

配置过程

路由器上配置如下：

```
inspur(config)#interface te_tunnel1
inspur(config-if-te_tunnel1)#ip unnumbered loopback1
inspur(config-if-te_tunnel1)#exit
inspur(config)#interface gre_tunnel1
inspur(config-if-gre_tunnel1)#ip unnumbered loopback1
inspur(config-if-gre_tunnel1)#exit
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#exit
```

配置验证

show命令验证配置：

```
inspur(config)#show ip interface gre_tunnel1
gre_tunnel1 AdminStatus is up, PhyStatus is up, line protocol is down
  Ip unnumbered loopback1  (use ip address:1.2.3.81)
  IP MTU is 1476 bytes

inspur(config)#show ip interface te_tunnel1
te_tunnel1 AdminStatus is up, PhyStatus is up, line protocol is down
  Ip unnumbered loopback1  (use ip address:1.2.3.81)
  IP MTU is 1500 bytes

inspur(config)#show ip interface v6_tunnel1
v6_tunnel1 AdminStatus is up, PhyStatus is up, line protocol is down
  IP MTU is 1460 bytes
```

3 IPv4 业务

3.1 ARP

ARP协议提供了一种报文请求、应答的工作机制，用来实现IP地址与MAC地址间的转换，以保证通信的顺利进行。

3.1.1 配置 ARP

本节介绍ARP功能的配置步骤和命令。

1.配置永久ARP条目。

步骤	命令	功能
1	inspur(config)#**arp**	从配置模式下进入ARP配置模式。
2	inspur(config-arp)#**arp** <*interface-name*> **permanent** <*ip-address*><*mac-address*>[<*extervlanid*>][<*intervlanid*>][<*interface-name*>]	配置永久的ARP条目进行永久绑定，当前生效，设备重启之后仍然生效。

2.配置ARP老化时间。

步骤	命令	功能
1	inspur(config)#**arp**	从配置模式下进入ARP配置模式。
2	inspur(config-arp)#**timeout** <*interface-name*><*seconds*>	配置ARP缓冲区中ARP表项的老化时间，范围1~2147483，单位：秒，缺省为14400秒。
3	inspur(config-arp)#**interface** <*interface-name*>	进入ARP接口配置模式 。
4	inspur(config-arp-if-interface-name)#**timeout** <*seconds*>	配置ARP缓冲区中ARP表项的老化时间 。 单位：秒，范围1~2147483，缺省为14400秒。

3.配置ARP保护。

步骤	命令	功能
1	inspur(config)#**arp**	从配置模式下进入ARP配置模式。
2	inspur(config-arp)#**protect** { **interface** <*interface-name*>| **whole** | **common-mac** | **special-mac** <*hardware-address*>}[**limit-num** < *num*>]	配置ARP的保护功能，默认为不进行ARP条目的保护。 **interface**表示ARP基于接口的保护。 **whole**表示ARP基于全局ARP条目个数的保护。 <*num*>为设置的ARP保护条目上限。
3	inspur(config-arp)#**interface** <*interface-name*>	进入ARP接口配置模式 。
4	inspur(config-arp-if-interface-name)#**protect** [**limit-num** <*num*>]	配置接口ARP的保护功能，默认为不进行ARP条目的保护。

4.配置ARP代理。

步骤	命令	功能
1	inspur(config)#**arp**	从配置模式下进入ARP配置模式。
2	inspur(config-arp)#**proxy** <*interface-name*>	配置ARP的代理功能，默认为不进行ARP代理。
3	inspur(config-arp)#**interface** <*interface-name*>	进入ARP接口配置模式。
4	inspur(config-arp-if-interface-name)#**proxy**	配置ARP的代理功能，默认为不进行ARP代理。
5	inspur(config-arp)#**local-proxy-arp** <*interface-name*>	配置本地的ARP代理，支持子接口物理口。
6	inspur(config-arp)#**proxy local** <*interface-name*>	配置同一VLAN下ARP代理功能， 默认为关闭。

5.配置ARP源过滤功能。

步骤	命令	功能
1	inspur(config)#**arp**	从配置模式下进入ARP配置模式。
2	inspur(config-arp)#**source-filtered** <*interface-name*>[**disable**]	开启ARP源过滤功能，默认为开启。
3	inspur(config-arp)#**interrface** <*interface-name*>	进入接口配置模式 。

步骤	命令	功能
4	inspur(config-arp-if-interface-name)#**source-filtered** [**disable**]	开启ARP源过滤功能，默认为开启。

6.配置ARP抑制。

步骤	命令	功能
1	inspur(config)#**arp**	进入ARP配置模式。
2	inspur(config-arp)#**port-speed** <*interface-name*><*speed*>	指定接口的抑制速率，即每秒钟允许上送报文的最大数，范围1~1000。
3	inspur(config-arp)#**limit-time** <*interface-name*><*time*>	指定接口的抑制时间，范围0~1000，单位：秒，默认为10秒。
4	inspur(config-arp)#**interface** <*interface-name*>	进入ARP接口配置模式。
5	inspur(config-arp-if-interface-name)#**port-speed** <*speed*>	配置该接口的抑制速率，即每秒钟允许上送报文的最大数，范围1~1000。
6	inspur(config-arp-if-interface-name)#**limit-time** <*time*>	配置该接口的抑制时间，单位：秒，范围0~1000，默认为10秒。

7.配置发送免费ARP。

步骤	命令	功能
1	inspur(config)#**arp**	从配置模式下进入ARP配置模式。
2	inspur#(config-arp)#**periodic freearp** <*interface-name*>[<*seconds*>]	配置接口周期性的发送免费ARP，范围10~14400，单位：秒，缺省为30秒。
3	inspur(config-arp)#**gratuitous-learn** <*interface-name*>	配置指定接口的免费ARP学习功能，默认为关闭。
4	inspur(config-arp)#**gratuitous-proxy-arp periodic** <*interface-name*>[<*seconds*>]	指定接口的免费代理ARP的定时发送功能并设置发送间隔，范围1~14400，单位：秒，缺省为30秒。
5	inspur(config-arp)#**gratuitous-proxy-arp** <*interface-name*><*begin-ip-address*><*end-ip-address*>	配置接口发送免费代理ARP使用的IP地址。
6	inspur(config-arp)#**interface** <*interface-name*>	进入ARP接口配置模式。

步骤	命令	功能
7	inspur((config-arp-if-interface-name)#**gratuitous-learn**	配置指定接口的免费ARP学习功能，默认为关闭。
8	inspur((config-arp-if-interface-name)#**gratuitous-proxy-arp periodic** [<*seconds*>]	指定接口的免费代理ARP的定时发送功能并设置发送间隔，范围1~14400，单位：秒，缺省为30秒。
9	inspur((config-arp-if-interface-name)#**gratuitous-proxy-arp**<*begin-ip-address*><*end-ip-address*>	配置接口发送免费代理ARP使用的IP地址。

8.配置ARP其它功能。

命令	功能
inspur(config-arp)#**to-static** [**interface** <*interface-name*>]	将动态的ARP条目转化为TS类型的条目。
inspur(config-arp)#**purge-delay** <*interface-name*><*value*>	配置在接口协议状态为down时，接口上ARP表项的清除时间，范围1~36000 ，单 位：秒，缺省为600秒。
inspur(config-arp-if-interface-name)#**purge-delay** <*value*>	
inspur(config-arp)#**learn-disable** <*interface-name*>	禁止ARP的学习功能。
inspur(config-arp-if-interface-name)#**learn-disable**	
inspur(config-arp)#**alarm-threshold learn-limit** <*interface-name*><*packet_num*>	配置指定接口的ARP学习限制保护的告警阈值，范围1~65535，缺省为300。
inspur(config-arp-if-interface-name)#**alarm-threshold learn-limit** <*packet_num*>	
inspur(config-arp)#**alarm-threshold source-filter** <*interface-name*><*packet_num*>	配置指定接口的ARP源过滤保护的告警阈值，范围1~65535，缺省为300。
inspur(config-arp-if-interface-name)#**alarm-threshold source-filter** <*packet_num*>	
inspur(config-arp)#**backupvrrp-learn** <*interface-name*>	配置指定接口的备VRRPARP学习功能，默认为关闭。
inspur(config-arp-if-interface-name)#**backupvrrp-learn**	
inspur(config-arp)#**learn-limit**<*interface-name*>	配置指定接口的ARP学习限制功能，默认为关闭。
inspur(config-arp-if-interface-name)#**learn-limit**	

9.验证配置结果。

命令	功能
inspur#**show arp** [<*ip-address*>| **dynamic** | **permanent** | **arp-to-static** | **ip-rang** | **vlan** | **interface**]<*interface-name*>[<*ip-address*>|[**detail**]|<*mac-address*>]| **include** | **exclude** | **begin** <*word*>	显示各类ARP条目。
inspur#**show running-config arp**	查看路由器上ARP配置信息。
inspur#**show running-config-interface** <*interface-name*>	查看路由器上指定接口下的配置信息。
inspur#**show arp statistics** <*interface-name*>	显示基于接口的报文统计计数。

10.维护ARP。

命令	功能
inspur#**debug arp** { **packets** |[**trace** { **send** | **receive**}]| **all** }{ **interface** <*interface-name*>| **source** <*ip-address*>|<*mac-address*>| **destination** <*ip-address*>|<*mac-address*>}	显示地址解析协议ARP处理收发包状态的调试信息，显示是否在发送或接收ARP报文。
inspur#**clear arp-cache** [**interface** < *interface-name*>][**ip** < *ip-address*>| **mac** < *hardware-address*>| **ip-range from** <*ip-address*> **to** <*ip-address*>]	清除动态ARP条目。
inspur#**clear arp-cache permanent** [**interface** <*interface-name*>]	按指定的范围清除永久ARP条目。
inspur#**clear arp-cache to-static** [**interface** <*interface-name*>]	按指定的范围清除静态ARP条目。
inspur#**clear arp statistics** <*interface-name*>	清除ARP报文统计计数。

3.1.2 永久 ARP 配置实例

配置说明

要在某个接口下配置永久ARP条目。

配置思路

在ARP模式下或者ARP接口模式下配置。

配置过程

方法一：在ARP模式下配置，需注意在某接口下配置永久ARP前需要该接口已经配置

了IP地址。

```
inspur(config)#arp
inspur(config-arp)#arp gei-0/1 permanent 120.1.1.1 0020.1122.3344
```

方法二：在ARP模式下进入接口模式进行配置。

```
inspur(config-arp)#interface gei-0/2
inspur(config-arp-if-gei-0/2)#arp permanent 120.1.1.3 0020.1122.3355
```

在子接口配置永久ARP，与实接口类似，唯一不同的是需要在最后加上VLAN-ID。

```
inspur(config-arp)#arp gei-0/1.1 permanent 120.1.1.5 0020.1122.3366 1
```

配置验证

用**show**命令查看配置结果。

```
inspur(config)#show arp permanent
The count is 1
IP                Hardware                Exter  Inter  Sub
Address      Age    Address        Interface    VlanID VlanID Interface
-------------------------------------------------------------------------
120.1.1.1     P      0020.1122.3344  gei-0/1     N/A    N/A    N/A

inspur(config)#show arp permanent gei-0/2
The count is 1
 IP                Hardware                Exter  Inter  Sub
Address      Age    Address        Interface    VlanID VlanID Interface
-------------------------------------------------------------------------
120.1.1.3     P      0020.1122.3355  gei-0/2     N/A    N/A    N/A

inspur(config)#show arp permanent gei-0/1.1
The count is 1
IP                Hardware                Exter  Inter  Sub
Address      Age    Address        Interface    VlanID VlanID Interface
-------------------------------------------------------------------------
120.1.1.5     P      0020.1122.3366  gei-0/1.1     1      N/A    N/A
```

3.1.3 ARP 常规属性配置实例

配置说明

要配置ARP的常规属性。

配置思路

在ARP模式下或者ARP接口模式下配置。

配置过程

配置ARP中的常用功能如下。

```
inspur(config-arp)#interface gei-0/3    /*进入某一接口*/
inspur(config-arp-if-gei-0/3)#learn-disable     /*关闭接口的ARP学习功能*/
inspur(config-arp-if-gei-0/3)#protect limit-num 10 /*设置ARP条目保护数为10条*/
```

```
inspur(config-arp-if-gei-0/3)#proxy                /*开启ARP代理功能*/
inspur(config-arp-if-gei-0/3)#purge-delay 10       /*设置延迟删除时间为10s*/
inspur(config-arp-if-gei-0/3)#no source-filtered   /*关闭源过滤功能*/
inspur(config-arp-if-gei-0/3)#timeout 10           /*设置老化时间为10s*/
```

配置验证

```
inspur(config-arp-if-gei-0/3)#show running-config arp
/*show命令查看配置结果*/
!<arp>
arp
interface gei-0/3
    timeout 10
    purge-delay 10
    protect limit-num 10
    proxy
    learn-disable
    source-filtered disable
  $
$
!</arp>
```

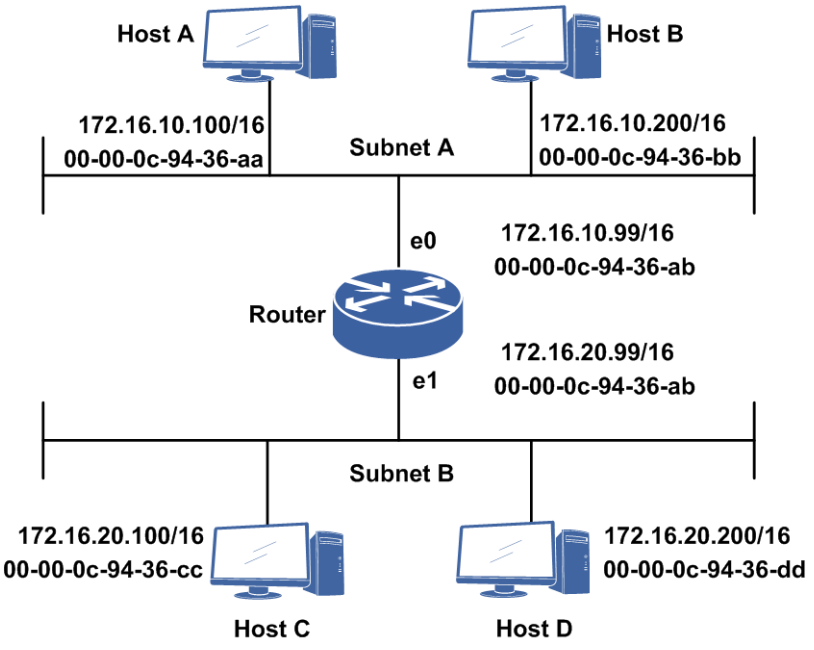
3.1.4 ARP 代理配置实例

配置说明

如*图 3-1*所示，主机A认为主机D和自己处于一个网段中（掩码判断），当主机A欲与主机D进行通信时，主机A向主机D发送ARP请求，参见下表。

MAC Addr of sender	IP of sender	Target MAC Addr	Target IP
00-00-0c-94-36-aa	172.16.10.100	00-00-00-00-00-00	172.16.20.200

图 3-1 ARP 代理应用配置实例拓扑图



该ARP请求不会到达主机D，因为通常情况下路由器不会转发广播，在没有使用ARP代理的条件下，通信就失败了。

当路由器具备ARP代理功能并打开时，会处理请求IP为路由器上除了接收端口IP外的所有有效IP地址，并用ARP报文入接口的MAC地址回应，参见下表。

MAC Addr of sender	IP of sender	Target MAC Addr	Target IP
00-00-0c-94-36-ab	172.16.20.200	00-00-0c-94-36-aa	172.16.10.100

配置思路

ARP接口模式下，配置代理功能。

配置过程

在路由器上开启ARP代理的配置如下。

```
inspur(config-arp)#interface gei-0/1
inspur(config-arp-if-gei-0/1)#proxy
inspur(config-arp-if-gei-0/1)#exit
inspur(config-arp)#exit
inspur(config)#show running-config arp
!<arp>
arp
  interface gei-0/1
    proxy
  $
$
!</arp>
```

配置验证

主机A的ARP表中新增ARP项，即在路由器上看到的。

```
inspur(config)#show arp
The count is 2
IP                  Hardware               Exter  Inter  Sub
Address       Age     Address       Interface   VlanID VlanID Interface
------------------------------------------------------------------------------
--
172.16.20.200  00:00:03 0000.0c94.36ab gei-0/1 N/A    N/A    gei-0/1
```

3.1.5 ARP 源过滤配置实例

配置说明

默认ARP源过滤开启，当ARP源过滤开启时，对于收到的ARP报文，会查找路由表，看ARP包的源IP是否有以该端口为出接口的路由，如果找到就学习，如果没有找到就丢弃。

配置思路

在ARP接口配置模式下，进行打开或者关闭源过滤功能。

配置过程

关闭源过滤配置。

```
inspur(config-arp)#interface gei-0/1
inspur(config-arp-if-gei-0/1)#source-filtered disable  /*关闭源过滤功能*/
```

打开源过滤配置。

```
inspur(config-arp)#interface gei-0/1
inspur(config-arp-if-gei-0/1)#source-filtered /*打开源过滤功能*/
```

配置验证

验证关闭源过滤配置。

```
inspur(config)#show running-config arp
!<arp>
arp
  interface gei-0/1
    source-filtered disable  /*关闭源过滤功能*/
  $
$
!</arp>
```

3.1.6 ARP 抑制配置实例

配置说明

在某个接口下配置ARP抑制，当通过该接口上发送的ARP报文数目超过**port-speed**值时，抑制生效。

配置思路

1.进入ARP配置模式。

2.在对应接口上配置port-speed。

3.配置ARP抑制的limit-time。

配置过程

方法一：在ARP模式下配置。

```
inspur(config)#arp
inspur(config-arp)#port-speed gei-0/1 50
inspur(config-arp)#limit-time gei-0/1 20
inspur(config-arp)#exit
```

方法二：在ARP模式下进入接口模式进行配置。

```
inspur(config)#arp
inspur(config-arp)#interface gei-0/1
inspur(config-arp-if-gei-0/1)#port-speed 50
inspur(config-arp-if-gei-0/1)#limit-time 20
inspur(config-arp-if)#exit
```

配置验证

查看ARP抑制配置和生效情况。

```
inspur#show running-config arp
!<arp>
arp
  interface gei-0/1
    port-speed 50
    limit-time 20
  $
$
!</arp>
```

3.2 DHCP

DHCP用于自动为网络中的客户端配置IP地址、DNS等信息。

DHCP协议支持C/S（客户端/服务器）结构，主要分为DHCP客户端（DHCP Client）、

DHCP中继（DHCP Relay）和DHCP服务器（DHCP Server）。

·DHCP Server为DHCP Client提供了分配IP地址和配置相关初始信息的功能。

·DHCP Client实现了设备动态获取IP地址的功能，主要包括：获取IP地址、掩码等信息，定时向DHCP Server续租地址，将获取的IP地址配置到对应接口上生成网段路由。

·DHCP报文采用广播方式，无法穿越多个不同的子网。如果DHCP报文需要穿越多个子网时，就需要配置DHCP Relay。

·DHCP Relay Proxy是DHCP Relay的扩展功能，直接回应用户的续租请求。从DHCP Client角度看DHCP Relay Proxy，其代理了DHCP Server的角色；在实际应用过程中又充当DHCP Client的角色，向真正的DHCP Server发送续租请求。

3.2.1 配置 DHCP Server

本节介绍DHCP Server功能的配置步骤和命令。

1.开启DHCP功能，配置接口的DHCP模式为DHCP Server。

步骤	命令	功能
1	inspur(config)#**dhcp**	进入DHCP配置模式。
2	inspur(config-dhcp)#**enable**	开启DHCP功能。
3	inspur(config-dhcp)#**interface**<*interface-name*>	进入DHCP接口配置模式。
4	inspur(config-dhcp-if-interface-name)#**mode server**	启用接口的DHCP工作模式为DHCP Server。

2.配置IP地址池。

步骤	命令	功能
1	inspur(config)#**ip pool** <*pool-name*>	配置IP地址池，进入IP地址池配置模式。
2	inspur(config-ip-pool)#**range** <*start-ip-address*><*end-ip-address*><*net-mask*>	配置IP地址池地址段范围。

3.配置DHCP Pool。

步骤	命令	功能
1	inspur(config)#**ip dhcp pool** <*dhcppool-name*>	配置DHCP Pool，进入DHCP Pool配置模式。
2	inspur(config-dhcp-pool)# **ip-pool**<*ippool-name*>	绑定指定的IP Pool到DHCP Pool。

步骤	命令	功能
3	inspur(config-dhcp-pool)#**lease-time** {[**infinite**][<*days*><*hours*><*minutes*>]}	设置DHCP服务器向客户端出租IP地址的租期，默认租期为1小时。 **infinite**表示无限长。
4	inspur(config-dhcp-pool)#**dns-server** <*ip-address*>[<*ip-address*>][<*ip-address*>][<*ip-address*>][<*ip-address*>][<*ip-address*>][<*ip-address*>][<*ip-address*>]	设置DHCP服务器返回给用户的DNS地址。
5	inspur(config-dhcp-pool)#**default-router** <*ip-address*>[<*ip-address*>][<*ip-address*>]	配置默认网关，最多可以配置8个。
6	inspur(config-dhcp-pool)#**import interface** <*interface-name*> **dns**	（可选）从动态获取的IP地址的接口中导入DNS，作为DHCP服务器的DNS地址。

4.配置DHCP Policy。

步骤	命令	功能
1	inspur(config)#**ip dhcp policy** < *policy-name*>< *priority-level*>	配置DHCP Policy，进入DHCP Policy配置模式。
2	inspur(config-dhcp-policy)#**dhcp-pool**<*dhcppool-name*>	绑定指定的DHCP Pool到DHCP Policy。
3	inspur(config-dhcp-policy)#**relay-agent** <*ip-address*>	指定relay agent地址。

5.接口绑定DHCP Policy并配置DHCP用户限额。

步骤	命令	功能
1	inspur(config-dhcp)#**interface**<*interface-name*>	进入DHCP接口配置模式。
2	inspur(config-dhcp-if-interface-name)#**policy** <*policy-name*>	接口绑定DHCP Policy。
3	inspur(config-dhcp-if-interface-name)#**user quota** <*limit-value*>	配置接口的DHCP用户限额，即接口上所允许的最大DHCP Client数目。

6.验证配置结果。

命令	功能
inspur#**show ip dhcp configuration**	显示DHCP进程模块的配置信息。
inspur#**show ip local pool**	显示配置的本地地址池信息。

命令	功能
inspur#**show ip dhcp server user** [**interface**<*interface-name*>[**total-count**]][**total-count**]	显示DHCP Server的当前在线用户信息。
inspur#**show running-config-interface** <*interface-name*>	显示接口相关的DHCP Server/Relay的配置信息。

7.维护DHCP Server。

命令	功能
inspur#**kick-off ip dhcp server user** [[**interface** <*interface-name*>][**mac** <*mac-address*>[**vrf-instance** <*vrf-name*>]][**ip** <*ip-address*>[**vrf-instance** <*vrf-name*>]]	按照指定属性（接口/MAC地址/IP地址）将Server上的在线用户下线。

3.2.2 配置 DHCP Relay

本节介绍DHCP Relay功能的配置步骤和命令。

1.开启DHCP功能。

步骤	命令	功能
1	inspur(config)#**dhcp**	进入DHCP配置模式。
2	inspur(config-dhcp)#**enable**	开启DHCP功能。

2.配置DHCP Relay参数。

步骤	命令	功能
1	inspur(config-dhcp)#**relay option82 format** {**china-tel** | **dsl-forum** | **user-configuration** | **telenor**}	配置DHCP进程在进行Relay转发时插入的82选项的格式。
2	inspur(config-dhcp)#**relay option82 option**	配置DHCP进程在进行Relay转发时插入82选项。
3	inspur(config-dhcp)#**relay option82 policy**{**add**| **keep** | **replace**}	配置当DHCP进程处理的Relay转发数据包已插入了82选项，而本地又配置需要插入82选项时，DHCP进程的处理策略。
4	inspur(config-dhcp)#**relay option82 uniform circuit-id** <*circuit-id string* >	配置基于统一模式的DHCP OPT82 circuit-id子选项内容。
5	inspur(config-dhcp)#**relay option82 uniform remote-id** <*remote-id string* >	配置基于统一模式的DHCP OPT82 remote-id子选项内容。
6	inspur(config-dhcp)#**relay option82**	配置基于统一模式的DHCP

步骤	命令	功能
	user-configuration policy { **uniform** | **interface** }	OPT82 用户配置选择策略，在选择agent-format 为 user-configuration （即用户配置模式之后），再用本命令选择用户配置模式的选择策略{uniform/interface}。
7	`inspur(config-dhcp)#`**relay max-user**	配置Relay的最大用户数。
8	`inspur(config-dhcp)#`**relay update arp**	打开Relay ARP开关。

china-tel：中国电信的82选项格式。

dsl-forum：DSL论坛的82选项格式 。

user-configuration：用户可配置模式的82选项格式。

telenor：telenor 82选项格式，在中国电信格式基础上，增加了remote-id字段。

keep：保持原有的82选项，并进行透传 。

replace：替换原有的82选项。

add：添加Relay的82选项。

3.配置DHCP Relay server group。

步骤	命令	功能
1	`inspur(config)#`**ip dhcp relay server group** *<group-number>*	进入DHCP Relay server group配置模式。
2	`inspur(config-dhcpr-server-group)#`**algorithm** {**first** | **round-robin** | **forward-all**}	配置DHCP Relay server group的选Server的算法策略。
3	`inspur(config-dhcpr-server-group)#`**server** *<server-number><ip-address>*{**security** | **standard**}[**master**][**dscp**]	配置该DHCP Relay server group的Server。
4	`inspur(config-dhcpr-server-group)#`**max-retry** *<retry-times>*	配置DHCP Relay向外部DHCP Server申请地址时发起重试的次数。

first：主备方式选择服务器。

round-robin：负载均衡方式选择服务器。

forward-all：全转发方式，向Server Group下绑定的所有server转发请求报文。

*<server-number>*为服务器的编号，一个Relay Server Group最多可绑定8个服务器，根据algorithm选择服务器，转发用户请求报文，范围：1~8。

security：服务器的工作模式是安全模式。

standard：服务器的工作模式是标准模式。

master：该服务器是否是主服务器，只有algorithm为**first**时，该参数才生效。

4.配置接口下绑定DHCP Relay server group组号。

步骤	命令	功能
1	inspur(config-dhcp)#**interface**<*interface-name*>	进入DHCP接口配置模式。
2	inspur(config-dhcp-if-interface-name)# **relay agent** <*ip-address*>	在连接客户机子网的接口上配置DHCP代理IP地址。
3	inspur(config-dhcp-if-interface-name)# **relay server group** <*group-number*>	接口下绑定DHCP Relay server group组号。
4	inspur(config-dhcp-if-interface-name)# **relay option82 circuit-id** <*circuit-id string* >	配置基于三层接口的DHCP OPT82 circuit-id子选项内容。
5	inspur(config-dhcp-if-interface-name)# **relay option82 remote-id** <*remote-id string* >	配置基于三层接口的DHCP OPT82 remote-id子选项内容。

5.验证配置结果。

命令	功能
inspur#**show ip dhcp configure**	显示DHCP进程模块的配置信息。
inspur#**show ip dhcp relay user** [**interface**<*interface-name*>[**total-count**]][[**total-count**]	显示DHCP Relay的当前在线用户信息。
inspur# **show running-config-interface** <*interface-name*>	显示接口相关的DHCP Server/Relay的配置信息。

6.维护DHCP Relay。

命令	功能
inspur#**kick-off ip dhcp relay user** [[**interface** <*interface-name*>]|[**mac** <*mac-address*>[**vrf-instance** <*vrf-name*>]]|[**ip** <*ip-address*>[**vrf-instance** <*vrf-name*>]]]	按照指定属性（接口/MAC地址/IP地址）将Relay上的在线用户下线。

3.2.3 配置 DHCP Proxy

本节介绍DHCP Proxy功能的配置步骤和命令。

1.开启DHCP功能，配置接口的DHCP模式为DHCP Proxy。

步骤	命令	功能
1	inspur(config)#**dhcp**	进入DHCP配置模式。

步骤	命令	功能
2	inspur(config-dhcp)#**enable**	开启DHCP功能。
3	inspur(config-dhcp)#**interface**<*interface-name*>	进入DHCP接口配置模式。
4	inspur(config-dhcp-if-interface-name)#**mode proxy**	启用接口的DHCP工作模式为DHCP Proxy。
5	inspur(config-dhcp-if-interface-name)#**relay agent** <*ip-address*>	在连接客户机子网的接口上配置DHCP代理IP地址。

2.配置DHCP Relay参数。

步骤	命令	功能
1	inspur(config-dhcp)#**relay option82 format** {**china-tel** | **dsl-forum** | **user-configuration** | **telenor**}	配置DHCP进程在进行Relay转发时插入的82选项的格式。
2	inspur(config-dhcp)#**relay option82 option**	配置DHCP进程在进行Relay转发时插入82选项。
3	inspur(config-dhcp)#**relay option82 policy**{**add**| **keep** | **replace**}	配置当DHCP进程处理的Relay转发数据包已插入了82选项，而本地又配置需要插入82选项时，DHCP进程的处理策略。
4	inspur(config-dhcp)#**relay option82 uniform circuit-id** <*circuit-id string* >	配置基于统一模式的DHCP OPT82 circuit-id子选项内容。
5	inspur(config-dhcp)#**relay option82 uniform remote-id** <*remote-id string* >	配置基于统一模式的DHCP OPT82 remote-id子选项内容。
6	inspur(config-dhcp)#**relay option82 user-configuration policy** { **uniform** | **interface** }	配置基于统一模式的DHCP OPT82 用户配置选择策略，在选择**agent-format**为**user-configuration**（即用户配置模式之后），再用本命令选择用户配置模式的选择策略。

china-tel：中国电信的82选项格式 。

dsl-forum：DSL论坛的82选项格式 。

user-configuration：用户可配置模式的82选项格式。

telenor：telenor 82选项格式，在中国电信格式基础上，增加了remote-id字段。

keep：保持原有的82选项，并进行透传 。

replace：替换原有的82选项。

add：添加Relay的82选项。

uniform：选择统一模式下配置的option 82字符串内容插入DHCP报文。

interface：选择接口下配置的option 82字符串内容插入DHCP报文。

3.配置DHCP Relay server group。

步骤	命令	功能
1	inspur(config)#**ip dhcp relay server group** <*group-number*>	配置接口的外部DHCP Server所在的组，进入DHCP Relay server group配置模式。
2	inspur(config-dhcpr-server-group)#**server** <*server-number*><*ip-address*>{**security** | **standard**}[**master**][**dscp**]	配置该DHCP Relay server group的Server。
3	inspur(config-dhcpr-server-group)#**max-retry** <*retry-times*>	配置DHCP Relay向外部DHCP Server申请地址时发起重试的次数。

4.配置接口下绑定DHCP Relay server group组号。

步骤	命令	功能
1	inspur(config-dhcp)#**interface**<*interface-name*>	进入DHCP接口配置模式。
2	inspur(config-dhcp-if-interface-name)#**relay server group** <*group-number*>	接口下绑定DHCP Relay server group组号
3	inspur(config-dhcp-if-interface-name)# **relay option82 circuit-id** <*circuit-id string* >	配置基于接口的DHCP OPT82 circuit-id子选项内容。
4	inspur(config-dhcp-if-interface-name)# **relay option82 remote-id** <*remote-id string* >	配置基于接口的DHCP OPT82 remote-id子选项内容。

5.验证配置结果。

命令	功能
inspur#**show ip dhcp configure**	显示DHCP进程模块的配置信息。
inspur#**show ip dhcp relay user** [**interface**<*interface-name*>[**total-count**]][**total-count**]	显示DHCP Relay的当前在线用户信息。
inspur#**show running-config-interface dhcp** [<*interface-name*>]	显示接口相关的DHCP Server/Relay的配置信息。

6.维护DHCP Proxy。

命令	功能
inspur#**kick-off ip dhcp relay user** [[**interface** <*interface-name*>]|[**mac** <*mac-address*>[**vrf-instance** <*vrf-name*>]]|[**ip** <*ip-address*>[**vrf-instance** <*vrf-name*>]]]	按照指定属性（接口/MAC地址/IP地址）将Relay上的在线用户下线。

3.2.4 配置 DHCP Client

本节介绍DHCP Client的配置步骤和命令。

1.开启DHCP功能，添加DHCP Client策略。

步骤	命令	功能
1	inspur(config)#**dhcp**	进入DHCP配置模式。
2	inspur(config-dhcp)#**enable**	开启DHCP功能。
3	inspur(config-dhcp)#**client policy** <*name*>	添加DHCP Client策略。
4	inspur(config-dhcp-client-policy)#**unicast**	配置单播功能。配置该单播功能后，DHCP Server回应的Offer报文和ACK报文都是以单播的方式发送，否则服务器是以默认的广播方式发送Offer报文和ACK报文。
5	inspur(config-dhcp-client-policy)#**request**{<*classless-static-route*>|<*domain-name*>|<*domain-name-server*>|< *tftp-server-address*>|< *tftp-server-name* >}	设置DHCP Client报文中携带的请求选项。

<*classless-static-route*>：请求无类静态路由。

<*classless-static-route*>：请求DNS地址。

<*classless-static-route*>：请求域名。

<*tftp-server-address*>：请求TFTP Server的地址。

<*tftp-server-name*>：请求TFTP Server的名称。

2.配置DHCP Client接口。

步骤	命令	功能
1	inspur(config-dhcp)#**interface** <*interface-name*>	添加需要获取IP地址的接口。
2	inspur(config-dhcp-interface-name)#**mode client**	设置接口的DHCP工作模式为DHCP Client。
3	inspur(config-dhcp-interface-name)#**client policy** <*name*>	接口绑定已配置的DHCP Client策略。
4	inspur(config-dhcp-interface-name)#**client start**	开始发送DHCP协议报文。
5	inspur(config-dhcp-interface-name)#**client stop**	（可选）关闭该接口的DHCP Client功能。

3.验证配置结果。

命令	功能
inspur#**show ip dhcp configuration**	显示DHCP进程模块的配置信息。
inspur#**show ip interface**<*interface-name*>	显示接口相关的DHCP信息。

3.2.5 配置限制 Relay 发包

DHCP Relay设备上对于是否向Server发送Release包实现可控制，这样易于人为控制设备发包。

1.限制Relay发包。

DHCP Relay设备上添加限制向Server发送Release包的命令，用来控制DHCP Relay设备是否向Server发送Release包。

步骤	命令	功能
1	inspur(config)#**dhcp**	进入DHCP配置模式。
2	inspur(config-dhcp)#**relay forbid send release**	打开Relay限制向Server发Release包的命令。

2.验证配置结果。

命令	功能
inspur#**show running-config dhcp**	显示DHCP的相关配置。

3.2.6 配置 Option82 改写功能

本节介绍option82改写功能的配置步骤和命令。

相关信息

BRAS设备在获取接入节点设备（如DSLAM）的接入线路信息后，根据BRAS的配置可透传接入线路信息，也可修改添加接入线路信息中与BRAS设备的相关的线路信息，形成完整的接入线路信息，如“eth 31/31/7:4096.1234 guangzhou001/0/31/63/31/127”。

DHCP Relay设备添加option82的策略选项add。当option82策略为add时，DHCP Relay设备收到的option82选项中保持接入节点设备（如DSLAM）的接入线路信息不变，修改添加接入线路信息中与BRAS设备的相关的线路信息，形成完整的接入线路信息。

1.配置option82改写。

步骤	命令	功能
1	inspur(config)#**dhcp**	进入DHCP配置模式。
2	inspur(config-dhcp)#**relay option82 policy {keep|replace|add}**	配置option82的策略。

2.验证配置结果。

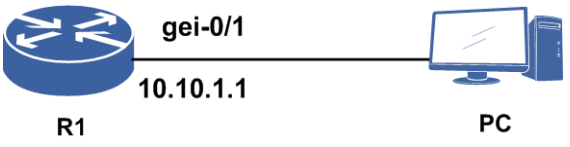
命令	功能
inspur#**show running-config dhcp**	显示DHCP的相关配置。

3.2.7 DHCP Server 配置实例

配置说明

如*图 3-2*所示，R1作为DHCP Server使用，同时充当默认网关，PC通过DHCP动态获取IP地址接入网络。

图 3-2 DHCP Server 配置实例拓扑图



R1全局下需要配置：IP Pool、DHCP Pool、DHCP Policy、开启DHCP功能。R1接口下需要配置：IP地址、DHCP Server模式、绑定DHCP Policy。

配置思路

1.配置IP Pool，IP Pool配置的是地址池范围等相关选项，地址池的范围要限制在一个网段内。

2.配置DHCP Pool，DHCP Pool需要绑定一个IP Pool，管理DNS、lease-time、default router等设置。

3.配置DHCP Policy，DHCP Policy是策略选项，同一个名字下支持多个优先级别，用于策略管理。

4.配置DHCP Server，在DHCP接口模式下配置为Server功能模式，并绑定配置的Policy。

5.配置全局开启DHCP功能。

配置过程

在R1上的配置如下。

```
/*配置接口的IP地址。*/
R1(config)#interface gei-0/1
R1(config-if-gei-0/1)#ip address 10.10.1.1 255.255.255.0
R1(config-if-gei-0/1)#no shutdown
R1(config-if-gei-0/1)#exit
/*配置IP POOL。*/
R1(config)#ip pool pool1
R1(config-ip-pool)#range 10.10.1.3 10.10.1.254 255.255.255.0
R1(config-ip-pool)#exit
/*将IP POOL和DHCP POOL绑定。*/
R1(config)#ip dhcp pool pool1
R1(config-dhcp-pool)#ip-pool pool1
R1(config-dhcp-pool)#dns-server 10.10.1.1
R1(config-dhcp-pool)#default-router 10.10.1.1
R1(config-dhcp-pool)#exit
/*将DHCP POOL和DHCP POLICY绑定。*/
R1(config)#ip dhcp policy policy1 1
R1(config-dhcp-policy)#dhcp-pool pool1
R1(config-dhcp-policy)#exit
/*开启DHCP功能。*/
R1(config)#dhcp
R1(config-dhcp)#enable
/*接口下配置SERVER模式以及选定POLICY。*/
R1(config-dhcp)#interface gei-0/1
R1(config-dhcp-if-gei-0/1)#mode server
R1(config-dhcp-if-gei-0/1)#policy policy1
R1(config-dhcp-if-gei-0/1)#exit
R1(config-dhcp)#exit
```

配置验证

在R1上查看IP POOL的配置。

```
R1(config)#show ip local pool
PoolName      Begin          End            Mask   Free      Used
Pool1        10.10.1.3      10.10.1.254     24     252       1
TotalPool: 1
```

在R1上查看DHCP Policy的配置。

```
R1(config)#show ip dhcp  policy
PolicyName  Priority  DhcpPool    RelayAgent   Vrf-instance  Option60
policy1       1       pool1
Total: 1
```

在R1上显示DHCP的配置。

```
R1(config)#show running-config dhcp
!<dhcp>
ip dhcp pool pool1
  dns-server 10.10.1.1
  default-router 10.10.1.1
  ip-pool pool1
$
ip dhcp policy policy1 1
  dhcp-pool pool1
$
dhcp
  enable
  interface gei-0/1
    mode server
```

```
    policy policy1
  $
$
!</dhcp>
```

PC申请地址，Server能分配IP地址。在R1上可以查看到。

```
R1#show ip dhcp server user
CLIENT MAC addr: 0000.6501.0102
  IP addr: 10.10.1.3
  State: BOUND
  Expiration: 09:32:35  06/12/2012
  Interface: gei-0/1
  VRF: 25
  SlotNo: 1
```

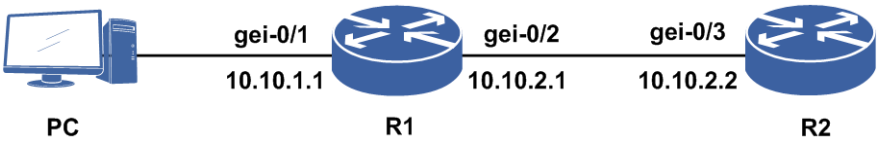
3.2.8 DHCP Relay 配置实例

配置说明

当DHCP客户机和服务器不在同一网络中时，需要直连用户端的路由器充当DHCP中继。

如*图 3-3*所示，启用DHCP中继功能，由一台单独的服务器10.10.2.2提供DHCP服务器的功能。在需要DHCP服务的主机比较多的情况下通常采用这种做法。

图 3-3 DHCP Relay 配置实例拓扑图



R1接口下需要配置：IP地址，DHCP Server地址，DHCP Relay模式。R2接口下需要配置：IP地址，绑定DHCP Policy，DHCP Server模式。R2全局下需要配置：开启DHCP功能，IP Pool，DHCP Pool，DHCP Policy，指向R1接口网段的路由。

配置思路

1.Server一定要有Relay接口地址的路由（测试的时候可以配置全局静态路由）。

2.Server的配置参见上节说明，配置Policy时需要配置Relay Agent为Relay接口的地址。

3.Relay主要在DHCP接口下配置相关参数，Relay接口地址应与Server对应的IP Pool内地址在同一网关内。

4.DHCP Relay配置：配置Relay模式，在DHCP接口模式下配置Relay功能，并配置其Relay Agent为Relay接口的地址，Relay Server为配置的Server的地址。这里Server接口的地址和Relay接口的地址不在同一个网段，分配的IP Pool和Relay接口的地址是同一网段。

配置过程

R1上的配置如下。

```
/*配置Relay接口。*/
R1(config)#interface gei-0/1
R1(config-if-gei-0/1)#ip address 10.10.1.1 255.255.255.0
R1(config-if-gei-0/1)#no shutdown
R1(config-if-gei-0/1)#exit
/*其他接口地址配置类似，省略。*/
/*指定Server。*/
R1(config)#ip dhcp relay server group 1
R1(config-dhcpr-server-group)#server 1 10.10.2.2 standard master
R1(config-dhcpr-server-group)#exit
/*开启DHCP功能。*/
R1(config)#dhcp
R1(config-dhcp)#enable
/*配置接口的DHCP模式和其他属性。*/
R1(config-dhcp)#interface gei-0/1
R1(config-dhcp-if-gei-0/1)#mode relay
R1(config-dhcp-if-gei-0/1)#relay agent 10.10.1.1
R1(config-dhcp-if-gei-0/1)#relay server group 1
R1(config-dhcp-if-gei-0/1)#exit
R1(config-dhcp)#exit
```

R2上的配置如下。

```
/*开启DHCP功能。*/
R2(config)#dhcp
R2(config-dhcp)#enable
R2(config-dhcp)#exit
R2(config)#interface gei-0/3
R2(config-if-gei-0/3)#ip address 10.10.2.2 255.255.255.0
R2(config-if-gei-0/3)#no shutdown
R2(config-if-gei-0/3)#exit
/*配置IP POOl。*/
R2(config)#ip pool pool1
R2(config-ip-pool)#range 10.10.1.3 10.10.1.254 255.255.255.0
R2(config-ip-pool)#exit
/*将IP POOL和DHCP POOL绑定。*/
R2(config)#ip dhcp pool pool1
R2(config-dhcp-pool)#ip-pool pool1
R2(config-dhcp-pool)#default-router 10.10.1.1
R2(config-dhcp-pool)#exit
/*将DHCP POOL和DHCP POLICY绑定。*/
R2(config)#ip dhcp policy policy1 1
R2(config-dhcp-policy)#dhcp-pool pool1
R2(config-dhcp-policy)#relay-agent 10.10.1.1
R2(config-dhcp-policy)#exit
R2(config)#dhcp
/*配置接口的DHCP模式。*/
R2(config-dhcp)#interface gei-0/3
R2(config-dhcp-if-gei-0/3)#mode server
R2(config-dhcp-if-gei-0/3)#policy policy1
R2(config-dhcp-if-gei-0/3)#exit
R2(config-dhcp)#exit
R2(config)#ip route 10.10.1.0 255.255.255.0 10.10.2.1
```

配置验证

在R2上显示IP POOL的配置。

```
R2(config)#show ip local pool
PoolName     Begin        End            Mask     Free    Used
```

```
pool1       10.10.1.3     10.10.1.254     24        252     0
Total:1
```

在R2上显示DHCP POOL的配置。

```
R2(config)#show ip dhcp pool
PoolName IpPool  LeaseTime  DnsNum RouterNum OptionNum BindNum
policy1     pool1   0  1  0        0      1        0        0
Total: 1
```

在R2上显示DHCP Policy的配置。

```
R2(config)#show ip dhcp  policy
PolicyName  Priority  DhcpPool   RelayAgent     Vrf-instance   Option60
pool1           1    pool1      10.10.1.1
Total: 1
```

在R2上显示DHCP的配置。

```
R2(config)#show running-config dhcp
!<dhcp>
ip dhcp pool pool1
  ip-pool pool1
  default-router 10.10.1.1
$
ip dhcp policy policy1 1
  dhcp-pool pool1
  relay-agent 10.10.1.1
$
dhcp
  enable
  interface gei-0/3
    mode server
    policy policy1
  $
$
!</dhcp>
```

在R1上显示指定接口下的DHCP配置。

```
R1#show running-config-interface gei-0/1
!<if-intf>
interface gei-0/1
  ip address 10.10.1.1 255.255.255.0
  no shutdown
$
!</if-intf>
!<dhcp>
dhcp
  interface gei-0/1
    mode relay
    policy policy1
    relay server group 1
    relay agent 10.10.1.1
  $
$
!</dhcp>
```

3.2.9 DHCP Proxy 配置实例

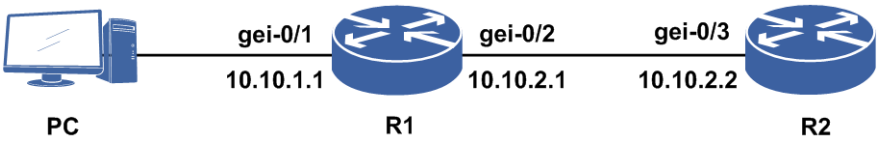
配置说明

当DHCP客户机和服务器不在同一网络中时，需要直连用户端的路由器充当DHCP代理。

如*图 3-4*所示，启用DHCP代理功能，由一台单独的服务器10.10.2.2提供DHCP服务器

的功能。

图 3-4 DHCP Proxy 配置实例拓扑图



R1接口下需要配置：IP地址，DHCP Server地址，DHCP Proxy模式。R2接口下需要配置：IP地址，绑定DHCP Policy，DHCP Server模式。R2全局下需要配置：开启DHCP功能，IP Pool，DHCP Pool，DHCP Policy，指向R1 Proxy接口网段的路由。

配置思路

1.Proxy主要在DHCP接口下配置相关参数，Proxy接口地址应与Server对应的IP Pool内地址在同一网关内。

2.DHCP Proxy配置：配置Proxy模式，并配置其relay agent为Proxy接口的地址，Relay Server为配置的Server的地址。这里Server接口的地址和Proxy接口的地址不在同一个网段，分配的IP Pool和Proxy接口的地址是同一网段。

3.Server一定要有Proxy接口地址的路由。

4.Server的配置：配置Policy时需要配置relay agent为Proxy接口的地址。

配置过程

R1上的配置如下。

```
/*配置Proxy接口。*/
R1(config)#interface gei-0/1
R1(config-if-gei-0/1)#ip address 10.10.1.1 255.255.255.0
R1(config-if-gei-0/1)#no shutdown
R1(config-if-gei-0/1)#exit
/*其他接口地址配置类似，省略。*/
/*指定Server。*/
R1(config)#ip dhcp relay server group 1
R1(config-dhcpr-server-group)#server 1 10.10.2.2 standard master
R1(config-dhcpr-server-group)#exit
/*开启DHCP功能。*/
R1(config)#dhcp
R1(config-dhcp)#enable
/*配置接口的DHCP模式和其他属性。*/
R1(config-dhcp)#interface gei-0/1
R1(config-dhcp-if-gei-0/1)#mode proxy
R1(config-dhcp-if-gei-0/1)#relay agent 10.10.1.1
R1(config-dhcp-if-gei-0/1)#relay server group 1
R1(config-dhcp-if-gei-0/1)#exit
R1(config-dhcp)#exit
```

R2上的配置如下。

```
/*开启DHCP功能。*/
R2(config)#dhcp
R2(config-dhcp)#enable
R2(config-dhcp)#exit
```

```
R2(config)#interface gei-0/3
R2(config-if-gei-0/3)#ip address 10.10.2.2 255.255.255.0
R2(config-if-gei-0/3)#no shutdown
R2(config-if-gei-0/3)#exit
/*配置IP POOL。*/
R2(config)#ip pool pool1
R2(config-ip-pool)#range 10.10.1.3 10.10.1.254 255.255.255.0
R2(config-ip-pool)#exit
/*将IP POOL和DHCP POOL绑定。*/
R2(config)#ip dhcp pool pool1
R2(config-dhcp-pool)#ip-pool pool1
R2(config-dhcp-pool)default-router 10.10.1.1
R2(config-dhcp-pool)#exit
/*将DHCP POOL和DHCP POLICY绑定。*/
R2(config)#ip dhcp policy policy1 1
R2(config-dhcp-policy)#dhcp-pool pool1
R2(config-dhcp-policy)#relay agent 10.10.1.1
R2(config-dhcp-policy)#exit
R2(config)#dhcp
/*配置接口的DHCP模式。*/
R2(config-dhcp)#interface gei-0/3
R2(config-dhcp-if-gei-0/3)#mode server
R2(config-dhcp-if-gei-0/3)#policy policy1
R2(config-dhcp-if-gei-0/3)#exit
R2(config-dhcp)#exit
R2(config)#ip route 10.10.1.0 255.255.255.0 10.10.2.1
```

配置验证

在R2上显示DHCP Policy的配置。

```
R2(config)#show ip dhcp  policy
PolicyName    Priority  DhcpPool     RelayAgent   Vrf-instance   Option60
policy1       1         pool1        10.10.1.1
Total: 1
```

在R1上显示指定接口下的DHCP配置。

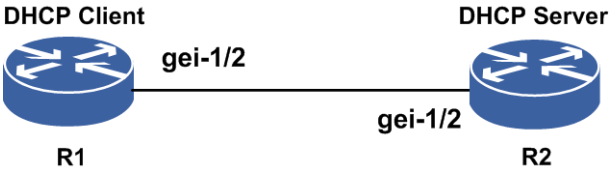
```
R1#show running-config-interface gei-0/1
!<if-intf>
interface gei-0/1
  ip address 10.10.1.1 255.255.255.0
  no shutdown
$
!</if-intf>
!<dhcp>
dhcp
  interface gei-0/1
    mode proxy
    relay server group 1
    relay agent 10.10.1.1
  $
$
!</dhcp>
```

3.2.10 DHCP Client 配置实例

配置说明

如*图 3-5*所示，R2作为DHCP Server使用，同时充当默认网关，R1通过DHCP动态获取IP地址接入网络。

图 3-5 DHCP Client 配置实例拓扑图



配置思路

1.在R1上开启DHCP Client功能。

2.在R2上配置DHCP Server。

配置过程

在R1上的配置如下。

```
R1(config)#dhcp
R1(config-dhcp)#enable
R1(config-dhcp)#interface gei-1/2
R1(config-dhcp-if-gei-1/2)#mode client
R1(config-dhcp-if-gei-1/2)#client start
R1(config-dhcp-if-gei-1/2)#exit
```

在R2上的配置如下。

```
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 191.1.1.200 255.255.255.0
R2(config-if-gei-1/2)#exit

R2(config)#ip pool Inspur
R2(config-ip-pool)#range 191.1.1.1 191.1.1.100 255.255.255.0
R2(config-ip-pool)#exit
R2(config)#ip dhcp pool Inspur
R2(config-dhcp-pool)#ip-pool Inspur
R2(config-dhcp-pool)#lease-time 0 1 0
R2(config-dhcp-pool)#exit
R2(config)#ip dhcp policy Inspur 1
R2(config-dhcp-policy)#dhcp-pool Inspur
R2(config-dhcp-policy)#exit

R2(config)#dhcp
R2(config-dhcp)#enable
R2(config-dhcp)#interface gei-1/2
R2(config-dhcp-if-gei-1/2)#mode server
R2(config-dhcp-if-gei-1/2)#policy Inspur
R2(config-dhcp-if-gei-1/2)#exit
```

配置验证

在R1上查看接口相关DHCP信息。

```
R1#show ip interface gei-1/2
gei-1/2 AdminStatus is up, PhyStatus is up, line protocol is up
  Internet address is 191.1.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by DHCP
  IP MTU 1500 bytes
```

如上所示，如果已经有IP地址，并且显示地址由DHCP分配的，说明该接口上的DHCP Client功能已经实现。

3.3 TCPv4 与 UDPv4

TCPv4是一种面向连接的全双工数据传输控制协议，为网络上的数据传输提供了可靠的保证。

UDPv4是用户数据报协议，是一种简单的面向无连接的数据报传输协议。相对于TCPv4，UDPv4传输机制具有不可靠性，其把应用程序传给IP层的数据发送出去，但是并不保证能到达目的地，而且其重传与纠错等动作执行与否要取决于上层应用。

3.3.1 配置 TCPv4

本节介绍TCPv4的配置步骤和命令。

1.配置全局TCPv4属性。

命令	功能
inspur(config)#**ip tcp synwait-time** <*seconds*>	设置等待试探建立一个TCP连接的时长，对以后建立的TCP连接起作用，单位：秒，范围30~80，缺省值为30秒。
inspur(config)#**ip tcp window-size** <*seconds*>	设置TCP侦听方窗口大小，对当前已经建立的TCP连接无效，单位：秒，范围100~65535，缺省值为32768字节。
inspur(config)#**ip tcp finwait-time** <*seconds*>	设置等待关闭一个TCP连接的时长，单位：秒，范围100~600，缺省值为150秒。
inspur(config)#**ip tcp mss** <*bytes*>	配置TCP报文发送最大分片大小，单位字节，范围68~10000，默认为该功能不开启。
inspur(config)#**ip tcp synflood-protect enable**	开启TCP防护功能，默认为不开启。
inspur(config)#**ip tcp synflood-protect defence** {<*defence-parameter-0*> **waittime** <*wait-time*> **num** <*half-connect-numbers*>|<*defence-parameter-1*> **num** <*half-connect-numbers*>|<*defence-parameter-2*> **waittime** <*wait-time*>}	配置防护的策略以及SYN等待超时时间以及半连接老化个数。在tcpsynflood防护功能打开的情况下，默认配置为防护策略类型是：减少SYN等待超时时间的同时还删除旧的半连接，SYN等待超时时间为30秒，半连接老化数为1。
inspur(config)#**ip tcp synflood-protect max-connect** {[**high** <*high-limit*>],[**low** <*low-limit*>]}	配置系统的总连接数门限值。 <*high-limit*> 数字常量，范围1~100，缺省值为90。

命令	功能
	<*low-limit*>数字常量，范围1~100，缺省值为60。
inspur(config)#**ip tcp synflood-protect one-minute** {[**high** <*high-limit*>],[**low** <*low-limit*>]}	配置系统一分钟内的总连接数门限值。 <*high-limit*> 数字常量，范围1~100，缺省值为80。 <*low-limit*>数字常量，范围1~100，缺省值为50。

2.配置接口转发时调整TCP-MSS的取值。

命令	功能
inspur(config)#**interface** <*interface-name*>	进入接口配置模式。
inspur(config-if-interface-name)#**ip tcp adjust-mss** <*max-segment-size*>	接口上配置转发时调整TCP-MSS的取值，取值范围500~1460，单位：字节。默认为不开启该功能。

3.查看TCP工作状态。

命令	功能
inspur#**show tcp**	显示所有TCP连接的相关参数。
inspur#**show tcp brief**	显示所有TCP连接的简要信息。
inspur#**show tcp config**	显示TCP配置参数信息。
inspur#**show tcp statistics**	显示TCP层的统计参数。
inspur#**show tcp tcb** <*tcb-index*>	显示指定TCB对应连接的相关参数。
inspur#**show tcp synflood-protect config**	显示系统的**tcp synflood-protect**配置信息。
inspur#**show tcp synflood-protect statistics**	显示系统的**tcp synflood-protect**统计信息。
inspur#**show tcp synflood-protect all**	显示系统的**tcp synflood-protect**所有信息。
inspur#**show debug tcp**	显示已经开启的TCP协议debug功能。

4.维护TCPv4。

命令	功能
inspur#**clear tcp connect** {<*local-ip-address*>|**mng** <*local-ip-address*>|**vrf** <*vrf-name*><*local-ip-address*>}<*local-port*><*remote-ip-address*><*remote-port*>	清除TCP连接。

命令	功能
inspur#**clear tcp statistics**	清除TCP统计信息。
inspur#**clear tcp tcb** *<tcb-index>*	清除TCP控制块信息，控制块号范围0~4294967295。
inspur#**debug ip tcp driver**	设置建立、关闭TCP连接相关信息的调试开关。 使用**no**命令关闭开关后，不再输出信息。
inspur#**debug ip tcp driver-pak**	设置TCP缓冲区管理信息的调试开关。 使用**no**命令关闭开关后，不再输出信息。
inspur#**debug ip tcp packet** [{[**address** *<ip address>*],[**port** *<port number>*],[{**out**|**in**}],[**detail**]}]	设置TCP发送、接收包的源、目的等信息的调试开关，可以指定源IP地址、目的IP地址或者端口号以及收包发包和详细信息进行打印。 使用**no**命令关闭开关后，不再输出信息。
inspur#**debug ip tcp transactions**	设置TCP状态迁移等信息的调试开关。 使用**no**命令关闭开关后，不再输出信息。
inspur#**debug ip tcp all**	打开TCP模块所有的调试开关。

3.3.2 维护 UDPv4

IR12000提供如下命令维护UDPv4。

命令	功能
inspur#**show debug udp**	显示已经打开的关于UDP的debug开关。
inspur#**debug ip udp**	设置UDP发送、接收包的源和目的信息等的调试开关。

3.4 DNS

DNS是一种应用于TCP/IP应用程序的分布式数据库，提供域名与IP地址之间的转换。通过DNS，用户进行某些应用时，可以直接使用便于记忆的、有意义的域名，由网络中的域名解析服务器解析为正确的IP地址。

IR12000支持静态域名解析和动态域名解析的客户端功能。

·静态域名解析是指手工建立域名和IP地址之间的对应关系。

·IR12000可以将自己作为DNS客户端，向DNS服务器发送DNS解析请求和接收DNS服务器响应报文。

3.4.1 配置 DNS

本节介绍DNS功能的配置步骤和命令。

1.配置动态域名解析。

步骤	命令	功能
1	inspur(config)#**ip domain name-server ipv4-address** *<ipv4-address>*	配置域名服务器的IP地址，必选，缺省情况下，没有配置域名服务器。
2	inspur(config)#**ip domain name** *<domain>*	配置域名后缀，可选，缺省情况下，没有配置域名后缀，最长为80个字符。
3	inspur(config)#**ip domain retry** *<times>*	配置DNS重传次数，可选，缺省情况下，为3次。
	inspur(config)#**ip domain timeout** *<second>*	DNS传输的超时时间，可选，缺省情况下，为3秒。
4	inspur(config)#**ip domain flush-cache**	清除DNS动态域名缓存信息。
5	inspur(config)#**ip domain resolve-type dynamic**	配置DNS解析类型。

2.配置静态域名解析。

步骤	命令	功能
1	inspur(config)#**ip domain lookup**	启动域名解析功能。
2	inspur(config)#**ip domain resolve-type static**	配置DNS解析类型。
3	inspur(config)#**ip domain hostname** *<host-name>* **ipv4-address** *<ipv4-address>*	配置域名与地址对应关系，最多可配置10条记录。

3.验证配置结果。

命令	功能
inspur#**show ip domain**	显示DNS缓存信息。
inspur#**show ip host**	查看静态域名解析表。

4.维护DNS。

命令	功能

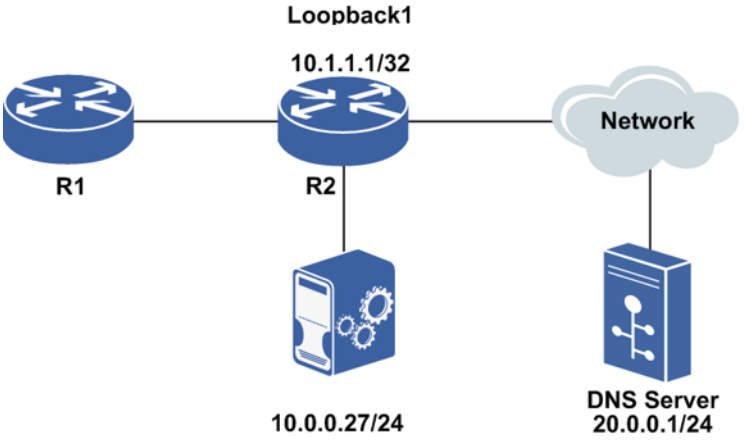
命令	功能
inspur#**debug ip domain**	打开debug开关，查看解析过程。
inspur#**show debug dns**	显示已开启的DNS协议debug开关。

3.4.2 DNS 配置实例

配置说明

如*图 3-6*所示，通过配置相关命令，使得R1（IR12000）作为DNS Client，通过DNS Server进行域名解析，能够使用域名（b.inspur.com.cn）访问IP地址为10.0.0.27/24的主机，并且使用域名管理（a.inspur.com.cn）R2。

图 3-6 DNS 配置组网图



配置思路

1.开启DNS域名解析功能。

2.配置DNS服务器的IP地址。

3.配置DNS域名后缀。

配置过程

IR12000上的配置如下。

```
R1(config)#ip domain lookup
R1(config)#ip domain name-server ipv4-address 20.0.0.1
R1(config)#ip domain name inspur.com.cn
```

配置验证

查看IR12000上的配置如下。

```
R1(config)#show running-config dns
!<dns>
ip domain lookup
ip domain name inspur.com.cn
ip domain name-server ipv4-address 20.0.0.1
!</dns>
```

从IR12000上PING域名b.Inspur.com.cn，触发DNS解析，完成后进行PING操作。

```
R1#ping b
Translating "b".succeed!
sending 5,100-byte ICMP echoes to 10.0.0.27,timeout is 2 seconds.
!!!!!
```

从IR12000上telnet域名a.Inspur.com.cn，触发DNS解析，完成后TELNET到R1上进行管理。

```
R1#telnet a
Open
Attention: Telnet Escape character is ctrl+']'

************************************************************
Welcome to Inspur Intelligent Router 12000
                of Inspur networking
************************************************************

Username:who
Password:
R1>
```

返回IR12000的操作界面，查看DNS缓存中表项信息。

```
R1#show ip domain
Host                            Age      Type     Record
b.Inspur.com.cn                 1075     IPv4     10.0.0.27
a.Inspur.com.cn                 1195     IPv4     10.1.1.1
```

提示：

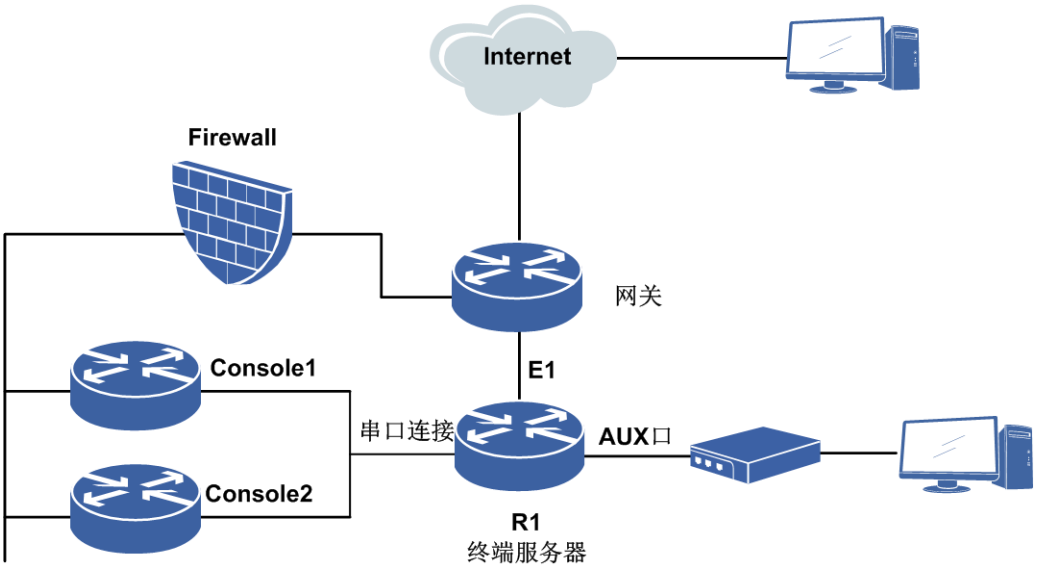
DNS缓存表项中的Age表示该条目剩余的老化时间，单位为秒。

3.5 反向 TELNET/TCP 和串口终端接入

由于组网和管理方式的需要，目前主流路由器设备厂商提供了一种反向TELNET的技术，利用该技术结合路由器设备的异步串口，可实现单一集中入口对多个网络设备或主机的统一管理。

反向TELNET应用主要有以下几种：构建终端服务器，实现对其它网络设备的集中管理、集中管理网络中多个主机设备、配置和管理异步串口上的外接Modem设备。应用场景如*图 3-7*所示。

图 3-7 反向 TELNET 应用场景图



R1设备作为一个终端服务器可实现对一组网络设备的管理。R1本身提供了多种管理用户的接入方式，包括以太网接入方式，或者AUX口远程拨号接入。R1把其它网络设备的Console口连接到本设备的各个异步串口之上。用户登录到R1以后，利用反向TELNET命令可以通过某个异步串口登录到该接口连接的网络设备Console口上，从而实现对该设备的管理操作。用户可以很方便地在不同的异步串口之间切换，从而登录到不同的设备上去完成操作。

反向TCP功能的实现借鉴了反向TELNET功能的实现方法，只是将TELNET客户端变成特殊的TCP应用客户端，串口终端服务器上直接进行TCP数据流的转发，串口终端设备运行相应的终端管理程序。

串口终端接入是利用路由器作为终端接入发起方，将服务器作为TCP连接的接收方，路由器负责其连接的串口终端和服务器之间数据的透明传输。应用业务通过运行于服务器的TTYD程序与发起方路由器交互，并通过路由器把业务画面推送到串口的终端上，完成业务交互处理。发起方与接收方之间的连接可以是TCP和UDP等IP协议。

3.5.1 配置反向 TELNET/TCP 和串口终端接入

本节介绍反向TELNET、反向TCP、串口终端接入功能的配置步骤和命令。

1.配置异步串口相关属性。

步骤	命令	功能
1	inspur(config)#**interface** *<interface-name>*	进入同/异步串口的接口模式。
2	inspur(config-if-interface-name)#**physical-mode** {**sync** | **async**}	配置同/异步串口工作模式，缺省为**sync**。 用于反向TELNET/TCP和终端接入应设置Serial接口工作在异步方式**async**。
3	inspur(config-if-interface-name-async)#**a**	配置异步串口的工作模式，缺

步骤	命令	功能
	sync mode {**flow** | **protocol**}	省为协议模式**protocol**。 用于反向TELNET/TCP和终端接入应采用**flow**流模式。
4	inspur(config-if-interface-name-async)#**baudrate** <*baudrate*>	配置异步串口的波特率，缺省为9600，单位：bit/s。
5	inspur(config-if-interface-name-async)#**char-len** {**5** | **6** | **7** | **8**}	配置异步串口的数据位比特数，缺省为8。
6	inspur(config-if-interface-name-async)#**detect dsr-dtr**{**enable** |**disable**}	配置异步串口DTR和DSR信号检测功能，缺省为开启。 用于反向TELNET时配置为**disable**。

2.配置反向TELNET和反向TCP。

步骤	命令	功能
1	inspur(config)#**line** <*begin-line-number*>[<*end-line-number*>]	创建line实例并进入line模式，可以对连续的多个端口进行配置。
2	inspur(config-line)#**rtelnet** {**enable** | **disable**}	开启或关闭串口line线路的rtelnet功能。
3	inspur(config-line)#**transport input** {**telnet** | **tcp**}	设置串口line的TELNET权限。
4	inspur(config-line)#**login authentication**	开启串口line的用户登录密码验证功能。
5	inspur(config-line)#**password** <*password*>	设置反向TELNET控制终端访问密码，缺省为空。
6	inspur(config-line)#**idle-timeout** <*idle-time*>	配置line连接的空闲超时时长，范围0~1000，缺省为120，单位：分钟，0表示永远不超时。 在反向TELNET/TCP登录后，若在连接<*idle-time*>分钟内控制终端PC无操作，则连接的会话被强制关闭。
7	inspur(config-line)#**absolute-timeout** <*absolute-time*>	配置line连接的绝对超时时长，范围0~10000，缺省为1440，单位：分钟，0表示永远不超时。 在反向TELNET/TCP登录时长达到<*absolute-time*>后，连接的会话将强制关闭，而不管控制终端有无操作。

3.配置串口终端接入。

步骤	命令	功能
1	inspur(config)#**line** <*begin-line-number*>[<*end-line-number*>]	创建line实例并进入line模式，可以对连续的多个端口进行配置。
2	inspur(config-line)#**rta**{**enable** | **disable**}	开启或关闭串口line线路的终端接入功能。
3	inspur(config-line)#**vty** <*vty-number*>{**telnet** | **tcp**} **remote** {**(ipv4** <*remote-ipv4addr*><*remote-port*>[**vrf** <*vrf-name*>][**source** <*source-ipv4addr*>]**)** | **(ipv6** <*remote-ipv6addr*><*remote-port*>[**vrf** <*vrf-name*>][**source** <*source-ipv6addr*>]**)**}	配置终端接入方式及远程服务器IP地址、VRF和端口号信息。 当串口终端登录时，路由器可以自动登录到远程服务器。
4	inspur(config-line)#**vty terminal type** <*vty-type*>	配置终端类型，字符长度为1~31，缺省为“VT100”。
5	inspur(config-line)#**screen width** <*width*> **height** <*height*>	配置屏幕窗口尺寸，以字符数为单位，缺省宽度值为80，高度值为24。 当串口终端以TELNET方式登录时，路由器与远程服务器建立TELNET会话并协商屏幕窗口尺寸参数。
6	inspur(config-line)#**idle-timeout** <*idle-time*>	配置line连接的空闲超时时长，范围0~1000，缺省为120，单位：分钟，0表示永远不超时。 在串口终端操作空闲时长超过<*idle-time*>，连接的会话被强制关闭。
7	inspur(config-line)#**absolute-timeout** <*absolute-time*>	配置line连接的绝对超时时长，范围0~10000，缺省为1440，单位：分钟，0表示永远不超时。 在串口终端登录时长达到<*absolute-time*>后，连接的会话将强制关闭，而不管串口终端是否真正做操作。

4.验证配置结果。

命令	功能
inspur#**show running-config-interface** <*interface-name*>	查看异步串口的配置信息。
inspur#**show line configuration** <*begin-line-number*>[<*end-line-number*>]	显示line线路的详细配置信息，包括缺省的参数值。

命令	功能
inspur#**show line configuration all**	显示所有line线路的配置情况。
inspur#**show tcp brief**	查看TCP连接情况，可查看串口管理软件是否已经同被管理的串口设备建立了连接。
inspur#**show lines**	查看当前设备所有异步串口线路的状态，对于已被某个活动所占用的串口线路，将列出该线路对应的连接基本信息，通过该命令可以查询获得空闲的线路资源。
inspur#**disconnect line** {<*line_number*>| **all**}	终止一个已有的会话，并释放所占用的异步串口线路资源。

5.维护反向TELNET/TCP和串口终端接入。

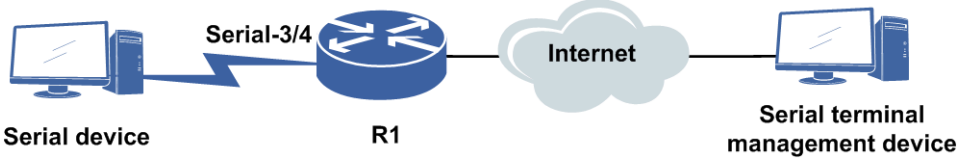
命令	功能
inspur#**disconnect line** {<*line_number*>| **all**}	终止一个已有的会话，并释放所占用的异步串口线路资源。

3.5.2 反向 TELNET 配置实例

配置说明

如*图 3-8*所示，在R1配置反向TELNET，终端串口管理设备连接到R1上的某个状态为Up的接口。

图 3-8 反向 TELNET 配置实例拓扑图



配置思路

1.配置异步串口相关属性。

2.Line模式下配置Rtelnet使能和传输模式。

配置过程

R1上的配置如下。

```
R1(config)#interface serial-3/4
R1(config-if-serial-3/4)#no shutdown
R1(config-if-serial-3/4)#physical-mode async
R1(config-if-serial-3/4-async)#async mode flow
R1(config-if-serial-3/4-async)#baudrate 115200
R1(config-if-serial-3/4-async)#detect dsr-dtr disable
R1(config-if-serial-3/4-async)#exit
R1(config-if-serial-3/4)#exit
R1(config)#
R1(config)#line 16
R1(config-line)#rtelnet enable
R1(config-line)#transport input telnet
R1(config-line)#exit
R1(config)#
```

配置验证

在R1上查看Line 16的配置情况。

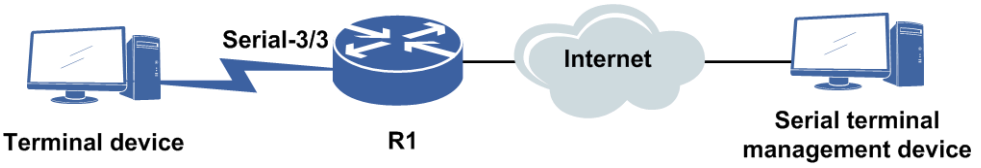
```
R1#show line configuration 16
 Line : 16
 Interface name          : serial-3/4
 Rtelnet                : Enable
 Transport input Protocal : Telnet
 Listen port             : 2016(LISTENING)
 Login flag              : Not need password login
 Password                :
 Absolute timeout         : 1440(minutes)
 Idle timeout            : 120(minutes)
 RTA                    : Disable
 VTY number              : 0
 RTA mode                : None
 Destination IP          :
 Destination port         : 0
 VRF name                :
 Source IP               :
 Terminal type           : VT100
 Screen width            : 80
 Screen height           : 24
         ------------------------------------
```

3.5.3 反向 TCP 配置实例

配置说明

如*图 3-9*所示，在R1上配置反向TCP，终端串口管理设备连接到R1上的某个状态为Up的接口。

图 3-9 反向 TCP 配置实例拓扑图



配置思路

1.配置异步串口相关属性。

2.Line模式下配置Rtelnet功能和传输模式。

配置过程

R1上的配置如下。

```
R1(config)#interface serial-3/3
R1(config-if-serial-3/3)#no shutdown
R1(config-if-serial-3/3)#physical-mode async
R1(config-if-serial-3/3-async)#async mode flow
R1(config-if-serial-3/3-async)#baudrate 115200
R1(config-if-serial-3/3-async)#exit
R1(config-if-serial-3/3)#exit
R1(config)#
R1(config)#line 15
R1(config-line)#rtelnet enable
R1(config-line)#transport input tcp
R1(config-line)#exit
R1(config)#
```

配置验证

在R1上查看Line 15的配置情况。

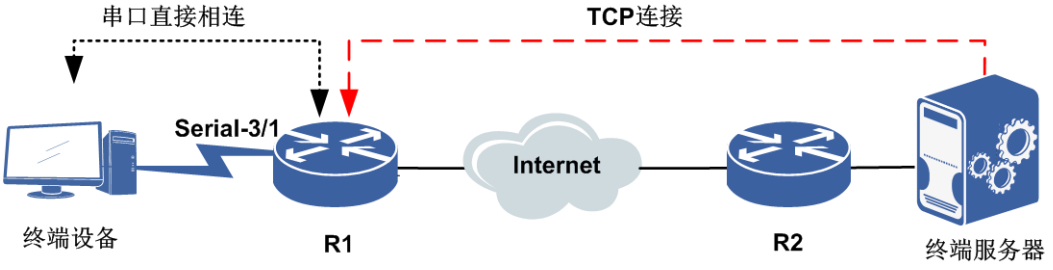
```
R1(config)#show line configuration 15
 Line : 15
 Interface name          : serial-3/3
 Rtelnet                 : Enable
 Transport input Protocal : Tcp
 Listen port             : 2015(LISTENING)
 Login flag              : Not need password login
 Password                :
 Absolute timeout        : 1440(minutes)
 Idle timeout            : 120(minutes)
 RTA                     : Disable
 VTY number              : 0
 RTA mode                : None
 Destination IP          :
 Destination port        : 0
 VRF name                :
 Source IP               :
 Terminal type           : VT100
 Screen width            : 80
 Screen height           : 24
          ------------------------------------
```

3.5.4 串口终端接入配置实例

配置说明

如*图 3-10*所示，在R1配置串口终端接入，终端串口管理设备连接到R1上的某个状态为Up的接口。

图 3-10 串口终端接入配置实例拓扑图



配置思路

1.配置异步串口相关属性。

2.Line模式下配置**rta**功能、终端接入方式和远程服务器地址信息。

配置过程

R1上的配置如下。

```
R1(config)#interface serial-3/1
R1(config-if-serial-3/1)#no shutdown
R1(config-if-serial-3/1)#physical-mode async
R1(config-if-serial-3/1-async)#async mode flow
R1(config-if-serial-3/1-async)#baudrate 115200
R1(config-if-serial-3/1-async)#exit
R1(config-if-serial-3/1)#exit
R1(config)#
R1(config)#line 13
R1(config-line)#rta enable
R1(config-line)#vty 0 tcp remote 129.186.9.152 23 source 129.186.35.6
R1(config-line)#exit
R1(config)#
```

配置验证

在R1上查看Line 13的配置情况。

```
inspur#show line configuration 13
 Line : 13
 Interface name          : serial-3/1
 Rtelnet                 : Disable
 Transport input Protocal : None
 Listen port             : 2013(CLOSED)
 Login flag              : Not need password login
 Password                :
```

```
Absolute timeout        : 1440(minutes)
Idle timeout           : 120(minutes)
RTA                   : Enable
VTY number             : 0
RTA mode               : Tcp
Destination IP          : 129.186.9.152
Destination port        : 23
VRF name               :
Source IP              : 129.186.35.6
Terminal type           : VT100
Screen width            : 80
Screen height           : 24
-----------------------------------
```

3.6 DDNS Client

DDNS是将用户的动态IP地址映射到一个固定的域名解析服务上，用户每次连接网络时，客户端程序就会通过信息传递把该主机的动态IP地址传送给位于服务商主机上的服务器程序，服务器程序负责提供DNS服务并实现动态域名解析。

DDNS提供了一种全新的解决方案，DDNS可以捕获用户每次变化的IP，并将其与域名相对应，这样用户就可以通过域名来提供服务了。

目前，IR12000支持www.3322.org和www.oray.cn两种DDNS服务商提供的DDNS更新服务。

3.6.1 配置 DDNS Client

本节介绍DDNS Client的配置步骤和命令。

1.配置DDNS更新策略。

步骤	命令	功能
1	inspur(config)#**ddns**	进入DDNS配置模式。
2	inspur(config-ddns)#**ip ddns update policy** <*policy-name*>	配置DDNS更新策略。 DDNS更新策略名，长度为1～32字符。
3	inspur(config-ddns-update-policy)#**url**<*url-address*>	配置DDNS Server提交更新请求的URL地址。
4	inspur(config-ddns-update-policy)#**username** <*username*> **password** <*password*>	配置用户名与密码，用于与DDNS Server建议HTTP会话时的认证。
5	inspur(config-ddns-update-policy)#**interval** <*interval-time*>	配置更新时间间隔，单位：分钟，缺省值为60，取值范围：1~525600。

每种DDNS Server提供商的URL地址格式并不相同，需要按照DDNS Server指定的格式进行填写。例如：

Oray的更新策略的URL格式如下：http://username:password@ddns.oray.com

3322的更新策略的URL格式如下：http://username:password@members.3322.org

2.配置端口绑定DDNS更新策略。

步骤	命令	功能
1	inspur(config)#**ddns**	进入DDNS配置模式。
2	inspur(config-ddns)#**interface** <*interface-name* > **bind ddns-policy** <*policy-name*> **domain-name** <*domain-name*>	在接口下绑定DDNS更新策略。

<*domain-name*>：指定设备申请的域名，长度：1～128字符。

3.配置静态DNS，以便和DDNS Server建链。

步骤	命令	功能
1	inspur(config)#**ip domain lookup**	启动域名解析功能。
2	inspur(config)#**ip domain resolve-type static**	配置DNS解析类型。
3	inspur(config)#**ip domain hostname** <*host-name*> **ipv4-address** <*ipv4-address*>	配置域名与地址对应关系。

目前，oray域名：ddns.oray.com，地址：202.105.21.204；3322域名：members.3322.org，地址：61.160.239.25。

4.验证配置结果。

命令	功能
inspur#**show ip ddns update policy** [<*policy-name*>]	查看设备配置的DDNS更新策略。
inspur#**show running-config ddns**	查看DDNS相关配置。
inspur#**show running-config dns**	查看DNS相关配置。

5.维护DDNS。

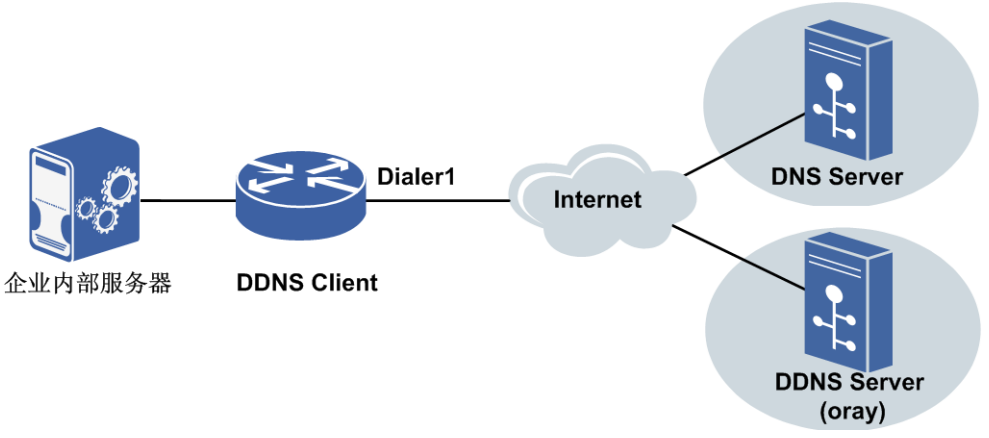
命令	功能
inspur#**debug ip ddns update all**	打开debug开关，查看更新过程。
inspur#**show debug ddns all**	显示已开启的DDNS的debug开关。

3.6.2 DDNS Server 为 Oray 的 DDNS Client 配置实例

配置说明

如*图 3-11*所示，企业内部服务器通过设备的拨号口Dialer1以PPPoE方式接入因特网，并使用Dialer1接口的IP地址作为公网IP地址，提供网络服务。企业在设备上配置DDNS客户端，DDNS客户端将服务器的公网IP地址的变化及时通过DDNS服务器反馈给DNS服务器，使DNS服务器记录最新的域名和IP地址的对应关系。DDNS服务器为oray。

图 3-11 DDNS Server 为 oray 的 DDNS Client 配置实例



配置思路

1.登录DDNS服务提供商的网站，注册帐户，并申请域名。

2.配置静态DNS。

3.配置DDNS动态更新策略，DDNS Server为oray。

4.Dialer接口绑定DDNS动态更新策略。

配置过程

Dialer接口的配置参考"PPPoE Client和SDC配置"。

IR12000上的配置如下。

```
inspur(config)#ip domain lookup
inspur(config)#ip domain resolve-type static
inspur(config)#ip domain hostname ddns.oray.com ipv4-address 202.105.21.204
inspur(config)#ddns
inspur(config-ddns)#ip ddns update policy oray
inspur(config-ddns-update-policy)#url
http://ddnsorayInspur:inspur@ddns.oray.com
inspur(config-ddns-update-policy)#username ddnsorayInspur password inspur
inspur(config-ddns-update-policy)#exit
inspur(config-ddns)#interface dialer1 bind ddns-policy oray domain-name ddnsor
ayInspur.eicp.net
inspur(config-ddns)#exit
```

配置验证

在IR12000上查看DDNS Client配置。

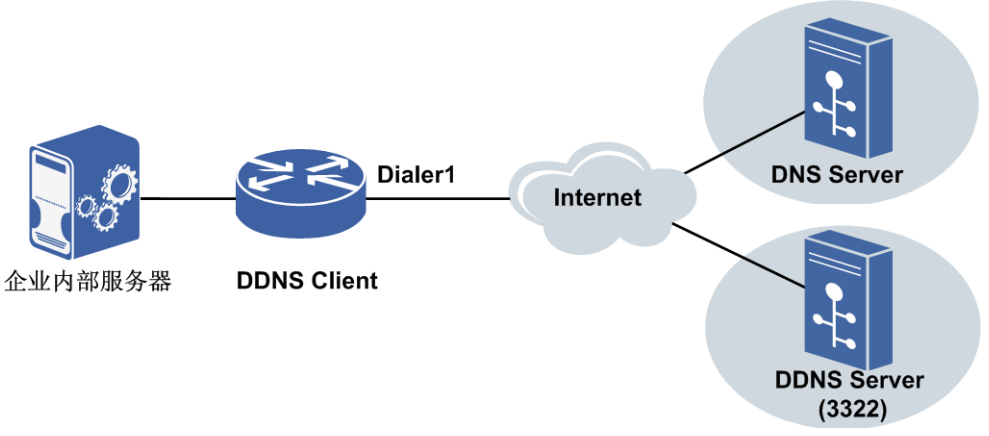
```
inspur(config)#show ip ddns update policy oray
   Policy Name : oray
   Policy interval time : 60
   Policy URL : http://ddnsorayInspur:inspur@ddns.oray.com
   Policy bind count : 1
   Interface : dialer1
```

3.6.3 DDNS Server 为 3322 的 DDNS Client 配置实例

配置说明

如*图 3-12*所示，企业内部服务器通过设备的拨号口Dialer1以PPPoE方式接入因特网，并使用Dialer1接口的IP地址作为公网IP地址，提供网络服务。企业在设备上配置DDNS客户端，DDNS客户端将服务器的公网IP地址的变化及时通过DDNS服务器反馈给DNS服务器，使DNS服务器记录最新的域名和IP地址的对应关系。DDNS服务器为3322。

图 3-12 DDNS Server 为 3322 的 DDNS Client 配置实例



配置思路

1.登录DDNS服务提供商的网站，注册帐户，并申请域名。

2.配置静态DNS。

3.配置DDNS动态更新策略，DDNS Server为3322。

4.Dialer接口绑定DDNS动态更新策略。

配置过程

Dialer接口的配置参考"PPPoE Client和SDC配置"。

IR12000上的配置如下。

```
inspur(config)#ip domain lookup
inspur(config)#ip domain resolve-type static
inspur(config)#ip domain hostname members.3322.org ipv4-address 61.160.239.25
inspur(config)#ddns
inspur(config-ddns)#ip ddns update policy 3322
inspur(config-ddns-update-policy)#url
http://ddns3322Inspur:inspur@members.3322.org
inspur(config-ddns-update-policy)#username ddns3322Inspur password inspur
inspur(config-ddns-update-policy)#exit
inspur(config-ddns)#interface dialer1 bind ddns-policy 3322 domain-name
ddns332
2Inspur.f3322.org
inspur(config-ddns)#exit
```

配置验证

在IR12000上查看DDNS Client配置。

```
inspur(config)#show ip ddns update policy 3322
   Policy Name : 3322
   Policy interval time : 60
   Policy URL : http://ddns3322Inspur:inspur@members.3322.org
   Policy bind count : 1
   Interface : dialer1
```

3.7 UDP Helper

IR12000提供了UDP Helper功能，通过该功能可以实现对指定UDP端口的广播报文进行中继转发。UDP Help可以将指定UDP端口的广播报文转换为单播报文发送给指定的目的服务器，起到中继的作用。

3.7.1 配置 UDP Helper

本节介绍UDP Helper功能的配置步骤和命令。

1.全局开启UDP Helper功能。

命令	功能
inspur(config)#**udp-helper** {**enable** | **disable**}	全局开启UDP Helper功能。缺省情况下，UDP Helper功能是关闭的。

2.配置UDP Helper的目的端口。

命令	功能
inspur(config)#**udp-helper port** {<*port-number*>| **dns** | **netbios-dgm** | **netbios-ns** | **tacacs** | **tftp** | **time**}	配置UDP Helper的目的端口。缺省无配置时，不支持任何协议的UDP报文的中继转发。

<*port-number*>：需要中继转发报文的UDP目的端口号，范围： 0~65535 。

dns：对DNS应用发送的UDP广播报文进行中继转发，UDP端口号为53。

netbios-dgm：对NetBIOS-DS应用发送的UDP广播报文进行中继转发，UDP端口号为138。

netbios-ns：对NetBIOS-NS应用发送的UDP广播报文进行中继转发，UDP端口号为137。

tacacs：对终端访问控制器访问控制系统发送的UDP广播报文进行中继转发，UDP端口号为49。

tftp：对简单文件传输协议的UDP广播报文进行中继转发，UDP端口号为69。

time：对时间服务应用的UDP广播报文进行中继转发， UDP端口号为37。

提示：

IR12000的UDP Helper功能不支持对DHCP报文的中继转发，即中继转发的UDP端口不能配置为67、68。

全局最多支持配置50个UDP helper的目的端口。

3.配置UDP Helper的目的服务器地址。

步骤	命令	功能
1	inspur(config)#**interface** <*interface-name*>	进入接口配置模式。
2	inspur(config-if-interface-name)#**udp-helper address** [**vrf** <*vpn-name*>]<*ip-address*>	配置中继转发的目的服务器地址，无缺省值。 每接口最多支持配置20个目的服务器地址。

<*interface-name*>：目前支持UDP Helper功能的接口有以太口、VLAN子接口、POS接口、Multilink接口、POSGroup接口、SuperVLAN接口、SmartGroup接口接口、ULEI接口 。

<*ip-address*>：目的服务器的单播地址，UDP Helper功能开启后，如果接口收到报文的UDP目的端口号与需要中继转发的UDP端口号相匹配，则将报文转发给该接口下所配置的目的服务器。

4.验证配置结果。

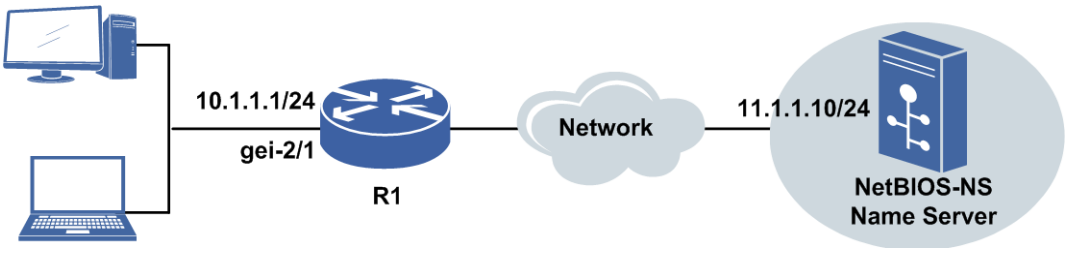
命令	功能
inspur#**show udp-helper address** [<*interface-name*>]	显示UDP helper的目的服务器的IP地址。

3.7.2 UDP Helper 配置实例

配置说明

如*图 3-13*所示，R1与NetBIOS-NS name服务器不在同一网段，但R1到NetBIOS-NS name服务器路由可达。R1的接口gei-2/1的IP地址为10.1.1.1/24。NetBIOS-NS name服务器的IP地址为11.1.1.10/24。

图 3-13 UDP Helper 配置实例组网图



配置将UDP目的端口号为137、目的IP地址为255.255.255.255和10.1.1.255的UDP广播报文中继转发到指定的目的NetBIOS-NS name服务器上。若R1接收到NetBIOS-NS Register的广播报文，将修改IP报文头的目的IP地址为NetBIOS-NS name服务器的IP地址，从而将报文发给指定的NetBIOS-NS name服务器。

配置思路

1.开启UDP Helper功能。

2.配置UDP Helper的目的端口。

3.在接口下配置接口IP地址和UDP Helper的目的服务器地址为NetBIOS-NS name服务器地址。

配置过程

R1上的配置如下。

```
R1(config)#udp-helper enable
R1(config)#udp-helper port netbios-ns
R1(config)#iinterface gei-2/1
R1(config-if-gei-2/1)#ip address 10.1.1.1 255.255.255.0
R1(config-if-gei-2/1)#udp-helper address 11.1.1.10
R1(config-if-gei-2/1)#exit
R1(config)#exit
```

配置验证

查看R1上的配置如下。

```
R1(config)#show running-config udp
!<udp>
interface gei-2/1
```

```
  udp-helper address 11.1.1.10
$
udp-helper enable
udp-helper port 137
!</udp>

R1(config)#show udp-helper address gei-2/1
Interface           Helper-Address  VPN Name
gei-2/1             11.1.1.10
```

接口gei-2/1中继转发的目的服务器为配置的NetBIOS-NS name 服务器。

4 IPv4 路由

4.1 路由简介

路由设备提供了将异构网络互联的机制，实现将数据包从一个网络发送到另一个网络的功能，而路由就是指导IP数据包发送的路径信息。

路由从产生方式来分，主要包括静态路由和动态路由。

- 静态路由由系统管理员手工配置，不随网络拓扑结构的变化而变化，适用于规模较小的网络。
- 动态路由由动态路由协议生成，能够根据网络的拓扑变化调整相应的路由信息，适应大规模、复杂的网络结构。

动态路由协议根据不同的标准，有多种不同的分类。通常情况下根据寻址算法的不同，动态路由协议分为距离矢量路由协议和链路状态路由协议。

- 距离矢量路由协议采用DV（Distance-Vector，距离矢量）算法，相邻的路由器之间互相交换整个路由表并进行矢量的叠加，最后学习到整个路由表。

  常见的距离矢量路由协议包括RIP、BGP等。

- 链路状态路由协议采用LS（Link State，链路状态）算法。链路状态是层次式的，执行LS算法的路由设备不是简单的从相邻的设备学习路由，而是把路由设备分成区域，收集区域内所有设备的链路状态信息，再根据链路状态信息生成网络拓扑结构，每一个路由设备根据生成的拓扑结构图计算路由。

  常见的链路状态路由协议包括OSPF、IS-IS等。

4.2 静态路由

静态路由是网络管理员通过手工配置指定的路由。当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。

静态路由不像动态路由那样根据路由算法建立路由表，也不能自动适应网络拓扑结构的变化。当网络发生故障或者拓扑发生变化后， 必须由网络管理员手工修改配置。

所有的静态路由项都必须明确下一跳地址，在发送报文时根据报文的目的地址寻找路由表中与之匹配的路由。只有指定了下一跳地址，链路层才能找到对应的链路层地址，并转发报文。

4.2.1 配置静态路由

网络管理员根据网络需求，手动配置静态路由条目，可以将配置的路由条目加入到路

由表中。

1.配置指定下一跳地址的静态路由。

命令	功能
inspur(config)#**ip route** [**vrf** < *vrf-name*>]< *prefix*>< *net-mask*>{< *nexthop-address* >[**global**]}[<*distance-metric*>][**metric** <*metric*>][**bfd enable**][**track** <*track-name*>][**tag** <*tag-value*>][**name** <*descript-name*>]	配置IPv4静态路由指定下一跳，< *nexthop-address* >可以为直连地址或非直连地址 **tag** <*tag-value*>：路由标识

配置静态路由时，指定路由的下一跳有以下两类情况：

▸指定直连下一跳

配置静态路由的下一跳地址为直连网络。

▸指定非直连下一跳

配置静态路由的下一跳地址为非直连网络时，需要对所配置的下一跳地址进行一次或多次的迭代解析，以便获得该地址对应的直连下一跳。迭代解析完成后，下发路由表的静态路由下一跳为直连下一跳地址。

2.配置指定出接口的静态路由。

命令	功能
inspur(config)#**ip route** [**vrf** < *vrf-name*>]< *prefix*>< *net-mask*>{< *interface-name*>|< *interface-name*>< *nexthop-address* >}[<*distance-metric*>][**metric** <*metric*>][**bfd enable**][**track** <*trackname*>][**name** <*descriptname*>][**tag** <*tag-value*>]	配置IPv4静态路由指定出接口，以太接口指定出接口时必须同时指定下一跳地址

对于点到点接口，配置静态路由只需指定出接口，因为指定出接口即隐含指定了下一跳地址，此时认为与该接口相连的对端接口地址就是路由的下一跳地址。

对于Null接口，配置静态路由指定Null接口应用于黑洞路由，匹配该路由的流量都会被直接丢弃。

3.配置静态路由FRR。

步骤	命令	功能
1	inspur(config)#**ip route-static** [**vrf** <*vrf-name*>] **fast-reroute**[**wtr**<*time-interval*>]	打开公网或VPN网络的静态路由备路由计算开关
2	inspur(config)#**ip route** [**vrf** <*vrf-name*>]<*prefix*>< *net-mask*>{<*forwarding-router's-address*>|<*interface-name*>|<*interface-name*><*forwarding-router's-address*>}[<*distance-metric*>][**metric** <*metric-number*>]	配置作为主路由的静态路由
	inspur(config)#**ip route** [**vrf** <*vrf-name*>]<*prefix*><*net-mask*>{<*forwarding-ro*	配置作为备路由的静态路由，目的地址、掩码需与主路由一

步骤	命令	功能
	uter's-address>|<*interface-name*>|<*interface-name*><*forwarding-router's-address*>}[<*distance-metric*>][**metric** <*metric-number*>]	致，出接口需与主路由不同，优先级或metric需次于主路由

wtr<*time-interval*>：静态路由使能FRR设置的WTR延迟。

<*distance-metric*>：管理距离，默认为1，范围：1~255。

<*metric-number*>：路由的度量值，默认为0，范围：0~255。

4.配置Global静态路由。

Global静态路由指的是配置了私网静态路由携带公网下一跳，用于实现VPN 穿越，即要到达的目的地址和经过的下一跳不在同一个VPN内。

命令	功能
inspur(config)#**ip route vrf** <*vrf-name*><*prefix*><*net-mask*><*nexthop-address*> **global** [<*distance-metric*>][**metric** <*metric*>][**bfd enable**][**track**]<*track-name* >[**name**]<*description*>	配置IPv4 私网静态路由指定公网下一跳

5.验证配置结果。

查看静态路由信息：

命令	功能
inspur#**show running-config static**	显示配置了哪些静态路由
inspur#**show ip protocol routing** [**vrf** <*vrf-name*>]	显示路由器的全局路由表
inspur#**show ip forwarding route** [**vrf** <*vrf-name*>]	显示路由器的转发表

查看静态路由FRR信息：

命令	功能
inspur#**show ip forwarding route** [**vrf** <*vrf-name*>]	查询转发表，可以看到当前主路由信息
inspur#**show ip forwarding backup route** [**vrf** <*vrf-name*>]	查询备用路由转发表，可以看到主用和备用路由信息

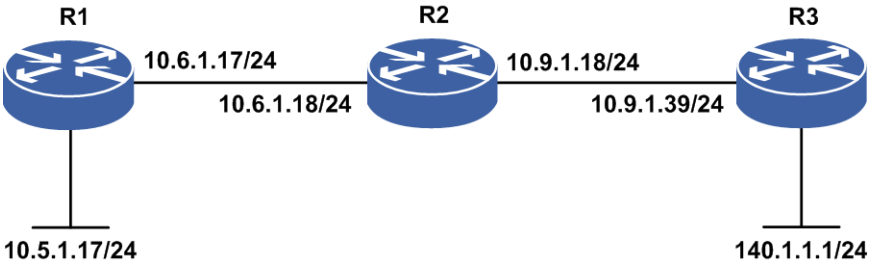
4.2.2 下一跳直连的静态路由配置实例

配置说明

如*图 4-1*所示，R1要想将报文传给远端网络10.9.1.0/24，必须将报文传给拥有IP地址10.6.1.18的R2，而R1和R2是直连的，那么此时就需要在R1上添加一条到达目的网段

10.9.1.0下一跳是10.6.1.18的静态路由。

图 4-1 静态路由配置实例示意图



配置思路

在R1上配置静态路由，有以下三种方法：

1.配置下一跳为IP地址，配置命令如下：

```
R1(config)#ip route 10.9.1.0  255.255.255.0 10.6.1.18
```

2.配置下一跳为出接口，配置命令如下：

```
R1(config)#ip route 10.9.1.0 255.255.255.0 pos3-0/1
```

这种配置方法和方法一类似，唯一的区别是方法一用的下一跳是IP地址，而这里用的本地出接口，也就是将所有去往目的网段10.9.1.0/24的报文通过R1接口pos3-0/1送出，而不是路由到下一跳的逻辑地址。

3.配置本地的出接口，但是同时配置直连的下一跳，配置命令如下：

```
R1(config)#ip route 10.9.1.0  255.255.255.0 gei-0/2 10.6.1.18
```

在这里请注意，方法三和方法二由于配置方式的不一样，是有些区别的。若配置出接口加下一跳，是为了指定出接口。若配置的是下一跳，如果配置的这个下一跳是直连的，那么这样的配置和配置出接口加下一跳没有区别，但是若配置的非直连的下一跳，则这个下一跳就会去进行递归解析。这两种的设计是为了满足直连和非直连的需求。

配置过程

R1上的配置如下：

```
R1(config)#ip route 10.9.1.0 255.255.255.0 10.6.1.18
```

配置验证

下面是用**show ip protocol routing**命令验证配置的结果。

在R1上查看配置结果：

```
R1(config)#show ip protocol routing network 10.9.1.0
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
       OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
       BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
```

```
      ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
      STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
      P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
      NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
      GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale
status codes: *valid, >best, i-internal, s-stale

    Dest             NextHop        RoutePrf   RouteMetric Protocol
*>  10.9.1.0/24       10.6.1.18       1          0          Static
```

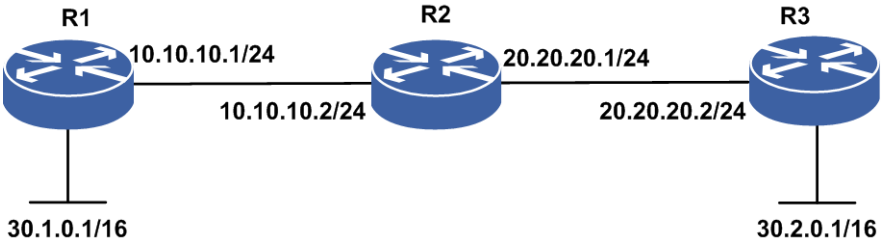
如果到达同一目的地的存在多条路径且掩码一样的情况下，则可以为路由器配置多条管理距离不同的静态路由，路由器会选择管理距离小的那条路由作为最优路由，而将管理距离相对大的那条路由作为次优路由，在路由表中将那条最优路由前面做上*>的标记。因为当路由器被告知到达某一网络有多个竞争资源时，管理距离最小的路由优先。

4.2.3 下一跳非直连的静态路由配置实例

配置说明

如*图 4-2*所示，在R1上配置到30.2.0.0/16的静态路由，下一跳为20.20.20.2（R3接口），该下一跳地址不是R1的直连网路。为使该静态路由生效，在路由表中必须存在到目的网络20.20.20.0/24的下一跳地址为10.10.10.2（R1的直连下一跳），此过程完成一次下一跳迭代解析。

图 4-2 静态路由指定非直连下一跳配置实例拓扑图



配置思路

1.R1上配置到R3上的静态路由，下一跳是20.20.20.2。

2.R1、R2、R3上各直连接口同时启用IS-IS动态路由协议。

配置过程

R1上的配置如下：

```
R1(config)#ip route 30.2.0.0 255.255.0.0 20.20.20.2
```

R1、R2、R3上各直连接口同时启用IS-IS动态路由协议。R1上IS-IS协议配置为：

```
R1(config)#router  isis
R1(config-isis-0)#area 01
```

```
R1(config-isis-0)#is-type level-2
R1(config-isis-0)#system-id 00D0.D0C7.5460
R1(config-isis-0)#interface gei-0/1
R1(config-isis-0-if-gei-0/1)#ip router isis
```

R2上IS-IS协议配置为：

```
R2(config)#router isis
R2(config-isis-0)#area 01
R2(config-isis-0)#is-type level-2
R2(config-isis-0)#system-id 00D0.D0C7.53E0
R2(config-isis-0)#interface gei-0/1
R2(config-isis-0-if-gei-0/1)#ip router isis
R2(config-isis-0-if-gei-0/1)#exit
R2(config-isis-0)#interface gei-0/2
R2(config-isis-if-gei-0/2)#ip router isis
```

R3上IS-IS协议配置为：

```
R3(config)#router isis
R3(config-isis-0)#area 01
R3(config-isis-0)#is-type level-2
R3(config-isis-0)#system-id 00D0.D0C7.5541
R3(config-isis-0)#interface gei-0/2
R3(config-isis-0-if-gei-0/2)#ip router isis
```

配置验证

下面是用**show**命令验证配置的结果。

在R1上查看转发表：

```
R1#show ip forwarding route
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest            Gw           Interface      Owner     Pri Metric
10.10.10.0/24    10.10.10.1    gei-0/1        Direct    0   0
10.10.10.1/32    10.10.10.1    gei-0/1        Address   0   0
20.20.20.0/24    10.10.10.2    gei-0/1        ISIS-L2   115 20
30.2.0.0/16      10.10.10.2    gei-0/1        Static    1   0
```

在本例中，使用了IS-IS动态路由协议，使R1的路由表中存在到20.20.20.0/24的下一跳地址为10.10.10.2（R1的直连下一跳）的路由条目。经过下一跳迭代解析后，路由表中到目的网络30.2.0.0/16的下一跳地址为10.10.10.2（R1的直连下一跳）。

4.2.4 静态路由汇总配置实例

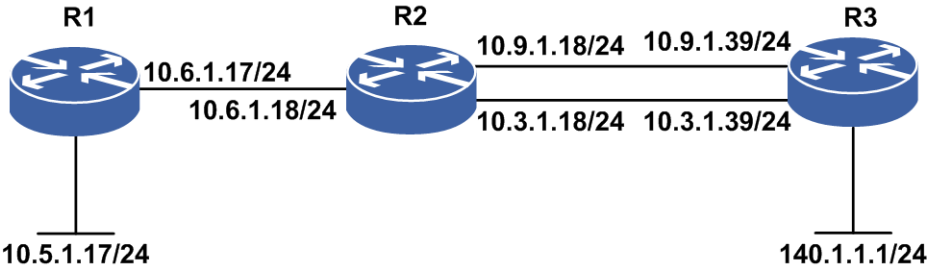
配置说明

汇总路由是一种特殊的静态路由，能够把两条或者多条特定的路由表达式汇总成一个表达式，从而在保证原来全部连接的基础上减少路由表中的条目。

如*图 4-3*所示，R2有两个网络10.9.1.0/24和10.3.1.0/24，R1要想到达这些网络，通常情况下，可以在R1上配置两条静态路由。当路由表中的路由数目很多时，可以使用汇总

静态路由来优化R1的路由表。

图 4-3 静态路由汇总配置实例示意图



配置思路

在R1上配置一条目的地址为10.0.0.0的静态路由，可以将多条到达目的网络的静态路由汇总成一条汇总静态路由，有利于优化路由表。

配置过程

R1上的配置如下：

```
R1(config)#ip route 10.0.0.0 255.0.0.0 10.6.1.18
```

配置验证

下面是用**show ip protocol routing**命令验证配置的结果。

在R1上查看配置结果：

```
R1#show ip protocol routing
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
       OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
       BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
       ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
       STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
       P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
       NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
       GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale
    Dest           NextHop        RoutePrf   RouteMetric  Protocol
*>  10.0.0.0/8     10.6.1.18        1          0          Static
```

4.2.5 默认路由配置实例

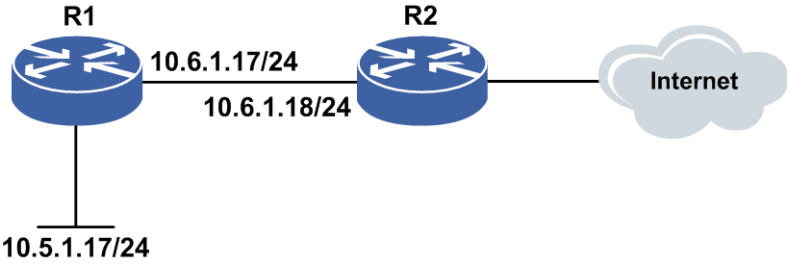
配置说明

默认路由又称为缺省路由，也是一种特殊的静态路由。当路由表中的所有路由都选择失败的时候，为使得报文有最终的一个发送地，将使用默认路由，从而大大减少了路由器的处理负担。

如果一个路由器不能为某个报文提供路由信息，那么这个报文只能被丢弃，而将报文丢弃到未知的目的地是不希望发生的，为了使路由器完全连接，一定要有个路由连到某个网络上。若路由器既要保持全连接，又不需要记录每个单独路由时，就可以使用默认路由。通过默认路由，可以指定一个单独的路由来表示所有的其它路由。

下面将通过实例说明默认路由的功能及使用方法。如*图 4-4*所示，由于R1上没有到达Internet的路由信息，因此在R1上可以使用默认路由，将找不到路由转发的报文直接送给R2处理。

图 4-4 默认路由配置实例示意图



配置思路

默认路由的配置方法和静态路由的配置完全相同，只是其网络部分和子网掩码部分都是0.0.0.0。

配置过程

R1上的配置如下：

```
R1(config)#ip route 0.0.0.0 0.0.0.0 10.6.1.18
```

配置验证

下面是用**show ip protocol routing**命令验证配置的结果。

在R1上查看配置结果：

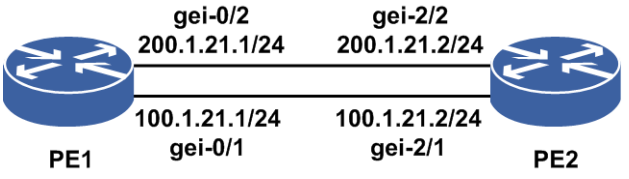
```
R1#show ip protocol routing
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
       OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
       BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
       ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
       STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
       P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
       NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
       GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale
    Dest          NextHop      RoutePrf   RouteMetric   Protocol
*>  0.0.0.0/0      10.6.1.18       1          0          Static
```

4.2.6 静态路由负荷分担配置实例

配置说明

负荷分担可使超出单个接口带宽的流量均分到多条链路上，实现流量在各条链路上的负载均衡。如*图 4-5*所示的网络中，采用静态路由的负荷分担来实现负载均衡。

图 4-5 静态路由负荷分担组网图



配置思路

1.配置接口地址，PE1、PE2路由器上各配置一个loopback地址分别为1.1.1.1/32、1.1.1.2/32。

2.在PE1上配置到1.1.1.2的2条静态路由，下一跳分别为100.1.21.2、200.1.21.2。

3.默认负荷分担方式为逐流负荷分担方式，可以修改逐包负荷分担方式。

配置过程

PE1上的配置如下：

```
PE1(config)#interface gei-0/1
PE1(config-if-gei-0/1)#ip address 100.1.21.1 255.255.255.0
PE1(config-if-gei-0/1)#no shutdown
PE1(config-if-gei-0/1)#exit
PE1(config)#interface gei-0/2
PE1(config-if-gei-0/2)#ip address 200.1.21.1 255.255.255.0
PE1(config-if-gei-0/2)#no shutdown
PE1(config-if-gei-0/2)#exit

PE1(config)#ip route 1.1.1.2 255.255.255.255 200.1.21.2
PE1(config)#ip route 1.1.1.2 255.255.255.255 100.1.21.2

PE1(config)#interface gei-0/1
PE1(config-if-gei-0/1)#ip load-sharing per-packet   /*选择逐包方式*/
PE1(config-if-gei-0/1)#exit
PE1(config)#interface gei-0/2
PE1(config-if-gei-0/2)#ip load-sharing per-packet   /*选择逐包方式*/
PE1(config-if-gei-0/2)#exit
```

PE2上的配置如下：

```
PE2(config)#interface gei-2/1
PE2(config-if-gei-2/1)#ip address 100.1.21.2 255.255.255.0
PE2(config-if-gei-2/1)#no shutdown
PE2(config-if-gei-2/1)#exit
PE2(config)#interface gei-2/2
PE2(config-if-gei-2/2)#ip address 200.1.21.2 255.255.255.0
```

```
PE2(config-if-gei-2/2)#no shutdown
PE2(config-if-gei-2/2)#exit
PE2(config)#interface gei-2/1
PE2(config-if-gei-2/1)#ip load-sharing per-packet
PE2(config-if-gei-2/1)#exit
PE2(config)#interface gei-2/2
PE2(config-if-gei-2/2)#ip load-sharing per-packet
PE2(config-if-gei-2/2)#exit
```

配置验证

用**show ip forwarding route static**命令查看PE1上的路由转发表：

```
PE1#show ip forwarding route static
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest            Gw          Interface      Owner     Pri  Metric
*>1.1.1.2/32     100.1.21.2    gei-0/1        Static    1    0
*>1.1.1.2/32     200.1.21.2    gei-0/2        Static    1    0
```

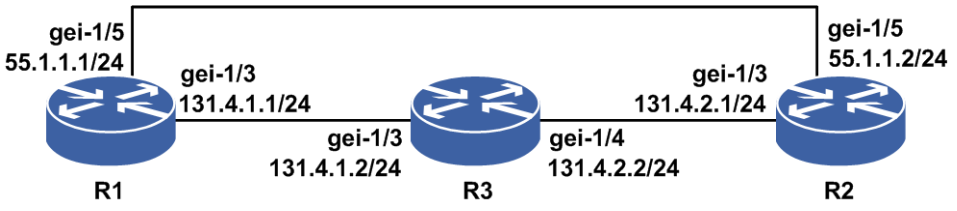
以上结果说明，到达目的地1.1.1.2/32的下一跳有两个，分别是100.1.21.2和200.1.21.2，出接口分别是gei-0/1和gei-0/2，达到了负载均衡的目的。

4.2.7 公网静态路由 FRR 配置实例

配置说明

FRR旨在当网络中链路或者节点失效后，为这些重要的节点或链路提供备份保护，实现快速重路由，减少链路或节点失效时对流量的影响，使流量实现快速恢复。公网静态路由FRR配置实例的组网图，如*图 4-6*所示。

图 4-6 公网静态路由 FRR 配置实例组网图



配置思路

1.在R1上打开公网静态路由备份路由计算开关。

2.配置作为主路由的静态路由。

3.配置作为备路由的静态路由，目的地址、掩码需与主路由一致，出接口需与主路由不同，优先级或metric需次于主路由。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#ip address 131.4.1.1 255.255.255.0
R1(config-if-gei-1/3)#exit
R1(config)#interface gei-1/5
R1(config-if-gei-1/5)#no shutdown
R1(config-if-gei-1/5)#ip address 55.1.1.1 255.255.255.0
R1(config-if-gei-1/5)#exit

R1(config)#ip route-static fast-reroute  /*开启FRR功能*/
R1(config)#ip route 2.2.2.50 255.255.255.255 131.4.1.2 metric 1
R1(config)#ip route 2.2.2.50 255.255.255.255 55.1.1.2 metric 10
/*配置两条静态路由不同的metric值*/
```

R3上的配置如下：

```
R3(config)#interface gei-1/3
R3(config-if-gei-1/3)#no shutdown
R3(config-if-gei-1/3)#ip address 131.4.1.2 255.255.255.0
R3(config-if-gei-1/3)#exit
R3(config)#interface gei-1/4
R3(config-if-gei-1/4)#no shutdown
R3(config-if-gei-1/4)#ip address 131.4.2.2 255.255.255.0
R3(config-if-gei-1/4)#exit

R3(config)#ip route 2.2.2.50 255.255.255.255 131.4.2.1
```

R2上的配置如下：

```
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#no shutdown
R2(config-if-gei-1/3)#ip address 131.4.2.1 255.255.255.0
R2(config-if-gei-1/3)#exit
R2(config)#interface gei-1/5
R2(config-if-gei-1/5)#no shutdown
R2(config-if-gei-1/5)#ip address 55.1.1.2 255.255.255.0
R2(config-if-gei-1/5)#exit
R2(config)#interface loopback50
R2(config-if-loopback50)#ip address 2.2.2.50 255.255.255.255
R2(config-if-loopback50)#exit
```

配置验证

FRR配置验证如下：

```
R1(config)#show ip forwarding route 2.2.2.50
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
   Dest          Gw         Interface       Owner    Pri Metric
*> 2.2.2.50/32   131.4.1.2  gei-1/3           Static   1   1

R1(config)#show ip forwarding backup route 2.2.2.50
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority,  M/S: Master/Slave,
```

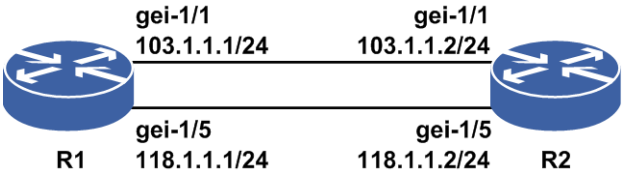
```
        Sta: Status;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
        MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
        ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
        GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
        GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best, M: Master, S: Slave, I: Inuse, U: Unuse;
   Dest         Gw        Interface     Owner    Pri Metric M/S Status
*> 2.2.2.50/32   131.4.1.2  gei-1/3       Static   1   1      M   I
*> 2.2.2.50/32   55.1.1.2   gei-1/5       Static   1   10     S   U
```

4.2.8 VRF 的静态路由 FRR 配置实例

配置说明

VRF的静态路由FRR配置实例组网如*图 4-7*所示。

图 4-7 VRF 的静态路由 FRR 配置实例组网图



配置思路

1.配置VRF

2.打开VPN网络的静态路由备份路由计算开关。

3.配置作为主路由的静态路由。

4.配置作为备路由的静态路由，目的地址、掩码需与主路由一致，出接口需与主路由不同，优先级或metric需次于主路由。

配置过程

R1上的配置如下：

```
R1(config)#ip vrf Inspur
R1(config-vrf-Inspur)#rd 1:100
R1(config-vrf-Inspur)#route-target both 1:100
R1(config-vrf-Inspur)#exit
R1(config-vrf-Inspur)#address-family ipv4
R1(config-vrf-Inspur-af-ipv4)#exit
R1(config-vrf-Inspur)#exit

R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ip vrf forwarding Inspur
R1(config-if-gei-1/1)#ip address 103.1.1.1 255.255.255.0
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/5
R1(config-if-gei-1/5)#no shutdown
```

```
R1(config-if-gei-1/5)#ip vrf forwarding Inspur
R1(config-if-gei-1/5)#ip address 118.1.1.1 255.255.255.0
R1(config-if-gei-1/5)#exit

R1(config)#ip route-static vrf Inspur fast-reroute
R1(config)#ip route vrf Inspur 2.2.2.50 255.255.255.255 103.1.1.2
R1(config)#ip route vrf Inspur 2.2.2.50 255.255.255.255 118.1.1.2 metric 10
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 103.1.1.2 255.255.255.0
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/5
R2(config-if-gei-1/5)#no shutdown
R2(config-if-gei-1/5)#ip address  118.1.1.2  255.255.255.0
R2(config-if-gei-1/5)#exit
R2(config)#interface loopback50
R2(config-if-loopback50)#ip address 2.2.2.50 255.255.255.255
R2(config-if-loopback50)#exit
```

配置验证

FRR配置验证如下：

```
R1(config)#show ip forwarding route vrf Inspur 2.2.2.50
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
   Dest         Gw        Interface      Owner      Pri Metric
*> 2.2.2.50/32   103.1.1.2  gei-1/1        Static     1   0

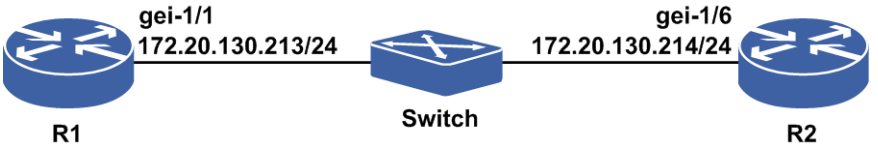
R1(config)#show ip forwarding backup route vrf Inspur 2.2.2.50
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority,  M/S: Master/Slave,
         Sta: Status;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best, M: Master, S: Slave, I: Inuse, U: Unuse;
   Dest         Gw         Interface      Owner     Pri Metric M/S Status
*> 2.2.2.50/32   103.1.1.2   gei-1/1        Static    1   0      M   I
*> 2.2.2.50/32   118.1.1.2   gei-1/5        Static    1   10     S   U
```

4.2.9 静态路由 BFD 配置实例

配置说明

如*图 4-8*所示，R1、R2之间运行静态路由协议，R1、R2配置静态路由BFD。

图 4-8 配置静态路由 BFD



配置思路

1.R1、R2配置静态路由。

2.R1、R2配置静态路由BFD。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 172.20.130.213 255.255.255.0
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 172.20.96.1 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#ip route 172.20.108.1 255.255.255.255 172.20.130.214 bfd enable
```

R2上的配置如下：

```
R2(config)#interface  gei-1/6
R2(config-if-gei-1/6)#ip address 172.20.130.214 255.255.255.0
R2(config-if-gei-1/6)#no shutdown
R2(config-if-gei-1/6)#exit
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 172.20.108.1 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#ip route 172.20.96.1 255.255.255.255 172.20.130.213 bfd enable
```

配置验证

正确配置后，静态路由 BFD会话应该能够成功建立，可以用如下命令查看结果：

用**show bfd neighbors [ip brief|ip detail]**来查看验证静态路由BFD是否生效。

R1上静态路由BFD生效情况查看：

```
R1(config)#show bfd neighbors ip brief
LocalAddr       PeerAddr          LD     RD     Hold    State   Interface
172.20.130.213   172.20.130.214     5      32     150     UP      gei-1/1

R1(config)#show bfd neighbors ip detail
------------------------------------------------------------------------------
-
LocalAddr: 172.20.130.213
PeerAddr : 172.20.130.214
Local Discr:2056          Remote Discr:2127          State:UP

Holdown(ms):150           Interface:---
Vpnid:0                 VRF Name:---
BFD Type:SingleHop
```

```
Instance Name:
------------------------------------------------------------------------------
Version:1               Dest UDP Port:4784       Final Bit:1
Local Diag:0            Demand Mode:0            Poll Bit:1
MinTxInt:50             MinRxInt:50              Multiplier:3
Received MinTxInt:50     Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24        Max BFD Length:24

Rx Count:0              Rx Interval (ms) min/max/avg:0     /0     /0
Tx Count:40             Tx Interval (ms) min/max/avg:48    /48    /46
Registered Protocols: STATIC
Uptime:0 day(s),0 hour(s),0 minute(s)
Control Plane Rcv Phy Interface Name: gei-1/1
==============================================================================
```

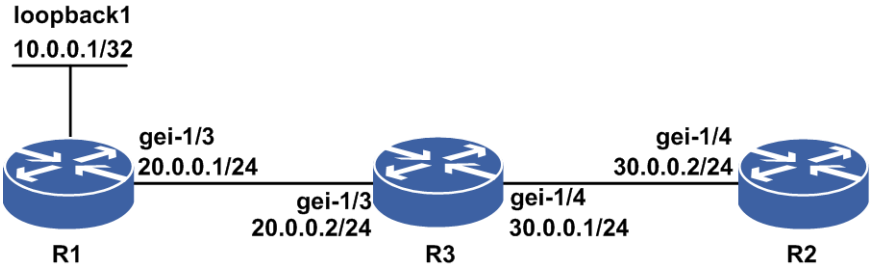
4.2.10 Loopback 提供静态多跳 BFD 的 local 地址配置实例

配置说明

配置静态路由私网路由公网下一跳带BFD检测，或者公网静态路由下一跳为非直连下一跳时，则创建BFD会话需要指定本端一个接口地址作为其local地址。该命令当前支持配置loopback接口来支持这个功能。若该接口没有地址或者没有配置该命令，则利用这个接口来创建BFD会话时将无法创建BFD会话。

如*图 4-9*所示，R1上loopback1的地址为10.0.0.1/32，gei-1/3地址为20.0.0.1/24；R3的gei-1/3地址为20.0.0.2/24，gei-1/4地址为30.0.0.1/24；R2的gei-1/4地址为30.0.0.2/24。

图 4-9 Loopback 提供静态多跳 BFD 的 local 地址配置实例



配置思路

1.在R1上配置静态路由，下一跳为R2的gei-1/4，并带BFD检测，欲在R1和R2之间创建一个BFD会话，检测该段链路，需要在R1上将链路打通。

2.在R3、R2上分别配置静态路由，在R2上利用BFD直接创建BFD会话。

配置过程

R1上的配置如下：

```
R1(config)#ip route 30.0.0.2 255.255.255.255 20.0.0.2
R1(config)#ip route 4.0.0.0 255.0.0.0 30.0.0.2 bfd enable /*非直连下一跳*/
R1(config)#ip route nexthop source loopback1
```

R2上的配置如下：

```
R2(config)#ip route 20.0.0.1 255.255.255.255 30.0.0.1
R2(config)#ip route 10.0.0.1 255.255.255.255 30.0.0.1
R2(config)#bfd
R2(config-bfd)#session 1 peer-bfd ipv4 30.0.0.2 10.0.0.1
```

R3上的配置如下：

```
R3(config)#ip route 10.0.0.1 255.255.255.255 20.0.0.1
```

配置验证

在R1上查看BFD会话：

```
R1(config)#show bfd neighbors ip brief
LocalAddr       PeerAddr        LD       RD       Hold   State  Interface
10.0.0.1        30.0.0.2        2049     0        0      UP     ----
```

在R2上查看BFD会话：

```
R2(config)#show bfd neighbors ip brief
LocalAddr       PeerAddr        LD       RD       Hold   State  Interface
30.0.0.2        10.0.0.1        2049     0        0      UP     ----
```

4.3 RIP

RIP是第一个实现动态选路的路由协议，是一种基于距离矢量（Distance-Vector）算法的协议。

RIP被设计用于使用同种技术的中小型网络，因此适用于大多数的校园网和使用速率变化不是很大的区域性网络。对于更复杂的网络环境，一般不建议使用RIP。

RIP包括RIPv1和RIPv2两个版本。

- RIPv1是有类别路由协议（Classful Routing Protocol），只支持以广播方式发布协议报文。RIPv1的每条消息包含1个命令（Command）、一个版本号（Version）以及一个或多个路由条目（最大25条）。
- RIPv2是一种无类别的路由协议（Classless Routing Protocol），消息格式的基本结构和RIPv1相同。

4.3.1 配置 RIP 基本功能

本节介绍RIP基本功能的配置步骤和命令。

1.启用RIP协议。

步骤	命令	功能
1	inspur(config)#**router rip**	启用RIP进程，进入RIP配置模式
2	inspur(config-rip)#**network** < *ip-address*>< *wildcard-mask*>	在指定网段使能RIP

2.调整RIP定时器。

步骤	命令	功能
1	inspur(config)#**router rip**	启用RIP进程，进入RIP配置模式
2	inspur(config-rip)#**timers basic** <*update*><*invalid*><*holddown*>< *flush*>	调整RIP网络计时器
3	inspur(config-rip)#**output-delay** < *packets*>< *delay*>	改变RIP更新发送的报文组间的延迟

<*update*>：更新发送间隔，单位：秒，范围1~65535，缺省为30秒。

<*invalid*>：路由宣布无效前的时间段单位：秒，范围1~65535，该值建议配置为update的3倍以上，缺省为180秒。从接收到某条路由的时刻开始计算，当invalid时间内没有该路由刷新时，路由无效，进入阻塞（holddown）状态，若holddown参数配置为0，则直接启动flush计时器。

<*holddown*>：抑制更佳路由信息时间段，单位：秒，范围0~65535，该值建议配置为update的3倍以上，缺省为180秒。当路由器接收到更新报，并获取路由不可达，或因为invalid计时器到期，路由无效，进入阻塞（holddown）状态，路由标为不可访问，并通告为不可达，但路由仍被用于转发报文分组。阻塞期过后，可以接受其它源通告的路由，路由又可被访问。

<*flush*>：从路由条目无效开始，到清除该路由须经过的时间段，单位：秒，范围1~65535，缺省为240秒。指定的时间值必须不小于holddown值，如果小于此值，就不能经过合适的阻塞期时间段，这将造成在阻塞期满前就接收新路由。

<*packets*>：报文的包个数，范围1~4294967295，缺省值为5。

<*delay*>：每发送完所定义的包数后，所间隔的时间，单位：毫秒，范围0~100，缺省值为100毫秒。

举例

配置RIP协议与时间相关的可选参数，具体配置如下：

```
inspur(config)#router rip
inspur(config-rip)#timers basic 5 15 15 30
inspur(config-rip)#output-delay 500 10
```

配置效果为：

·RIP更新发送的间隔为5秒

·路由宣布无效前等待的时间为15秒

·路由器进入阻塞状态后，等待的时间为15秒

·从路由条目无效开始，到清除该路由须等待的时间为30秒

·每发送500个报文，间隔10毫秒

4.3.2 配置 RIP 增强功能

本节介绍RIP增强功能的配置步骤和命令。

1.配置RIP邻居。

步骤	命令	功能
1	inspur(config)#**router rip**	进入RIP配置模式
2	inspur(config-rip)#**neighbor** <*ip-address*>	定义与本路由器交换路由信息的相邻路由器

在非广播链路上，需要配置该命令，目前最多可以同时发现或配置255个邻居。

此命令允许以点对点（非广播）的方式交换RIP路由信息。一旦指定了邻居，与该接口属于同一网络的接口不再以广播（组播）方式交换RIP路由信息。

2.配置RIP认证。

RIPv2支持明文认证和MD5认证。给接口设置密码，网络邻居必须在该网络上使用相同的认证方式和密码。RIPv1不支持认证。

RIP报文简单认证配置如下：

步骤	命令	功能
1	inspur(config-rip)#**interface** <*interface-name*>	进入接口配置模式
2	inspur(config-rip-if-interface-name)#**ip rip authentication mode text**	指定接口使用明文方式对RIP报文进行认证
3	inspur(config-rip-if-interface-name)#**ip rip authentication key** {**encrypted** <*key-encrypted*>|<*key-cleared*>}	指定可用于接口简单文本认证的密钥值，长度为1~16个字符，或以密文方式配置密钥，长度为1~24个字符

RIP报文MD5认证配置如下：

步骤	命令	功能
1	inspur(config-rip)#**interface** <*interface-name*>	进入接口配置模式
2	inspur(config-rip-if-interface-name)#**ip rip authentication mode md5**	指定接口使用MD5方式对RIP报文进行认证
3	inspur(config-rip-if-interface-name)#**ip rip authentication key-chain** <*key-id*><*key-string*>	为接口配置MD5认证时提供key-chain

3.配置水平分割和毒性逆转。

步骤	命令	功能
1	inspur(config-rip)#**interface** <*interface-name*>	进入接口配置模式
2	inspur(config-rip-if-interface-name)#**ip split-horizon**	使水平分割机制有效，缺省为有效
3	inspur(config-rip-if-interface-name)#**ip poison-reverse**	使毒性逆转机制有效，缺省为有效

一般不推荐改变水平分割命令的缺省状态。除非为了正确通告路由，而必须在应用系统中改变缺省状态。如果串行接口（且接口与分组交换网络连接）上的水平分割无效，则必须使网络上相关的所有路由器和访问服务器的水平分割无效。

4.配置路由重分发。

从一个路由域向RIP路由域再分配路由的配置步骤如下：

步骤	命令	功能
1	inspur(config)#**router rip**	进入RIP配置模式
2	inspur(config-rip)#**redistribute** <*protocol*>[<*process-id*>][**metric** <*metric-value*>][**route-map** <*name*>]	重分配其它路由协议的路由到RIP中

[<*process-id*>]：实例号，在重分配OSPF或者ISIS路由时需要配置实例号。配置范围，OSPF：1~65535，ISIS：0~65535。如果不配置，缺省为0。

<*protocol*>：路由再分配的源路由协议，可以是以下关键词：ospf-ext，ospf-int，static，bgp-ext，bgp-int，connected，isis-1，isis-2，isis-1-2，nat，natpt，subscriber-host，subscriber-aggregation，ps-busi-addr，ps-user-addr等。

metric <*metric-value*>：指定以多大的路由权值引入路由，如果不指定，则按缺省路由权（default-metric）引入，范围1~16。

route-map <*map-tag*>：用于再分配的路由映射名称，长度为1~31个字符。

5.配置RIP BFD。

i.使能某个实例下的BFD。

命令	功能
inspur(config-rip)#**bfd**	打开RIP实例下所有接口的BFD功能开关

ii.使能某个接口下的BFD。

步骤	命令	功能
1	inspur(config-rip)#**interface**	进入接口配置模式

步骤	命令	功能
	<*interface-name*>	
2	inspur(config-rip-if-interface-name)#**ip rip bfd**{ **enable** | **disable** }	使能或者去使能此接口上BFD检测功能

RIP BFD是在两个RIP邻居之间进行的BFD双向检测。

ip rip bfd与RIP协议配置模式及RIP协议VRF配置模式下的bfd命令配合使用。如果未配置**ip rip bfd**命令，RIP接口上的BFD使能状态以RIP实例下的BFD使能状态为准；如果配置了**ip rip bfd**命令，RIP接口上的BFD使能状态以该接口上的BFD使能状态为准。

另外是否创建BFD会话，以是否发现邻居为准，若未接收到对端发送的路由，就不能将对方加为邻居，即没有自动发现的邻居，则无法在本RIP的接口和邻居之间创建BFD会话。

若接口disable，或者删除发现的邻居，则会发送BFD session Remove的信息给BFD server。若RIP不再关联BFD检测，则会发送BFD admin down的信息给BFD server，BFD server 再将该信息通知给BFD会话的另外一端。

4.3.3 配置 RIP 版本

本节介绍RIP版本的配置步骤和命令。

1.指定接收或发送的RIP的版本。

步骤	命令	功能
1	inspur(config)#**router rip**	进入RIP配置模式
2	inspur(config-rip)#**version** {**1**|**2**}	配置RIPv1或RIPv2，缺省为RIPv2

2.设置接口可接收或发送的RIP的版本。

如果针对接口设置可接收或发送的RIP的版本，则可忽略由**version**命令指定的RIP缺省状态。

步骤	命令	功能
1	inspur(config-rip)#**interface** <*interface-name*>	进入接口配置模式
2	inspur(config-rip-if-interface-name)#**ip rip receive version** {**1** | **2**}	指定接口可以接收的RIP版本为RIPv1或RIPv2，如果未配置**version**命令，则使用默认值，即接收版本1和2

步骤	命令	功能
3	inspur(config-rip-if-interface-name)#**ip rip send version** {1 | 2 {**broadcast** | **multicast**}}	指定接口可以发送的RIP版本为RIPv1或RIPv2

1：接口上仅发送RIP版本1的包。

2：接口上仅发送RIP版本2的包，此时可以选择broadcast或multicast方式。

broadcast：在发送版本为2的前提下，可以通过广播地址发送该报文。

multicast：在发送版本为2的前提下，可以通过组播地址发送该报文。

4.3.4 配置 RIP 路由负荷分担

本节介绍RIP路由负荷分担的配置步骤和命令。

相关信息

路由负荷分担有两个主要的功能：

- 提高链路可靠性：网络的传输层对稳定性和可靠性要求很高。这种可靠性表现在除了链路本身可靠外还应表现在当某条链路出现故障的时候不影响其他路径上的报文转发或者减少转发失败的影响。
- 提高带宽：路由负荷分担功能使得路由器能够将流量分配到多条路径上，从而充分利用带宽资源。通过路由协议或静态配置，可以使得转发表中，对于同一个目的地址，有多条可用的路由条目。

负荷分担的转发机制支持两种方法，per-packet （逐包模式）和 per-destination（逐流模式），下表给出了这两种方法的优缺点。

模式	优点	缺点
逐流模式	到给定目的的包可以保证走同一条路径，即使在有多条可用路径的情况下；到不同目的的包可以走不同的路径。	当流量中只有少量的目的地址时，可能会引起流量集中在少数路径上，分担不均衡；当流量中目的地址增加时，负荷分担会更有效。
逐包模式	路径利用率高，因为per-packet 使用轮转法来确定数据包走的路径，使得转发负荷均匀地分布在各条路径上。	对于到给定目的的流量可能会选择不同的路径，造成接收端的排序，对于VoIP和其他要求有序的流量不适用。

1.配置RIP支持路由负荷分担。

步骤	命令	功能
1	inspur(config)#**router rip**	进入RIP路由配置模式。
2	inspur(config-rip)#**maximum-paths** <*number*>	配置协议支持负荷分担的路由数目，范围1~32，缺省为1。

2.配置接口负荷分担。

步骤	命令	功能
1	inspur(config)#**interface** < *interface-name*>	进入接口配置模式。
2	inspur(config-if-interface-name)#**ip load-sharing** {**per-destination** | **per-packet**}	配置接口负荷分担模式：负荷分担是在出接口上配置的，默认情况下为**per-destination**。只有所有的接口配置为**per-packet**模式，负荷分担的模式才是**per-packet**。
3	inspur(config-if-interface-name)#**load-sharing bandwidth** < *bandwidth-value*>	配置接口负荷分担的权重：权重设置在出接口上，只有配置了优先级后，配置的权重才有效；权重范围不同的接口大小值不同。

4.3.5 验证及维护 RIP

验证RIP配置结果

IR12000提供了以下命令查看RIP相关信息：

命令	功能
inspur(config)#**show ip rip** [**vrf** <*vrf-name*>]	显示RIP运行的基本信息
inspur(config)#**show ip rip interface** [**vrf** <*vrf-name*>]<*interface-name*>	查看RIP接口的现行配置和状态
inspur(config)#**show ip rip database** [**vrf** <*vrf-name*>][**network** <*ip-address*>[**mask** <*net-mask*>]]	显示由RIP协议产生的路由条目
inspur(config)#**show ip rip networks** [**vrf** <*vrf-name*>]	显示用户命令配置的所有RIP接口信息
inspur(config)#**show ip rip neighbors** [**vrf** <*vrf-name*>]	显示RIP邻居信息

维护RIP

IR12000提供了debug命令对RIP协议进行调试，来跟踪相关信息：

命令	功能
inspur#**debug ip rip**	跟踪RIP的基本收发包过程
inspur#**debug ip rip all**	打开所有RIP调试信息的开关

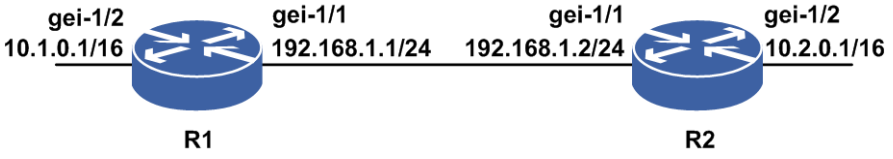
命令	功能
inspur#**debug ip rip events**	跟踪和RIP有关的事件
inspur#**debug ip rip database**	跟踪RIP路由表的变化过程
inspur#**debug ip rip trigger**	跟踪RIP触发事件

4.3.6 RIP 基本配置实例

配置说明

作为实现原理和配置方法都比较简单的RIP路由协议，主要都应用在比较简单的组网环境中。*图 4-10*为RIP的典型组网图，下面以该图说明RIP协议的基本配置，要求在R1和R2上运行RIP。

图 4-10 RIP 配置实例拓扑图



配置思路

1.配置接口IP地址。

2.配置RIP协议。

3.在接口上启用RIP协议相关配置。

4.测试配置结果，确认两台设备已正确建立邻居，从两个设备上分别能够学到对端通告路由。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 192.168.1.1 255.255.255.0
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip address 10.1.0.1 255.255.0.0
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#exit
R1(config)#router rip
R1(config-rip)#network 192.168.1.0 0.0.0.255
R1(config-rip)#network 10.1.0.0 0.0.255.255
R1(config-rip)#neighbor 192.168.1.2
R1(config-rip)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 192.168.1.2 255.255.255.0
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 10.2.0.1 255.255.0.0
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#exit
R2(config)#router rip
R2(config-rip)#network 192.168.1.0 0.0.0.255
R2(config-rip)#network 10.2.0.0 0.0.255.255
R2(config-rip)#neighbor 192.168.1.1
R2(config-rip)#end
```

配置验证

上述的配置完成以后，在两端的设备上应该能够看到如下的信息，表明双方已经正确建立邻居，并且都能学到和ping通对端的接口路由，说明配置成功。

R1上的配置验证：用**show running-config rip**命令查看RIP的配置是否正确。

```
R1(config-rip)#show running-config rip
!<rip>
router rip
  neighbor 192.168.1.2
  network 192.168.1.0 0.0.0.255
  network 10.1.0.0 0.0.255.255
$
!</rip>

R1(config)#show ip rip database
Routes of rip:
h : is possibly down,in holddown time
f : out holddown time before flush

    Dest           Metric    RtPrf  InstanceID  Time         From
 *> 10.0.0.0/8       2         120     0        00:00:12     192.168.1.2
 *  10.0.0.0/8       1         254     0        00:00:29     0.0.0.0
 *> 10.1.0.0/16      0          0      0        00:00:00     0.0.0.0
 *> 192.168.1.0/24   0          0      0        00:00:00     0.0.0.0

R1(config)#show ip rip neighbors
  neighbor address                interface
  192.168.1.2                     gei-1/1
```

R2上的配置验证：用**show running-config rip**命令查看RIP的配置是否正确。

```
R2(config)#show running-config rip
!<rip>
router rip
  neighbor 192.168.1.1
  network 192.168.1.0 0.0.0.255
  network 10.2.0.0 0.0.255.255
$
!</rip>

R2(config)#show ip rip database
Routes of rip:
h : is possibly down,in holddown time
f : out holddown time before flush

    Dest           Metric     RtPrf  InstanceID  Time         From
 *> 10.0.0.0/8       1         254     0        00:00:03     0.0.0.0
 *> 10.2.0.0/16      0          0      0        00:00:00     0.0.0.0
 *> 192.168.1.0/24    0         0      0        00:00:00     0.0.0.0
```

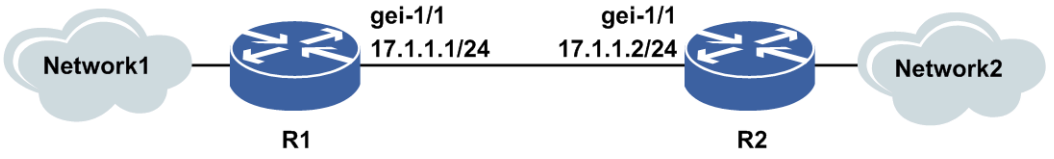
```
R2(config)#show ip rip neighbors
  neighbor address                  interface
  192.168.1.1                      gei-1/1
```

4.3.7 RIP 路由汇总配置实例

配置说明

版本v2的RIP路由支持路由汇总，因为RIP-2报文携带掩码位，所以支持子网划分。如*图 4-11*所示，路由器R1和R2直连，在R1上实现路由汇总。

图 4-11 RIP 路由汇总配置实例示意图



配置思路

1.按*图 4-120*所示搭建网络，配置IP地址。

2.在R1上配置RIP路由及路由汇总。

3.在R2上和R1直连的接口启用RIP协议。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface loopback2
R1(config-if-loopback2)#ip address 1.1.1.2 255.255.255.255
R1(config-if-loopback2)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 17.1.1.1 255.255.255.0
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#router rip   /*配置rip*/
R1(config-rip)#network 17.1.1.0 0.0.0.255
R1(config-rip)#network 1.1.1.1 0.0.0.0
R1(config-rip)#network 1.1.1.2 0.0.0.0
R1(config-rip)#interface gei-1/1
R1(config-rip-if-gei-1/1)#ip rip send version 2 multicast
R1(config-rip-if-gei-1/1)#exit
R1(config-rip)#auto-summary   /*配置聚合*/
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 17.1.1.2 255.255.255.0
```

```
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#router rip   /*配置rip*/
R2(config-rip)#network 17.1.1.0 0.0.0.255
R2(config-rip)#interface gei-1/1
R2(config-rip-if-gei-1/1)#ip rip send version 2 multicast
```

配置验证

下面是用**show**命令验证配置的结果。

在R1上查看配置结果：

```
R1(config)#show ip rip databas
Routes of rip:
h : is possibly down,in holddown time
f : out holddown time before flush

   Dest           Metric     RtPrf    InstanceID   Time         From
 *> 1.0.0.0/8       1          254       0          00:00:13     0.0.0.0
 *> 1.1.1.1/32      0          0         0          00:00:00     0.0.0.0
 *> 1.1.1.2/32      0          0         0          00:00:00     0.0.0.0
 *> 17.0.0.0/8      1          254       0          00:00:21     0.0.0.0
 *> 17.1.1.0/24     0          0         0          00:00:00     0.0.0.0
```

在R2上查看配置结果：

```
R2(config)#show ip rip database
Routes of rip:
h : is possibly down,in holddown time
f : out holddown time before flush

   Dest           Metric     RtPrf    InstanceID  Time         From
 *> 1.0.0.0/8       2          120       0          00:00:16     7.1.1.1
 *> 17.0.0.0/8      1          254       0          00:00:20     0.0.0.0
 *> 17.1.1.0/24     0          0         0          00:00:00     0.0.0.0
```

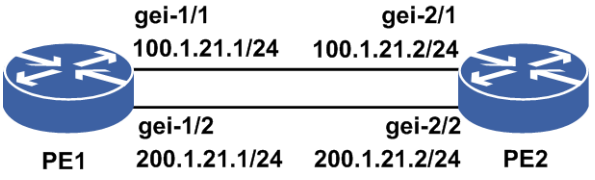
R1上聚合成自然网段的路由，R2上学习到了。

4.3.8 RIP 路由负荷分担配置实例

配置说明

负荷分担可使超出单个接口带宽的流量均分到多条链路上，实现流量在各条链路上的负载均衡。在如*图 4-12*所示的网络中，要用RIP路由的负荷分担实现负载均衡。

图 4-12 RIP 路由负荷分担组网图



配置思路

1.配置接口地址， PE2路由器上配置一个loopback 1.1.1.2/32。

2.PE1和PE2上启用RIP协议，通告各接口地址，并配置**maxinum-paths**，使负荷分担生效。

3.可以更改负荷分担方式即逐包或者逐流。

配置过程

PE1上的配置如下：

```
PE1(config)#interface gei-0/1
PE1(config-if-gei-0/1)#ip address 100.1.21.1 255.255.255.0
PE1(config-if-gei-0/1)#no shutdown
PE1(config-if-gei-0/1)#exit
PE1(config)#interface gei-0/2
PE1(config-if-gei-0/2)#ip address 200.1.21.1 255.255.255.0
PE1(config-if-gei-0/2)#no shutdown
PE1(config-if-gei-0/2)#exit

PE1(config)#router rip
PE1(config-rip)#network 100.1.21.0 0.0.0.255
PE1(config-rip)#network 200.1.21.0 0.0.0.255
PE1(config-rip)#maximum-paths 2     /*负荷分担支持路由数目为2*/
PE1(config-rip)#exit
```

PE2上的配置如下：

```
PE2(config)#interface gei-2/1
PE2(config-if-gei-2/1)#ip address 100.1.21.2 255.255.255.0
PE2(config-if-gei-2/1)#no shutdown
PE2(config-if-gei-2/1)#exit
PE2(config)#interface gei-2/2
PE2(config-if-gei-2/2)#ip address 200.1.21.2 255.255.255.0
PE2(config-if-gei-2/2)#no shutdown
PE2(config-if-gei-2/2)#exit
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 1.1.1.2  255.255.255.255
PE2(config-if-loopback1)#exit

PE2(config)#router rip
PE2(config-rip)#network 100.1.21.0 0.0.0.255
PE2(config-rip)#network 200.1.21.0 0.0.0.255
PE2(config-rip)#network 1.1.1.2  0.0.0.0
PE2(config-rip)#maximum-paths 2     /*负荷分担支持路由数目为2*/
PE2(config-rip)#exit
```

配置验证

用**show ip forwarding route**命令验证配置结果：

```
R1#show ip forwarding route rip
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
```

```
   Dest          Gw           Interface      Owner   Pri  Metric
*> 1.1.1.2/32    100.1.21.2    gei-0/1        RIP     120   2
*> 1.1.1.2/32    200.1.21.2    gei-0/2        RIP     120   2
```

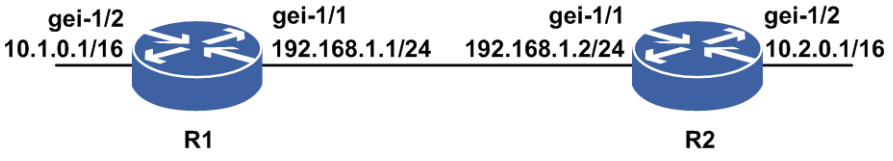
可以看到，到达目的地1.1.1.2/32有两个下一跳，不同的出接口，负载均衡配置成功。

4.3.9 RIP BFD 配置实例

配置说明

如*图 4-13*所示组网，举例BFD关联RIP的配置。

图 4-13 BFD 关联 RIP 配置实例拓扑图



配置思路

1.配置接口IP地址。

2.配置RIP协议。

3.在接口上启用RIP协议相关配置。

4.测试配置结果，确认两台设备已正确建立邻居，从两个设备上分别能够学到对端通告路由。

5.在RIP模式下使能BFD。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 192.168.1.1 255.255.255.0
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip address 10.1.0.1 255.255.255.0
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#exit
R1(config)#router rip
R1(config-rip)#network 192.168.1.0 0.0.0.255
R1(config-rip)#network 10.1.0.0 0.0.0.255
R1(config-rip)#bfd
R1(config-rip)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 192.168.1.2 255.255.255.0
R2(config-if-gei-1/1)#no shutdown
```

```
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 10.2.0.1 255.255.255.0
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#exit
R2(config)#router rip
R2(config-rip)#network 192.168.1.0 0.0.0.255
R2(config-rip)#network 10.2.0.0 0.0.0.255
R2(config-rip)#bfd
R2(config-rip)#end
```

配置验证

上述的配置完成以后，在两端的设备上应该能够看到如下的信息，表明双方已经正确建立邻居，并且都能学到和ping通对端的接口路由，说明配置成功。

R1上的配置验证：用**show running-config rip**命令查看RIP的配置是否正确。

```
R1(config-rip)#show running-config rip
!<rip>
router rip
  bfd
  network 192.168.1.0 0.0.0.255
  network 10.1.0.0 0.0.0.255
$
! </rip>

R1(config)#show ip rip database
Routes of rip:
h : is possibly down,in holddown time
f : out holddown time before flush

      Dest          Metric    RtPrf  InstanceID  Time        From
 *> 10.0.0.0/8        2        120     0      00:00:12     192.168.1.2
 *  10.1.0.0/24       1         254     0      00:00:29     0.0.0.0
 *> 192.0.0.0/8       0         0       0      00:00:00     0.0.0.0
 *> 192.168.1.0/24    0         0       0      00:00:00     0.0.0.0

R1(config)#show ip rip neighbors
  neighbor address                interface
  192.168.1.2                    gei-1/1

R1(config)#show bfd neighbors ip brief
LocalAddr      PeerAddr       LD       RD       Hold   State     Interface
192.168.1.1    192.168.1.2      2052     2053     150    UP       gei-1/1

R1(config)#show bfd neighbors ip detail
------------------------------------------------------------------------------
--
LocalAddr: 192.168.1.1
PeerAddr : 192.168.1.2
Local Discr:2052          Remote Discr:2053          State:UP
Holdown(ms):150           Interface:gei-1/1
Vpnid:0                  VRF Name:---
BFD Type:SingleHop
Instance Name:
------------------------------------------------------------------------------
--
Version:1               Dest UDP Port:3784       Final Bit:1
Local Diag:0            Demand Mode:0            Poll Bit:0
MinTxInt:50             MinRxInt:50              Multiplier:3
Received MinTxInt:50     Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24        Max BFD Length:24

Rx Count:2381           Rx Interval (ms) min/max/avg:30    /110   /59
```

```
Tx Count:1939           Tx Interval (ms) min/max/avg:40    /100   /40
Registered Protocols:RIP
Uptime:0 day(s),0 hour(s),3 minute(s)
Control Plane Rcv Phy Interface Name:gei-1/1
================================================================================
==
```

R2上的配置验证：用**show running-config rip**命令查看RIP的配置是否正确。

```
R2(config)#show running-config rip
!<rip>
router rip
  bfd
  network 192.168.1.0 0.0.0.255
  network 10.2.0.0 0.0.0.255
$
! </rip>

R2(config)#show ip rip database
Routes of rip:
h : is possibly down,in holddown time
f : out holddown time before flush

      Dest           Metric     RtPrf  InstanceID  Time         From
 *> 10.0.0.0/8         1         254     0        00:00:03     0.0.0.0
 *> 10.2.0.0/24        0         0       0        00:00:00     0.0.0.0
 *> 192.168.1.0/24     0         0       0        00:00:00     0.0.0.0

R2(config)#show ip rip neighbors
  neighbor address                  interface
  192.168.1.1                      gei-1/1

R2(config-rip)#show bfd neighbors ip brief
LocalAddr      PeerAddr       LD       RD       Hold   State     Interface
192.168.1.2    192.168.1.1      2053     2052     150    UP        gei-1/1

R2(config)#show bfd neighbors ip detail
--------------------------------------------------------------------------------
LocalAddr: 192.168.1.2
PeerAddr : 192.168.1.1
Local Discr:2053          Remote Discr:2052          State:UP
Holdown(ms):150           Interface:gei-1/1
Vpnid:0                  VRF Name:---
BFD Type:SingleHop
Instance Name:
--------------------------------------------------------------------------------
Version:1                Dest UDP Port:3784        Final Bit:1
Local Diag:0             Demand Mode:0             Poll Bit:0
MinTxInt:50              MinRxInt:50               Multiplier:3
Received MinTxInt:50      Received MinRxInt:50      Received Multiplier:3
Length:24                Min Echo Interval:0
Min BFD Length:24         Max BFD Length:24

Rx Count:3207            Rx Interval (ms) min/max/avg:0     /100   /39
Tx Count:2989            Tx Interval (ms) min/max/avg:50    /100   /59
Registered Protocols:RIP
Uptime:0 day(s),0 hour(s),5 minute(s)
Control Plane Rcv Phy Interface Name:gei-1/1
================================================================================
```

4.4 OSPF

OSPF协议是IETF开发的一个基于链路状态的自治系统内部路由协议（IGP），用于在单一AS（Autonomous system，自治系统）内决策路由。

在IP网络上，OSPF通过收集和传递自治系统的链路状态来动态地发现并传播路由。OSPF路由设备与相连的其它OSPF路由设备建立邻居关系，同步双方的链路状态数据库，得到LSDB，最后运行SPF算法计算得到OSPF路由。

OSPF将不同的网络拓扑抽象为四种类型：

·Stub Networks：接口所连的网段中只有路由设备自己。

·P2P（Point-to-point）：接口通过点到点的网络与路由设备相连。

·Broadcast or NBMA Networks：接口通过广播或NBMA网络与多台路由器相连。

·P2MP（Point-to-multipoint）：接口通过点到多点的网络与多台路由器相连。

当网络规模日益扩大，网络中的路由设备数量不断增加时且都运行OSPF路由协议时，会遇到许多问题。OSPF通过划分区域（Area）来减少庞大的LSA数量、屏蔽网络变化波及的范围、减少LSDB同步的时间以及减轻CPU负荷和网络带宽压力。

OSPF如果被划分成多个区域，则必须有一个区域是骨干区域，且保证其它区域与骨干区域直接相连或逻辑上相连，并且骨干区域自身也必须是连通的。

OSPF根据路由设备在区域中的不同位置，将设备分为四种类型。

·区域内路由器（IAR），所有接口都属于同一个OSPF区域。

·区域边界路由器（ABR），属于两个以上的区域且其中一个必须是骨干区域。

·骨干路由器（BBR），至少有一个接口属于骨干区域。

·自治系统边界路由器（ASBR），与其它AS区域交换路由信息的路由器称为ASBR。只要一台OSPF路由器引入了外部的路由信息，该OSPF路由器就是ASBR。

4.4.1 配置 OSPF 基本功能

本节介绍OSPF基本功能的配置步骤和命令。

1.启动OSPF。

在路由器上启动OSPF进程，使得路由器之间能通过OSPF协议学习到路由。

步骤	命令	功能
1	inspur(config)#**router ospf** <*process-id*>[**vrf** <*vrf-name*>]	启动OSPF进程，运行OSPF协议，并进入OSPF协议配置模式
2	inspur(config-ospf-process-id)#**area** <*area-id*>	创建区域
3	inspur(config-ospf-process-id-area-id)#**network** <*ip-address*><*wildcard-mask*>	定义OSPF协议运行的接口

协议启动后，将会自动从当前的接口中选择一个作为OSPF协议的Router-ID地址。路由器上没有接口有IP地址时，将会选不到Router-ID，可以通过配置一个接口地址让OSPF动态获取或者手动配置Router-ID并重启OSPF的进程。

2.配置路由器的Router-ID。

配置路由器的Router-ID，在路由器重启或该OSPF进程手工重启后生效。

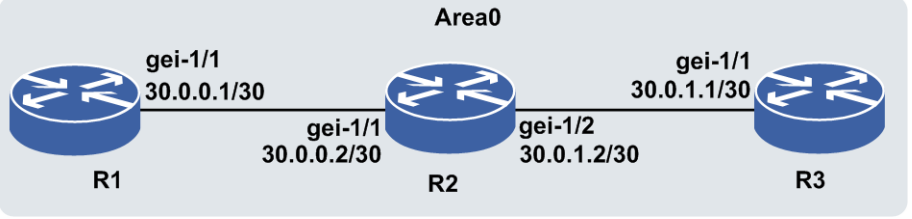
步骤	命令	功能
1	inspur(config-ospf-process-id)#**router-id** <*ip-address*>	配置路由器的Router-ID 建议使用loopback地址作为路由器的Router-ID
2	inspur(config-ospf-process-id)#**end**	返回到特权模式
3	inspur#**clear ip ospf process** <*process-id*>	重新启动OSPF进程

举例

如*图 4-14*所示，要在R1、R2和R3接口上配置启动OSPF，各个设备的Router-ID如下：

设备	Router-ID
R1	1.1.1.2
R2	1.1.1.3
R3	1.1.1.4

图 4-14 *OSPF 基本配置实例*



R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 30.0.0.1 255.255.255.252
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#router ospf 10
R1(config-ospf-10)#area 0
R1(config-ospf-10-area-0)#network 30.0.0.0 0.0.0.3
R1(config-ospf-10-area-0)#exit
```

此时查看OSPF的信息：

```
R1(config)#show ip ospf 10
OSPF 10 Router ID 30.0.0.1 enable
 Domain ID type 0x5,value 0.0.0.10
 Enabled for 00:00:51,Debug on
 Number of areas 1, Normal 1, Stub 0, NSSA 0
 Number of interfaces 1
……
    Area 0.0.0.0 enable (Demand circuit available)
       Enabled for 00:00:28
       Area has no authentication
       Times spf has been run 0
       Number of interfaces 1. Up 0
```

至此，R1中OSPF基本配置已完成，OSPF进程成功启动，此时的Router-ID为OSPF进

程所选的gei-1/1接口地址。

配置R2，以loopback地址建立OSPF连接，必须配置一个loopback地址，再启动OSPF进程，配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.3 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 30.0.0.2 255.255.255.252
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 30.0.1.2 255.255.255.252
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#exit
R2(config)#router ospf 10
R2(config-ospf-10)#area 0
R2(config-ospf-10-area-0)#network 30.0.0.0 0.0.0.3
R2(config-ospf-10-area-0)#network 30.0.1.0 0.0.0.3
R2(config-ospf-10-area-0)#exit
```

查看OSPF信息，此时可看到OSPF自动选取了loopback1的地址作为Router-ID。

```
R2(config)#sho ip ospf 10
OSPF 10 Router ID 1.1.1.3 enable
Domain ID type 0x5,value 0.0.0.10
 Enabled for 00:02:42,Debug on
Number of areas 1, Normal 1, Stub 0, NSSA 0
Number of interfaces 2
```

R3上的配置如下：

```
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 1.1.1.4 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-1/2
R3(config-if-gei-1/2)#ip address 30.0.1.1 255.255.255.252
R3(config-if-gei-1/2)#no shutdown
R3(config-if-gei-1/2)#exit
R3(config)#router ospf 10
R3(config-ospf-10)#area 0
R3(config-ospf-10-area-0)#network 30.0.1.0 0.0.0.3
R3(config-ospf-10-area-0)#exit
```

在R3上查看协议表，如下：

```
R3(config)#show ip protocol routing
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
  GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale
 Dest  NextHopRoutePrf
*> 1.1.1.4/32   1.1.1.40           0            Address
* 1.1.1.4/32    1.1.1.4 0          0              Direct
*> 30.0.0.0/30  30.0.1.2    110          2             OSPF
*> 30.0.1.0/30  30.0.1.1    00             Direct
* 30.0.1.0/30   30.0.1.0    110          1             OSPF
*> 30.0.1.1/32  30.0.1.1    0            0             Address
```

此时R3能ping通R1，说明路由正常，OSPF运行正常。

4.4.2 配置 OSPF 接口属性

本节介绍OSPF接口属性的配置步骤和命令。

1.进入OSPF接口配置模式。

步骤	命令	功能
1	inspur(config)#**router ospf** <*process-id*>[**vrf** <*vrf-name*>]	进入OSPF配置模式
2	inspur(config-ospf-process-id)#**interface** <*interface-name*>	进入接口配置模式

2.配置OSPF接口属性。

通过修改OSPF接口的各种属性，使得OSPF能成功建立起邻居关系。不同厂商设备对接时，通常要修改这些属性。

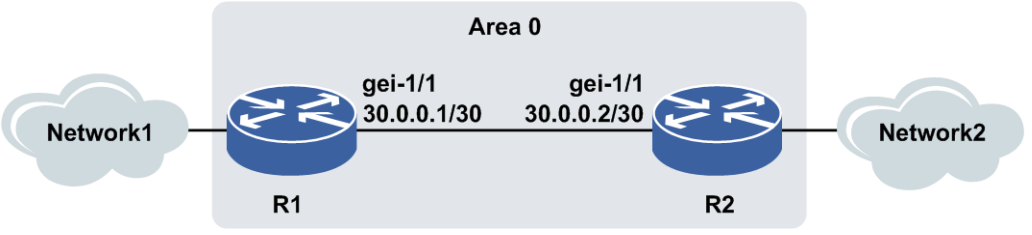
命令	功能
inspur(config-ospfv-process-id-if-interface-name)#**hello-interval** <*seconds*>	指定接口发送HELLO报文的时间间隔，单位：秒，范围1~65535，缺省为10秒
inspur(config-ospf-process-id-if-interface-name)#**dead-interval** <*seconds*>	指定接口上邻居的死亡时间，单位：秒，范围1~65535，缺省为40秒
inspur(config-ospf-process-id-if-interface-name)#**retransmit-interval** <*seconds*>	指定接口重传LSA的时间间隔，单位：秒，范围1~65535，缺省为5秒
inspur(config-ospf-process-id-if-interface-name)#**transmit-delay** <*seconds*>	指定接口传输一个链路状态更新数据包的迟延，单位：秒，范围1~65535，缺省为1秒
inspur(config-ospf-process-id-if-interface-name)#**cost** <*cost*>	设置接口开销，范围1~65535，缺省为100M/接口带宽，接口metric=65535的route lsa不参与路由计算
inspur(config-ospf-process-id-if-interface-name)#**priority** <*priority*>	设置接口优先级，范围0~255，缺省为1
inspur(config-ospf-process-id-if-interface-name)#**network** <*network type*>	设置接口类型，类型包括broadcast，non-broadcast，point-to-multipoint，point-to-point，缺省类型为广播
inspur(config-ospf-process-id-if-interface-name)#**mtu-ignore**	设置接口在接收到DD报文时忽略MTU字段的检查
inspur(config-ospf-process-id-if-interface-name)#**ttl-security hops** <*hops*>	设置ospf接口的邻居TTL跳数，确保接收到的报文不是非法报文，范围为1~254
inspur(config-ospf-process-id-if-interface-name)#**mpls ldp sync** [**disable**]	设置接口多协议标签交换参数

举例

如*图 4-15*所示，要在R1、R2运行OSPF的接口上改变OSPF的默认参数，各个设备的Router-ID如下：

设备	Router-ID
R1	1.1.1.2
R2	1.1.1.3

图 4-15 OSPF 接口属性配置



在R1和R2上启动OSPF协议，并通告网段。

在R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 30.0.0.1 255.255.255.252
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#router ospf 10
R1(config-ospf-10)#area 0
R1(config-ospf-10-area-0)#network 30.0.0.0 0.0.0.3
R1(config-ospf-10-area-0)#exit
```

在R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.3 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 30.0.0.2 255.255.255.252
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#router ospf 10
R2(config-ospf-10)#area 0
R2(config-ospf-10-area-0)#network 30.0.0.0 0.0.0.3
R2(config-ospf-10-area-0)#exit
```

在接口上改变OSPF的默认属性。

在R1上的配置如下：

```
R1(config)#router ospf 10
R1(config-ospf-10)#interface gei-1/1
R1(config-ospf-10-if-gei-1/1)#hello-interval 20
/*指定接口发送HELLO报文的时间间隔为20秒*/
R1(config-ospf-10-if-gei-1/1)#dead-interval 80
/*指定接口上邻居的死亡时间为80秒*/
R1(config-ospf-10-if-gei-1/1)#retransmit-interval 10
/*指定接口重传LSA的时间间隔为10秒*/
R1(config-ospf-10-if-gei-1/1)#transmit-delay 2
/*指定接口传输一个链路状态更新数据包的迟延为2秒*/
R1(config-ospf-10-if-gei-1/1)#cost 10
```

```
/*指定接口OSPF的开销为10*/
R1(config-ospf-10-if-gei-1/1)#priority 10
/*设置接口优先级为10*/
R1(config-ospf-10-if-gei-1/1)#network point-to-point
/*设置接口类型为点到点*/
R1(config-ospf-10-if-gei-1/1)#mtu-ignore
/*接收DD报文时忽略接口的MTU值检查*/
R1(config-ospf-10-if-gei-1/1)#ttl-security hops 1
/*设置接口安全的跳数为1*/
R1(config-ospf-10-if-gei-1/1)#mpls ldp sync
/*设置接口多协议标签交换参数，保证标签分发协议的同步*/
```

4.4.3 配置 OSPF 认证

为了增强网络上路由进程的安全性，可以在路由器上配置OSPF认证。

1.配置OSPF区域认证。

步骤	命令	功能
1	inspur(config)#**router ospf** <*process-id*>[**vrf** <*vrf-name*>]	进入OSPF路由模式
2	inspur(config-ospf-process-id)#**area** <*area-id*>	创建OSPF区域
3	inspur(config-ospf-process-id-area-id)#**authentication** [**message-digest**]	在OSPF区域上开启认证功能

2.配置OSPF接口认证。

给接口设置密码，OSPF的邻居必须在该网络上使用相同的密码。

步骤	命令	功能
1	inspur(config-oospf-process-id)#**interface** <*interface-name*>	进入接口配置模式
2	inspur(config-ospf-process-id-if-interface-name)#**authentication** [**null**|**message-digest**]	为接口配置认证方式
3	inspur(config-ospf-process-id-if-interface-name)#**authentication-key** [**encrypted**]<*password*>	为简单口令认证类型的接口设置口令
	inspur(config-ospf-process-id-if-interface-name)#**message-digest-key** <*keyid*> **md5** {<*password*>| **encrypted**< *password*>|[**delay** <*time*>]	为采用报文摘要口令认证类型的接口设置口令序号和认证口令

<*keyid*>：口令序号，为1~255之间的整数。

md5 <*password*>：认证口令，长度为1~16个字符（不包含空格）。

delay <*time*>：延迟时间，单位：分钟，范围0~100000。

encypted：对设置的口令进行加密。

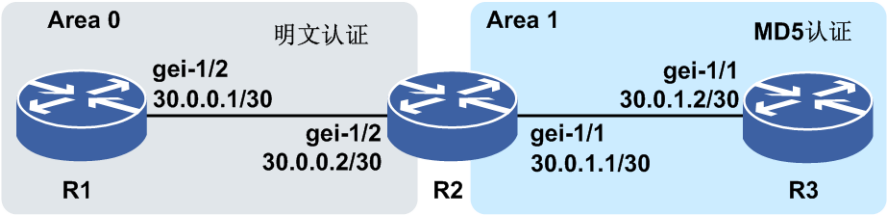
举例

如*图 4-16*所示，要在R1、R2和R3的OSPF接口上配置认证功能。

各个设备的Router-ID如下：

设备	Router-ID
R1	1.1.1.2
R2	1.1.1.3
R3	1.1.1.4

图 4-16 OSPF 认证配置实例



在区域area 0里，R1和R2之间建立OSPF邻居关系；在区域area 1里，R2和R3之间建立OSPF邻居关系。

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip address 30.0.0.1 255.255.255.252
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#exit
R1(config)#router ospf 10
R1(config-ospf-10)#area 0
R1(config-ospf-10-area-0)#network 30.0.0.0 0.0.0.3
R1(config-ospf-10-area-0)#exit
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.3 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 30.0.0.2 255.255.255.252
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 30.0.1.1 255.255.255.252
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#router ospf 10
R2(config-ospf-10)#area 0
R2(config-ospf-10-area-0)#network 30.0.0.0 0.0.0.3
R2(config-ospf-10-area-0)#exit
R2(config-ospf-10)#area 1
R2(config-ospf-10-area-1)#network 30.0.1.0 0.0.0.3
R2(config-ospf-10-area-1)#exit
```

R3上的配置如下：

```
R3(config)#interface loopback1
```

```
R3(config-if-loopback1)#ip address 1.1.1.4 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-1/1
R3(config-if-gei-1/1)#ip address 30.0.1.2 255.255.255.252
R3(config-if-gei-1/1)#no shutdown
R3(config-if-gei-1/1)#exit
R3(config)#router ospf 10
R3(config-ospf-10)#area 1
R3(config-ospf-10-area-1)#network 30.0.1.0 0.0.0.3
R3(config-ospf-10-area-1)#exit
```

在area 0的接口上启动明文认证，设置认证报文为Inspur。

R1上的配置如下：

```
R1(config)#router ospf 10
R1(config-ospf-10)#interface gei-1/2
R1(config-ospf-10-if-gei-1/2)#authentication
R1(config-ospf-10-if-gei-1/2)#authentication-key Inspur
R1(config-ospf-10-if-gei-1/2)#exit
```

R2上的配置如下：

```
R2(config-ospf-10)#interface gei-1/2
R2(config-ospf-10-if-gei-1/2)#authentication
R2(config-ospf-10-if-gei-1/2)#authentication-key Inspur
R2(config-ospf-10-if-gei-1/2)#exit
```

此时用命令**show ip ospf**可看到area 0上的简单认证已生效：

```
R2(config)#show ip ospf
OSPF 10 Router ID 1.1.1.2 enable
 Domain ID type 0x5,value 0.0.0.1
 Enabled for 02:37:38,Debug on
 Number of areas 2, Normal 2, Stub 0, NSSA 0
 ……
    Area 0.0.0.0 enable(Demand circuit available)
        Enabled for 02:37:38
        Area has simple password authentication
        Times spf has been run 32
        Number of interfaces 1. Up 1
        Number of ASBR local to this area 0
        Number of ABR local to this area 1
 ……
```

在area 1的接口上启动MD5认证，口令序号为1，认证口令为Inspur。

R2上的配置如下：

```
R2(config)#router ospf 10
R2(config-ospf-10)#interface gei-1/1
R2(config-ospf-10-if-gei-1/1)#authentication message-digest
R2(config-ospf-10-if-gei-1/1)#message-digest-key 1 md5 Inspur
R2(config-ospf-10-if-gei-1/1)#exit
```

R3上的配置如下：

```
R3(config)#router ospf 10
R3(config-ospf-10)#interface gei-1/1
R3(config-ospf-10-if-gei-1/1)#authentication message-digest
R3(config-ospf-10-if-gei-1/1)#message-digest-key 1 md5 Inspur
R3(config-ospf-10-if-gei-1/1)#exit
```

在R3上查看OSPF的接口信息，可以看到认证方式为MD5认证：

```
R3(config-ospf-10)#sho ip ospf interface gei-1/1
 OSPF Router with ID (1.1.1.4) (Process ID 10)

gei-1/1 is up
Track State is unknown
Internet Address 30.0.1.1 255.255.255.252 enable
```

```
Up for 00:24:41
In the area 0.0.0.0 DR
Cost 1, Priority 1, Network Type broadcast
Transmit Delay(sec) 1, Authentication Type message-digest
TTL security disabled
LDP sync disabled
……
```

4.4.4 配置 OSPF STUB 区域

配置OSPF STUB区域可以减少路由表中路由信息的数量，减少区域内路由器对内存容量的需求。

前提

路由器间已成功运行OSPF协议，且要配置的区域为非骨干区域。

1.进入OSPF路由模式并创建区域。

步骤	命令	功能
1	inspur(config)#**router ospf** <*process-id*>[**vrf** <*vrf-name*>]	进入OSPF路由模式
2	inspur(config-ospf-process-id)#**area** <*area-id*>	创建OSPF区域

2.配置AREA为STUB区域。

命令	功能
inspur(config-ospf-process-id-area-id)#**stub** [**default-cost** <*cost*>]	配置此AREA为STUB区域
inspur(config-ospf-process-id-area-id)#**stub no-summary** [**default-cost** <*cost*>]	配置ABR 在STUB AREA不引进任何3型路由信息，只有一条缺省3型路由信息

no-summary：禁止ABR将汇总路由信息发送到该STUB区域。

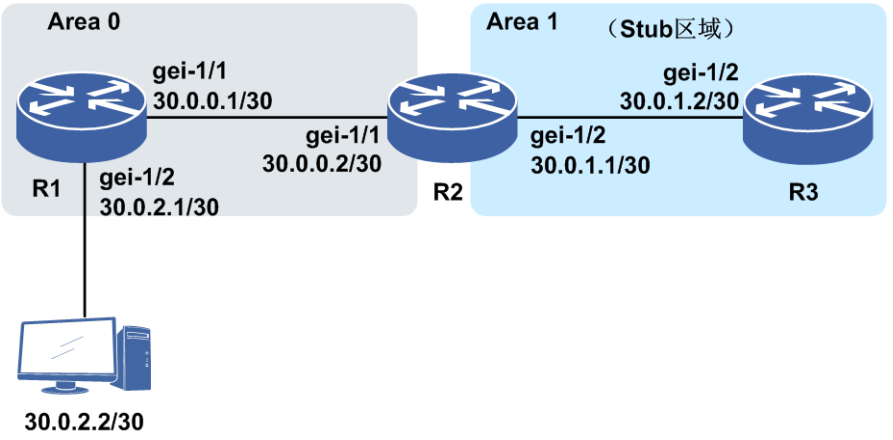
default-cost <*cost*>：向该STUB区域通告的缺省路由的开销，范围1~65535。

举例

如*图 4-17*所示，要把area 1配置成STUB区域，各个设备的Router-ID如下：

设备	Router-ID
R1	1.1.1.2
R2	1.1.1.3
R3	1.1.1.4

图 4-17 OSPF 末节与完全末节区域配置实例



R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 30.0.0.1 255.255.255.252
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip address 30.0.2.1 255.255.255.252
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#exit
R1(config)#router ospf 10
R1(config-ospf-10)#area 0
R1(config-ospf-10-area-0)#network 30.0.0.0 0.0.0.3
R1(config-ospf-10-area-0)#redistribute connected
R1(config-ospf-10-area-0)#exit
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.3 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 30.0.0.2 255.255.255.252
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 30.0.1.1 255.255.255.252
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#exit
R2(config)#router ospf 10
R2(config-ospf-10)#area 0
R2(config-ospf-10-area-0)#network 30.0.0.0 0.0.0.3
R2(config-ospf-10-area-0)#exit
R2(config-ospf-10)#area 1
R2(config-ospf-10-area-1)#network 30.0.1.0 0.0.0.3
R2(config-ospf-10-area-1)#stub
R2(config-ospf-10-area-1)#exit
```

R3上的配置如下：

```
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 1.1.1.4 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-1/2
R3(config-if-gei-1/2)#ip address 30.0.1.2 255.255.255.252
R3(config-if-gei-1/2)#no shutdown
R3(config-if-gei-1/2)#exit
R3(config)#router ospf 10
```

```
R3(config-ospf-10)#area 1
R3(config-ospf-10-area-1)#network 30.0.1.0 0.0.0.3
R3(config-ospf-10-area-1)#stub
R3(config-ospf-10-area-1)#exit
```

如果要将area 1配置成完全末节区域，则R2上的相关配置改为：

```
R2(config)#router ospf 10
R2(config-ospf-10)#area 1
R2(config-ospf-10-area-1)#stub no-summary
R2(config-ospf-10-area-1)#exit
```

R3上的相关配置改为：

```
R3(config)#router ospf 10
R3(config-ospf-10)#area 1
R3(config-ospf-10-area-1)#stub no-summary
R3(config-ospf-10-area-1)#exit
```

4.4.5 配置 NSSA 区域

本节介绍OSPF NSSA区域的配置步骤和命令。

前提

路由器间已成功运行OSPF协议，且要配置的区域为非骨干区域或者STUB区域。

相关信息

NSSA区域允许外部路由通告到OSPF自主系统内部，而同时保留自主系统其余部分的末梢区域特征。为了做到这点，NSSA区域中的路由器从该区域的ASBR接收AS外部路由，但是来自其他区域的外部路由信息将被阻断。

由于网络中有些路由器不支持NSSA配置。也无法识别Type 7类型的LSA，所以协议规定：在NSSA的ABR上将NSSA内部产生的Type 7类型的LSA转化为Type 5类型的LSA再发布出去，并同时更改LSA的发布者为ABR自己，这是OSPF中的路由翻译。这样NSSA区域外的路由器就可以完全不用支持该属性。

1.进入OSPF路由模式并创建区域。

步骤	命令	功能
1	inspur(config)#**router ospf** <*process-id*>[**vrf** <*vrf-name*>]	进入OSPF路由模式
2	inspur(config-ospf-process-id)#**area** <*area-id*>	创建OSPF区域

2.配置指定的区域为NSSA区域。

命令	功能
inspur(config-ospf-process-id-area-id)#**nssa** [**no-redistribution**][**default-information-originate** [**metric** <*metric-value*>][**metric-type** <*type*>]][**no-summary**][**trans-type7-suppress-fa**][**translator-role** {**always** | **candidate**}][**translator-stab-intv** <*stab-intv*>]	配置此区域为NSSA区域，可以同时指定是否需要禁止ABR将汇总路由信息发送到该NSSA区域，是否向NSSA区域导入7型外部链路状态通告，以及是否产生7型缺省链路状态通告

命令	功能
	缺省为不禁止汇总路由，导入7型链路通告，ABR产生缺省7型链路通告，非ABR不产生缺省7型链路通告

no-redistribution：不向该NSSA区域再分配外部链路状态通告。

default-information-originate：产生7型缺省路由链路状态通告。

metric <*metric-value*>：7型缺省路由链路状态通告的费用值，范围1~16777214。

metric-type <*type*>：7型缺省路由链路状态通告的类型，分为ext-1和ext-2两种类型。

no-summary：不向该NSSA区域发送汇总链路状态通告。

trans-type7-suppress-fa：在7型转5型时抑制转发地址。

translator-role：7型转5型过程中所处的翻译角色。

{ **always** | **candidate** }：两种翻译角色：**always**和**candidate**。

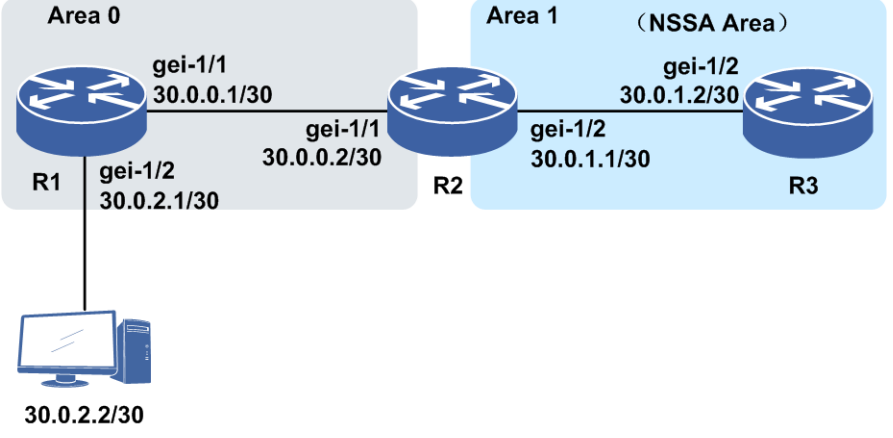
translator-stab-intv <*stab-intv*>：失去翻译资格后继续保持翻译角色的时间长度，缺省为40 s。

举例

如*图 4-18*所示，要把area 1配置成NSSA区域，各个设备的Router-ID如下：

设备	Router-ID
R1	1.1.1.2
R2	1.1.1.3
R3	1.1.1.4

图 4-18 NSSA 区域配置实例



R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
R1(config-if-loopback1)#exit
```

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 30.0.0.1 255.255.255.252
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip address 30.0.2.1 255.255.255.252
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#exit
R1(config)#router ospf 10
R1(config-ospf-10)#area 0
R1(config-ospf-10-area-0)#network 30.0.0.0 0.0.0.3
R1(config-ospf-10-area-0)#redistribute connected
R1(config-ospf-10-area-0)#exit
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.3 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 30.0.0.2 255.255.255.252
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 30.0.1.1 255.255.255.252
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#exit
R2(config)#router ospf 10
R2(config-ospf-10)#area 0
R2(config-ospf-10-area-0)#network 30.0.0.0 0.0.0.3
R2(config-ospf-10-area-0)#exit
R2(config-ospf-10)#area 1
R2(config-ospf-10-area-1)#network 30.0.1.0 0.0.0.3
R2(config-ospf-10-area-1)#nssa default-information-originate
R2(config-ospf-10-area-1)#exit
```

R3上的配置如下：

```
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 1.1.1.4 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-1/2
R3(config-if-gei-1/2)#ip address 30.0.1.2 255.255.255.252
R3(config-if-gei-1/2)#no shutdown
R3(config-if-gei-1/2)#exit
R3(config)#router ospf 10
R3(config-ospf-10)#area 1
R3(config-ospf-10-area-1)#network 30.0.1.0 0.0.0.3
R3(config-ospf-10-area-1)#redistribute connected
R3(config-ospf-10-area-1)#nssa
R3(config-ospf-10-area-1)#exit
```

如果要在ABR路由器R2上配置命令，使得类型3的路由不通告进NSSA区域，则R2上的相关配置更改为：

```
R2(config)#router ospf 10
R2(config-ospf-10)#area 1
R2(config-ospf-10-area-1)#nssa default-information-originate no-summary
R2(config-ospf-10-area-1)#exit
```

4.4.6 配置区域间路由聚合

路由聚合可节约骨干区域的资源，通过公告一组网络地址为一个聚合地址来实现。

前提

配置区域间路由聚合的前提是已创建该区域，且只能在ABR上用此命令。

1.进入OSPF路由模式并创建区域。

步骤	命令	功能
1	inspur(config)#**router ospf** <*process-id*>[**vrf** <*vrf-name*>]	进入OSPF路由模式
2	inspur(config-ospf-process-id)#**area** <*area-id*>	创建OSPF区域

2.配置OSPF区域间路由聚合。

命令	功能
inspur(config-ospf-process-id-area-id)#**range** <*ip-address*><*net-mask*>{**summary-link** | **nssa-external-link**}[**advertise** | **not-advertise**][**cost**<*cost*>][**tag** <*tag-value*>]	配置区域内的汇总地址范围

summary-link：3型汇总。

nssa-external-link：7型汇总。

advertise：通告汇总3型或7型链路状态通告。

not-advertise：禁止通告汇总3型链路状态通告，在其他区域中不会收到关于此网段的路由信息。

cost：设置汇总LSA的cost值，范围1~16777214。

tag <*tag-value*>：设置汇总LSA的tag，7型汇总有该配置，范围0~4294967295。

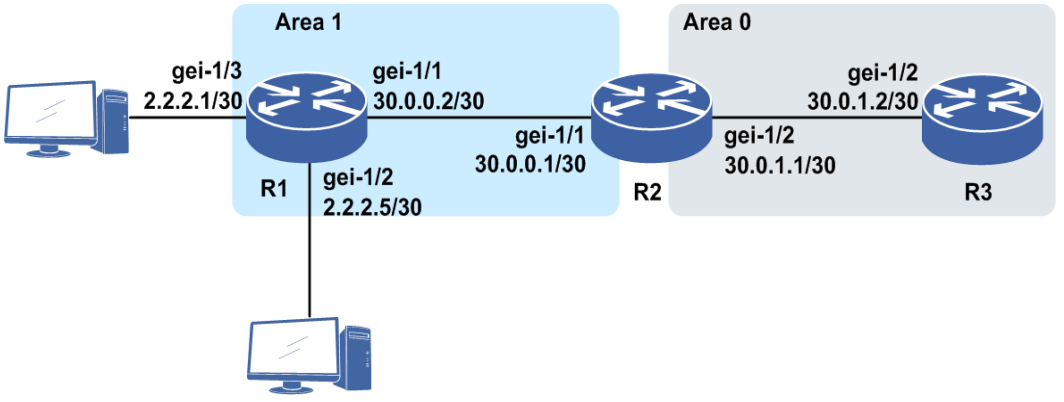
举例

如*图 4-19*所示，要在R1、R2、R3上配置OSPF，R2作为ABR，并在R2上配置路由聚合。

各个设备的Router-ID如下：

设备	Router-ID
R1	1.1.1.2
R2	1.1.1.3
R3	1.1.1.4

图 4-19 区域间路由聚合配置实例



在R1、R2和R3上进行一般配置。

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 30.0.0.2 255.255.255.252
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip address 2.2.2.5 255.255.255.252
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#exit
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#ip address 2.2.2.1 255.255.255.252
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 1
R1(config-ospf-1-area-1)#network 30.0.0.0 0.0.0.3
R1(config-ospf-1-area-1)#network 2.2.2.0 0.0.0.3
R1(config-ospf-1-area-1)#network 2.2.2.4 0.0.0.3
R1(config-ospf-1-area-1)#exit
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.3 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 30.0.0.1 255.255.255.252
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 30.0.1.1 255.255.255.252
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 1
R2(config-ospf-1-area-1)#network 30.0.0.0 0.0.0.3
R2(config-ospf-1-area-1)#exit
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 30.0.1.0 0.0.0.3
R2(config-ospf-1-area-0)#exit
```

R3上的配置如下：

```
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 1.1.1.4 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-1/2
```

```
R3(config-if-gei-1/2)#ip address 30.0.1.2 255.255.255.252
R3(config-if-gei-1/2)#no shutdown
R3(config-if-gei-1/2)#exit
R3(config)#router ospf 1
R3(config-ospf-1)#area 0
R3(config-ospf-1-area-0)#network 30.0.1.0 0.0.0.3
R3(config-ospf-1-area-0)#exit
```

配置完以后，在R3上查看路由表，发现有未聚合的路由：

```
R3(config)#show ip forwarding route
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
 Dest Gw Interface Owner Pri Metric
*> 1.1.1.4/32 1.1.1.4 loopback1 Address 0 0
*> 2.2.2.0/30 30.0.1.1 gei-1/2  OSPF 110 3
*> 2.2.2.4/30 30.0.1.1 gei-1/2  OSPF 110 3
*> 30.0.0.0/30 30.0.1.1 gei-1/2  OSPF 110 2
*> 30.0.1.0/30 30.0.1.2 gei-1/2  Direct 0 0
*> 30.0.1.2/32 30.0.1.2 gei-1/2  Address 0 0
```

在R2上配置进行区域间路由聚合：

```
R2(config)#router ospf 1
R2(config-ospf-1)#area 1
R2(config-ospf-1-area-1)#range 2.2.2.0 255.255.255.248 summary-link
R2(config-ospf-1-area-1)#exit
```

则此时R3上的路由表中已经形成了2.2.2.0/29的聚合路由：

```
R3(config)#show ip forwarding route
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
 Dest Gw Interface Owner Pri Metric
*> 1.1.1.4/32 1.1.1.4 loopback1 Address 0 0
*> 2.2.2.0/29 30.0.1.1 gei-1/2  OSPF 110 3
*> 30.0.0.0/30 30.0.1.1 gei-1/2  OSPF 110 2
*> 30.0.1.0/30 30.0.1.2 gei-1/2  Direct 0 0
*> 30.0.1.2/32 30.0.1.2 gei-1/2  Address 0 0
```

注意命令area 1 range 2.2.2.0 255.255.255.248 缺省为**advertise**，若选择**not-advertise**，则R3不显示2.2.2.0网段的聚合路由，且ping不通该网段，如下：

```
R3(config)#show ip forwarding route
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
  GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
 Dest Gw Interface Owner Pri Metric
*> 1.1.1.4/32 1.1.1.4 loopback1 Address 0 0
*> 30.0.0.0/30 30.0.1.1 gei-1/2 OSPF 110 2
*> 30.0.1.0/30 30.0.1.2 gei-1/2 Direct 0 0
*> 30.0.1.2/32 30.0.1.2 gei-1/2 Address 0 0
```

由上面的结果可知R3没有学习到2.2.2.0网段的路由信息。R2的数据库中虽然仍有2.2.2.0网段的聚合信息，但是不通告给其他区域。

4.4.7 配置路由重分布时的路由聚合

当其它路由协议的路由重分布到OSPF中之后，每条单独的路由作为一个外部的LSA被通告。可以通过聚合将这些外部路由作为一条单独的路由进行通告，这将大大减小OSPF的链路状态数据库的大小。

1.进入OSPF路由模式。

命令	功能
inspur(config)#**router ospf** <*process-id*>[**vrf** <*vrf-name*>]	进入OSPF路由模式

2.配置ASBR的路由聚合。

路由重分布时的路由聚合只能用在自治系统边界路由器上。

命令	功能
inspur(config-ospf-process-id)#**summary-address** <*ip-address*><*net-mask*> **cost**<*cost*>	为OSPF建立聚合地址，汇总重新分配到OSPF的其他路由选择协议的路径，cost值的范围为1~16777214

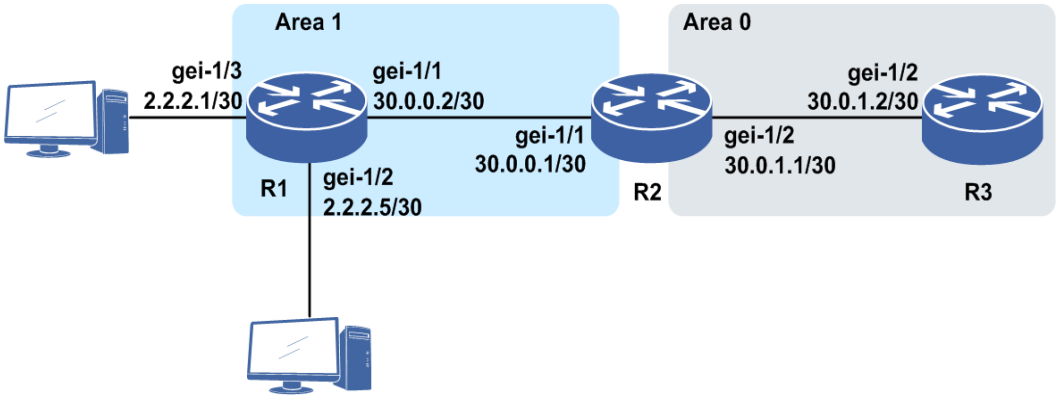
举例

如*图 4-20*所示，要在R1、R2、R3上配置OSPF，把R1上的外部路由进行通告，并在R1上配置ASBR路由聚合。

各个设备的Router-ID如下：

设备	Router-ID
R1	1.1.1.2
R2	1.1.1.3
R3	1.1.1.4

图 4-20 路由重分布时路由聚合配置实例



R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 30.0.0.2 255.255.255.252
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip address 2.2.2.5 255.255.255.252
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#exit
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#ip address 2.2.2.1 255.255.255.252
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 1
R1(config-ospf-1-area-1)#network 30.0.0.0 0.0.0.3
R1(config-ospf-1-area-1)#exit
R1(config-ospf-1)#redistribute connected
R1(config-ospf-1)#summary-address 2.2.2.0 255.255.255.248
R1(config-ospf-1)#exit
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.3 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 30.0.0.1 255.255.255.252
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 30.0.1.1 255.255.255.252
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 1
R2(config-ospf-1-area-1)#network 30.0.0.0 0.0.0.3
R2(config-ospf-1-area-1)#exit
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 30.0.1.0 0.0.0.3
R2(config-ospf-1-area-0)#exit
```

R3上的配置如下：

```
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 1.1.1.4 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-1/2
R3(config-if-gei-1/2)#ip address 30.0.1.2 255.255.255.252
```

```
R3(config-if-gei-1/2)#no shutdown
R3(config-if-gei-1/2)#exit
R3(config)#router ospf 1
R3(config-ospf-1)#area 0
R3(config-ospf-1-area-0)#network 30.0.1.0 0.0.0.3
R3(config-ospf-1-area-0)#exit
```

查看R2上的路由表，发现路由表中存在是经过聚合后的网段2.2.2.0/29：

```
R2(config-ospf-1)#show ip forwarding route
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
  ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
 Dest Gw Interface Owner Pri Metric
*> 1.1.1.2/32 30.0.0.2 gei-1/1 OSPF 110 20
*> 1.1.1.3/32 1.1.1.3 loopback1 Address 0 0
*> 2.2.2.0/29 30.0.0.2 gei-1/1 OSPF 110 20
*> 30.0.0.0/30 30.0.0.1 gei-1/1 Direct 0 0
*> 30.0.0.1/32 30.0.0.1 gei-1/1 Address 0 0
*> 30.0.1.0/30 30.0.1.1 gei-1/2 Direct 0 0
*> 30.0.1.1/32 30.0.1.1 gei-1/2 Address 0 0
```

4.4.8 配置重分布其他路由协议

把其它路由协议的路由信息通告到OSPF中，不同的动态路由协议通过路由重分布可以实现路由信息共享。

1.启动OSPF进程，进入OSPF路由模式。

命令	功能
inspur(config)#**router ospf** <*process-id*>[**vrf** <*vrf-name*>]	启动OSPF进程，运行OSPF协议

2.配置OSPF重分布其他路由协议的路由。

命令	功能
inspur(config-ospf-process-id)#**redistribute** <*protocol*>[**as** <*as-number*>][**peer** <*peer-address*>][**tag** <*tag-value*>][**metric** <*metric-value*>][**metric-type** <*type*>][**route-map** <*map-tag*>]	控制其他协议符合条件的路由导入OSPF自治系统中 缺省：其他协议的路由不被导入OSPF自治系统；metric在重分配BGP路由时为1，其他路由时为20

<*protocol*>：根据协议过滤，取值有：connected，static，rip，bgp-ext，bgp-int，isis-1，isis-1-2，isis-2，ospf-int，ospf-ext，nat ，natpt ，ps-busi-addr， ps-user-addr ，sl-nat64-ipv4 ，subscriber-aggregation ，subscriber-host，user-special。

as <*as-number*>：表示对端AS号，范围<1~65535>或者<1~65535>.<0~65535>。

tag <*tag-value*>：设置再分配后的LSA的tag，范围0~4294967295。

metric <*metric-value*>：设置再分配后的LSA的metric，缺省情况下使用系统的缺省metric， 范围1~16777214。

metric-type <*type*>：设置再分配后的lsa的metric-type，取值为ext-1或ext-2，缺省为ext-2。

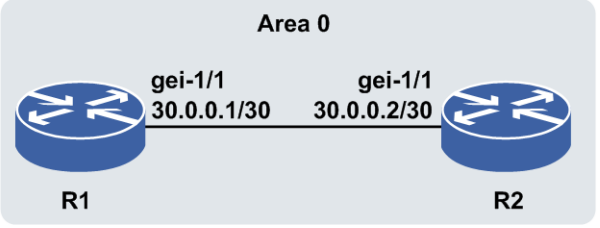
route-map <*map-tag*>：设置当前协议再分配的路由映射名称，长度为1~31个字符。

举例

如*图 4-21*所示，要在area 0中重分布RIP路由。各个设备的Router-ID如下：

设备	Router-ID
R1	1.1.1.2
R2	1.1.1.3

图 4-21 OSPF 重分布路由配置实例



1.R1和R2建立OSPF邻居。

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 30.0.0.1 255.255.255.252
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 30.0.0.0 0.0.0.3
R1(config-ospf-1-area-0)#exit
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.3 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 30.0.0.2 255.255.255.252
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 30.0.0.0 0.0.0.3
R2(config-ospf-1-area-0)#exit
```

2.R1上配置静态路由。

```
R1(config)#ip route 1.2.3.4 255.255.255.255 null1
```

3.在R1配置上重分发静态路由。

```
R1(config)#router ospf 1
R1(config-ospf-1)#redistribute static
```

```
R1(config-ospf-1)#exit
```

此时R2上能看到1.2.3.4网段的信息，如下：

```
R2#show ip protocol routing
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE =
rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale
    Dest             NextHop        RoutePrf  RouteMetric  Protocol
*>  1.2.3.4/32        30.0.0.1        110       20          OSPF
*>  30.0.0.0/30       30.0.0.2        0         0           Direct
 *  30.0.0.0/30       30.0.0.0        110       1           OSPF
*>  30.0.0.2/32       30.0.0.2        0         0           Address
```

4.4.9 配置 OSPF 缺省路由

本节介绍OSPF缺省路由的配置步骤和命令。

1.进入OSPF路由模式。

命令	功能
inspur(config)#**router ospf** <*process-id*>[**vrf** <*vrf-name*>]	进入OSPF路由模式

2.配置OSPF缺省路由。

命令	功能
inspur(config-ospf-process-id)#**notify default route** [**always**][**metric** <*metric-value*>][**metric-type** <*type*>][**route-map** <*map-tag*>]	当本路由器通过其他协议或配置静态路由方式获得一条缺省路由时，需要将其通告；没有缺省路由时，则按正常方式通告具体的可达路由，使用该命令后路由器成为一个ASBR

always：指定always表示不论本路由器是否存在缺省路由，都通告缺省路由；如果没有指定always则根据路由器的路由表中是否有缺省路由来决定是否通告，若存在缺省路由则通告，否则不通告。

metric <*metric-value*>：指定缺省路由的费用，范围1~16777214，缺省为1。

metric-type <*type*>：指定缺省路由的类型，取值为ext-1或ext-2，缺省为ext-2。

route-map <*map-tag*>：指定产生该缺省路由的路由映射名称，长度为1~31个字符。

4.4.10 配置 OSPF 虚链路

OSPF网络中的所有非骨干区域必须直接连接到骨干区域并且骨干区域不能分离，为了解决这个问题，可以用虚链路的方式来使一个远程区域通过其他区域连接到骨干区域上或者使两个分离的骨干区域相连。

1.进入OSPF路由模式并创建区域。

步骤	命令	功能
1	inspur(config)#**router ospf** <*process-id*>[**vrf** <*vrf-name*>]	进入OSPF路由模式
2	inspur(config-ospf-process-id)#**area** <*area-id*>	创建OSPF区域

2.配置OSPF虚链路。

命令	功能
inspur(config-ospf-process-id-area-id)#**virtual-link** <*router-id*>[**hello-interval** <*seconds*>][**retransmit-interval** <*seconds*>][**transmit-delay** <*seconds*>][**dead-interval** <*seconds*>][**authentication-key** <*key*>][**message-digest-key** <*keyid*> **md5** <*cryptkey*>[**delay** <*time*>]][**authentication** [**null**|**message-digest**]]	定义OSPF虚拟链路 不能在STUB区域，NSSA区域和骨干区域建立虚链路

<*area-id*>：虚拟链路经过的传输区域ID，不能为STUB，NSSA区域和骨干区域。

hello-interval <*seconds*>：虚拟链路上发送Hello报文的时间间隔，单位：秒，范围1~8192，缺省为10秒。

retransmit-interval <*seconds*>：虚拟链路上重传间隔，单位：秒，范围1~8192，缺省为5秒。

transmit-delay <*seconds*>：虚拟链路上发送一个链路状态更新数据包的迟延，单位：秒，范围1~8192，缺省为1秒。

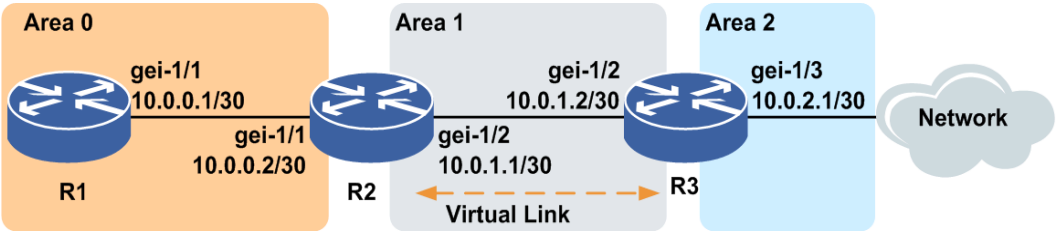
dead-interval <*seconds*>：虚拟链路上邻居死亡时间，单位：秒，范围1~8192，缺省为40秒。

举例

如*图 4-22*所示，要在R2和R3的互联接口上建立虚链路连接。各个设备的Router-ID如下：

设备	Router-ID
R1	1.1.1.2
R2	1.1.1.3
R3	1.1.1.4

图 4-22 OSPF 虚链路配置实例



R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 10.0.0.1 255.255.255.252
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 10.0.0.0 0.0.0.3
R1(config-ospf-1-area-0)#exit
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.3 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 10.0.0.2 255.255.255.252
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 10.0.1.1 255.255.255.252
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 10.0.0.0 0.0.0.3
R2(config-ospf-1-area-0)#exit
R2(config-ospf-1)#area 1
R2(config-ospf-1-area-1)#network 10.0.1.0 0.0.0.3
R2(config-ospf-1-area-1)#virtual-link 1.1.1.4
R2(config-ospf-1-area-1)#exit
```

R3上的配置如下：

```
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 1.1.1.4 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-1/2
R3(config-if-gei-1/2)#ip address 10.0.1.2 255.255.255.252
R3(config-if-gei-1/2)#no shutdown
R3(config-if-gei-1/2)#exit
R3(config)#interface gei-1/3
R3(config-if-gei-1/3)#ip address 10.0.2.1 255.255.255.252
R3(config-if-gei-1/3)#no shutdown
R3(config-if-gei-1/3)#exit
R3(config)#router ospf 1
R3(config-ospf-1)#area 1
R3(config-ospf-1-area-1)#network 10.0.1.0 0.0.0.3
R3(config-ospf-1-area-1)#virtual-link 1.1.1.3
R3(config-ospf-1-area-1)#exit
R3(config-ospf-1)#area 2
R3(config-ospf-1-area-2)#network 10.0.2.0 0.0.0.3
R3(config-ospf-1-area-2)#exit
```

4.4.11 配置 Sham-link

本节介绍Sham-link的配置步骤和命令。

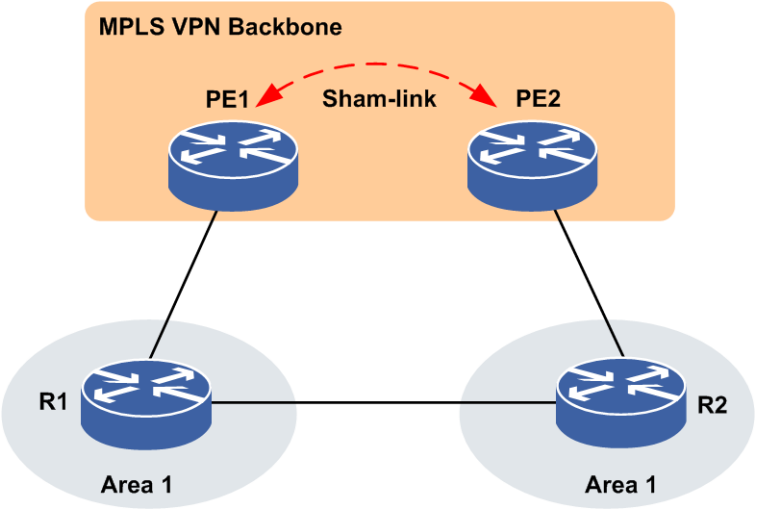
相关信息

通常情况下，BGP对等体之间通过BGP扩展团体属性在MPLS VPN骨干网上承载路由信息。PE通过将BGP路由重分发到OSPF，利用MPBGP携带的信息可以生成区域间的OSPF路由。

如*图 4-23*所示，如果本地CE R1和远端的CE R2存在链路互连，并在区域1建立OSPF邻居，这时由于CE之间的路由是区域路由，其优先级要高于经过MPLS VPN骨干网的区域间路由，所以会导致VPN流量不通过骨干网，而走了CE之间的链路。这条CE之间的链路相对于MPLS VPN骨干网的链路是旁门小路，因此称这条链路为后门链路。

为了解决这一个问题，可以在PE路由器之间建立OSPF sham-link邻居，使经过MPLS VPN骨干网的路由也成为OSPF区域内路由，这样通过更改路由的花费值，就可以使流量走带宽更大的MPLS VPN骨干网链路。当然，也可以根据用户的实际需要，选择后门链路。

图 4-23 Sham-link 示意图



在PE路由器之间启用sham-link，建立邻居，交互数据库，这样同一域的私网路由器会学到两个域内路由，一个走sham-link（MPLS VPN Backbone），一个走私网，只需要改变路由的metric属性，就可以改变选路。

在PE路由器上启用Sham-link，配置步骤如下。

1.进入OSPF路由模式并创建区域。

步骤	命令	功能
1	`inspur(config)#`**router ospf** *<process-id>*[**vrf** *<vrf-name>*]	进入OSPF路由模式
2	`inspur(config-ospf-process-id)#`**area** *<area-id>*	创建OSPF区域

2.配置Sham-link。

命令	功能
inspur(config-ospf-process-id-area-id)#**sham-link** <*ip-address1*><*ip-address2*> **cost**<*cost*>	两PE路由器之前建立通过MPLS VPN来传递OSPF协议包的连接

<*area-id*>：区域标识符，可以指定为十进制数值（0~4294967295）或一个十进制点分形式的IP地址。

<*ip-address1*>：Shamlink链路本地建立shamlink的loopback的IP地址，为十进制点分形式的IP地址。

<*ip-address2*>：Shamlink链路对端建立shamlink的loopback的IP地址，为十进制点分形式的IP地址。

<*cost*>：Shamlink的cost值，范围为1~65535。

4.4.12 配置 max-metric

基于流量、管理等方面的要求，有时需要使某些路由器只是路由的终点而不是传输点，作为没有穿越能力的节点被包括到网络的拓扑中，这可以通过max-metric功能实现。

1.进入OSPF配置模式。

命令	功能
inspur(config)#**router ospf** <*process-id*>[**vrf** <*vrf-name*>]	进入OSPF路由模式

2.配置max-metric。

命令	功能
inspur(config-ospf-process-id)#**max-metric router-lsa**	配置的路由器学习不到任何OSPF路由，本地router-lsa的transit network的metric会置为65535 其它路由器只能学习这台路由器发起的路由，这台路由器在拓扑上依然可达，只是不能穿越而已
inspur(config-ospf-process-id)#**max-metric router-lsa on-startup wait-for-bgp**	等待BGP邻居建立后过1分钟路由器才可穿越 如果邻居起不来，要等待10分钟路由器才可穿越
inspur(config-ospf-process-id#**max-metric router-lsa on-startup timeout** <*seconds*>	配置的重启以后持续防止路由黑洞的时间，单位：秒，范围为5~86400，即重启这段时间后路由器才可穿越

例如当路由器刚刚重新启动，BGP路由尚未收敛，通过配置**max-metric router-lsa on-startup wait-for-bgp**命令，防止路由黑洞。

4.4.13 配置 OSPF 路由负荷分担

本节介绍OSPF路由负荷分担的配置步骤和命令。

相关信息

路由负荷分担有两个主要的功能：

- 提高链路可靠性：网络的传输层对稳定性和可靠性要求很高。这种可靠性表现在除了链路本身可靠外还应表现在当某条链路出现故障的时候不影响其他路径上的报文转发或者减少转发失败的影响。
- 提高带宽：路由负荷分担功能使得路由器能够将流量分配到多条路径上，从而充分利用带宽资源。通过路由协议或静态配置，可以使得转发表中，对于同一个目的地址，有多条可用的路由条目。

负荷分担的转发机制支持两种方法，**per-packet**（逐包模式）和**per-destination**（逐流模式），下表给出了这两种方法的优缺点：

模式	优点	缺点
逐流模式	到给定目的的包可以保证走同一条路径，即使在有多条可用路径的情况下；到不同目的的包可以走不同的路径	当流量中只有少量的目的地址时，可能会引起流量集中在少数路径上，分担不均衡；当流量中目的地址增加时，负荷分担会更有效
逐包模式	路径利用率高，因为per-packet 使用轮转法来确定数据包走的路径，使得转发负荷均匀地分布在各条路径上	对于到给定目的的流量可能会选择不同的路径，造成接收端的排序，对于VoIP和其他要求有序的流量不适用

1.配置OSPF支持路由负荷分担。

步骤	命令	功能
1	`inspur(config)#`**router ospf** < *process-id*>[**vrf** < *vrf-name*>]	进入OSPF路由配置模式
2	`inspur(config-ospf-process-id)#`**maximum-paths** < *number*>	配置协议支持负荷分担的路由数目，范围1~32，缺省为1

路由表中最多保存32条等开销路由条目以进行负载均衡，此命令可以支持最多达32条相同度量值路径，缺省为1条。

2.配置OSPF接口负荷分担。

步骤	命令	功能
1	`inspur(config)#`**interface** < *interface-name*>	进入接口配置模式
2	`inspur(config-if-interface-name)#`**ip load-sharing** {**per-destination** | **per-packet**}	配置接口负荷分担模式：负荷分担是在出接口上配置的，默认情况下为**per-destination**。只有所有的接口配置为

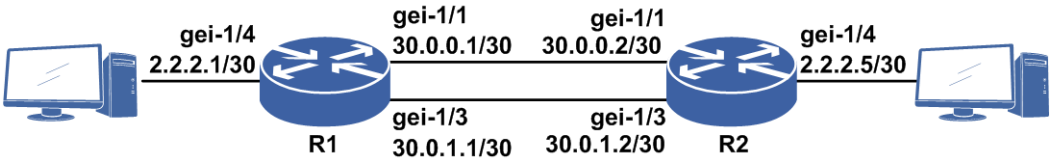
步骤	命令	功能
		per-packet模式，负荷分担的模式才是**per-packet**
3	inspur(config-if-interface-name)#**load-sharing bandwidth** < *bandwidth-value*>	配置接口负荷分担的权重：权重设置在出接口上，只有配置了优先级后，配置的权重才有效；权重的范围不同的接口大小值不同

举例

如*图 4-24*所示，要在R1，R2上启用OSPF，并在R1、R2间启用路由负载均衡，配置OSPF协议负载均衡时支持的最大路由数目为2。

设备	Router-ID
R1	1.1.1.2
R2	1.1.1.3

图 4-24 OSPF 路由负载均衡配置实例



R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 30.0.0.1 255.255.255.252
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#ip address 30.0.1.1 255.255.255.252
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#exit
R1(config)#interface gei-1/4
R1(config-if-gei-1/4)#ip address 2.2.2.1/30
R1(config-if-gei-1/4)#no shutdown
R1(config-if-gei-1/4)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 30.0.0.0 0.0.0.3
R1(config-ospf-1-area-0)#network 30.0.1.0 0.0.0.3
R1(config-ospf-1-area-0)#network 2.2.2.0 0.0.0.3
R1(config-ospf-1-area-0)#exit
R1(config-ospf-1)#maximum-paths 2
/*设置OSPF协议负载均衡时支持的最大路由数目为2*/
R1(config-ospf-1)#exit
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.3 255.255.255.255
```

```
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 30.0.0.2 255.255.255.252
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#ip address 30.0.1.2 255.255.255.252
R2(config-if-gei-1/3)#no shutdown
R2(config-if-gei-1/3)#exit
R2(config)#interface gei-1/4
R2(config-if-gei-1/4)#ip address 2.2.2.5 255.255.255.252
R2(config-if-gei-1/4)#no shutdown
R2(config-if-gei-1/4)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#router-id 1.1.1.2
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 30.0.0.0 0.0.0.3
R2(config-ospf-1-area-0)#network 30.0.1.0 0.0.0.3
R2(config-ospf-1-area-0)#network 2.2.2.4 0.0.0.3
R2(config-ospf-1-area-0)#exit
R2(config-ospf-1)#maximum-paths 2
/*设置OSPF协议负载均衡时支持的最大路由数目为2*/
R2(config-ospf-1)#exit
```

查看R1的路由表，看到两条目的地相同的OSPF路由条目2.2.2.4/30：

```
R1(config)#show ip forwarding route
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
  ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
 Dest Gw Interface Owner Pri Metric
*> 1.1.1.2/32 1.1.1.2 loopback1 Address 0 0
*> 2.2.2.0/30 2.2.2.1 gei-1/4 Direct 0 0
*> 2.2.2.1/32 2.2.2.1 gei-1/4 Address 0 0
*> 2.2.2.4/30 30.0.0.2 gei-1/1 OSPF 110 2
*> 2.2.2.4/30 30.0.1.2 gei-1/3 OSPF 110 2
*> 30.0.0.0/30 30.0.0.1 gei-1/1 Direct 0 0
*> 30.0.0.1/32 30.0.0.1 gei-1/1 Address 0 0
*> 30.0.1.0/30 30.0.1.1 gei-1/3 Direct 0 0
*> 30.0.1.1/32 30.0.1.1 gei-1/3 Address 0 0
```

类似地，在R2上也能看到相似的路由条目。

4.4.14 配置 OSPF FRR

本节介绍OSPF FRR的配置步骤和命令。

1.配置OSPF FRR路由备份方式。

步骤	命令	功能
1	inspur(config)#**router ospf** <*process-id*>[**vrf** < *vrf-name*>]	进入OSPF路由配置模式
2	inspur(config-ospf-process-id)#**fast-reroute per-prefix**	开启FRR功能

步骤	命令	功能
3	inspur(config-ospf-process-id)#**fast-reroute dynamic-remote-lfa priority** <*priority*>	配置动态远端LFA优先级
4	inspur(config-ospf-process-id)#**fast-reroute static-remote-lfa priority** <*priority*>	配置静态远端LFA优先级
5	inspur(config-ospf-process-id)#**fast-reroute lfa priority** <*priority*>	配置LFA优先级

2.配置OSPF FRR接口。

步骤	命令	功能
1	inspur(config-ospf-process-id)#**interface** < *interface-name*>	进入协议接口配置模式
2	inspur(config-ospf-process-id-if-interface-name)#**cost** <*value*>	配置当前接口的开销。开启FRR自动计算备份路由后，开销大的路由计算为备份路由
3	inspur(config-ospf-process-id-if-interface-name)#**fast-reroute** [**backup-interface** <*interface-name*>| **disable**]	指定本接口为FRR备份接口。当步骤2中定义的自动FRR路由计算条件不满足时，这个静态的FRR生效。但是因为是静态的缘故，不能过滤环路。

4.4.15 配置 OSPF Graceful Restart

本节介绍OSPF Graceful Restart的配置步骤和命令。

1.进行OSPF配置模式。

命令	功能
inspur(config)#**router ospf** <*process-id*>[**vrf** < *vrf-name*>]	进入OSPF配置模式

2.配置OSPF启用Graceful Restart功能。

命令	功能
inspur(config-ospf-process-id)#**nsf**	配置OSPF使能Graceful Restart，如果是help方的话，表示使能支持邻居倒换的功能

3.（可选）配置OSPF Graceful Restart时间。

命令	功能

命令	功能
inspur(config-ospf-process-id)#**grace-period** <*time*>	配置OSPF Graceful Restart时间，默认是120秒，如果倒换方路由条目较多时，可将此时间设置稍长一点

4.（可选）指定接口上邻居的死亡时间。

步骤	命令	功能
1	inspur(config-ospf-process-id)#**interface** <*interface-name*>	进入OSPF接口配置模式
2	inspur(config-ospf-process-id-if-interface-name)#**dead-interval** <*time*>	指定接口上邻居的死亡时间，在设备倒换时间较长时需配置这个命令，缺省为4倍的缺省hello-interval时长

4.4.16 配置 OSPF 路由过滤

在IR12000上可以通过三种方式配置OSPF路由过滤：distribute-list过滤路由、filter过滤路由、area filter-list过滤路由。本节介绍OSPF三种路由过滤的配置步骤和命令。

1.配置distribute-list过滤路由。

步骤	命令	功能
1	inspur(config)#**router ospf** <*process-id*>[**vrf** < *vrf-name*>]	进入OSPF配置模式
2	inspur(config-ospf-process-id)#**distribute-list** {**access-list** <*access-list-name*>{**in** | **out**}| **prefix** <*name of an IP prefix-list*>{**gateway** <*name of an IP prefix-list*> **in** | **in** | **out**}|**gateway** <*name of an IP prefix-list*> **in** |**route-map** <*name of a route-map*> **in** [**local-mt**]}	配置distribute-list过滤路由

<*access-list-name*>：名字型的ACL，第一个字符可以是数字，可以使用当前不存在的ACL。

<*name of an IP prefix-list*>：借用prefix-list模板的名字。

<*name of a route-map*>：借用route-map模板的名字。

in | out：In表示指定的模板用于路由的过滤，0ut表示指定的模板用于对重分配进行补充。

2.配置filter过滤路由。

步骤	命令	功能

步骤	命令	功能
1	inspur(config)#**router ospf** <*process-id*>[**vrf** < *vrf-name*>]	进入OSPF配置模式
2	inspur(config-ospf-process-id)#**filter** [**exact**]<*ip-address*><*net-mask*><*prefence*>	配置filter过滤路由

exact：表示精确匹配。

<*ip-address*> <*net-mask*>：描述过滤路由的范围，为十进制点分形式。没有**exact**关键字时对所有ip-address、net-mask范围的路由进行过滤，有**exact**关键字表示路由必须精确匹配ip-address、net-mask。

<*prefence*>：描述导入匹配路由的优先级，范围：1–255。

3.配置area filter-list过滤路由。

步骤	命令	功能
1	inspur(config)#**router ospf** <*process-id*>[**vrf** < *vrf-name*>]	进入OSPF配置模式
2	inspur(config-ospf-process-id)#**area** <*area-id*> **filter-list prefix** <*prefix-list*>{**out** | **in** }	配置filter过滤路由

<*area-id*>**exact**：区域标识符，可以指定为一个十进制点分形式的IP地址或十进制数值，数值范围：0–4294967295。

prefix <*prefix-list*> ：前缀列表的名称。

in | out：从该区域中导出或导入路由信息时进行过滤。

4.4.17 验证及维护 OSPF

验证OSPF配置结果

IR12000提供了以下命令查看OSPF相关信息：

命令	功能
inspur#**show ip ospf** [<*process-id*>]	显示OSPF协议的概要信息以及各个OSPF区域的概要信息
inspur#**show ip ospf interface** [<*interface-name*>][**process** <*process-id*>]	显示OSPF接口的信息
inspur#**show ip ospf database** [**database-summary** | **adv-router** <*router-id*>|**self-originate**][**area** <*area-id*>][**process** <*process-id*>]	显示OSPF链路数据库相关信息
inspur#**show ip ospf database router** [<*link-state-id*>][**adv-router**	显示OSPF链路状态数据库中router LSA的信息

命令	功能
<*router-id*>|**self-originate**][**area** <*area-id*>][**process** <*process-id*>]	
inspur#**show ip ospf database network** [<*link-state-id*>][**adv-router** <*router-id*>|**self-originate**][**area** <*area-id*>][**process** <*process-id*>]	显示OSPF链路状态数据库中network LSA的信息
inspur#**show ip ospf database database-summary** [<*link-state-id*>][**adv-router** <*router-id*>|**self-originate**][**area** <*area-id*>][**process** <*process-id*>]	显示OSPF链路状态数据库中summary LSA的信息
inspur#**show ip ospf database asbr-summary** [< *link-state-id*>][**adv-router** <*router-id*>| **self-originate**][**area** < *area-id*>][**process** < *process-id*>]	显示OSPF链路状态数据库中asbr-summary LSA的信息
inspur#**show ip ospf database external** [< *link-state-id*>][**adv-router** <*router-id*>| **self-originate**][**area** < *area-id*>][**process** < *process-id*>]	显示OSPF链路状态数据库中external LSA的信息
inspur#**show ip ospf database nssa** [< *link-state-id*>][**adv-router** <*router-id*>| **self-originate**][**area** < *area-id*>][**process** < *process-id*>]	显示OSPF链路状态数据库中nssa LSA的信息
inspur#**show ip ospf database** {**opaque-area** | **opaque-link**}[< *link-state-id*>][**adv-router** <*router-id*>| **self-originate**][**area** < *area-id*>][**process** < *process-id*>]	显示OSPF链路状态数据库中opaque-area LSA和opaque-link LSA的信息
inspur#**show ip ospf neighbor** [<*process-id*>]	显示OSPF状态信息
inspur#**show ip ospf nsf**	显示OSPF无中断转发的信息。
inspur#**show ip ospf request-list** [<*neighbor-id*>|**interface** <*interface-name*>|**process** <*process-id*>]	显示路由器请求的链路状态通告列表
inspur#**show ip ospf retransmission-list** [<*neighbor-id*>|**interface** <*interface-name*>|**process** <*process-id*>]	显示路由器重传的所有链路状态列表
inspur#**show ip ospf boarder-routers** [**router-id** <*router-id*>|**process** <*process-id*>]	显示路由器路由信息
inspur#**show ip ospf boarder-lfas** [**router-id** <*router-id*>|**process** <*process-id*>]	显示替代快速重计算路由的非自环路由信息
inspur#**show ip ospf virtual-links** [**process** <*process-id*>]	显示路由器的虚拟链路信息
inspur#**show ip ospf sham-links** [**process** <*process-id*>]	显示OSPF后门链路信息
inspur#**show ip ospf mpls traffic-eng link**[**area** <*area-id*>|**process**<*process-id*>]	显示OSPF流量工程链路信息

维护OSPF

IR12000提供了debug命令对OSPF协议进行调试，来跟踪相关信息：

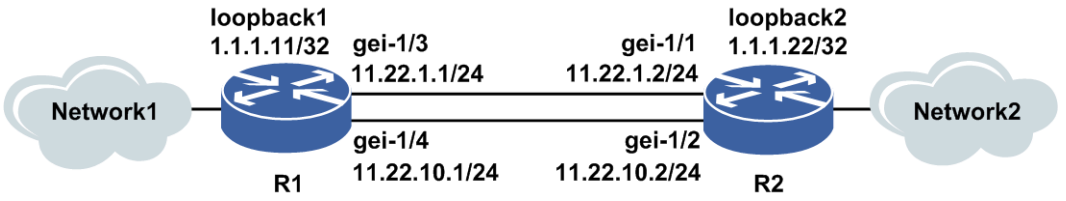
命令	功能
inspur#**debug ip ospf adj** *<process-id>*	打开回送OSPF邻接事件调试信息的开关
inspur#**debug ip ospf all** [*<process-id>*]	打开所有OSPF调试信息的开关
inspur#**debug ip ospf cspf***<process-id>*	打开OSPF基于约束的最短路径计算的调试信息的开关，调试OSPF基于约束的最短路径计算
inspur#**debug ip ospf database-timer***<process-id>*	打开回送OSPF链路状态数据库定时器事件调试信息的开关
inspur#**debug ip ospf events** *<process-id>*	打开回送OSPF重要事件调试信息的开关
inspur#**debug ip ospf fast-reroute**[**external** | **inter** | **intra** | **nbrspf**]*<process-id>*	打开回送OSPF快速重路由调试信息的开关
inspur#**debug ip ospf flood** *<process-id>*	打开回送OSPF洪泛事件调试信息的开关
inspur#**debug ip ospf lsa-generation** *<process-id>*	打开回送OSPF生成链路状态通告事件调试信息的开关
inspur#**debug ip ospf packet** *<process-id>*	打开回送OSPF收发包事件调试信息的开关，监听所有OSPF包的接收和发送
inspur#**debug ip ospf retransmission** *<process-id>*	打开回送OSPF重传队列事件调试信息的开关
inspur#**debug ip ospf spf** [**external** | **inter** | **intra**]*<process-id>*	打开回送OSPF路由计算事件调试信息的开关
inspur#**debug ip ospf te-topology-change** *<process-id>*	打开回送OSPF拓扑变化通知RSVP事件调试信息开关

4.4.18 OSPF 建链功能配置实例

配置说明

如*图 4-25*所示，R1和R2通过两条链路建链，通告各自的一个回环地址路由。

图 4-25 OSPF 建链功能拓扑图



配置思路

1.R1和R2两条链路配置直连接口地址，并配置回环接口地址。

2.将各个接口加入到OSPF区域0里面。

3.双方配置负荷分担，可以看到从两个链路学到各自通告过来的回环地址的路由。

配置过程

R1上的配置：

```
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#ip address  11.22.1.1 255.255.255.0
R1(config-if-gei-1/3)#exit
R1(config)#interface gei-1/4
R1(config-if-gei-1/4)#no shutdown
R1(config-if-gei-1/4)#ip address  11.22.10.1 255.255.255.0
R1(config-if-gei-1/4)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.11 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 11.22.1.0 0.0.0.255
R1(config-ospf-1-area-0)#network 11.22.10.0 0.0.0.255
R1(config-ospf-1-area-0)#network 1.1.1.11 0.0.0.0
R1(config-ospf-1-area-0)#exit
R1(config-ospf-1)#maximum-paths 2
R1(config-ospf-1)#exit
```

R2上的配置：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address  11.22.1.2 255.255.255.0
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#ip address  11.22.10.2 255.255.255.0
R2(config-if-gei-1/2)#exit
R2(config)#interface loopback2
R2(config-if-loopback2)#ip address 1.1.1.22 255.255.255.255
R2(config-if-loopback2)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#router-id 1.1.1.22
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 11.22.1.0 0.0.0.255
R2(config-ospf-1-area-0)#network 11.22.10.0 0.0.0.255
R2(config-ospf-1-area-0)#network 1.1.1.22 0.0.0.0
R2(config-ospf-1-area-0)#exit
R2(config-ospf-1)#maximum-paths 2
```

```
R2(config-ospf-1)#exit
```

配置验证

上述的配置完成以后，在两端的设备上应该能够看到如下的信息，表明双方已经正确建立邻居。最后从两台设备上ping对端的loopback接口，都能够ping通，说明配置成功。

```
R1#show ip ospf neighbor

          OSPF Router with ID (1.1.1.11) (Process ID 1)

Neighbor ID    Pri State      DeadTime    Address      Interface
1.1.1.22       1   FULL/DR    00:00:40    11.22.1.2    gei-1/3
1.1.1.22       1   FULL/DR    00:00:37    11.22.10.2   gei-1/4

R1(config)#show ip forwarding route 1.1.1.22
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
        MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
        ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
        GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
        GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest           Gw           Interface      Owner    Pri  Metric
1.1.1.22/32    11.22.1.2    gei-1/3        OSPF     110  2
1.1.1.22/32    11.22.10.2   gei-1/4        OSPF     110  2
```

用ping测试连通性：

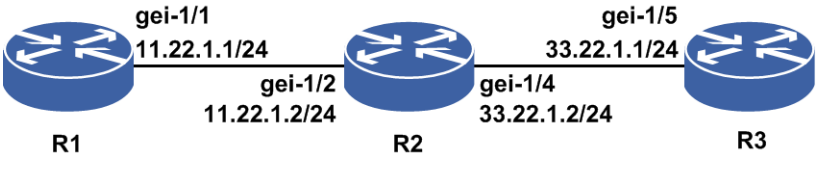
```
R1#ping 1.1.1.22
sending 5,100-byte ICMP echoes to 1.1.1.22,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.
```

4.4.19 OSPF NSSA 区域配置实例

配置说明

如*图 4-26*所示，R1不希望学到骨干区域的外部路由，但是需要将自己的外部路由通告出去。此时R1和R2应该建立NSSA区域，R2和R3在骨干区域中建链。

图 4-26 OSPF NSSA 区域配置拓扑图



配置思路

1.R1和R2在NSSA区域255建链，R2和R3在区域0建链。

2.R3上重分发直连路由，R1上重分发直连路由。

3.R2上配置NSSA缺省路由通告（也可以不配置，系统会自动产生7型0.0.0.0默认路由）。

4.可以看到R1上不能学到具体的R3上的地址明细路由，但是会有缺省路由指向R2，R3上可以学到R1上重分发过来的直连路由信息。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 11.22.1.1 255.255.255.0
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.11 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 255
R1(config-ospf-1-area-255)#network 11.22.1.0 0.0.0.255
R1(config-ospf-1-area-255)#nssa
R1(config-ospf-1-area-255)#exit
R1(config-ospf-1)#redistribute connected
R1(config-ospf-1)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#ip address 11.22.1.2 255.255.255.0
R2(config-if-gei-1/2)#exit
R2(config)#interface gei-1/4
R2(config-if-gei-1/4)#no shutdown
R2(config-if-gei-1/4)#ip address 33.22.1.2 255.255.255.0
R2(config-if-gei-1/4)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 255
R2(config-ospf-1-area-255)#network 11.22.1.0 0.0.0.255
R2(config-ospf-1-area-255)#nssa default-information-originate
 /*也可以不配置，系统会自动产生7型0.0.0.0默认路由*/
R2(config-ospf-1-area-255)#exit
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 33.22.1.0 0.0.0.255
R2(config-ospf-1-area-0)#exit
```

R3上的配置如下：

```
R3(config)#interface gei-1/5
R3(config-if-gei-1/5)#ip address 33.22.1.1 255.255.255.0
R3(config-if-gei-1/5)#no shutdown
R3(config-if-gei-1/5)#exit
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 1.1.1.33 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#router ospf 1
R3(config-ospf-1)#redistribute connected
R3(config-ospf-1)#area 0
R3(config-ospf-1-area-0)#network 33.22.1.0 0.0.0.255
R3(config-ospf-1-area-0)#exit
```

配置验证

在R1上用**show ip forwarding route 1.1.1.33**命令查看有没有到R3的具体路由信息：

```
R1(config)#show ip forwarding route 1.1.1.33
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
        MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
        ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
        GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
        GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest          Gw         Interface     Owner      Pri  Metric
*> 0.0.0.0/0   11.22.1.2   gei-1/1       OSPF       110  1
```

在R1上用**show ip forwarding route 0.0.0.0**命令查看是否有默认路由指向R2：

```
R1(config)#show ip forwarding route 0.0.0.0
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
        MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
        ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
        GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
        GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest          Gw        Interface     Owner      Pri  Metric
*> 0.0.0.0/0   11.22.1.2  gei-1/1       OSPF       110   1
```

在R3上用**show ip forwarding route 1.1.1.11**命令查看是否有到R1的具体路由信息：

```
R3(config)#show ip forwarding route 1.1.1.11
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
        MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
        ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
        GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
        GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest          Gw         Interface     Owner     Pri   Metric
1.1.1.11/32    33.32.1.1   gei-1/5       OSPF     110   2
```

在R3上测试到R1的连通性：

```
R3#ping 1.1.1.11
sending 5,100-byte ICMP echoes to 1.1.1.11,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.
```

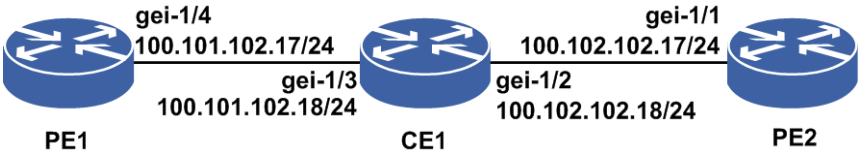
4.4.20 OSPF 多实例配置实例

配置说明

允许用户配置多个协议实体，这些协议实体可以属于同一个VPN/公网，也可以分属不同的VPN。不同的协议实体相互独立，各自维护自己的邻居关系，链路状态数据库，并独立的计算路由。但是属于同一个VPN/公网的多个实例共用同一个VPN/公网路由表。主要目的是进行网络的分割和隔离。主要体现在多个实例之间相互独立，维护各自的邻居关系，链路状态数据库，各自独立计算路由。

下面的配置实例是实现CE1上对PE1发送的OSPF泛洪信息和PE2发送的泛洪信息实现隔离功能。配置实例的拓扑图如*图 4-27*所示。

图 4-27 OSPF 多实例配置拓扑图



配置思路

1.PE1和CE1建立OSPF接入关系。

2.PE2和CE1建立OSPF接入关系。

3.PE2上不能学到vpn1上相关的链路状态信息。

配置过程

PE1上的配置：

```
PE1(config)#ip vrf vpn1
PE1(config-vrf-vpn1)#rd 100:100
PE1(config-vrf-vpn1)#route-target 100:100
PE1(config-vrf-vpn1)#address-family ipv4
PE1(config-vrf-vpn1-af-ipv4)#exit
PE1(config-vrf-vpn1)#exit
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip vrf forwarding vpn1
PE1(config-if-loopback1)#ip address 1.1.1.17 255.255.255.255
PE1(config-if-loopback1)#exit
PE1(config)#interface gei-1/4
PE1(config-if-gei-1/4)#no shutdown
PE1(config-if-gei-1/4)#ip vrf forwarding vpn1
PE1(config-if-gei-1/4)#ip address 100.101.102.17 255.255.255.0
PE1(config-if-gei-1/4)#exit
PE1(config)#router ospf 1 vrf vpn1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 1.1.1.17 0.0.0.0
PE1(config-ospf-1-area-0)#network 100.101.102.0 0.0.0.255
PE1(config-ospf-1-area-0)#exit
```

CE1上的配置：

```
CE1(config)#interface loopback1
CE1(config-if-loopback1)#ip address 1.1.1.18 255.255.255.255
CE1(config-if-loopback1)#exit
CE1(config)#interface loopback2
CE1(config-if-loopback2)#ip address 2.2.2.18 255.255.255.255
CE1(config-if-loopback2)#exit
CE1(config)#interface gei-1/3
CE1(config-if-gei-1/3)#no shutdown
CE1(config-if-gei-1/3)#ip address 100.101.102.18 255.255.255.0
CE1(config-if-gei-1/3)#exit
CE1(config)#interface gei-1/2
CE1(config-if-gei-1/2)#no shutdown
CE1(config-if-gei-1/2)#ip address 100.102.102.18 255.255.255.0
CE1(config-if-gei-1/2)#exit
CE1(config)#router ospf 1
CE1(config-ospf-1)#area 0
CE1(config-ospf-1-area-0)#network 1.1.1.18 0.0.0.0
CE1(config-ospf-1-area-0)#network 100.101.102.0 0.0.0.255
CE1(config-ospf-1-area-0)#exit
```

```
CE1(config)#router ospf 2
CE1(config-ospf-2)#area 0
CE1(config-ospf-2-area-0)#network 2.2.2.18 0.0.0.0
CE1(config-ospf-2-area-0)#network 100.102.102.0 0.0.0.255
CE1(config-ospf-2-area-0)#exit
```

PE2上的配置：

```
PE2(config)#ip vrf vpn2
PE2(config-vrf-vpn2)#rd 200:200
PE2(config-vrf-vpn2)#route-target 200:200
PE2(config-vrf-vpn2)#address-family ipv4
PE2(config-vrf-vpn2-af-ipv4)#exit
PE2(config-vrf-vpn2)#exit
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip vrf forwarding vpn2
PE2(config-if-loopback1)#ip address 1.1.1.19 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#interface gei-1/1
PE2(config-if-gei-1/1)#no shutdown
PE2(config-if-gei-1/1)#ip vrf forwarding vpn2
PE2(config-if-gei-1/1)#ip address 100.102.102.17 255.255.255.0
PE2(config-if-gei-1/1)#exit
PE2(config)#router ospf 1 vrf vpn2
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 1.1.1.19 0.0.0.0
PE2(config-ospf-1-area-0)#network 100.102.102.0 0.0.0.255
PE2(config-ospf-1-area-0)#exit
```

配置验证

配置完成后，CE1可以学到PE1通告的looback1的路由，也可以学到PE2通告的loopback1的路由，但是PE2和PE1上都学不到对方的路由。故说明OSPF多实例起到了作用。

```
CE1#show ip forwarding route ospf
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest              Gw              Interface       Owner    Pri Metric
1.1.1.17/32       100.101.102.17  gei-1/3           OSPF     110 1
1.1.1.19/32       100.102.102.17  gei-1/2           OSPF     110 1

PE2#show ip forwarding route vrf vpn2
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest              Gw              Interface       Owner    Pri Metric
2.2.2.18/32       100.102.102.18  gei-1/2           OSPF     110 1

PE1#show ip forwarding route vrf vpn1
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
```

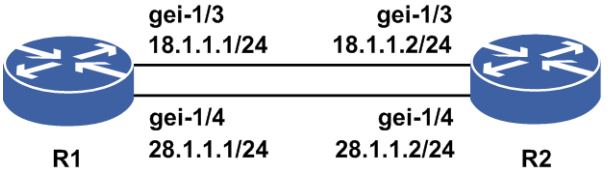
```
        GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
        GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest              Gw            Interface      Owner    Pri Metric
1.1.1.18/32       100.101.102.18  gei-1/4        OSPF     110 1
```

4.4.21 OSPF FRR 配置实例

配置说明

如*图 4-28*所示，R1和R2之间，直连两条物理链路，R1上形成到R2的路由的主备链路。

图 4-28 OSPF FRR 配置实例示意图



配置思路

1.R1和R2建立两条链路，启用OSPF协议。

2.R2上通告路由，启用R1上FRR配置。

3.断开R1到R2的主链路，观察R1到R2的流量丢包情况。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#ip address 18.1.1.1 255.255.255.0
R1(config-if-gei-1/3)#exit
R1(config)#interface gei-1/4
R1(config-if-gei-1/4)#ip address 28.1.1.1 255.255.255.0
R1(config-if-gei-1/4)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 10.10.10.1 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#fast-reroute per-prefix
R1(config-ospf-1)#interface gei-1/3
R1(config-ospf-1-if-gei-1/3)#cost 4
R1(config-ospf-1-if-gei-1/3)#exit
R1(config-ospf-1)#interface gei-1/4
R1(config-ospf-1-if-gei-1/4)#cost 5
R1(config-ospf-1-if-gei-1/4)#exit
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 18.1.1.0 0.0.0.255
R1(config-ospf-1-area-0)#network 28.1.1.0 0.0.0.255
R1(config-ospf-1-area-0)#network 10.10.10.1 0.0.0.0
R1(config-ospf-1-area-0)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#ip address 18.1.1.2 255.255.255.0
R2(config-if-gei-1/3)#exit
R2(config)#interface gei-1/4
R2(config-if-gei-1/4)#ip address 28.1.1.2 255.255.255.0
R2(config-if-gei-1/4)#exit
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 10.10.10.1 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 18.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#network 28.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#network 10.10.10.2 0.0.0.0
R2(config-ospf-1-area-0)#exit
```

配置验证

R1上形成到R2的路由的主备链路。

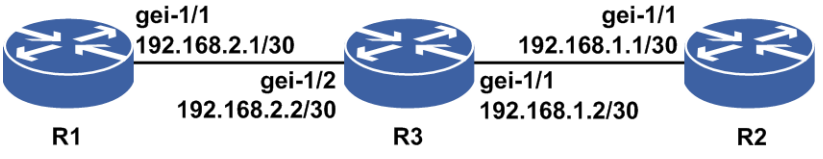
```
R1#show ip forwarding backup route
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority,  M/S: Master/Slave,
         Sta: Status;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best, M: Master, S: Slave, I: Inuse, U: Unuse;
   Dest             Gw         Interface       Owner  Pri Metric M/S  Sta
*> 10.10.10.2/32   18.1.1.2       gei/3         OSPF   110 5      M    I
*  10.10.10.2/32   28.1.1.2       gei/4         OSPF   110 6      S    U
```

4.4.22 OSPF 区域间路由聚合配置实例

配置说明

如*图 4-29*所示，在R1、R3和R2上都启用OSPF协议，在R3上配置路由聚合，简化了路由表。

图 4-29 OSPF 区域间路由聚合配置实例示意图



配置思路

1.按*图 4-29*所示搭建环境，在R1、R3和R2上都启用OSPF协议。配置R1和R3建立OSPF邻居，处于area0中，R2和R3建立OSPF邻居，处于area1中，并在R2上配置4个连续网段的loopback地址，均宣告进OSPF中。

2.在R3上做路由聚合，查看R1上路由学习情况。

配置过程

R1的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 2.2.2.2 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 192.168.2.1 255.255.255.252
R1(config-if-gei-1/1)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 192.168.2.0 0.0.0.255
R1(config-ospf-1-area-0)#network 2.2.2.2 0.0.0.0
R1(config-ospf-1-area-0)#exit
```

R3的配置如下：

```
R3(config)#interface gei-1/1
R3(config-if-gei-1/1)#ip address 192.168.1.2 255.255.255.252
R3(config-if-gei-1/1)#exit
R3(config)#interface gei-1/2
R3(config-if-gei-1/2)#ip address 192.168.2.2 255.255.255.252
R3(config-if-gei-1/2)#exit
R3(config)#router ospf 1
R3(config-ospf-1)#area 0
R3(config-ospf-1-area-0)#network 192.168.2.0 0.0.0.255
R3(config-ospf-1)#area 1
R3(config-ospf-1-area-1)#network 192.168.1.0 0.0.0.255
R3(config-ospf-1-area-1)#range 1.1.0.0 255.255.0.0 summary-link advertise
R3(config-ospf-1-area-1)#exit
```

R2的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface loopback2
R2(config-if-loopback2)#ip address 1.1.1.2 255.255.255.255
R2(config-if-loopback2)#exit
R2(config)#interface loopback3
R2(config-if-loopback3)#ip address 1.1.1.3 255.255.255.255
R2(config-if-loopback3)#exit
R2(config)#interface loopback4
R2(config-if-loopback4)#ip address 1.1.1.4 255.255.255.255
R2(config-if-loopback4)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 192.168.1.1 255.255.255.252
R2(config-if-gei-1/1)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 1
R2(config-ospf-1-area-1)#network 192.168.1.0 0.0.0.3
R2(config-ospf-1-area-1)#network 1.1.1.1 0.0.0.0
R2(config-ospf-1-area-1)#network 1.1.1.2 0.0.0.0
R2(config-ospf-1-area-1)#network 1.1.1.3 0.0.0.0
R2(config-ospf-1-area-1)#network 1.1.1.4 0.0.0.0
R2(config-ospf-1-area-1)#exit
```

配置验证

查看R1的路由，只能学习到R2的4个loopback地址网段的聚合路由信息。

```
R1#show ip forwarding  route
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
   Dest              Gw           Interface          Owner      Pri Metric
*> 1.1.0.0/16       192.168.2.2      gei-2/1           OSPF       110   22
```

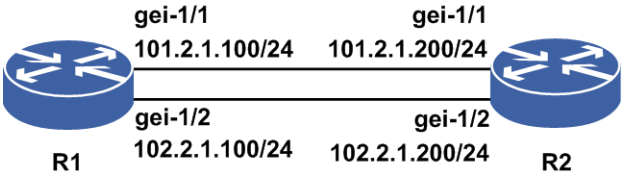
4.4.23 OSPF 路由负荷分担配置实例

配置说明

负荷分担可使超出单个接口带宽的流量均分到多条链路上，实现流量在各条链路上的负载均衡。

如*图 4-30*所示，同一邻居节点在同一区域有多条链路可达，且其链路代价相同，启用负荷分担，则可实现OSPF的负荷分担。

图 4-30 OSPFv2 路由负荷分担配置实例



配置思路

1.配置接口，并配置逐包的负荷分担（默认为逐流分担）。

2.启用并配置OSPF协议。

3.在R1上配置OSPF的负荷分担。

配置过程

R1的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 101.2.1.100 255.255.255.0
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip address 102.2.1.100 255.255.255.0
R1(config-if-gei-1/2)#exit

R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 101.2.1.0 0.0.0.255
R1(config-ospf-1-area-0)#network 102.2.1.0 0.0.0.255
R1(config-ospf-1-area-0)#exit
```

```
R1(config-ospf-1)#maximum-paths 2
R1(config-ospf-1)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip load-sharing per-packet
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip load-sharing per-packet
R1(config-if-gei-1/2)#exit
```

R2的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 101.2.1.200 255.255.255.0
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 102.2.1.200 255.255.255.0
R2(config-if-gei-1/2)#exit
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.200 255.255.255.255
R2(config-if-loopback1)#exit

R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 101.2.1.0 0.0.0.255
R2(config-ospf-1-area-0)#network 102.2.1.0 0.0.0.255
R2(config-ospf-1-area-0)#network 1.1.1.200 0.0.0.0
R2(config-ospf-1-area-0)#end
```

配置验证

用show命令验证配置结果：

```
R1#show ip forwarding route ospf
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest          Gw           Interface      Owner   Pri  Metric
1.1.1.200/32   101.2.1.200    gei-1/1        OSPF    110  2
1.1.1.200/32   102.2.1.200    gei-1/2        OSPF    110  2
```

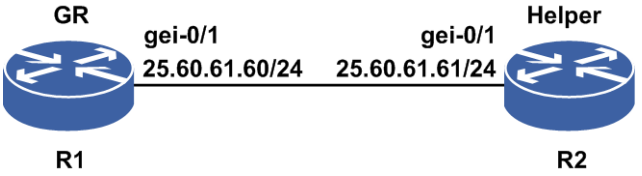
可以看到，到达统一目的地有两条路由，分别走不同的出接口，负荷分担配置成功。

4.4.24 OSPF Graceful Restart 配置实例

配置说明

如*图 4-31*所示，路由器R1、R2是OSPF邻居，现在R1和R2上开启Graceful Restart功能，使得能够在R1或R2主备倒换时仍然能够正常转发数据报文。

图 4-31 配置 OSPF Graceful Restart



配置思路

1.配置路由器R1、R2形成OSPF邻居

2.在R1、R2上开启Graceful Restart功能

配置过程

R1上的配置如下：

```
R1(config)#interface gei-0/1
R1(config-if-gei-0/1)#no shutdown
R1(config-if-gei-0/1)#ip address 25.60.61.60 255.255.255.0
R1(config-if-gei-0/1)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 25.60.61.0 0.0.0.255
R1(config-ospf-1-area-0)#exit
R1(config-ospf-1)#nsf
```

R2上的配置如下：

```
R2(config)#interface gei-0/1
R2(config-if-gei-0/1)#no shutdown
R2(config-if-gei-0/1)#ip address 25.60.61.61 255.255.255.0
R2(config-if-gei-0/1)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 25.60.61.0 0.0.0.255
R2(config-ospf-1-area-0)#exit
R2(config-ospf-1)#nsf
```

配置验证

主备倒换R1后，流量仍然能够正常转发。

R1上相关信息

查看GR中的路由器信息：

```
R1(config)#show ip ospf nsf
        OSPF Router with ID (221.11.129.142) (Process ID 1)
OSPF instance is graceful restarting
   Restart reason is switch to redundant control processor
   Grace period 120
   Start time 00:12:46
   Time to leave 22 s

   Helper 221.11.129.141
```

```
     In the area 0.0.0.0
     via interface gei-0/1 25.60.61.61
     Neighbor is BDR
     State FULL
```

查看GR功能时的type-9型LSA的信息：

```
R1(config)#show ip ospf database opaque-link
          OSPF Router with ID (221.11.129.142) (Process ID 1)
          Type-9 Opaque Link-local Link States (Area 0.0.0.0)
  LS age: 62
  Options: (No TOS-capability, DC)
  LS Type: Opaque Link-local
  Link State ID: 3.0.0.0
  Opaque Type: 3
  Opaque ID: 0
  Advertising Router: 221.11.129.142
  LS Seq Number: 0x80000001
  Checksum: 0xfdd5
  Length: 44
  Fragment number: 0

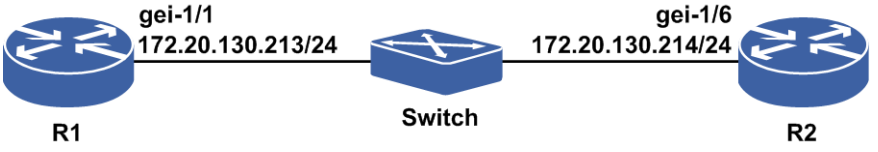
    Grace period: 120
     NSF reason: switch to redundant control processor
      Interface ip address: 25.60.61.60
```

4.4.25 OSPF BFD 配置实例

配置说明

如*图 4-32*所示，R1、R2之间运行OSPF 协议，R1、R2协议接口下使能BFD。

图 4-32 OSPF BFD 配置实例



配置思路

1.R1、R2之间运行OSPF 协议。

2.R1、R2协议接口下使能BFD。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 172.20.130.213 255.255.255.0
R1(config-if-gei-1/1)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 0
```

```
R1(config-ospf-1-area-0)#network 172.20.130.0 0.0.0.255
R1(config-ospf-1-area-0)#bfd
R1(config-ospf-1-area-0)#end
```

R2上的配置如下：

```
R2(config)#interface gei-1/6
R2(config-if-gei-1/6)#ip address 172.20.130.214 255.255.255.0
R2(config-if-gei-1/6)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 172.20.130.0 0.0.0.255
R2(config-ospf-1-area-0)#bfd
R2(config-ospf-1-area-0)#end
```

配置验证

正确配置后，OSPF BFD会话应该能够成功建立，可以用如下命令查看结果：

用**show bfd neighbors** [**ip brief**|**ip detail**]来查看验证OSPF BFD是否生效。

R1上OSPF BFD生效情况查看：

```
R1(config)#show bfd neighbors ip brief
LocalAddr        PeerAddr        LD     RD     Hold   State   Interface
172.20.130.213   172.20.130.214  3      3      150    UP      gei-1/1

R1(config)#show bfd neighbors ip detail
------------------------------------------------------------------------------
--
LocalAddr:172.20.130.213
PeerAddr :172.20.130.214
Local Discr:1              Remote Discr:3          State:UP

Holdown(ms):150           Interface: gei-1/1
Vpnid:0                   VRF Name:---
BFD Type:SingleHop
Instance Name:
------------------------------------------------------------------------------
--
Version:1               Dest UDP Port:3784       Final Bit:1
Local Diag:0            Demand Mode:0            Poll Bit:1
MinTxInt:50             MinRxInt:50              Multiplier:3
Received MinTxInt:50     Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24        Max BFD Length:24

Rx Count:0              Rx Interval (ms) min/max/avg:0     /0     /0
Tx Count:0              Tx Interval (ms) min/max/avg:0     /0     /0
Registered Protocols:OSPF
Uptime:0 day(s),0 hour(s),0 minute(s)
Control Plane Rcv Phy Interface Name: gei-1/1
==============================================================================
```

4.5 IS-IS

IS-IS协议是由国际标准化组织提出的用于无连接网络服务（CLNS）的路由协议，是OSI协议模型中的网络层协议。通过对IS-IS协议进行扩充，增加了对IP路由的支持，形成了集成化的IS-IS协议，现在使用的IS-IS协议都是指集成化的IS-IS协议。

IS-IS已作为一种内部网关协议（IGP）在网络中大量使用，其工作机制与OSPF类似。

通过将网络划分成区域，区域内的路由设备只管理区域内路由信息，从而节省路由设备开销，此特点使其能适应中大型网络的需要。

如果一组路由设备具有相同的区域ID，那么属于同一区域。IS-IS区域的划分在链路上，IS-IS路由设备完全处于一个区域内，与OSPF按照接口进行区域划分的概念不同。

IS-IS协议使用两层路由体系：Level-1和Level-2。

- Level-1路由器只知道本区域中的拓扑（包括所有的路由设备和主机），而不知道区域以外的路由设备及其目的地。Level-1路由器将去往其它区域的所有流量都转发给本区域内最近的Level-1-2路由设备，该设备知道Level-2的拓扑。

  Level-1-2路由设备是不同区域的边界路由设备，提供区域连接。

- Level-2骨干区域实际是一个虚拟的IS-IS区域，由参与Level-2路由选择的路由设备组成。

  在IS-IS网络中，Level-2区域必须是连续的，所有路由设备必须完全互联。

4.5.1 配置 IS-IS 基本信息

本节介绍IS-IS基本信息的配置步骤和命令。

1.启动IS-IS，设置IS-IS的区域和系统ID。

步骤	命令	功能
1	inspur(config)#**router isis** <*process-id*>[**vrf** <*vrf-name*>]	启动IS-IS路由协议，进入IS-IS 路由配置模式
2	inspur(config-isis-process-id)#**area** <*area-address*>	IS-IS路由模式下设定IS-IS区域，指定该路由器属于该区域 所配置的区域地址为1~13个字节的16进制字符串
3	inspur(config-isis-process-id)#**system-id** <*system-id*>[**range** <*range-number*>]	设置IS-IS的系统ID，用于在该区域中标识该路由器，是6个字节的16进制字符串，通常以该路由器某一接口MAC地址表示

2.设置运行IS-IS的接口。

步骤	命令	功能
1	inspur(config-isis-process-id)#**interface** <*interface-name*>	进入接口配置模式
2	inspur(config-isis-process-id-if-interface-name)#**ip router isis**	指定该接口运行IS-IS 配置IS-IS时，必须要在路由器上指定哪个接口运行IS-IS协议

4.5.2 配置 IS-IS 全局参数

如果该网络中运行的都是inspur系列设备，在配置IS-IS时，使用缺省参数即可。但在与其他厂家设备对接时，相关的接口参数和定时器可能需要加以调整，以使IS-IS协议在网络中能够更加高效的运行。

1.进入IS-IS路由配置模式。

命令	功能
inspur(config)#**router isis** < *process-id*>[**vrf** < *vrf-name*>]	启动IS-IS路由协议 ，进入IS-IS路由配置模式

2.配置IS-IS全局参数。

命令	功能
inspur(config-isis-process-id)#**is-type** {**level-1** | **level-1-2** | **level-2-only**}	设置本路由器的Level级别，可设置的级别为：level-1、level-1-2、level-2-only 缺省情况下，运行IS-IS协议的路由器被标识为level-1-2
inspur(config-isis-process-id)#**metric-style** < **narrow** | **wide** >	设置metric-style，Narrow模式仅有6bits位来携带metric值，wide模式有24bits位来携带metric值，且支持携带更多的TLV扩展 缺省配置为narrow模式 当设备对接邻居建立后，由于metric-style类型的不一致，会导致拓扑建立不成功
inspur(config-isis-process-id)#**lsp-refresh-time** < *refresh-time* >	设置本地LSP刷新间隔，单位：秒，范围1~65535 在网络稳定的情况下定期更新本地生成的LSP，缺省情况下的LSP的刷新间隔为900秒
inspur(config-isis-process-id)#**max-lsp-lifetime** < *time* >	设置本地LSP最大保活时间，即设置本地产生的LSP报文在所有可达节点数据库中的存活时间，单位：秒，范围1~65535 缺省情况下的LSP的最大保活时间为1200秒
inspur(config-isis-process-id)#**distance** < *value* >	设置IS-IS协议在本地的协议优先级别，与其它协议进行优先级比较，范围1~255，默认为115
inspur(config-isis-process-id)#**set-overload-bit** [**on-start-up** {<*5-86400*>| **auto** | **wait-for-bgp**}][**suppress** {**all** | **external** | **interlevel**}]	设置IS-IS的OL标志位，该标志在本路由器处理能力不足时，用来向运行IS-IS的其它路由器发出通告，拓扑及路由信息不能通过本路由器再向下传递
inspur(config-isis-process-id)#**default-information originate** [**always**][**metric** <*metric-value*>][**metric-type** <*type*>][**level-1** | **level-1-2** | **level-2**]	配置该命令产生缺省路由 当配置路由重分发时，路由器需要使用这个命令才能将路由条目中的默认路由重分发进IS-IS域 **always:** 无论再分配路由条目中是否有缺省

命令	功能
	路由，系统总是生成一个缺省路由通告条目。如果不设置此参数，只有在重分配路由中有缺省路由时才通告
inspur(config-isis-process-id)#**summary-address** <*ip-address*><*net-mask*>[**metric** <*metric-value*>][**level-1** | **level-1-2** | **level-2**]	配置路由汇聚 IS-IS可以将路由表中的部分条目汇聚后产生一个聚合路由向外通告，而不用再通告具体的路由条目
inspur(config-isis-process-id)#**hello padding** {**multi-point** | **point-to-point** }	配置将发送的Hello报文填充至最大报文长度，分为广播网和点到点报文两种填充方式
inspur(config-isis-process-id-if-interface-name)#**network point-to-point**	配置使能了IS-IS的广播链路接口模拟为点到点接口

on-start-up { **5-86400** | **auto** | **wait-for-bgp** }：

- 5~86400：在重启后可以选择等待5~86400中的某段时间后OL取消置位。
- **auto**：选择数据库同步完成后OL取消置位。
- **wait-for-bgp**：等待BGP同步完成后OL取消置位。

suppress {**all** | **external** | **interlevel**}：

- **all**：同时抑制重分发及level-1和level-2间的路由泄露。
- **external**：抑制重分发路由的本地学习。
- **interlevel**：抑制level-1和level-2间的路由泄漏。

4.5.3 配置 IS-IS 接口参数

本节介绍IS-IS接口参数的配置步骤和命令。

1.进入IS-IS接口配置模式。

步骤	命令	功能
1	inspur(config)#**router isis** < *process-id*>[**vrf** < *vrf-name*>]	进入IS-IS路由配置模式
2	inspur(config-isis-process-id)#**interface** <*interface-name*>	进入IS-IS接口配置模式

2.配置IS-IS接口可选参数。

命令	功能
inspur(config-isis-process-id-if-interface-name)#**circuit-type** {**level-1**|**level-1-2**|**level-2-only**}	这是IS-IS配置中的一个基本参数设置，用于指定该接口的level类型，默认为level-1-2，该值需要与IS-IS全局操作类型匹

命令	功能
	配，直连建邻居的两端也要有匹配项
inspur(config-isis-process-id-if-interface-name)#**hello-interval** <*interval*>[**level-1** | **level-2**]	配置端口发送Hello的间隔时间，单位：秒，范围1~65535，缺省为10秒 广播链路DIS选举出来后，在DIS端定时间隔为3秒，不可修改 不带可选参数时表示该interval同时对level-1、level-2的发送间隔生效
inspur(config-isis-process-id-if-interface-name)#**hello-multiplier** <*multiplier*>[**level-1** | **level-2**]	配置接口的保存时间与hello间隔时间的倍数，multiplier的范围3~1000，缺省为3 不带可选参数时表示该multiplier同时对level-1、level-2的间隔倍数生效
inspur(config-isis-process-id-if-interface-name)#**lsp-interval** <*interval*>[**level-1** | **level-2**]	配置LSP的传输间隔，单位：秒，范围33~4294967040，缺省为33秒 不带可选参数时表示该interval同时对level-1、level-2的传输间隔生效
inspur(config-isis-process-id-if-interface-name)#**retransmit-interval** <*interval*>[**level-1** | **level-2**]	设置LSP的重传间隔，单位：秒，范围1~65535，缺省为5秒 该配置仅在点到点链路下生效，不带可选参数时表示该retransmit-interval对level-1、level-2的重传间隔都生效
inspur(config-isis-process-id-if-interface-name)#**priority** <*priority*>[**level-1** | **level-2**]	配置接口的DIS选举优先级，范围0~127，缺省为64，值较大的当选为DIS 该配置仅对广播链路生效，不带可选参数时表示该priority对level-1、level-2的接口优先级都生效
inspur(config-isis-process-id-if-interface-name)#**metric** <*metric-value*>[**level-1** | **level-2**]	设置IS-IS接口度量值，缺省为10，**wide**模式下该度量值取值范围是1~16777215，**narrow**模式下取值范围是1~63 不带可选参数时表示该metric-value对该接口的level-1、level-2度量值都生效
inspur(config-isis-process-id-if-interface-name)#**csnp-interval** <*interval*>[**level-1** | **level-2**]	设置CSNP传输间隔，单位：秒，范围1~65535，在广播链路上缺省为10秒，在点到点链路上缺省为3600秒 不带可选参数时表示该interval对该接口的level-1、level-2 csnp发送间隔都生效
inspur(config-isis-process-id-if-interface-name)#**psnp-interval** <*interval*>[**level-1** | **level-2**]	在端口上设置设置PSNP的传输间隔，单位：秒，范围1~65535，缺省为3秒 不带可选参数时表示该interval对该接口的level-1、level-2 psnp发送间隔都生效

4.5.4 配置 IS-IS 认证

IR12000支持明文认证和MD5认证两种认证方式。本节介绍IS-IS认证的配置步骤和命令。

相关信息

IR12000支持四种类型的IS-IS认证：

·邻居之间认证

·区域内部认证

·区域之间认证

·SNP之间认证

1.配置IS-IS认证方式、认证密码及认证区域。

步骤	命令	功能
1	inspur(config)#**router isis** <*process-id*>[**vrf** < *vrf-name*>]	启动IS-IS路由协议 ，进入IS-IS路由配置模式
2	inspur(config-isis-process-id)#**authentication-type** <*type*>[**level-1** | **level-2**]	配置认证方式，认证类型为text 或MD5方式 不带可选参数时表示该认证类型同时对level-1、level-2 生效
3	inspur(config-isis-process-id)#**authentication** {<*password*>|[**encrypt**< *password*>|**clear** <*password*>]}[**level-1** | **level-2**]	路由模式下配置IS-IS认证，明文密码长度为1~100个字符，加密密码长度为24~140个字符 不带可选参数时表示该认证同时对level-1、level-2的SNP报文生效

默认情况路由模式下的认证同时是对SNP及LSP报文的认证，如果仅对LSP报文进行加密，则配置**disable-snp-authentication**命令可以实现。

2.配置IS-IS接口认证。

步骤	命令	功能
1	inspur(config-isis-process-id)#**interface** <*interface-name*>	进入IS-IS接口配置模式
2	inspur(config-isis-process-id-if-interface-name)#**authentication-type** <*type*>[**level-1** | **level-2**]	接口模式下配置认证方式，认证类型为text 或 md5方式 不带可选参数时表示该认证类型同时对level-1、level-2 生效
3	inspur(config-isis-process-id-if-interface-name)#**authentication** {<*password*>|[**encrypt**< *password*>|**clear** <*password*>]}[**level-1** | **level-2**]	配置hello报文的认证，明文密码长度为1~100个字符，加密密码长度为24~140个字符 不带可选参数时表示该认证同时对

步骤	命令	功能
		level-1、level-2的hello报文生效

3.（可选）设置对SNP报文的认证。

步骤	命令	功能
1	inspur(config)#**router isis** <*process-id*>[**vrf** <*vrf-name*>]	启动IS-IS路由协议，进入IS-IS路由配置模式
2	inspur(config-isis-process-id)#**enable-snp-authentication**	在配置了LSP认证之后，同时对SNP报文也设置同样的认证码，默认情况下对SNP报文也同时进行认证

4.5.5 配置 IS-IS Hostname

本节介绍IS-IS Hostname的配置步骤和命令。

1.进入IS-IS路由配置模式

命令	功能
inspur(config)#**router isis** <*process-id*>[**vrf** <*vrf-name*>]	进入IS-IS路由配置模式

2.配置IS-IS Hostname。

命令	功能
inspur(config-isis-process-id)#**hostname dynamic** {**enable** | **disable**}	设置IS-IS的动态获取系统名称功能，默认已启动该功能，故配置后配置信息中不显示该条配置

4.5.6 配置 IS-IS mesh-group

本节介绍IS-IS mesh-group的配置步骤和命令。

1.进入IS-IS接口配置模式。

步骤	命令	功能
1	inspur(config)#**router isis** <*process-id*>[**vrf** <*vrf-name*>]	启动IS-IS路由协议 ，进入IS-IS路由配置模式
2	inspur(config-isis-process-id)#**inter**	进入接口配置模式

步骤	命令	功能
	face <*interface-name*>	

2.配置IS-IS mesh-group。

步骤	命令	功能
1	inspur(config-isis-process-id-if-interface-name)#**mesh-group blocked**	配置mesh-group的属性为meshBlocked，即在此接口上阻塞LSP信息
2	inspur(config-isis-process-id-if-interface-name)#**mesh-group** <*mesh-group-number*>	配置接口属于哪个mesh-group，mesh-group范围为1~4294967295

4.5.7 配置 IS-IS 重分发

本节介绍IS-IS重分发其它路由协议路由的配置步骤和命令。

1.进入IS-IS路由配置模式。

命令	功能
inspur(config)#**router isis** < *process-id*>[**vrf** < *vrf-name*>]	启动IS-IS路由协议 ，进入IS-IS路由配置模式

2.配置IS-IS重分发其它路由协议路由。

命令	功能
inspur(config-isis-process-id)#**redistribute** <*protocol*>[**level-1**][**level-1-2**][**level-2**][**metric-type** <*metric-type*>][**metric** <*metric-value*>][**route-map** <*map-tag*>][**with-originate-metric**]	在IS-IS路由模式下，配置重分发

<*protocol*>：路由来源，可以为connected、static、rip、isis <process-id>、ospf <process-id>、bgp、nat、natpt、ps-busi-addr、ps-user-addr、sl-nat64-ipv4、subscriber-aggregation、subscriber-host和user-special，这是必选项，若重分配isis/ospf路由，则需要指定相应的实例号。

level-1：设置重分发的路由信息进入Level-1。

level-1-2：设置重分发的路由信息同时进入Level1和Level-2。

level-2：设置重分发的路由信息进入Level2 。

<*metric-type*>：设置重分发的路由是携带external还是internal的metric值。

<*metric-value*>：Metric值，范围0~4261412864。

route-map <*map-name*>：引用一个route-map。

4.5.8 配置 IS-IS 负荷分担

IS-IS支持负荷分担，负荷分担指到目的地有多条开销相同的链路可以用来分担流量。

相关信息

路由负荷分担有两个主要的功能：

- 提高链路可靠性：网络的传输层对稳定性和可靠性要求很高。这种可靠性表现在除了链路本身可靠外还应表现在当某条链路出现故障的时候不影响其他路径上的报文转发或者减少转发失败的影响。
- 提高带宽：路由负荷分担功能使得路由器能够将流量分配到多条路径上，从而充分利用带宽资源。通过路由协议或静态配置，可以使得转发表中，对于同一个目的地址，有多条可用的路由条目。

负荷分担的转发机制支持两种方法，per-packet （逐包模式）和 per-destination（逐流模式），下表给出了这两种方法的优缺点：

—	逐流模式	逐包模式
优点	到给定目的的包可以保证走同一条路径，即使在有多条可用路径的情况下；到不同目的的包可以走不同的路径	路径利用率高，因为per-packet 使用轮转法来确定数据包走的路径，使得转发负荷均匀地分布在各条路径上
缺点	当流量中只有少量的目的地址时，可能会引起流量集中在少数路径上，分担不均衡；当流量中目的地址增加时，负荷分担会更有效	对于到给定目的的流量可能会选择不同的路径，造成接收端的排序，对于VoIP和其他要求有序的流量不适用

1.配置IS-IS支持负荷分担。

步骤	命令	功能
1	inspur(config)#**router isis** [<*process-id*>][**vrf** <*vrf-name*>]	进入IS-IS路由配置模式
2	inspur(config-isis-process-id)#**maximum-paths** < *number*>	配置协议支持负荷分担的路由数目，范围1~32，缺省为1

2.配置IS-IS接口负荷分担。

步骤	命令	功能
1	inspur(config)#**interface** < *interface-name*>	进入接口配置模式
2	inspur(config-if-interface-name)#**ip load-sharing** {**per-destination** | **per-packet**}	配置接口负荷分担模式：负荷分担是在出接口上配置的，默认情况下为**per-destination**

步骤	命令	功能
		只有所有的接口配置为**per-packet**模式，负荷分担的模式才是**per-packet**
3	inspur(config-if-interface-name)#**load-sharing bandwidth** < *bandwidth-value*>	配置接口负荷分担的权重：权重设置在出接口上，只有配置了优先级后，配置的权重才有效；权重的范围不同的接口大小值不同

4.5.9 配置 IS-IS 流量工程

IR12000上IS-IS IPv4支持公网TE功能。

1.进入IS-IS路由配置模式。

命令	功能
inspur(config)#**router isis** < *process-id*>[**vrf** < *vrf-name*>]	启动IS-IS路由协议，进入IS-IS路由配置模式

2.配置IS-IS流量工程。

步骤	命令	功能
1	inspur(config-isis-process-id)#**metric-style wide**	在IS-IS路由模式下，配置宽度量
2	inspur(config-isis-process-id)#**mpls traffic-eng level-1**	在IS-IS Level-1上使能TE
3	inspur(config-isis-process-id)#**mpls traffic-eng level-2**	在IS-IS Level-2上使能TE

4.5.10 配置 IS-IS FRR

IS-IS FRR功能主要用于计算备份拓扑，当主链路失效时，流量可以立即转向备份链路，避免数据流失。

1.开启IS-IS FRR。

步骤	命令	功能
1	inspur(config)#**router isis** < *process-id*>[**vrf** < *vrf-name*>]	启动IS-IS路由协议，进入IS-IS路由配置模式

步骤	命令	功能
2	inspur(config-isis-process-id)#**fast-reroute lfa** {**enable** | **disable**}	在IS-IS路由模式下，开启或关闭快速重路由，默认为关闭快速重路由

2.配置IS-IS FRR路由备份方式。

命令	功能
inspur(config-isis-process-id)#**fast-reroute lfa alternate-type down-stream-path**	配置 IS-IS FRR计算方式为down-stream-path，默认为LFA

3.配置IS-IS FRR接口。

步骤	命令	功能
1	inspur(config-isis-process-id)#**interface** <*interface-name*>	进入接口配置模式
2	inspur(config-isis-process-id-interface-name)#**fast-reroute lfa block**	设置该接口不参与IS-IS FRR计算，不用于形成备份链路

4.5.11 配置 IS-IS Graceful Restart

本节介绍IS-IS Graceful Restart的配置步骤和命令。

1.启动IS-IS，设置IS-IS的区域和系统ID。

步骤	命令	功能
1	inspur(config)#**router isis**	进入IS-IS配置模式
2	inspur(config-isis-process-id)#**area** <***area-address***>	配置IS-IS区域地址
3	inspur(config-isis-process-id)#**system-id** <*system-id*>[**range** <*range-number*>]	配置IS-IS系统ID

2.开启IS-IS Graceful Restart，设置IS-IS T2、T3定时器。

步骤	命令	功能
1	inspur(config-isis-process-id)#**restart enable**	配置IS-IS GR使能
2	inspur(config-isis-process-id)#**restart t2-timer** <*t2-interval*>[**level-1** | **level-2**]	配置IS-IS T2（Graceful Restart的数据库同步定时器）时间间隔，范围：5~65535，单位：秒

步骤	命令	功能
3	inspur(config-isis-process-id)#**restart t3-timer** {**adjacency** | **manual** <*t3-interval*>}	配置IS-IS T3（设置raceful Restart的完成时间定时器）时间间隔，范围：1~65535，单位：秒

adjacency：指根据邻居通告的hello报文中设置的保持时间确定T3。

manual：指根据手工配置的值确定T3。

3.配置IS-IS Graceful Restart接口。

步骤	命令	功能
1	inspur(config-isis-process-id)#**interface** <*interface-name*>	进入IS-IS接口配置模式
2	inspur(config-isis-process-id-if-interface-name)#**ip router isis**	配置IS-IS接口使能IPv4
3	inspur(config-isis-process-id-if-interface-name)#**hello-multiplier** <*multiplier*>[**level-1** | **level-2**]	配置IS-IS邻居关系保活乘数，缺省为3，范围：3~1000
4	inspur(config-isis-process-id-if-interface-name)#**restart t1-retry** <*retry-timers*>[**level-1** | **level-2**]	配置IS-IS接口t1定时器重置最大次数，缺省为3次，范围：1~65535
5	inspur(config-isis-process-id-if-interface-name)#**restart t1-timer** <*interval*>[**level-1** | **level-2**]	配置IS-IS接口t1定时器时间间隔，单位：秒，缺省为3秒，范围：1~65535

4.5.12 配置 IS-IS LSP 报文 Buffer 大小

介绍IS-IS LSP报文Buffer大小的配置步骤和命令。

1.启动IS-IS，设置IS-IS的区域和系统ID。

步骤	命令	功能
1	inspur(config)#**router isis** < *process-id*>[**vrf** < *vrf-name*>]	启动IS-IS路由协议，进入IS-IS路由配置模式
2	inspur(config-isis-process-id)#**area** <*area-address*>	IS-IS路由模式下设定IS-IS区域，指定该路由器属于该区域 所配置的区域地址为1~13个字节的16进制字符串
3	inspur(config-isis-process-id)#**system-id** <*system-id*>[**range** <*range-number*>]	设置IS-IS的系统ID，用于在该区域中标识该路由器，是6个字节的16进制字符串，通常以该路由器某一接口MAC地址表示

2.配置IS-IS LSP报文接收Buffer大小。

命令	功能
inspur(config-isis-process-id)#**lsp-size receive** <*buf-size*>	配置IS-IS LSP报文接收Buffer大小，范围512~7680

3.配置IS-IS LSP报文生成Buffer大小。

命令	功能
inspur(config-isis-process-id)#**lsp-size originate** <*buf-size*>	配置IS-IS LSP报文生成Buffer大小，范围512~7680

4.5.13 验证及维护 IS-IS

验证IS-IS配置结果

IR12000提供了以下命令来查看IS-IS相关信息：

命令	功能
inspur#**show isis adjacency** [**up-time**][**level-1** | **level-2**][**process-id** <*process-id*>]	查看邻接关系，显示当前邻居状态
inspur#**show isis circuits** [**detail**][**process-id** <*process-id*>]	显示当前IS-IS接口信息
inspur#**show isis database** [**LSP-ID**][**level-1**| **level-2**][**verbose**][**detail**][**process-id** <*process-id*>]	查看IS-IS数据库的信息
inspur#**show isis topology** [**level-1**|**level-2**][**process-id**<*process-id*>]	显示当前IS-IS的拓扑结构
inspur#**show isis mpls traffic-eng tunnel** [**process-id**<*process-id*>]	显示当前IS-IS SPF计算使用隧道情况
inspur#**show isis fast-reroute-topology** [**level-1**|**level-2**][**process-id**<*process-id*>]	显示当前IS-IS的备份拓扑结构

维护IS-IS

IR12000提供了debug命令对IS-IS协议进行调试，跟踪相关信息：

命令	功能
inspur#**debug isis all** [**process-id**<*process-id*>]	打开IS-IS相关的所有debug开关
inspur#**debug isis adj-packets**[**process-id**<*process-id*>]	跟踪显示IS-IS收到和发出的Hello报文

命令	功能
inspur#**debug isis snp-packets**[process-id<*process-id*>]	跟踪显示IS-IS收到和发出的SNP报文及相关处理事件
inspur#**debug isis spf-events**[process-id<*process-id*>]	跟踪显示IS-IS路由计算事件调试信息
inspur#**debug isis update-packets**[process-id<*process-id*>]	跟踪显示IS-IS LSP包处理事件调试信息
inspur#**debug isis nsf-event**[process-id<*process-id*>]	跟踪显示IS-IS GR相关信息
inspur#**debug isis mpls traffic-eng events**[process-id<*process-id*>]	跟踪显示IS-IS CSPF路由计算事件调试信息

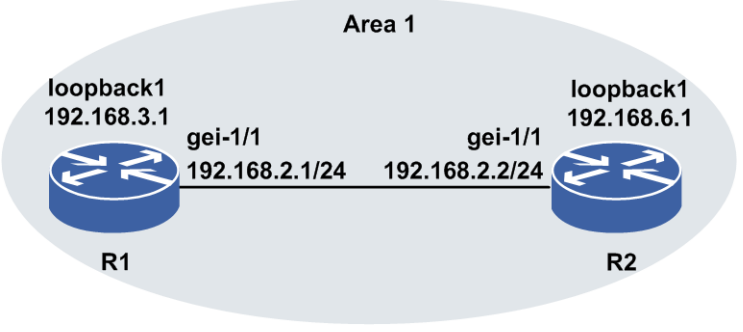
4.5.14 单区域 IS-IS 配置实例

配置说明

在配置IS-IS之前应对整个网络进行分析，根据网络大小决定网络拓扑，是否需要划分多个区域，是否有多种路由协议在网络中运行。如果网络规模不是很大，只需要在单区域内配置IS-IS。

如*图 4-33*所示为单区域IS-IS配置的典型图例，下面以该图说明IS-IS协议的基本配置。

图 4-33 单区域 IS-IS 配置实例拓扑图



配置思路

1.配置接口IP地址。

2.配置IS-IS协议。

3.在接口上启用IS-IS协议。

4.测试配置结果，确认两台设备已正确建立邻居，并正确计算出拓扑；从两个设备上分别能够ping通对端loopback接口。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 192.168.2.1 255.255.255.0
R1(config-if-gei-1/1)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 192.168.3.1 255.255.255.0
R1(config-if-loopback1)#exit
R1(config)#router isis
R1(config-isis-0)#area 01
R1(config-isis-0)#system-id 00D0.D0C7.5460
R1(config-isis-0)#interface gei-1/1
R1(config-isis-0-if-gei-1/1)#ip router isis
R1(config-isis-0-if-gei-1/1)#exit
R1(config-isis-0)#interface loopback1
R1(config-isis-0-if-loopback1)#ip router isis
R1(config-isis-0-if-loopback1)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 192.168.2.2 255.255.255.0
R2(config-if-gei-1/1)#exit
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 192.168.6.1 255.255.255.0
R2(config-if-loopback1)#exit
R2(config)#router isis
R2(config-isis-0)#area 01
R2(config-isis-0)#system-id 00D0.D0C7.53E0
R2(config-isis-0)#interface gei-1/1
R2(config-isis-0-if-gei-1/1)#ip router isis
R2(config-isis-0-if-gei-1/1)#exit
R2(config-isis-0)#interface loopback1
R2(config-isis-0-if-loopback1)#ip router isis
R2(config-isis-0-if-loopback1)#end
```

配置验证

上述的配置完成以后，在两端的设备上应该能够看到如下的信息，表明双方已经正确建立邻居，并计算出拓扑。最后从两台设备上ping对端的loopback接口，都能够ping通，说明配置成功。

R1的配置验证，用**show running-config isis**命令查看IS-IS的配置是否正确：

```
R1(config)#show running-config isis
!<isis>
router isis 0
  area 01
  system-id 00D0.D0C7.5460
  interface gei-0/1
    ip router isis
  $
  interface loopback1
    ip router isis
  $
$
!<isis>
```

在R1上使用**show isis adjacency**命令查看邻居状态是否正常，主要看state字段的邻居状态是否为UP的，邻居状态建立以后会显示UP状态：

```
R1(config)#show isis adjacency
Process ID: 0
```

```
Interface     System id      State  Lev  Holds  SNPA(802.2)    Pri   MT
gei-1/1       00D0.D0C7.53E0 UP/UP  L1L2 8/7    0030.3144.5566 64/64
```

在R1上用**show isis topology**命令查看拓扑是否正确计算出来，如果正确计算出来，在命令执行的结果中应该能够看到如下的条目，metric为“--”，表示本机；metric为**，表示不可达：

```
R1(config)#show isis topology
Process ID: 0
IS-IS paths to Level-1 routers
System id     Metric     Next-Hop      Interface       SNPA
00D0.D0C7.53E0 10         00D0.D0C7.53E0 gei-1/1      0030.3144.5566
00D0.D0C7.5460 --

IS-IS paths to Level-2 routers
System id     Metric     Next-Hop      Interface       SNPA
00D0.D0C7.53E0 10         00D0.D0C7.53E0 gei-1/1      0030.3144.5566
00D0.D0C7.5460 --
```

在R1上用**show isis circuits**命令查看接口信息，及DIS的选举情况，如果接口状态为UP表示接口状态正常，如果为down，则表示不正常，需要查看链路状态及IP配置：

```
R1(config)#show isis circuits
Process ID: 0
Interface    State Lev  CirId Level1-DR        Level2-DR    Pri(L1/L2)
loopback1      Up    L1L2 0     Disabled       Disabled         -/-
gei-1/1       Up    L1L2 2   00D0.D0C7.53E0-02 00D0.D0C7.53E0-02 64/64

R1#ping 192.168.6.1
sending 5,100-byte ICMP echoes to 192.168.6.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 12/22/54 ms.
```

在R2上验证配置结果：

```
R2(config)#show running-config isis
!<isis>
router isis 0
  area 01
  system-id 00D0.D0C7.53E0
  interface gei-0/1
    ip router isis
  $
  interface loopback1
    ip router isis
  $
!</isis>

R2(config)#show isis circuits
Process ID: 0IS interface database:
Interface     State Lev  CirId Level1-DR       Level2-DR   Pri(L1/L2)
loopback1     Up    L1L2 0     Disabled        Disabled        -/-
gei-1/1       Up    L1L2 2     Dis is me       Dis is me       64/64

R2(config)#show isis adjacency
Process ID: 0
Interface     System id     State  Lev  Holds  SNPA(802.2)    Pri   MT
gei-1/1       00D0.D0C7.5460 UP/UP  L1L2 23/23  0030.3144.5560 64/64

R2(config)#show isis topology
IS-IS paths to Level-1 routers
System id     Metric     Next-Hop      Interface         SNPA
00D0.D0C7.53E0 --
00D0.D0C7.5460 10         00D0.D0C7.5460 gei-1/1        0030.3144.5560

IS-IS paths to Level-2 routers
System id     Metric     Next-Hop      Interface         SNPA
00D0.D0C7.53E0 --
```

```
00D0.D0C7.5460 10         00D0.D0C7.5460 gei-1/1       0030.3144.5560

R2#ping 192.168.3.1
sending 5,100-byte ICMP echoes to 192.168.3.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 10/20/52 ms.
```

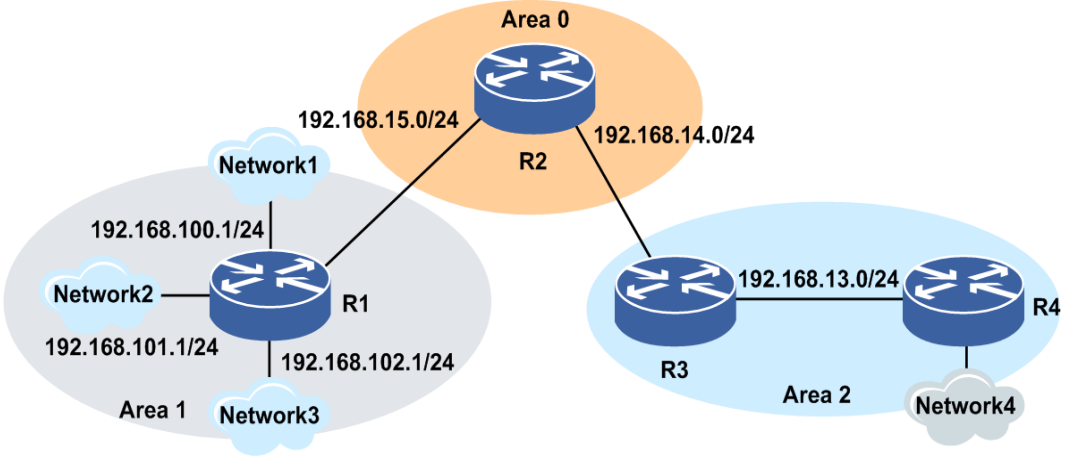
4.5.15 多区域 IS-IS 配置实例

配置说明

在网络较大时，应该考虑在IS-IS中使用多个区域。可根据地域及功能将相近的路由器划分在一个区域内，区域的划分有助于减少内存的需求。使区域内的路由器只需要维护较小的链路状态数据库。

如*图 4-34*所示是一个配置有多区域的IS-IS实例，其中R1属于区域1； R2属于区域0；R3，R4属于区域2。在R1中对区域1的网段进行了路由聚合。在R4上将默认路由再分配到了IS-IS中。

图 4-34 多区域 IS-IS 配置实例拓扑图



配置思路

1.配置接口IP地址。

2.配置IS-IS协议。

3.在接口上启用IS-IS协议。

4.在R1设备上启用路由聚合。

5.在R4设备上配置默认静态路由，并重分发默认路由。

6.测试配置结果，确认设备已正确建立邻居，并正确计算出拓扑。从两端（R1、R4）设备上分别能够ping通对端设备的IS-IS接口。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#ip address 192.168.15.1 255.255.255.0
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#exit
R1(config)#interface gei-1/4
R1(config-if-gei-1/4)#ip address 192.168.100.1 255.255.255.0
R1(config-if-gei-1/4)#no shutdown
R1(config-if-gei-1/4)#exit
R1(config)#interface gei-1/5
R1(config-if-gei-1/5)#ip address 192.168.101.1 255.255.255.0
R1(config-if-gei-1/5)#no shutdown
R1(config-if-gei-1/5)#exit
R1(config)#interface gei-1/6
R1(config-if-gei-1/6)#ip address 192.168.102.1 255.255.255.0
R1(config-if-gei-1/6)#no shutdown
R1(config-if-gei-1/6)#exit

R1(config)#router isis
R1(config-isis-0)#area 01
R1(config-isis-0)#system-id 00D0.D0C7.5460
R1(config-isis-0)#hostname dynamic disable
R1(config-isis-0)#is-type level-1-2
R1(config-isis-0)#interface gei-1/3
R1(config-isis-0-if-gei-1/3)#ip router isis
R1(config-isis-0-if-gei-1/3)#circuit-type level-2
R1(config-isis-0-if-gei-1/3)#exit
R1(config-isis-0)#interface gei-1/4
R1(config-isis-0-if-gei-1/4)#ip router isis
R1(config-isis-0-if-gei-1/4)#circuit-type level-2
R1(config-isis-0-if-gei-1/4)#exit
R1(config-isis-0)#interface gei-1/5
R1(config-isis-0-if-gei-1/5)#ip router isis
R1(config-isis-0-if-gei-1/5)#circuit-type level-2
R1(config-isis-0-if-gei-1/5)#exit
R1(config-isis-0)#interface gei-1/6
R1(config-isis-0-if-gei-1/6)#ip router isis
R1(config-isis-0-if-gei-1/6)#circuit-type level-2
R1(config-isis-0-if-gei-1/6)#exit
R1(config-isis-0)#summary-address 192.168.100.0 255.255.252.0
R1(config-isis-0)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#ip address 192.168.15.2 255.255.255.0
R2(config-if-gei-1/3)#no shutdown
R2(config-if-gei-1/3)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 192.168.14.1 255.255.255.0
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit

R2(config)#router isis
R2(config-isis-0)#area 00
R2(config-isis-0)#system-id 00D0.D0C7.53E0
R2(config-isis-0)#hostname dynamic disable
R2(config-isis-0)#is-type level-1-2
R2(config-isis-0)#interface gei-1/1
R2(config-isis-0-if-gei-1/1)#ip router isis
R2(config-isis-0-if-gei-1/1)#circuit-type level-2
R2(config-isis-0-if-gei-1/1)#exit
R2(config-isis-0)#interface gei-1/3
R2(config-isis-0-if-gei-1/3)#ip router isis
R2(config-isis-0-if-gei-1/3)#circuit-type level-2
R2(config-isis-0-if-gei-1/3)#exit
```

R3上的配置如下：

```
R3(config)#interface gei-1/1
R3(config-if-gei-1/1)#ip address 192.168.14.2 255.255.255.0
R3(config-if-gei-1/1)#no shutdown
R3(config-if-gei-1/1)#exit
R3(config)#interface gei-1/3
R3(config-if-gei-1/3)#ip address 192.168.13.1 255.255.255.0
R3(config-if-gei-1/3)#no shutdown
R3(config-if-gei-1/3)#exit

R3(config)#router isis
R3(config-isis-0)#area 02
R3(config-isis-0)#system-id EF00.AB00.DF12
R3(config-isis-0)#hostname dynamic disable
R3(config-isis-0)#is-type level-1-2
R3(config-isis-0)#interface gei-1/1
R3(config-isis-0-if-gei-1/1)#ip router isis
R3(config-isis-0-if-gei-1/1)#circuit-type level-2
R3(config-isis-0-if-gei-1/1)#exit
R3(config-isis-0)#interface gei-1/3
R3(config-isis-0-if-gei-1/3)#ip router isis
R3(config-isis-0-if-gei-1/3)#circuit-type level-1
R3(config-isis-0-if-gei-1/3)#exit
```

R4上的配置如下：

```
R4(config)#interface gei-1/3
R4(config-if-gei-1/3)#ip address 192.168.13.2 255.255.255.0
R4(config-if-gei-1/3)#no shutdown
R4(config-if-gei-1/3)#exit

R4(config)#router isis
R4(config-isis-0)#area 02
R4(config-isis-0)#system-id 00DE.FD11.AD00
R4(config-isis-0)#hostname dynamic disable
R4(config-isis-0)#is-type level-2-only
R4(config-isis-0)#interface gei-1/3
R4(config-isis-0-if-gei-1/3)#ip router isis
R4(config-isis-0-if-gei-1/3)#circuit-type level-2-only
R4(config-isis-0-if-gei-1/3)#exit
R4(config-isis-0)#exit

R4(config)#ip route 0.0.0.0 0.0.0.0 192.168.13.1
R4(config)#router isis
R4(config-isis-0)#default-information originate
R4(config-isis-0)#redistribute static metric 10
R4(config-isis-0)#end
```

配置验证

上述的配置完成以后，在两端的设备上应该能够看到如下的信息，表明双方已经正确建立邻居，并计算出拓扑。最后从两台设备上ping对端的接口地址，都能够ping通，说明配置成功。

在R1的相关信息中可以看到上述的配置，使用**show ip protocol routing**命令可以看到由R4重分发的默认静态路由：

```
R1(config)#show running-config isis
!<isis>
router isis 0
  area 01
  system-id 00D0.D0C7.5460
  hostname dynamic disable
  summary-address 192.168.100.0 255.255.252.0
  interface gei-1/3
```

```
    ip router isis
    circuit-type level-2-only
  $
  interface gei-1/4
    ip router isis
    circuit-type level-2-only
  $
  interface gei-1/5
    ip router isis
    circuit-type level-2-only
  $
  interface gei-1/6
    ip router isis
    circuit-type level-2-only
  $
$
!</isis>
R1(config)#show isis adjacency
Interface     System id     State  Lev  Holds  SNPA(802.2)    Pri   MT
gei-1/3      00D0.D0C7.53E0 UP     L2   7      0030.3144.5566 64

R1(config)#show isis topology
Process ID: 0
IS-IS paths to Level-1 routers
System id     Metric     Next-Hop      Interface          SNPA
00D0.D0C7.5460 --

IS-IS paths to Level-2 routers
System id     Metric     Next-Hop      Interface          SNPA
00D0.D0C7.53E0 10         00D0.D0C7.53E0 gei-1/3       0030.3144.5566
00D0.D0C7.5460 --
Router        30         00D0.D0C7.53E0 gei-1/3       0030.3144.5566
Router        20         00D0.D0C7.53E0 gei-1/3       0030.3144.5566

R1(config)#show ip protocol routing
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
  BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale

    Dest             NextHop        RoutePrf   RouteMetric Protocol
*>  192.168.2.0/24     192.168.15.2    115        20          ISIS-L2
*>  192.168.14.0/24    192.168.15.2    115        20          ISIS-L2
*>  192.168.15.0/24    192.168.15.1    0          0           Direct
 *  192.168.15.0/24    192.168.15.2    115        20          ISIS-L2
```

同样在R2上查看配置结果：

```
R2(config)#show running-config isis
!<isis>
router isis 0
  area 00
  system-id 00D0.D0C7.53E0
  hostname dynamic disable
  interface gei-1/1
    ip router isis
    circuit-type level-2-only
  $
  interface gei-1/3
    ip router isis
    circuit-type level-2-only
  $
$
!</isis>
```

```
R2(config)#show isis adjacency
Process ID: 0
Interface      State Lev  CirId Level1-DR      Level2-DR     Pri(L1/L2)
gei-1/3        Up    L2   3     Disabled       Dis is me       64/64
gei-1/1        Up    L2   2     Disabled       Router.01       64/64
Process ID: 0
Interface        System id       State     Lev     Holds      SNPA(802.2)
Pri     MT
gei-1/1       EF00.AB00.DF12     UP        L2      6          00D0.1234.561F
64
gei-1/3       00D0.D0C7.53E0     UP        L2      27         0001.12AC.121A
64

R2(config)#show ip protocol routing
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale

    Dest              NextHop         RoutePrf   RouteMetric Protocol
*>  192.168.14.0/24    192.168.14.1    0          0           Direct
*>  192.168.14.1/32    192.168.14.1    0          0           Address
*>  192.168.15.0/24    192.168.15.2    0          0           Direct
 *  192.168.15.0/24    192.168.15.1    115        20          ISIS-L2
*>  192.168.15.2/32    192.168.15.2    0          0           Address
*>  192.168.100.0/22   192.168.15.1    115        10          ISIS-L2
```

在R3上查看配置结果：

```
R3(config)#show running-config isis
!<isis>
router isis 0
  area 02
  system-id EF00.AB00.DF12
  hostname dynamic disable
  interface gei-1/1
    ip router isis
    circuit-type level-2-only
  $
  interface gei-1/3
    ip router isis
    circuit-type level-1
  $
$
! </isis>

R3(config)#show isis adjacency
Process ID: 0
Interface        System id       State     Lev     Holds     SNPA(802.2)
Pri     MT
gei-1/1          00D0.D0C7.53E0   UP        L2      22        0077.AB13.3301
64
```

在R4上查看配置结果：

```
R4(config)#show running-config isis
!<isis>
router isis 0
  area 02
  system-id 00de.fb11.ad00
  hostname dynamic disable
  is-type level-2
  redistribute static ip metric 10
  default-information originate
  interface gei-1/3
```

```
   ip router isis
   circuit-type level-2
  $
$
!</isis>

R4#show ip protocol routing network 192.168.100.0
Protocol routes:
status codes: *valid, >best, i-internal, s-stale

   Dest             NextHop        RoutePrf   RouteMetric Protocol
*>  192.168.100.0/22   192.168.2.1     115       20          ISIS-L2

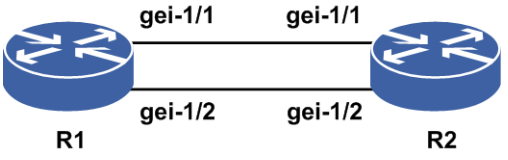
R4#ping 192.168.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 192/709/1148 ms
```

4.5.16 IS-IS 多实例配置实例

配置说明

R1上起两个实例，实例1加入gei-1/1，实例2加入接口gei-1/2。R2上也创建2个实例，把两个接口分别加入实例1和实例2，如*图 4-35*所示。

图 4-35 IS-IS 多实例配置实例拓扑图



配置思路

1.配置接口IP地址（直连链路配置同一网段的IP地址）。

2.在实例100下，R1的gei-1/1和R2的gei-1/1口建立邻居关系。

3.在实例200下，R1的gei-1/2和R2的gei-1/2建立邻接关系。

4.在R1的两个实例下重分发直连路由，在R2上查看能否在不同实例间形成负荷分担（实际情况是不能形成负荷分担，不同实例相同前缀实例号小的路由优先）。

配置过程

R1上的配置如下：

```
R1(config)#router isis 100
R1(config-isis-100)#system-id 1111.0100.0000
R1(config-isis-100)#area 10
R1(config-isis-100)#redistribute connected
R1(config-isis-100)#interface gei-1/1
R1(config-isis-100-if-gei-1/1)#ip router isis
```

```
R1(config-isis-100-if-gei-1/1)#exit
R1(config-isis-100)#exit
R1(config)#router isis 200
R1(config-isis-200)#system-id 1111.0200.0000
R1(config-isis-200)#area 10
R1(config-isis-200)#redistribute connected
R1(config-isis-200)#interface gei-1/2
R1(config-isis-200-if-gei-1/2)#ip router isis
R1(config-isis-200-if-gei-1/2)#exit
R1(config-isis-200)#exit
```

R2上的配置如下：

```
R2(config)#router isis 100
R2(config-isis-100)#system-id 2222.0100.0000
R2(config-isis-100)#area 10
R2(config-isis-100)#interface gei-1/1
R2(config-isis-100-if-gei-1/1)#ip router isis
R2(config-isis-100-if-gei-1/1)#exit
R2(config-isis-100)#exit
R2(config)#router isis 200
R2(config-isis-200)#system-id 2222.0200.0000
R2(config-isis-200)#area 10
R2(config-isis-200)#interface gei-1/2
R2(config-isis-200-if-gei-1/2)#ip router isis
R2(config-isis-200-if-gei-1/2)#exit
R2(config-isis-200)#exit
/*接口IP地址配置省略，具体参考单区域IS-IS配置实例*/
```

配置验证

```
R1#show isis adjacency
Process ID: 100
Interface        System id     State    Lev  Holds  SNPA(802.2)    Pri     MT
gei-1/1             R2       UP/UP    L1L2 26/26  0021.8844.5541 64/64
Process ID: 200
Interface        System id     State    Lev  Holds  SNPA(802.2)    Pri     MT
gei-1/2             R2       UP/UP    L1L2 25/25  0021.8844.5541 64/64
```

路由下一跳接口为gei-1/1，即实例号小的优先：

```
R2#show ip forwarding route isis-l2
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest             Gw            Interface          Owner      Pri Metric
1.1.1.12/32       56.3.3.2       gei-1/1           ISIS-L2    115 10
88.6.5.5/32       56.3.3.2       gei-1/1           ISIS-L2    115 10
```

4.5.17 IS-IS FRR 配置实例

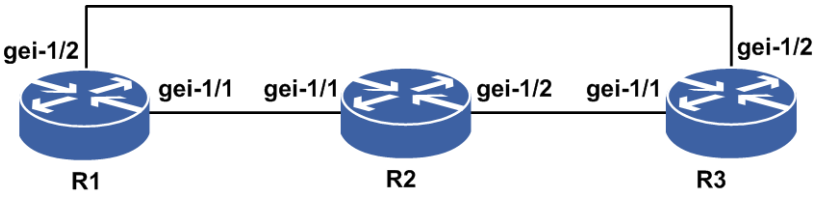
配置说明

FRR旨在当网络中链路或者节点失效后，为这些重要的节点或链路提供备份保护，实现快速重路由，减少链路或节点失效时对流量的影响，使流量实现快速恢复。

FRR典型组网有以下两种：

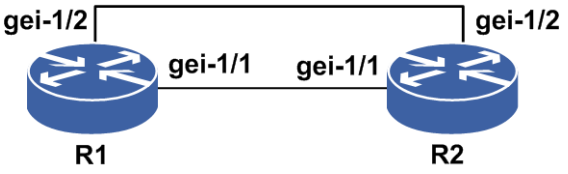
1.节点保护典型组网如*图 4-36*所示。

图 4-36 FRR 节点保护典型组网示意图



2.链路保护典型组网如*图 4-37*所示，通过两链路建立IS-IS的邻居拓扑，配置形成主优次优链路情况。

图 4-37 链路保护典型组网示意图



配置思路

1.配置接口IP地址（直连链路配置同一网段的IP地址）。

2.配置IS-IS协议。

3.在形成FRR关系的节点上同一目的有两个以上的下一跳可达，且到同一个目的地址的路由有不同的开销。

4.在选定的设备上的相关路由协议下启用FRR功能。

配置过程

具体配置信息如下：

1.节点保护类型的FRR配置以BGP协议为例，具体配置参见BGP FRR配置实例。

2.链路保护类型

以*图 4-146*中的IS-IS协议为例来配置FRR。

R1的配置：

```
R1(config)#router isis
R1(config-isis-0)#area 01
R1(config-isis-0)#system-id 00D0.D0C7.5460
R1(config-isis-0)#fast-reroute lfa enable
R1(config-isis-0)#interface gei-1/1
R1(config-isis-0-if-gei-1/1)#ip router isis
R1(config-isis-0-if-gei-1/1)#exit
R1(config-isis-0)#interface gei-1/2
R1(config-isis-0-if-gei-1/2)#ip router isis
R1(config-isis-0-if-gei-1/2)#metric 20
R1(config-isis-0-if-gei-1/2)#exit
```

R2的配置：

```
R2(config)#router isis
R2(config-isis-0)#area 01
R2(config-isis-0)#system-id 00D0.D0C7.6788
R2(config-isis-0)#redistribute connected
R2(config-isis-0)#interface gei-1/1
R2(config-isis-0-if-gei-1/1)#ip router isis
R2(config-isis-0-if-gei-1/1)#exit
R2(config-isis-0)#interface gei-1/2
R2(config-isis-0-if-gei-1/2)#ip router isis
R2(config-isis-0-if-gei-1/2)#end
```

配置验证

用**show ip forwarding backup route**验证配置结果是否使FRR最终生效。

R1上IS-IS的FRR生效情况查看：

```
R1#show isis fast-reroute-topology
Process ID:0
IS-IS ipfrr paths to Level-1 routers
System id      Interface    Ipfrr interface  Ipfrr type metric
00D0.D0C7.6788  gei-1/1     gei-1/2         Link      20
IS-IS ipfrr paths to Level-2 routers
System id      Interface    Ipfrr interface  Ipfrr type metric
00D0.D0C7.6788  gei-1/1     gei-1/2         Link      20

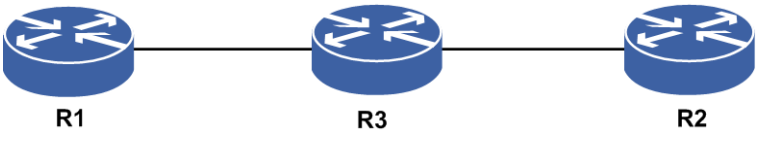
R1#show ip forwarding backup route
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority,  M/S: Master/Slave,
        Sta: Status;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
        MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
        ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
        GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
        GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best, M: Master, S: Slave, I: Inuse, U: Unuse;
   Dest        Gw          Interface     Owner       Pri  Metric  M/S Status
*> 1.1.1.0/24  180.1.1.200   gei-1/1      ISIS_LEVEL1  115  20      M   I
*  1.1.1.0/24  190.1.1.200   gei-1/2      ISIS_LEVEL1  115  30      S   U
/*1.1.1.0是R2上的直连路由，R2重分发直连路由通告到R1上。*/
```

4.5.18 IS-IS 重分发配置实例

配置说明

IS-IS路由模式下，可以重分发Connect、Static、RIP、IS-IS、OSPF和BGP等到IS-IS路由下，举例组网图如*图 4-38*所示。

图 4-38 IS-IS 重分发配置实例示意图



配置思路

1.按*图 4-38*所示搭建环境，配置接口IP地址（直连链路配置同一网段的IP地址），使R1与R3建立L1L2邻居关系。

2.在R3上配置重分发来自R2的其它路由协议（OSPF、BGP、RIP等），并配置重分发的路由级别和度量值，查看R1的路由表。

配置过程

R3的配置如下：

```
R3(config)#router isis
R3(config-isis-0)#redistribute connected metric 11 level-1
R3(config-isis-0)#redistribute static metric 12 level-1
R3(config-isis-0)#redistribute ospf  process-id metric 13 level-1
R3(config-isis-0)#exit
```

配置验证

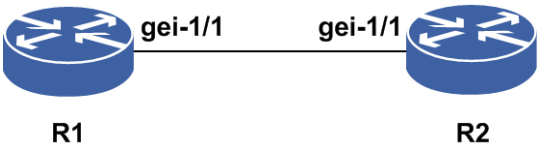
在R1对应的路由表中可以学到重分布进来的路由，并具有正确的度量值。

4.5.19 IS-IS 认证配置实例

配置说明

IS-IS认证配置，包括接口密码认证和区域密码认证配置。两端的密码一致，才能建立IS-IS邻居和交换LSP。举例组网图如*图 4-39*所示。

图 4-39 IS-IS 密码认证配置实例示意图



配置思路

1.按*图 4-148*所示搭建环境，在R1和R2上配置接口IP地址（直连链路配置同一网段的IP地址）、配置IS-IS协议，使R1和R2建立L1邻居关系。

2.在R1的接口上配置验证密码（R2不配置验证密码），观察邻居建立情况。

3.在R2的接口上配置相同的验证密码，观察邻居建立情况。

配置过程

明文认证（R1和R2配置相同）：

```
R1(config)#router isis
R1(config-isis-0)#interface gei-1/1
R1(config-isis-0-if-gei-1/1)#authentication-type TEXT level-1
R1(config-isis-0-if-gei-1/1)#authentication Inspur level-1
R1(config-isis-0-if-gei-1/1)#exit
```

密文认证（R1和R2配置相同）：

```
R1(config)#router isis
R1(config-isis-0)#interface gei-1/1
R1(config-isis-0-if-gei-1/1)#authentication-type MD5 level-1
R1(config-isis-0-if-gei-1/1)#authentication Inspur level-1
R1(config-isis-0-if-gei-1/1)#exit
```

配置验证

根据配置思路中的三步分别验证配置结果：

1.R1和R2建立了L1邻居关系。

2.R1和R2无法建立邻居关系。

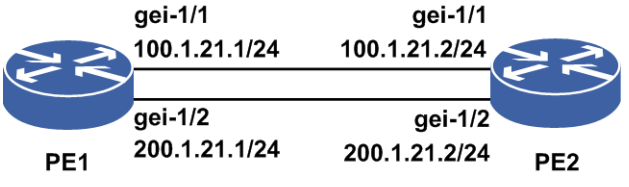
3.R1和R2建立了L1邻居关系。

4.5.20 IS-IS 路由负荷分担配置实例

配置说明

负荷分担可使超出单个接口带宽的流量均分到多条链路上，实现流量在各条链路上的负载均衡。如所示*图 4-40*，采用IS-IS路由的负荷分担实现负载均衡。

图 4-40 IS-IS 路由负荷分担配置实例



配置思路

1.配置接口地址， PE2路由器上配置一个loopback 1.1.1.2/32。

2.PE1和PE2上启用IS-IS协议，通告各接口地址，并配置**maxinum-paths**，使负荷分担生效。

3.可以更改负荷分担方式即逐包或者逐流。

配置过程

PE1上的配置如下：

```
PE1(config)#interface gei-1/1
PE1(config-if-gei-1/1)#ip address 100.1.21.1 255.255.255.0
PE1(config-if-gei-1/1)#exit
PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#ip address 200.1.21.1 255.255.255.0
PE1(config-if-gei-1/2)#exit

PE1(config)#router isis 1
PE1(config-isis-1)#area 00
PE1(config-isis-1)#system-id 0000.1111.1111
PE1(config-isis-1)#maximum-paths 2      /*负荷分担支持路由数目为2*/
PE1(config-isis-1)#interface gei-1/1
PE1(config-isis-1-if-gei-1/1)#ip router isis
PE1(config-isis-1-if-gei-1/1)#exit
PE1(config-isis-1)#interface gei-1/2
PE1(config-isis-1-if-gei-1/2)#ip router isis
PE1(config-isis-1-if-gei-1/2)#exit

PE1(config)#interface gei-1/1
PE1(config-if-gei-1/1)#ip load-sharing per-packet    /*选择逐包方式*/
PE1(config-if-gei-1/1)#exit
PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#ip load-sharing per-packet    /*选择逐包方式*/
PE1(config-if-gei-1/2)#exit
```

PE2上的配置如下：

```
PE2(config)#interface gei-1/1
PE2(config-if-gei-1/1)#ip address 100.1.21.2 255.255.255.0
PE2(config-if-gei-1/1)#exit
PE2(config)#interface gei-1/2
PE2(config-if-gei-1/2)#ip address 200.1.21.2 255.255.255.0
PE2(config-if-gei-1/2)#exit
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 1.1. 1.2 255.255.255.255
PE2(config-if-loopback1)#exit

PE2(config)#router isis 1
PE2(config-isis-1)#area 00
PE2(config-isis-1)#system-id 0000.1111.2222
PE2(config-isis-1)#maximum-paths 2      /*负荷分担支持路由数目为2*/
PE2(config-isis-1)#interface gei-1/1
PE2(config-isis-1-if-gei-1/1)#ip router isis
PE2(config-isis-1-if-gei-1/1)#exit
PE2(config-isis-1)#interface gei-1/2
PE2(config-isis-1-if-gei-1/2)#ip router isis
PE2(config-isis-1-if-gei-1/2)#exit
PE2(config-isis-1)#interface loopback1
PE2(config-isis-1-if-loopback1)#ip router isis
PE2(config-isis-1-if-loopback1)#exit

PE2(config)#interface gei-1/1
PE2(config-if-gei-1/1)#ip load-sharing per-packet
PE2(config-if-gei-1/1)#exit
PE2(config)#interface gei-1/2
PE2(config-if-gei-1/2)#ip load-sharing per-packet
PE2(config-if-gei-1/2)#exit
```

配置验证

在PE1上查看配置结果：

```
R1#show ip forwarding route isis-l2
IPv4 Routing Table:
 Status codes: *valid, >best;
   Dest          Gw           Interface      Owner     Pri   Metric
*> 1.1.1.2/32    100.1.21.2    gei-1/1       isis-l2    115   1
*> 1.1.1.2/32    200.1.21.2    gei-1/2       isis-l2    115   1
```

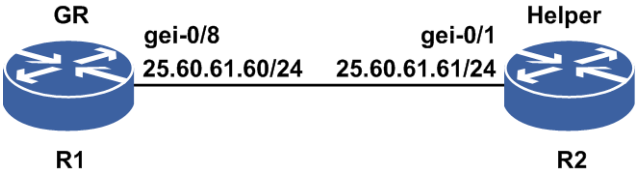
可以看到，到达统一目的地有两条路由，分别走不同的出接口，负荷分担配置成功。

4.5.21 IS-IS Graceful Restart 配置实例

配置说明

如*图 4-41*所示，路由器R1、R2是ISIS邻居，现在R1和R2上开启Graceful Restart功能，一台路由器做GR，一台路由器做helper。使得能够在R1或R2主备倒换时仍然能够正常转发数据报文。

图 4-41 IS-IS Graceful Restart 配置实例



配置思路

1.配置接口IP地址（直连链路配置同一网段的IP地址）。

2.配置路由器R1、R2形成IS-IS邻居。

3.在R1、R2上开启Graceful Restart功能。

配置过程

R1上的配置如下：

```
R1(config)#router isis 1
R1(config-isis-1)#system-id 0000.0000.0001
R1(config-isis-1)#area 00
R1(config-isis-1)#is-type level-2
R1(config-isis-1)#restart enable
R1(config-isis-1)#restart t2-timer 100
R1(config-isis-1)#restart t3-timer manual 90
R1(config-isis-1)#interface gei-0/8
R1(config-isis-1-if-gei-0/8)#ip router isis
R1(config-isis-1-if-gei-0/8)#circuit-type level-2-only
R1(config-isis-1-if-gei-0/8)#exit
```

R2上的配置如下：

```
R2(config)#router isis 1
R2(config-isis-1)#system-id 0000.0000.0002
R2(config-isis-1)#area 00
```

```
R2(config-isis-1)#is-type level-2
R2(config-isis-1)#restart enable
R2(config-isis-1)#restart t2-timer 100
R2(config-isis-1)#restart t3-timer manual 90
R2(config-isis-1)#interface gei-0/1
R2(config-isis-1-if-gei-0/1)#ip router isis
R2(config-isis-1-if-gei-0/1)#circuit-type level-2-only
R2(config-isis-1-if-gei-0/1)#exit
```

配置验证

主备倒换R1后，流量仍然能够正常转发。

R1上相关信息

查看GR中的路由器信息：

```
R1#show isis nsf
Process ID 0:
    NSF is ENABLE
    NSF mode is Restart
    NSF L1 active interface: 0
    NSF L2 active interface: 4
    NSF L1 T2 remaining: 0 seconds
    NSF L2 T2 remaining: 93 seconds
    NSF T3 using Manual
    NSF T3 remaining: 83 seconds

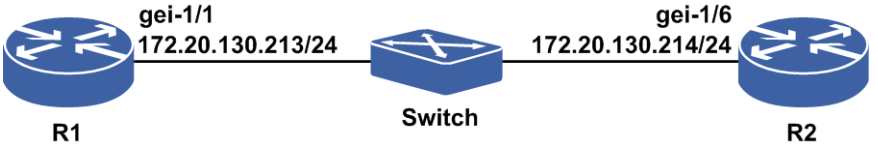
    Interface:gei-0/8
    NSF L1 restart state: Finished
    NSF L1 helper in restart state: Other
    NSF L1 T1 remaining: 0 seconds
    NSF L1 T1 retransmissions: 0
    NSF L2 restart state: Running
    NSF L2 helper in restart state: Other
    NSF L2 T1 remaining: 2 seconds
    NSF L2 T1 retransmissions: 3
```

4.5.22 IS-IS BFD 配置实例

配置说明

如*图 4-42*所示，R1、R2之间运行IS-IS协议，R1、R2协议接口下使能BFD。

图 4-42 IS-IS BFD 配置实例



配置思路

1.R1、R2之间运行IS-IS协议。

2.R1、R2协议接口下使能BFD。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 172.20.130.213 255.255.255.0
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit

R1(config)#router isis
R1(config-isis-0)#area 49.0172
R1(config-isis-0)#system-id 0020.0096.0001
R1(config-isis-0)#interface gei-1/1
R1(config-isis-0-if-gei-1/1)#ip router isis
R1(config-isis-0-if-gei-1/1)#bfd-enable
R1(config-isis-0-if-gei-1/1)#end
```

R2上的配置如下：

```
R2(config)#interface gei-1/6
R2(config-if-gei-1/6)#ip address 172.20.130.214 255.255.255.0
R2(config-if-gei-1/6)#no shutdown
R2(config-if-gei-1/6)#exit

R2(config)#router isis
R2(config-isis-0)#area 49.0172
R2(config-isis-0)#system-id 0020.0096.0002
R2(config-isis-0)#interface gei-1/6
R2(config-isis-0-if-gei-1/6)#ip router isis
R2(config-isis-0-if-gei-1/6)#bfd-enable
R2(config-isis-0-if-gei-1/6)#end
```

配置验证

正确配置后，IS-IS BFD会话应该能够成功建立，可以用如下命令查看结果：

用**show bfd neighbors** [**ip brief**|**ip detail**]来查看验证ISIS BFD是否生效。

R1上ISIS BFD生效情况查看：

```
R1(config)#show bfd neighbors ip brief
LocalAddr       PeerAddr       LD     RD     Hold   State    interface
172.20.130.213  172.20.130.214   1      3      150    UP       gei-1/1

R1(config)#show bfd neighbors ip detail
------------------------------------------------------------------------------
LocalAddr:172.20.130.213
PeerAddr :172.20.130.214
Local Discr:1              Remote Discr:3          State:UP

Holdown(ms):150           Interface: gei-1/1
Vpnid:0                   VRF Name:---
BFD Type:SingleHop
Instance Name:
------------------------------------------------------------------------------
Version:1               Dest UDP Port:3784       Final Bit:1
Local Diag:0            Demand Mode:0            Poll Bit:1
MinTxInt:50             MinRxInt:50             Multiplier:3
Received MinTxInt:50     Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24        Max BFD Length:24
```

```
Rx Count:0              Rx Interval (ms) min/max/avg:0     /0     /0
Tx Count:0              Tx Interval (ms) min/max/avg:0     /0     /0
Registered Protocols:ISIS
Uptime:0 day(s),0 hour(s),0 minute(s)
Control Plane Rcv Phy Interface Name: gei-1/1
==========================================================================
```

4.6 BGP

BGP是一种既可以用于不同AS之间，又可以用于同一AS内部的动态路由协议。当BGP运行于同一AS内部时称为IBGP，当BGP运行于不同AS之间时称为EBGP。

早期发布的三个版本分别是BGP-1、BGP-2和BGP-3，当前使用的版本是BGP-4。BGP-4作为事实上的Internet外部路由协议标准，被广泛应用于ISP之间。

提示：

若不做特殊说明，文中出现的BGP均指BGP-4。

BGP路由属性是一组参数，对特定的路由进行了进一步的描述，使得BGP能够对路由进行过滤和选择。

几种主要的BGP路由属性介绍如下。

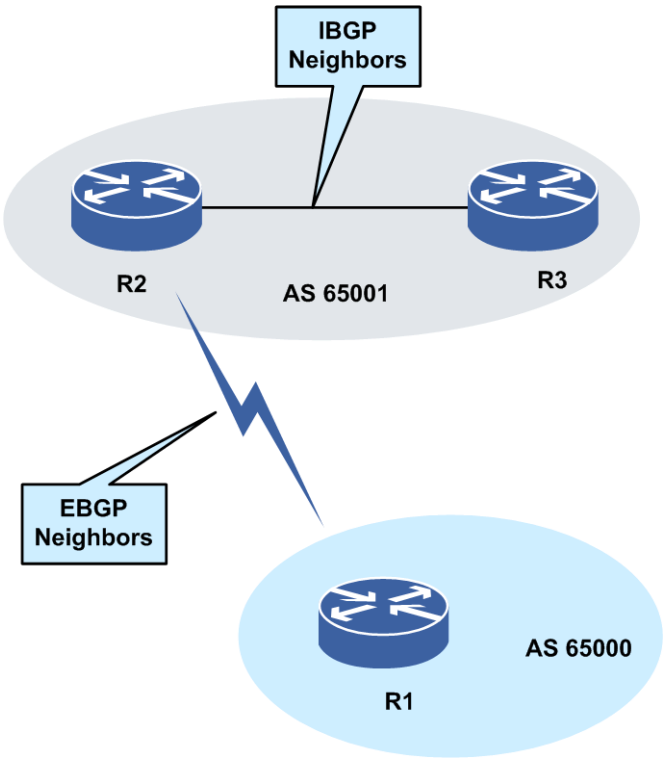
- 源（ORIGIN）属性：定义路由信息的来源，标记一条路由是怎么成为BGP路由的。
- AS 路径（AS_PATH）属性：按一定次序记录了某条路由从本地到目的地址所要经过的所有AS。
- 下一跳（NEXT_HOP）属性：BGP路由的下一跳属性。
- MED属性：仅在相邻两个AS之间交换，收到此属性的AS一方不会再将其通告给任何其他第三方AS，该属性相当于IGP路由中的Metric值。
- 本地优先（LOCAL_PREF）属性：LOCAL_PREF属性仅在IBGP对等体之间交换，不通告给其他AS，表面BGP路由的优先级。
- 团体（COMMUNITY）属性：用来简化路由策略的应用和降低维护管理的难度，是一组有相同特征的目的地址的集合，没有物理上的边界，与其所在的AS无关。

4.6.1 建立 BGP 邻居

建立了BGP会话连接的路由器被称作对等体（peers）或邻居（neighbors）。对等体的连接有两种模式：IBGP（Internal BGP）和EBGP（External BGP）。如果两个交换BGP报文的路由器属于同一个自治系统，那么这两台路由器就是IBGP的连接模式；如果两个交换BGP报文的路由器属于不同的自治系统，那么这两台路由器就是EBGP的连接模式。

如*图 4-43*所示，R1和R2是EBGP邻居，R2和R3是IBGP邻居。

图 4-43 IBGP 和 EBGP 示意图



4.6.1.1 建立 EBGP 邻居

本节介绍EBGP邻居的配置步骤和命令。

前提

在配置EBGP邻居之前先要保证节点之间物理连接正常，且两个节点在不同的AS中。

相关信息

在EBGP的连接案例中，一般两台路由器物理直接连接的情况比较多，原则上也是这么要求，这时候可以使用互连端口的IP地址建立BGP连接，也可以指定双方的Loopback地址建立BGP连接。

对于EBGP的使用，在路由器配置的时候，需要特别注意，如果使用非物理直连来建立EBGP连接，那么必须指定“多跳”连接，这是因为缺省情况下，路由器对于EBGP通信的BGP协议数据包的TTL值设置为1，即使底层的TCP连接能够建立，但是OPEN报文无法送达对端路由器的CPU，会导致BGP连接无法进入Established状态。

1.启动BGP进程。

命令	功能
`inspur(config)#`**router bgp** *<as-number>*	启动BGP进程并指定本路由器所在的AS号 *<as-number>*指本路由器所在的自治系统号，范围为1~65535。目前也支持4字节的AS，其范围为1~4294967295

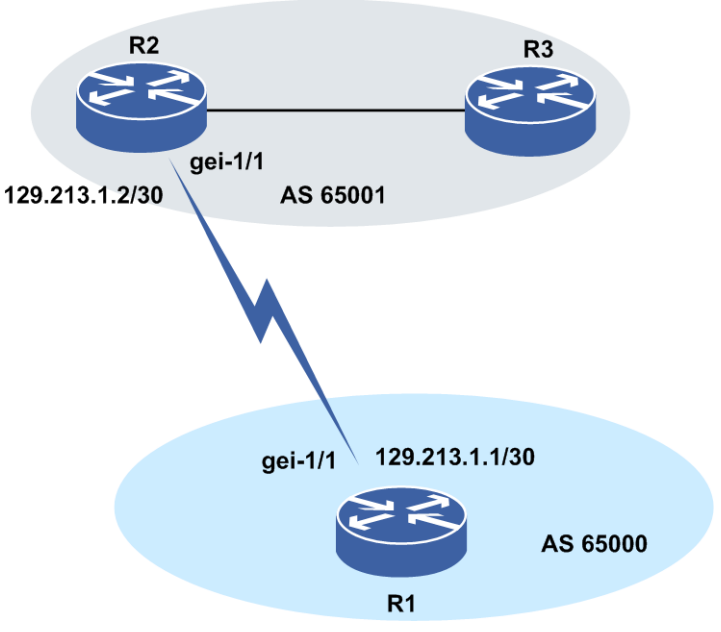
2.配置EBGP邻居。

步骤	命令	功能
1	inspur(config-bgp)#**neighbor** [<*ipv4-address*>|<*peer-group-name*>] **remote-as** <*number*>	配置一个BGP邻居或配置一个邻居对等体组及其自治系统号
2	inspur(config-bgp)#**neighbor** [<*ipv4-address*>|<*peer-group-name*>] **ebgp-multihop** [**ttl** <*value*>]	（可选）在非物理直连建立EBGP时使用该命令。配置能在不直接相连的网络上建立EBGP邻居 <*value*>：TTL的跳数，范围1~255
3	inspur(config-bgp)#**neighbor** [<*ipv4-address*>|<*peer-group-name*>] **update-source** <*interface-name*>	（可选）在使用Loopback地址建立EBGP连接时使用该命令。指定本地Loopback地址作为建立TCP连接的源IP地址 <*interface-name*>：指定BGP会话中建立TCP连接时所使用的作为源地址的接口名称

通过直连地址建立EBGP

如*图 4-44*所示，R1和R2分别在AS65000和AS65001中。现在要在R1和R2之间用物理口直接建立EBGP邻居关系。

图 4-44 EBGP 间物理直连配置拓扑图



R1上的配置如下：

```
R1#config terminal
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 129.213.1.1 255.255.255.252
R1(config-if-gei-1/1)#exit
R1(config)#router bgp 65000
R1(config-bgp)#neighbor 129.213.1.2 remote-as 65001
R1(config-bgp)#exit
```

R2上的配置如下：

```
R2#config terminal
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 129.213.1.2 255.255.255.252
R2(config-if-gei-1/1)#exit
R2(config)#router bgp 65001
R2(config-bgp)#neighbor 129.213.1.1 remote-as 65000
R2(config-bgp)#exit
```

查看配置结果：

在R1上用**show ip bgp neighbor**命令查看建立的BGP邻居关系情况。

```
R1#show ip bgp neighbor
BGP neighbor is 129.213.1.2, remote AS 65001, external link
  BGP version 4, remote router ID 129.213.1.2
  BGP state = Established, up for 00:04:21
  hold time is 180 seconds, keepalive interval is 60 seconds
……
  Connections established 1
  Local host: 129.213.1.1, Local port: 179
  Foreign host: 129.213.1.2, Foreign port: 1024
```

从上面的输出可以了解以下的信息：BGP的邻居是129.213.1.2，邻居属于AS65001中，建立了EBGP连接。邻居的router ID是129.213.1.2，状态是Established，会话已经建立4分21秒。

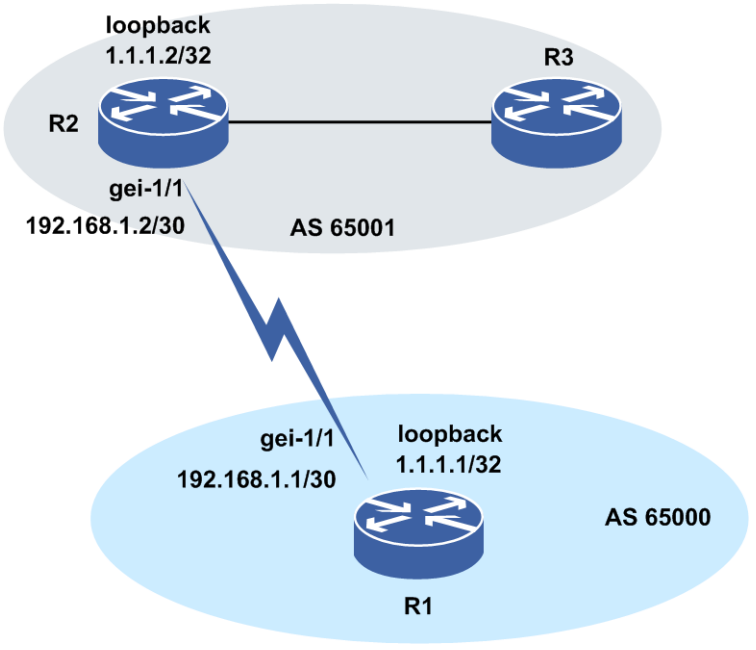
在R2上用**show ip bgp neighbor**命令查看建立的BGP邻居关系情况，解释同上。

```
R2#show ip bgp neighbor
BGP neighbor is 129.213.1.1, remote AS 65000, external link
  BGP version 4, remote router ID 129.213.1.1
  BGP state = Established, up for 00:00:27
  hold time is 180 seconds, keepalive interval is 60 seconds
……
  Connections established 1
  Local host: 129.213.1.2, Local port: 1024
  Foreign host: 129.213.1.1, Foreign port: 179
```

通过loopback地址建立EBGP

如*图 4-45*所示，要在R1和R2之间通过Loopback地址建立EBGP邻居关系。

图 4-45 EBGP 间用 Loopback 连接配置拓扑图



R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 192.168.1.1 255.255.255.252
R1(config-if-gei-1/1)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#router bgp 65000
R1(config-bgp)#neighbor 1.1.1.2 remote-as 65001
R1(config-bgp)#neighbor 1.1.1.2 ebgp-multihop ttl 5
R1(config-bgp)#neighbor 1.1.1.2 update-source Loopback1
R1(config-bgp)#exit
R1(config)#ip route 1.1.1.2 255.255.255.255 192.168.1.2
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 192.168.1.2 255.255.255.252
R2(config-if-gei-1/1)#exit
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#router bgp 65001
R2(config-bgp)#neighbor 1.1.1.1 remote-as 65000
R2(config-bgp)#neighbor 1.1.1.1 ebgp-multihop ttl 5
R2(config-bgp)#neighbor 1.1.1.1 update-source Loopback1
R2(config-bgp)#exit
R2(config)#ip route 1.1.1.1 255.255.255.255 192.168.1.1
```

需要说明的是，如果在语句**ebgp-multihop**后面不指明具体的跳数的话，系统会缺省把TTL设置为8。

查看配置结果，在R1上用**show ip bgp neighbor**命令查看建立的BGP邻居关系情况：

```
R1#show ip bgp neighbor
BGP neighbor is 1.1.1.2, remote AS 65001, external link
  BGP version 4, remote router ID 1.1.1.2
  BGP state = Established, up for 00:01:01
  hold time is 180 seconds, keepalive interval is 60 seconds
……
  Connections established 1
```

```
  Local host: 1.1.1.1, Local port: 179
  Foreign host: 1.1.1.2, Foreign port: 1026
```

可以看到，本地R1和位于AS65001中的1.1.1.2路由器建立了EBGP连接。

在R2上用**show ip bgp neighbor**命令查看建立的BGP邻居关系情况。

```
R2#show ip bgp neighbor
BGP neighbor is 1.1.1.1, remote AS 65000, external link
  BGP version 4, remote router ID 1.1.1.1
  BGP state = Established, up for 00:02:03
  hold time is 180 seconds, keepalive interval is 60 seconds
……
  Connections established 1
  Local host: 1.1.1.2, Local port: 1026
  Foreign host: 1.1.1.1, Foreign port: 179
```

可以看到，本地R2和位于AS65000中的1.1.1.1路由器建立了EBGP连接。

4.6.1.2 建立 IBGP 邻居

IBGP的作用是在AS内部完成BGP更新信息的交换，维护AS内部连通性。

前提

在配置IBGP邻居之前先要保证节点之间物理连接正常，且两个节点在相同的AS中。

相关信息

BGP规定，一个IBGP的路由器不能将来自另一IBGP路由器的路由发送给第三方IBGP路由器。这也可以理解为通常所说的Split-horizon规则。

当路由器通过EBGP接收到更新信息时，会对这个更新信息进行处理，并发送到所有的IBGP及余下的EBGP对等体；而当路由器从IBGP接收到更新信息时，会对其进行处理并仅通过EBGP传送，而不会向IBGP传送。

所以，在AS中，BGP路由器必须要通过IBGP会话建立完全连接的网状连接，以此来保持BGP的连通性。

1.启动BGP进程。

命令	功能
inspur(config)#**router bgp** <*as-number*>	启动BGP进程并指定本路由器所在的AS号

2.配置IBGP邻居。

步骤	命令	功能
1	inspur(config-bgp)#**neighbor** [<*ipv4-address*>|<*peer-group-name*>] **remote-as** <*number*>	配置一个BGP邻居或配置一个邻居对等体组及其自治系统号
2	inspur(config-bgp)#**neighbor** [<*ipv4-address*>|<*peer-group-name*>] **update-source** <*interface-name*>	（可选）在使用Loopback地址建立 EBGP连接时使用该命令。指定本地 Loopback地址作为建立TCP连接的 源IP地址

<*interface-name*>：指定BGP会话TCP连接使用的作为源地址的接口名称。

3.强制使用自身接口地址作为通告路由的下一跳。

命令	功能
inspur(config-bgp)#**neighbor** [<*ipv4-address*>|*peer-group-name*>] **next-hop-self**	强制使用自身接口地址作为通告路由的下一跳

“下一跳”（NEXT_HOP）属性是BGP的公认必选属性，该属性描述了到公布目的地址的路径的下一跳路由器的IP地址，分三种情况：

- 如果正在进行路由通告的路由器和接收的路由器在不同的AS中（外部对等体），下一跳为宣告路由器的接口IP地址。
- 如果正在宣告的路由器和接收的路由器在同一个AS内（内部对等体），并且更新消息中 NLRI指向的是同一AS内的目的地，则下一跳是宣告该路由的邻居的IP地址。
- 如果正在宣告的路由器和接收的路由器是内部对等体，并且更新消息的NLRI指向不同AS内的目的地，则下一跳为学习到路由的外部对等实体的IP地址。

4.关闭同步。

命令	功能
inspur(config-bgp)#**no synchronization**	关闭同步使BGP不等待IGP同步就能通告网络路由
inspur(config-bgp)#**synchronization disable**	关闭同步使BGP不等待IGP同步就能通告网络路由

同步规则是指当一个AS为另一个AS提供了过渡服务时，只有当本地AS内部所有的路由器都通过IGP的路由信息的传播收到这条路由信息以后，BGP才能向外发送这条路由信息。当路由器从IBGP收到一条路由更新信息时，在转发给其他EBGP对等体之前，路由器会对同步性进行验证。只有该路由器上IGP认识这个更新的目的时（即IGP路由表中有相应的条目），路由器才会将其通过EBGP转发；否则，路由器不会转发该更新信息。

同步规则的主要目的是为了保证AS内部的连通性，防止路由循环的黑洞。但是在实际的应用中，一般都会将同步功能禁用，而使用AS内IBGP的全网状连接结构来保证连通性，这样即可以避免向IGP中注入大量BGP路由，加快路由器处理速度，又可以保证数据包不丢失。要安全的禁用同步，需要满足以下两个条件之一：

- 所处的AS是单口的，或者说是末端AS（Stub AS），即是指只有一个点与外界网络连接。
- 虽然所处的AS是过渡型的（指一个AS可以通过本地AS，与第三方AS建立连接的），但是在AS内部的所有路由器都运行BGP。

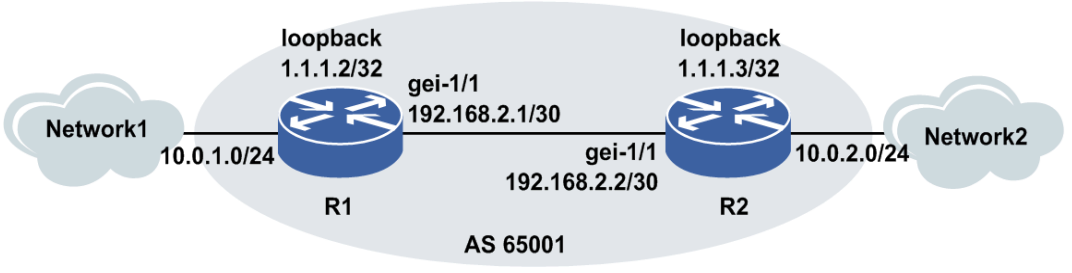
第2种情况是很常见的，因为AS内所有的路由器都有BGP信息，所以IGP只需要为本地AS传送路由信息。

同步功能在路由器上缺省是关闭的，可以用命令**synchronization**来启动同步。

举例：通过loopback地址建立IBGP

如*图 4-46*所示，R1和R2在同一个AS中，要在R1和R2之间用Loopback地址建立IBGP连接。

图 4-46 IBGP 配置拓扑图



R1上的配置如下：

```
R1#config terminal
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 192.168.2.1 255.255.255.252
R1(config-if-gei-1/1)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#router bgp 65001
R1(config-bgp)#neighbor 1.1.1.3 remote-as 65001
R1(config-bgp)#neighbor 1.1.1.3 update-source Loopback1
R1(config-bgp)#neighbor 1.1.1.3 next-hop-self
R1(config-bgp)#no synchronization
R1(config-bgp)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 192.168.2.0 0.0.0.3
R1(config-ospf-1-area-0)#network 1.1.1.2 0.0.0.0
R1(config-ospf-1-area-0)#exit
```

R2上的配置如下：

```
R2#config terminal
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 192.168.2.2 255.255.255.252
R2(config-if-gei-1/1)#exit
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.3 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#router bgp 65001
R2(config-bgp)#neighbor 1.1.1.2 remote-as 65001
R2(config-bgp)#neighbor 1.1.1.2 update-source Loopback1
R2(config-bgp)#neighbor 1.1.1.2 next-hop-self
R2(config-bgp)#no synchronization
R2(config-bgp)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 192.168.2.0 0.0.0.3
R2(config-ospf-1-area-0)#network 1.1.1.3 0.0.0.0
R2(config-ospf-1-area-0)#exit
```

在R1上用**show ip bgp neighbor**命令查看建立的BGP邻居关系情况。

```
R1#show ip bgp neighbor
BGP neighbor is 1.1.1.3, remote AS 65001, internal link
  BGP version 4, remote router ID 1.1.1.3
  BGP state = Established, up for 00:01:25
  hold time is 1800 seconds, keepalive interval is 60 seconds
……
  Connections established 1
```

```
  last error code is 6
  Local host: 1.1.1.2, Local port: 179
  Foreign host: 1.1.1.3, Foreign port: 1096
```

可以看到R1已经和1.1.1.3（R2）建立了IBGP邻居。

在R2上用**show ip bgp neighbor**命令查看建立的BGP邻居关系情况。

```
R2#show ip bgp neighbor
BGP neighbor is 1.1.1.2, remote AS 65001, internal link
  BGP version 4, remote router ID 1.1.1.2
  BGP state = Established, up for 00:03:07
  hold time is 180 seconds, keepalive interval is 60 seconds
……
  Connections established 1
  last error code is 5
  Local host: 1.1.1.3, Local port: 1096
  Foreign host: 1.1.1.2, Foreign port: 179
```

可以看到R2已经和1.1.1.2（R1）建立了IBGP连接。

4.6.1.3 配置 BGP 邻居认证密码

为了使在两个BGP对等体间的TCP连接上的MD5认证有效，可以配置邻居认证密码。为了使BGP建链有更好的保密性，还能对密码进行密文显示。

1.进入BGP路由配置模式。

命令	功能
inspur(config)#**router bgp** <*as-number*>	启动BGP进程并指定本路由器所在的AS号

2.配置BGP认证密码。

命令	功能
inspur(config-bgp)#**neighbor** <*ip-address*> **password** [<*string 1*>| **encrypted**< *string 2*>]	配置BGP邻居的认证，密码以密文的方式显示

举例

下面通过实例说明BGP邻居密码认证和密码密文显示配置：

```
inspur(config)#router bgp 100
inspur(config-bgp)#neighbor 192.168.0.2 remote-as 100
inspur(config-bgp)#neighbor 192.168.0.2 password 789
inspur(config-bgp)#show running-config bgp
!<bgp>
router bgp 100
  neighbor 192.168.0.2 password encrypt u5pd4oR1YGR1E+My5y4ec1dbC7
eZf4gsX0qhVYXcb6KV1CMnm8VFlX9dcceOjgUYrxPGh3Gy7Rl8VxSlqtHcujwZ5qzj
LbVOkiKWz41nHPk=
  $
$
!</bgp>
```

4.6.1.4 重启 BGP 进程

当BGP邻居进入异常状态时可以通过重起BGP的邻居进程尝试恢复。

重启BGP进程。

该操作在全局配置模式下进行，可以重启一个BGP邻居：

命令	功能
inspur(config)#**reset ip bgp** [**vrf** <*vrf-name*>][<*ipv4-address*>|<*peer-group-name*>][<*ipv6-address*>]	重启BGP实例或者某一个对等体或者对等体组

4.6.2 配置 BGP 路由通告

BGP要通告的路由必须先存在于IGP路由表中，是BGP路由更新的来源，将IGP路由信息注入BGP，直接影响到因特网的路由稳定性。路由注入有两种方式：动态注入和静态注入。

动态注入又分为完全动态注入和选择性动态注入。

完全动态注入是指将所有的IGP路由再分布（Redistribution）到BGP中。这种方式的优点是配置简单，但是可控性弱，效率低。

选择性动态注入则是将IGP路由表中的一部分路由信息注入BGP（如使用network命令）。这种方式会先验证地址及掩码，大大增强了可控性，提高了效率，可以防止错误的路由信息注入。

但是无论哪种动态注入方式，都会造成路由的不稳定。因为动态注入完全依赖于IGP信息，当IGP路由发生路由波动时，不可避免的会影响到BGP的路由更新。这种路由的不稳定会发出大量的更新信息，浪费大量的带宽。对于这种缺陷，可以使用在边界处使用路由衰减和聚合技术来改善。

静态注入可以有效解决路由不稳定的问题。静态注入是将静态路由的条目注入到BGP中去。由于静态路由条目是人为加入的，不会受到IGP波动的影响，所以很稳定。静态注入的稳定性防止了路由波动引起的反复更新。但是，如果网络中的子网划分边界不是非常分明的话，静态注入也会产生数据流阻塞等问题。

归纳起来，BGP通告路由的方法有以下三种：

- 用**network**命令通告路由
- 用**redistribute**命令将别的路由协议学习到的路由再分配到BGP中
- 用**aggregate-address**命令聚合路由之后再通告

4.6.2.1 配置 network 通告路由

本节介绍BGP通过**network**通告路由的配置步骤和命令。

前提

被BGP以**network**命令通告出去的路由必须在IGP中存在。

相关信息

BGP通告路由的常用方法就是使用**network**命令选择欲通告的网段，该命令指定了目的网段和掩码，这样在IGP路由表中的准确匹配该条件的路由都进入到BGP路由信息表中，被策略筛选后通告出去。

如BGP中使用**network 18.0.0.0 255.0.0.0**命令后，如果路由表中有18.0.0.0/8的网段，会被归入到BGP路由信息表中。如果路由表中无该网段或其子网，则无路由进入到BGP路由信息表中。因此，有时候为了配合BGP路由的通告，需要在路由器上配置一些指向Loopback地址的静态路由。

值得注意的是，进入到BGP路由信息表中的路由并不一定能够通告出去，这跟BGP的路由过滤或者路由策略有关。

在BGP中，可以使用**network**命令通告本路由器已知的网络。已知网络可以是通过直连、静态路由、动态路由学习到的网络。**network**命令在BGP协议中的使用不同于在IGP协议中的使用。

1.进入BGP路由配置模式。

命令	功能
inspur(config)#**router bgp** <*as-number*>	启动BGP进程并指定本路由器所在的AS号

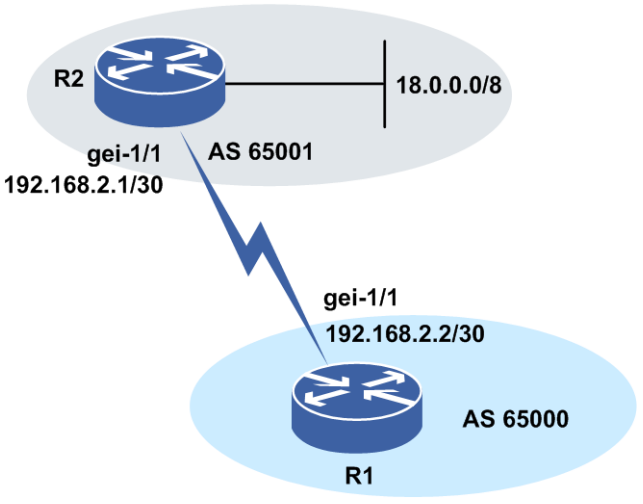
2.配置BGP通过network通告路由。

命令	功能
inspur(config-bgp)#**network**<*ip-address*><*net-mask*>[**route-map**<*map-tag*>]	把要通告路由输出到BGP路由信息表中，这些路由可以来自已连接的路由、动态路由选择以及静态路由

举例

如*图 4-47*所示，R2运行的IGP协议是OSPF。现在R2想将由OSPF发现的网段18.0.0.0/8在BGP中进行通告。

图 4-47 用 network 命令通告 BGP 路由拓扑图



R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 192.168.2.1 255.255.255.252
R2(config-if-gei-1/1)#exit
R2(config)#router bgp 65001
R2(config-bgp)#neighbor 192.168.2.2 remote-as 65000
R2(config-bgp)#network 18.0.0.0 255.0.0.0
R2(config-bgp)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 18.0.0.0 0.255.255.255
R2(config-ospf-1-area-0)#exit
```

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 192.168.2.2 255.255.255.252
R1(config-if-gei-1/1)#exit
R1(config)#router bgp 65000
R1(config-bgp)#neighbor 192.168.2.1 remote-as 65001
R1(config-bgp)#exit
```

查看配置信息，用**show ip bgp route** 命令查看R1上的BGP路由表情况。

```
R1#show ip bgp route
Status codes: *-valid, >-best, i-internal,s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete

   Network        NextHop     Metric   LocPrf   RtPrf   Path
*>18.0.0.0/8      192.168.2.1                  20      65001 i
```

在**show ip bgp route**的输出结果中，可以看到路由条目前边的“*”表示该路由是有效路由；带有“>”标志的路由是最佳路由，带有“i”标志的路由是IBGP路由；没有“i”标志的路由则是EBGP路由或者本地产生的路由。Next-hop条目下的地址表示BGP路由的下一跳，全0的下一跳表示该路由是本路由器自我产生的。Local-Pref下的值是BGP学习到的路由的本地优先级，缺省是100。Path字段表明了该路由的起源，有IGP、EGP、Incomplete三种类型。

在上面的例子中可以看到刚才18.0.0.0/8网段的路由已经存在于R1的BGP路由信息表中了，下一跳是R2的接口地址192.168.2.1。

4.6.2.2 配置 redistribute 重分发路由

本节介绍BGP通过**redistribute**重分发路由的配置步骤和命令。

前提

路由器上必须先配置好IGP路由协议。

相关信息

在路由条目数量很多，聚合不方便的情况下，BGP路由通告不得不选择完全动态注入的方式，将某一种或多种的IGP路由再分布（Redistribution）到BGP中，这样配置快捷方便。

使用**redistribute**命令可以将IGP协议（RIP、OSPF、IS-IS）的路由再分配到BGP中。使用该命令时要防止将IGP从BGP学习到的路由再次分配到BGP中，必要时使用过滤命令防止环路发生。

1.进入BGP路由配置模式。

命令	功能
`inspur(config)#`**router bgp** *<as-number>*	启动BGP进程并指定本路由器所在的AS号

2.配置BGP以redistribute重分发路由。

命令	功能
`inspur(config-bgp)#`**redistribute** *<protocol>*[**metric** *<metric-value>*][**route-map** *<map-tag>*]	将其它路由协议学习到路由再分配进BGP路由信息表

<protocol>：其它协议名称，目前有connected，static，rip，ospf-int，ospf-ext，isis-1，isis-2，isis–1–2，nat，natpt，ps-busi-addr，ps-user-addr，ldp，subscriber-aggregation，subscriber-host，sl-nat64-ipv4，user-special，address。

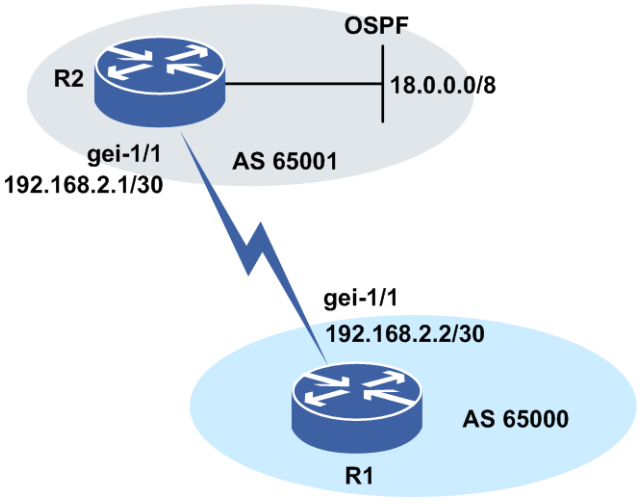
<metric-value>：再分配路由的metric值，不指定时使用缺省值，范围0~4294967295。

<map-tag>：再分配路由的路由映射名称，长度为1~31个字符。

举例

如*图 4-48*所示，R2运行的IGP协议是OSPF，现要将R2中的OSPF路由信息全部导入到BGP中。

图 4-48 重分发 OSPF 路由到 BGP 中的拓扑图



R2上的配置如下：

```
R2#config terminal
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 192.168.2.1 255.255.255.252
R2(config-if-gei-1/1)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 18.0.0.0 0.255.255.255
R2(config-ospf-1-area-0)#exit
R2(config)#router bgp 65001
R2(config-bgp)#neighbor 192.168.2.2 remote-as 65000
R2(config-bgp)#redistribute ospf-int 1
R2(config-bgp)#redistribute connected
R2(config)#exit
```

查看配置信息，用**show ip bgp route**命令查看R1上的BGP路由表情况：

```
R1#show ip bgp route
Status codes: *-valid, >-best, i-internal,s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete
   Network         NextHop     Metric   LocPrf   RtPrf   Path
*>  18.0.0.0/8    192.168.2.1                20      65001 ?
```

如果R2需要引入OSPF外部路由，并设其metric值为5，则应如下配置：

```
R2#config terminal
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 192.168.2.1 255.255.255.252
R2(config-if-gei-1/1)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 18.0.0.0 0.255.255.255
R2(config-ospf-1-area-0)#exit
R2(config)#router bgp 65001
R2(config-bgp)#neighbor 1.1.1.1 remote-as 65000
R2(config-bgp)#redistribute ospf-ext 1 metric 5
R2(config-bgp)#redistribute connected
R2(config)#exit
```

4.6.2.3 配置路由聚合

BGP协议可以将学习到的多条路由信息汇聚成一条路由信息对外通告，从而大大减少路由表中的路由条目。

1.进入BGP路由配置模式。

命令	功能
inspur(config)#**router bgp** <*as-number*>	启动BGP进程并指定本路由器所在的AS号

2.配置BGP路由聚合。

在路由器上配置路由聚合必须聚合完全相等的掩码，以防止出现路由黑洞。

命令	功能
inspur(config-bgp)#**aggregate-address** <*ip-address*><*net-mask*>[**count** <*count*>][**as-set**][**summary-only**][**strict**][**subnet** <*ip-address*><*net-mask*>]	在BGP路由选择表中创建一条聚合路由策略

<*ip-address*>：要生成的聚合网络，为十进制点分形式。

<*net-mask*>：要生成的聚合掩码，为十进制点分形式。

<*count*>：指明聚合操作时要求待聚合路由满足聚合子网的子网个数，范围0~255，缺省为1。

as-set：配置该参数后，聚合路由会根据子路由所带的as-path来计算聚合后的as-path。

summary-only：配置该参数后，向BGP邻居只通告聚合路由而不包含被聚合的子网路由。

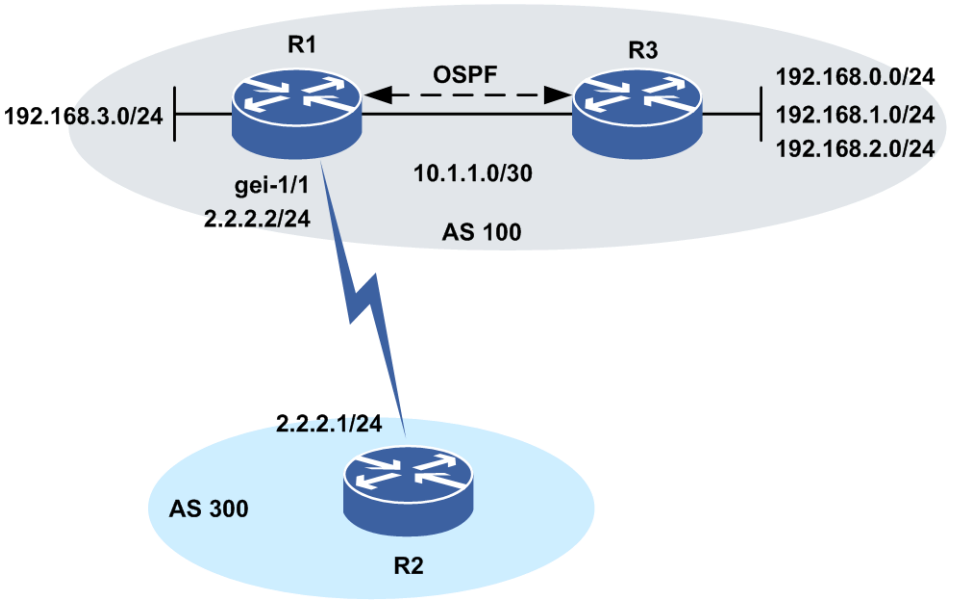
strict：只有对MED相同的路由才能聚合。否则聚合条件放宽，不考虑MED属性。

subnet：形成聚合路由的子网。

举例

如*图 4-49*所示，路由器R1要将自己和R3的AS内路由网段192.168.0.0/24、192.168.1.0/24、192.168.2.0/24、192.168.3.0/24通告给AS300中的路由器R2，R1和R3之间运行OSPF路由协议。

图 4-49 路由聚合配置实例



路由器R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 2.2.2.2 255.255.255.0
R1(config-if-gei-1/1)#exit
R1(config)#router bgp 100
R1(config-bgp)#neighbor 2.2.2.1 remote-as 300
R1(config-bgp)#aggregate-address 192.168.0.0 255.255.252.0 count 0
 summary-only
R1(config-bgp)#redistribute ospf-int 1
R1(config-bgp)#redistribute connected
R1(config-bgp)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 192.168.3.0 0.0.0.255
R1(config-ospf-1-area-0)#network 10.1.1.0 0.0.0.3
R1(config-ospf-1-area-0)#exit
```

如上配置的话，R1通过IBGP学习到192.168.0.0/24、192.168.1.0/24、192.168.2.0/24、192.168.3.0/24四条路由，但只向EBGP R2通告聚合后的一条路由192.168.0.0/22。注意聚合通告命令中的参数**summary-only**，如没有配置该参数，则R2通告聚合路由的同时将通告具体路由。

查看配置结果，用**show ip bgp route**命令来查看R2上接收聚合BGP路由过后的路由表：

```
R2#show ip bgp route
Status codes: *valid, >best, i-internal
Origin codes: i-IGP, e-EGP, ?-incomplete
Netwrok           NextHop    Metric    LocPrf    RtPrf  Path
*>192.168.0.0/22    2.2.2.2                        20    100 i

R2#show ip bgp route detail 192.168.0.0 255.255.252.0
BGP routing table entry for 192.168.0.0/22
  01:02:19 received from 2.2.2.2
   origin i,nexthop 2.2.2.2,atomic,aggr 100 2.2.2.2,
   as path [100]
```

在实施了聚合以后，AS300的路由器R2的BGP路由表里只有一条路由，这大大减少了路由表的规模。同时，聚合路由携带的原子聚合和聚合属性，指出了聚合点。

如果不配置聚合命令中的参数**summary-only**，则R2通告聚合路由的同时将通告具体路由。

```
R2#show ip bgp route
Status codes: *valid, >best, i-internal
Origin codes: i-IGP, e-EGP, ?-incomplete

Netwrok            NextHop    Metric   LocPrf   RtPrf    Path
*>192.168.0.0/22    2.2.2.2                  20      100 i
*>192.168.0.0/24    2.2.2.2                  20      100 i
*>192.168.1.0/24    2.2.2.2                  20      100 i
*>192.168.2.0/24    2.2.2.2                  20      100 i
*>192.168.3.0/24    2.2.2.2                  20      100 i
```

BGP中除了有一条聚合过后的192.168.0.0/22的路由条目以外，仍然包含了192.168.0.0/24、192.168.1.0/24、192.168.2.0/24、192.168.3.0/24这四条具体的路由条目。

参数<*count*>指明了聚合操作时要求等待聚合路由满足聚合子网的子网个数。范围为0~255，缺省为1，表示发布路由时自身IGP中必须存在的子网个数。如果选择参数为0，则只需IGP路由中出现192.168.0.0 255.255.252.0中的任意一子网时聚合发布路由192.168.0.0/22。如果count参数为1或者其他数值，则需要额外使用下列命令来指定相应的子网网段：

aggregate-address <*ip-address*><*net-mask*> **subnet** <*subnet-address*><*subnet-mask*>

以上命令的意思是只有IGP路由表中出现了命令中指定子网网段的路由信息并且同时出现的个数达到**count**参数后定义的个数时，才能聚合发布相应的路由信息。

这时候，只要192.168.1.0/24、192.168.2.0/24、192.168.3.0/24正常通告，不论192.168.0.0/24是否正常，R2都将向R1通告聚合之后的一条路由：192.168.0.0/22。但是如果192.168.1.0/24、192.168.2.0/24、192.168.3.0/24三个网段中只要有一个不正常，则破坏了以上的规则，R2不会向R1通告聚合之后的路由192.168.0.0/22。

运行在R1上的IGP如果确认192.168.0.0/24、192.168.1.0/24、192.168.2.0/24、192.168.3.0/24中后三条路由的话就向R2发送聚合之后的192.168.0.0/22的路由信息。

路由器R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 2.2.2.2 255.255.255.0
R1(config-if-gei-1/1)#exit
R1(config)#router bgp 100
R1(config-bgp)#neighbor 2.2.2.1 remote-as 300
R1(config-bgp)#aggregate-address   192.168.0.0   255.255.252.0   count   3
summary-only
R1(config-bgp)#aggregate-address 192.168.0.0 255.255.252.0 subnet 192.168.1.0
 255.255.255.0
R1(config-bgp)#aggregate-address 192.168.0.0 255.255.252.0 subnet 192.168.2.0
 255.255.255.0
R1(config-bgp)#aggregate-address 192.168.0.0 255.255.252.0 subnet 192.168.3.0
 255.255.255.0
R1(config-bgp)#redistribute ospf-int 1
R1(config-bgp)#redistribute connected
R1(config-bgp)#exit
R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 192.168.3.0 0.255.255.255
R1(config-ospf-1-area-0)#network 10.1.1.0 0.0.0.3
R1(config-ospf-1-area-0)#exit
```

4.6.3 配置 BGP 可靠性

BGP支持配置路由负荷分担、FRR和GR来增强网络的可靠性。

路由负荷分担有两个主要的功能：

•提高链路可靠性：网络的传输层对稳定性和可靠性要求很高。这种可靠性表现在除了链路本身可靠外还应表现在当某条链路出现故障的时候不影响其他路径上的报文转发或者减少转发失败的影响。

•提高带宽：路由负荷分担功能使得路由器能够将流量分配到多条路径上，从而充分利用带宽资源。通过路由协议或静态配置，可以使得转发表中，对于同一个目的地址，有多条可用的路由条目。

负荷分担的转发机制支持两种方法，**per-packet**（逐包模式）和**per-destination**（逐流模式），下表给出了这两种方法的优缺点：

优/缺点	逐流模式	逐包模式
优点	到给定目的的包可以保证走同一条路径，即使在有多条可用路径的情况下；到不同目的的包可以走不同的路径	路径利用率高，因为per-packet 使用轮转法来确定数据包走的路径，使得转发负荷均匀地分布在各条路径上
缺点	当流量中只有少量的目的地址时，可能会引起流量集中在少数路径上，分担不均衡；当流量中目的地址增加时，负荷分担会更有效	对于到给定目的的流量可能会选择不同的路径，造成接收端的排序，对于VoIP和其他要求有序的流量不适用

FRR技术能够实现以下功能：

•快速的发现链路失效

•当链路失效后，迅速的提供一条恢复路径

•在后继网络恢复过程中，避免出现转发环路“micro-loop”

在很多情况下，路由器的偶发中断是不可预见的，这将导致转发数据流的中断和路由振荡。如果路由器的控制功能能够和转发功能相分离，则可以采用某种策略，使得中断事件对重启路由器及其邻居带来的影响减为最小，这种策略就是GR。

4.6.3.1 配置 BGP 负荷分担

本节介绍BGP负荷分担的配置步骤和命令。

1.配置BGP支持负荷分担。

步骤	命令	功能
1	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**maximum-paths ibgp**< *number*>	配置协议支持负荷分担的路由数目，范围1~32，缺省为1（针对IBGP的负荷分担）
	inspur(config-bgp)#**maximum-paths** < *number*>	配置协议支持负荷分担的路由数目，范围1~32，缺省为1（针对EBGP的负荷分担）
	inspur(config-bgp)#**maximum-paths**	配置协议支持负荷分担的路由

步骤	命令	功能
	eibgp< *number*>	数目，范围1~32，缺省为1（对ebgp和ibgp同时生效）

2.配置接口负荷分担。

步骤	命令	功能
1	inspur(config)#**interface** < *interface-name*>	进入接口配置模式
2	inspur(config-if-interface-name)#**ip load-sharing** {**per-destination** | **per-packet**}	配置接口负荷分担模式：负荷分担是在出接口上配置的，默认情况下为**per-destination** 只有所有的接口配置为**per-packet**模式，负荷分担的模式才是**per-packet**

4.6.3.2 配置 BGP FRR

本节介绍BGP FRR的配置步骤和命令。

1.进入BGP路由配置模式。

命令	功能
inspur(config)#**router bgp** <*as-number*>	进入BGP路由配置模式

2.配置BGP FRR。

步骤	命令	功能
1	inspur(config-bgp)#**bgp frr** [**enhanced**]	启用BGP快速重路由功能
2	inspur(config-bgp)#**bgp frr wtr** [<*wtr*>]	（可选）为BGPFRR配置WTR（等待时间间隔）。当网络故障消失后，需要将流量从备份路径切换回原有的主路径，回切流量时需要按照WTR时间延迟后再回切，如果WTR为0，则立即回切

enhanced：如果BGP路由无其它明细路由作为备路由的时候，可以选择默认路由形成FRR。

4.6.3.3 配置 BGP Graceful Restart

本节介绍BGP Graceful Restart的配置步骤和命令。

1.进入BGP路由配置模式。

命令	功能
inspur(config)#**router bgp** <*as-number*>	进入BGP配置模式

2.开启BGP Graceful Restart 。

命令	功能
inspur(config-bgp)#**bgp graceful-restart**	配置BGP支持GR功能

3.设置BGP Graceful Restart参数。

步骤	命令	功能
1	inspur(config-bgp)#**bgp graceful-restart restart-time** <*time*>	配置GR路由器协商重启时间，范围1~3600，单位：秒
2	inspur(config-bgp)#**bgp graceful-restart stalepath-time** <*time*>	配置HELPER路由器发现GR路由器主备倒换后删除“保持路由”的时间，范围1~3600，单位：秒

4.6.4 配置 BGP 属性和路由过滤

BGP路由协议中定义了各种各样的属性，每个BGP属性都有不同的用处，这也使得BGP协议成为扩展性最好的、最灵活的以及高度可控的路由协议。

BGP路由属性是BGP路由协议的核心概念，是一组参数，在UPDATE消息中被发给连接对等体。这些参数记录了BGP路由的各种特定信息，用于路由选择和过滤路由，可以被理解为选择路由的度量尺度（Metric）。

路由过滤与属性设置是进行BGP决策的基础。通过路由过滤操作，可以根据需要对输入或输出的路由属性进行控制。

4.6.4.1 通过路由图过滤路由

本节介绍BGP通过路由图过滤路由的配置步骤和命令。

相关信息

路由过滤与属性设置是进行BGP决策的基础。通过路由过滤操作，可以根据需要对输入或输出的路由属性进行控制。

路由图用于控制路由信息，在路由域之间通过定义条件实现路由再分配。路由图通常

配合路由属性对路由进行决策。

1.创建路由图。

命令	功能
inspur(config)#**route-map** <*map-tag*>[**permit** | **deny**][<*sequence-number*>]	创建路由图

<*map-tag*>：路由映射的名称，长度为1~31个字符。

permit：如果路由映射符合匹配条件，允许再分配或被策略路由标志。

deny：如果路由映射符合匹配条件，不允许再分配或不被策略路由标志。

<*sequence-number*>：序列号，范围0~65535。

2.创建ACL、定义ACL规则。

步骤	命令	功能
1	inspur(config)#**ipv4-access-list** < *acl-name*>	创建ACL规则并命名
2	inspur(config-ipv4-acl)#**rule** <*rule-id* >{**permit** | **deny**}{<*source*>[<*source-wildcard*>]| **any**}	定义ACL的规则

<*acl-name*>：标准ACL表名，长度不超过31个字符。

<*rule-id* >：规则在ACL表中的唯一标识，该ID决定了规则在表中的顺序，范围1~2147483644。

permit：允许匹配该规则的包通过。

deny：禁止匹配该规则的包通过。

<*source*>：源IP地址。

<*source-wildcard*>：源IP地址的反掩码。

any：表示任意源IP地址。

3.BGP绑定指定的路由图。

步骤	命令	功能
1	inspur(config)#**router bgp** <*as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**neighbor** [<*ipv4-address*>|<*peer-group-name*>] **route-map** <*map-tag*>{**in** | **out**}	绑定指定的路由图，对BGP路由进行匹配或更改路由属性

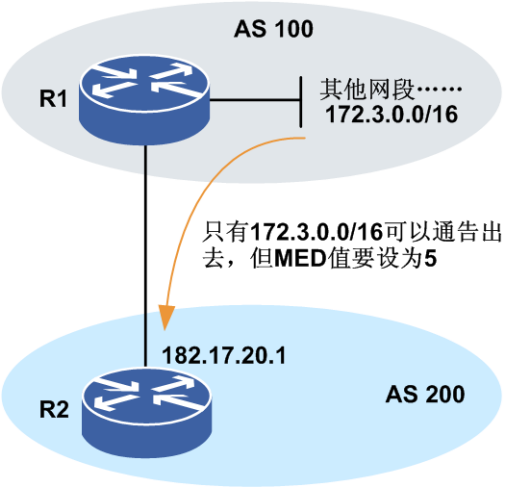
<*map-tag*>：路由映射的名称，长度为1~31个字符。

in | out：表示应用于输出还是输入路由

举例

如*图 4-50*所示，路由器R1和R2之间建立了EBGP连接。现要在路由器R1上配置一个路由图，该路由图将允许通告网络172.3.0.0/16给自治系统200，并将其MED值设置为5。

图 4-50 用 Route-Map 过滤路由拓扑图



配置R1：

```
R1(config)#router bgp 100
R1(config-bgp)#neighbor 182.17.20.1 remote-as 200
R1(config-bgp)#network 172.3.0.0 255.255.0.0
R1(config-bgp)#network 172.5.0.0 255.255.0.0
R1(config-bgp)#network 172.7.0.0 255.255.0.0
R1(config-bgp)#neighbor 182.17.20.1 route-map MAP1 out
R1(config-bgp)#neighbor 182.17.20.1 send-med
R1(config-bgp)#exit
R1(config)#route-map MAP1 permit 10
R1(config-route-map)#match ip address 1
R1(config-route-map)#set ip metric 5
R1(config-route-map)#exit
R1(config)#ipv4-access-list 1
R1(config-ipv4-acl)#rule 10 permit 172.3.0.0 0.0.255.255
R1(config-ipv4-acl)#exit
```

在使用路由图进行路由过滤操作时，通常配合**match**命令和**set**命令使用，**match**命令定义了匹配的标准，**set**命令定义了满足**match**匹配条件时执行的动作。

上面配置中**neighbor 182.17.20.1 send-med**命令的意思是：配置向邻居182.17.20.1通告路由时发送MED属性。

查看配置结果，用**show ip bgp route**命令查看此时路由器R2上的BGP路由表。

```
R2#show ip bgp route
Status codes: *-valid, >-best, i-internal,s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete

 Network          NextHop        Metric   LocPrf   RtPrf   Path
*>172.3.0.0/16     182.17.20.2     5        20       100     i

R2#show ip bgp route detail 172.3.0.0 255.255.0.0
BGP routing table entry for 172.3.0.0/16
  07:18:49 received from 182.17.20.2 (172.3.0.1)
   origin i,nexthop 182.17.20.2,metric 5,
   as path [100]
```

从上面的输出可以看到，R2上只学习到了172.3.0.0/16网段的路由，并且其metric值为5。

4.6.4.2 通过 NLRI 过滤路由

本节介绍BGP通过NLRI过滤路由的配置步骤和命令。

相关信息

为了限制路由器获得或通告选路信息，可以对送往或来自某个特定相邻设备的路由更新进行过滤。过滤器包括一个用于送往或来自一个相邻体的更新列表。

1.创建路由图。

命令	功能
inspur(config)#**route-map** <*map-tag*>[**permit** | **deny**][<*sequence-number*>]	创建路由图

<*map-tag*>：路由映射的名称，长度为1~31个字符。

permit：如果路由映射符合匹配条件，允许再分配或被策略路由标志。

deny：如果路由映射符合匹配条件，不允许再分配或不被策略路由标志。

<*sequence-number*>：序列号，范围0~65535。

2.创建ACL、定义ACL规则。

步骤	命令	功能
1	inspur(config)#**ipv4-access-list** < *acl-name*>	创建ACL规则并命名
2	inspur(config-ipv4-acl)#**rule** <*rule-id* >{**permit** | **deny**}{<*source*>[<*source-wildcard*>]| **any**}	定义ACL的规则

<*acl-name*>：标准ACL表名，长度不超过31个字符。

<*rule-id* >：规则在ACL表中的唯一标识，该ID决定了规则在表中的顺序，范围1~2147483644。

permit：允许匹配该规则的包通过。

deny：禁止匹配该规则的包通过。

<*source*>：源IP地址。

<*source-wildcard*>：源IP地址的反掩码。

any：表示任意源IP地址。

3.BGP绑定指定路由图。

步骤	命令	功能
1	inspur(config)#**router bgp** <*as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**neighbor** [<*ipv4-address*>|<*peer-group-name*>]	绑定指定路由图，对BGP路由进行匹配或更改路由属性

步骤	命令	功能
	route-map <*map-tag*>{**in** | **out**}	

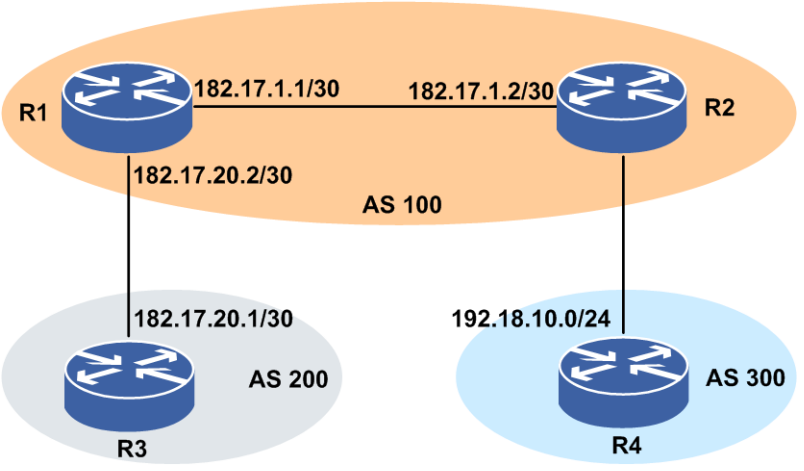
<*map-tag*>：路由映射的名称，长度为1~31个字符。

in | out：表示应用于输出还是输入路由

举例

如*图 4-51*所示，R1与R2互为IBGP对等体，R1与R3互为EBGP对等体，R2与R4互为EBGP对等体。为了避免AS100充当过渡自治系统的角色，防止R1将来自AS300的网络192.18.10.0/24通告给AS200，在R1上配置过滤功能。

图 4-51 通过 NLRI 过滤路由的拓扑图



路由器R1上的配置如下（端口配置和IGP配置略）：

```
R1(config)#router bgp 100
R1(config-bgp)#no synchronization
R1(config-bgp)#neighbor 182.17.1.2 remote-as 100
R1(config-bgp)#neighbor 182.17.1.2 next-hop-self
R1(config-bgp)#neighbor 182.17.20.1 remote-as 200
R1(config-bgp)#neighbor 182.17.20.1 route-map MAP1 out
R1(config-bgp)#exit
R1(config)#route-map MAP1 permit 10
R1(config-route-map)#match ip address 1
R1(config-route-map)#exit
R1(config)#ipv4-access-list 1
R1(config-ipv4-acl)#rule 1 deny 192.18.10.0 0.0.0.255
R1(config-ipv4-acl)#rule 2 permit any
```

使用**route-map**命令和访问控制列表，防止R1把前缀192.18.10.0/24的路由条目传播给AS200，也就是在R1上过滤掉了本条目。这样在R3上便无法学习到192.18.10.0/24的路由条目了。

用**show ip bgp route**命令查看此时路由器R3上的BGP路由表。

```
R3#show ip bgp route
Status codes: *-valid, >-best, i-internal,s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete

Network            NextHop     Metric  LocPrf  RtPrf  Path
*>192.168.11.0/24   182.17.20.2              20     300 100 i
*>192.168.12.0/24   182.17.20.2              20     300 100 i
```

```
*>192.168.13.0/24   182.17.20.2              20     300 100 i
```

由以上可以看到，处在AS200中的路由器R3没有学习到去往192.18.10.0/24网段的路由。

4.6.4.3 限制邻居所接受的路由通告数

BGP可以限制一个邻居所接受的路由条目数量。

1.进入BGP路由配置模式。

命令	功能
inspur(config)#**router bgp** <*as-number*>	启动BGP进程并指定本路由器所在的AS号

2.设置邻居所接受的最大路由通告数。

命令	功能
inspur(config-bgp)#**neighbor** <*ip-address*> **maximum-prefix** <*value*>[<*threshold-value*>| **drop-routes** | **restart** <*time*>| **warning-only**]	设置一个邻居所接受的最大路由条目数

<*value*>：可以从邻居接收的最大路由数，范围1~4294967295，缺省为4294967295。

<*threshold-value*>：当达到限制条目指定百分比的时候就产生一条告警信息，单位：%。

drop-routes：超过限制条目时就丢弃路由。

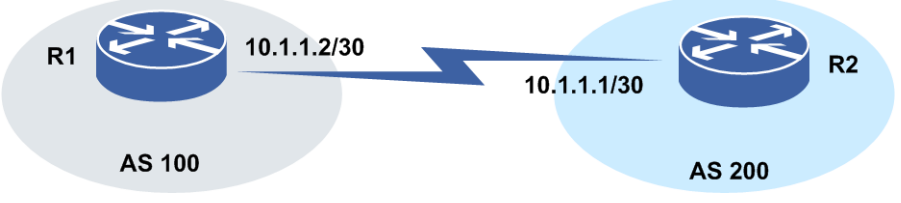
<*time*>：超过限制条目时就断链，并在指定的时间后重新建立邻居，单位：分钟，取值范围1~30000。

warning-only：超过限制条目时仅打印告警信息。

举例

如*图 4-52*所示例子中，R1限制R2通告给自己的路由条目数为10条，超过10条就会丢弃路由；R2限制R1通告给自己的路由条目数为20条，超过20条邻居就会断链，并在1分钟后重新建立邻居。

图 4-52 限制邻居所接受路由条目数



R1上的配置如下：

```
R1(config)#router bgp 100
R1(config-bgp)#neighbor 10.1.1.1 remote-as 200
R1(config-bgp)#neighbor 10.1.1.1 maximum-prefix 10 drop-routes
```

R2上的配置如下：

```
R2(config)#router bgp 200
R2(config-bgp)#neighbor 10.1.1.2 remote-as 100
R2(config-bgp)#neighbor 10.1.1.2 maximum-prefix 20 restart 1
```

当不配置重连时间，当R1通告给R2的路由超过20条，想要在R2上只是打印告警信息，不做任何处理，则选用**warning-only**。

R2上的配置如下：

```
R2(config)#router bgp 200
R2(config-bgp)#neighbor 10.1.1.2 remote-as 100
R2(config-bgp)#neighbor 10.1.1.2 maximum-prefix 20 warning-only
```

4.6.4.4 设置 AS_PATH 属性来过滤路由

本节介绍设置AS_PATH属性来过滤路由的配置步骤和命令。

相关信息

自治系统路径（AS_PATH）属性是公认必遵的属性。该属性包括了路由到达一个目的地所经过的一系列自治系统号码组成的路径段。产生路由的AS把路由发送到其外部BGP对等体时，同时加上自己的AS号码。此后，每个接收路由并传送给其它BGP对等体的AS都将把自己的AS号码加到AS序列的最前面。

BGP使用自治系统路径属性作为其路由更新的要素，以实现互联网络的无循环拓扑。每个路由都将包含一个自己经过的所有AS的排列表，如果一条路由被通告给产生该路由的AS时，AS检测到其AS号码在AS序列中已经存在，将不再接收此路由。同时，在决策最佳路由时将用到自治系统路径属性。当到达同一目的地有多条路由存在，而其它属性相同时，BGP协议通过自治系统路径属性挑选最短路径路由作为最佳路由使用。因此，在有些场合，可以通过增加AS路径的方式来影响路由器的BGP路由选择。

当一个或多个AS中的所有路由都需要过滤时，通常使用基于AS路径信息的路由过滤方式，可以避免基于前缀过滤造成的复杂性。

1.创建路由图。

命令	功能
inspur(config)#**route-map** <*map-tag*>[**permit** | **deny**][<*sequence-number*>]	创建路由图

<*map-tag*>：路由映射的名称，长度为1~31个字符。

permit：如果路由映射符合匹配条件，允许再分配或被策略路由标志。

deny：如果路由映射符合匹配条件，不允许再分配或不被策略路由标志。

<*sequence-number*>：序列号，范围0~65535。

2.定义与BGP AS_PATH属性相关的as-path access-list。

命令	功能
inspur(config)#**ip as-path access-list** <*access-list-number*>{**permit** | **deny**}<*as-regular-expression*>	定义与BGP AS_PATH属性相关的as-path access-list

<*access-list-number*>：指定正则表达式访问表的号。

permit：允许再分配或被策略路由标志。

deny： 不允许再分配或不被策略路由标志。

<*as-regular-expression*>：在访问表中使用正则表达式的自治系统。

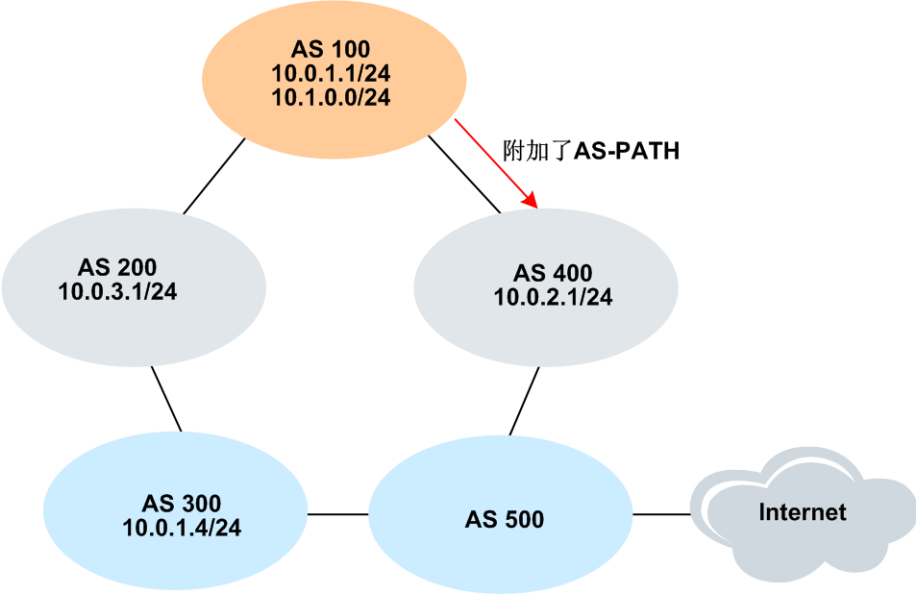
3.修改BGP AS_PATH属性。

步骤	命令	功能
1	`inspur(config)#`**route-map** <*map-tag*>[**permit** | **deny**][<*sequence-number*>]	进入路由映射配置模式
2	`inspur(config-route-map)#`**set as-path prepend** <*as-path-number*>[<*as-path-number*>]	修改BGP路由自治系统路径

举例

多个AS的网络拓扑如*图 4-53*所示，要求Internet访问AS100中10.1.0.0/24网段的路径为优先选择AS500→AS300→AS200→AS100的路径。

图 4-53 利用 AS_PATH 属性选择路由的拓扑图



配置AS100中的出口路由器：

```
inspur_AS100(config)#router bgp 100
inspur_AS100(config-bgp)#network 10.0.1.0 255.255.255.0
inspur_AS100(config-bgp)#network 10.1.0.0 255.255.255.0
inspur_AS100(config-bgp)#neighbor 192.168.1.2 remote-as 400
inspur_AS100(config-bgp)#neighbor 192.168.1.2 activate
inspur_AS100(config-bgp)#neighbor 192.168.1.2 route-map PATH out
inspur_AS100(config-bgp)#neighbor 192.168.1.6 remote-as 200
inspur_AS100(config-bgp)#neighbor 192.168.1.6 activate
inspur_AS100(config-bgp)#neighbor 172.16.0.1 remote-as 500
inspur_AS100(config-bgp)#neighbor 172.16.0.1 activate
inspur_AS100(config-bgp)#exit
inspur_AS100(config)#ipv4-access-list 1
```

```
inspur_AS100(config-ipv4-acl)#permit 10.1.0.0 0.0.0.255
inspur_AS100(config-ipv4-acl)#exit
inspur_AS100(config)#route-map PATH permit 0
inspur_AS100(config_route-map)#match ip address 1
inspur_AS100(config_route-map)#set as-path prepend 100 100 100 100
inspur-AS100(config-route-map)#exit
```

通过使用路由策略，对发布路由进行AS_Path的附加，从而影响到AS500对于访问AS100网段的路径的选择。

查看配置结果，用**show ip bgp route**命令查看AS500路由器上的BGP路由表情况。

```
inspur_AS500#show ip bgp route
Status codes: *valid, >best, i-internal
Origin codes: i-IGP, e-EGP, ?-incomplete

Network        NextHop     Metric LocPrf   RtPrf    Path
*>10.0.1.0/24  192.168.1.17       20        300 200 100 i
*>10.0.2.0/24  192.168.1.17       20        300 200 100 400 i
*>10.0.3.0/24  192.168.1.17       20        300 200 i
*>10.0.4.0/24  192.168.1.17       0         300 i
*>10.1.0.0/24  192.168.1.17       20        300 200 100 i
>10.1.0.0/24   192.168.1.13       20     400 100 100 100 100 100 i

inspur_AS500#show ip bgp route detail 10.1.0.0 255.255.255.0
BGP routing table entry for 10.1.0.0/24
  01:19:50 received from 192.168.1.11 (10.0.2.1)
   origin i,nexthop 192.168.1.13,
as path [400 100 100 100 100 100]
```

从上面的输出结果可知，使用AS_Path附加之后，AS500得知：从AS400到达的所要经过的AS个数为6个，而从AS300到达的所要经过的AS个数为3个。因此，在其他优先级缺省的情况下，BGP会优选择所经过AS数少的，即会选择从AS300到达AS100的目标网段，满足了先前提出的要求。

4.6.4.5 设置 LOCAL_PREF 属性来选择路由

本节介绍设置LOCAL_PREF属性来选择路由的配置步骤和命令。

相关信息

BGP的本地优先（LOCAL_PREF）属性是公认自决属性。inspur路由器识别并使用该属性，该属性的缺省值为100。

当BGP路由器向自治系统内部的其他BGP路由器广播路由时需要包含该属性，属性值的大小直接影响到路径的优先级。在路由决策中将选择本地优先值大的路由作为最佳路由。该属性影响本地出站流量，且仅用在本地AS内部，不会传到其他AS，也就是说本地优先属性只在IBGP邻居间被交换，而不会通告给EBGP邻居。

1.创建路由图。

命令	功能
inspur(config)#**route-map** <*map-tag*>[**permit** | **deny**][<*sequence-number*>]	创建路由图

<*map-tag*>：路由映射的名称，长度为1~31个字符。

permit：如果路由映射符合匹配条件，允许再分配或被策略路由标志。

deny：如果路由映射符合匹配条件，不允许再分配或不被策略路由标志。

<*sequence-number*>：序列号，范围0~65535。

2.创建ACL、定义ACL规则。

步骤	命令	功能
1	inspur(config)#**ipv4-access-list** < *acl-name*>	创建ACL规则并命名
2	inspur(config-ipv4-acl)#**rule** <*rule-id* >{**permit** | **deny**}{<*source*>[<*source-wildcard*>]| **any**}	定义标准ACL的规则

<*acl-name*>：标准ACL表名，长度不超过31个字符。

<*rule-id* >：规则在ACL表中的唯一标识，该ID决定了规则在表中的顺序，范围1~2147483644。

permit：允许匹配该规则的包通过。

deny：禁止匹配该规则的包通过。

<*source*>：源IP地址。

<*source-wildcard*>：源IP地址的反掩码。

any：表示任意源IP地址。

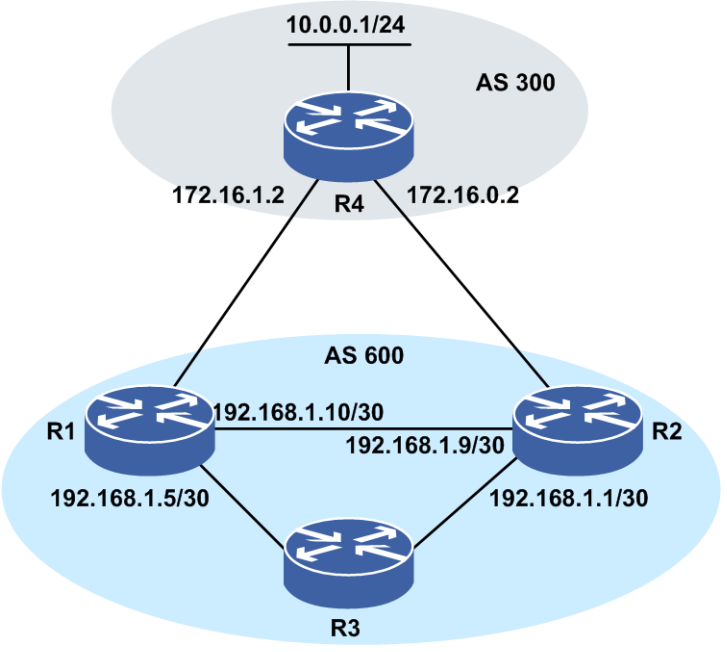
3.修改LOCAL_PREF属性值。

步骤	命令	功能
1	inspur(config)#**route-map** <*map-tag*>[**permit** | **deny**][<*sequence-number*>]	进入路由映射配置模式
2	inspur(config-route-map)#**set local-preference** <*value*>	为自治系统路径指定优先级权值，范围0~4294967295

举例

如*图 4-54*所示，路由器R1、R2、R3为IBGP全连接。用BGP的本地优先属性来满足“让所有外出业务优选R1的出口到达AS300”的要求。

图 4-54 用 BGP 本地优先属性选择路由拓扑图



路由器R1上的配置如下：

```
R1(config)#router bgp 600
R1(config-bgp)#no synchronization
R1(config-bgp)#neighbor 172.16.1.2 remote-as 300
R1(config-bgp)#neighbor 172.16.1.2 activate
R1(config-bgp)#neighbor 192.168.1.9 remote-as 600
R1(config-bgp)#neighbor 192.168.1.9 activate
R1(config-bgp)#neighbor 192.168.1.9 next-hop-self
R1(config-bgp)#neighbor 192.168.1.5 remote-as 600
R1(config-bgp)#neighbor 192.168.1.5 activate
R1(config-bgp)#neighbor 192.168.1.5 next-hop-self
R1(config-bgp)#neighbor 172.16.1.2 route-map Local_Pref in
R1(config-bgp)#exit
R1(config)#ipv4-access-list 1
R1(config-ipv4-acl)#permit any
R1(config)#route-map Local_Pref permit 10
R1(config-route-map)#match ip address 1
R1(config-route-map)#set local-preference 200
```

路由器R2上的配置如下：

```
R2(config)#router bgp 600
R2(config-bgp)#no synchronization
R2(config-bgp)#neighbor 172.16.0.2 remote-as 300
R2(config-bgp)#neighbor 172.16.0.2 activate
R2(config-bgp)#neighbor 192.168.1.1 remote-as 600
R2(config-bgp)#neighbor 192.168.1.1 activate
R2(config-bgp)#neighbor 192.168.1.1 next-hop-self
R2(config-bgp)#neighbor 192.168.1.10 remote-as 600
R2(config-bgp)#neighbor 192.168.1.10 activate
R2(config-bgp)#neighbor 192.168.1.10
R2(config-bgp)#neighbor 172.16.0.2 route-map Local_Pref in
R2(config)#ipv4-access-list 1
R2(config-ipv4-acl)#rule 1 permit any
R2(config)#route-map Local_Pref permit 10
R2(config-route-map)#match ip address 1
R2(config-route-map)#set local-preference 100
```

查看配置结果，用**show ip bgp route**命令查看路由器R3上的BGP路由表情况。

```
R3#show ip bgp route
Status codes: *valid, >best, i-internal
Origin codes: i-IGP, e-EGP, ?-incomplete
```

```
Network            NextHop     Metric   LocPrf   RtPrf  Path
*>i 10.0.0.0/24   192.168.1.6            200    200    300 i
 *i 10.0.0.0/24   192.168.1.2            100    200    300 i

R3#show ip bgp route detail 10.0.0.0 255.255.255.0
BGP routing table entry for 10.0.0.0/24
  01:24:10 received from 192.168.1.2 (172.16.0.1)
   origin i,nexthop 192.168.1.2, localpref 100,
   as path [300]
  01:21:46 received from 192.168.1.6 (172.16.1.1)
   origin i,nexthop 192.168.1.6, localpref 200,
   as path [300]
```

通过对路由器R1修改Local_Pref值，从而为内部设备流出本AS的业务指定出口。本例中，去往AS300的10.0.0.0/24网段的流量，优选从R1转发，因为从R1流出的路由，拥有更高的Local_Pref值。

4.6.4.6 设置 MED 属性来选择路由

本节介绍设置MED属性来选择路由的配置步骤和命令。

相关信息

MED属性属于BGP的任选非传递属性，Local_Pref仅影响离开AS的业务量，而MED用于影响流入AS的业务量。当这个AS有多个入口时，MED值较小的那个入口成为外部邻居路由器进入本AS的入口。对于BGP来说，再分配的路由MED默认值为0。

1.创建路由图。

命令	功能
inspur(config)#**route-map** <*map-tag*>[**permit** | **deny**][<*sequence-number*>]	定义一个路由图

<*map-tag*>：路由映射的名称，长度为1~31个字符。

permit：如果路由映射符合匹配条件，允许再分配或被策略路由标志。

deny：如果路由映射符合匹配条件，不允许再分配或不被策略路由标志。

<*sequence-number*>：序列号，范围0~65535。

2.创建ACL、定义ACL规则。

步骤	命令	功能
1	inspur(config)#**ipv4-access-list** < *acl-name*>	创建ACL规则并命名
2	inspur(config-ipv4-acl)#**rule** <*rule-id* >{**permit** | **deny**}{<*source*>[<*source-wildcard*>]| **any**}	定义ACL的规则

<*acl-name*>：标准ACL表名，长度不超过31个字符。

<*rule-id* >：规则在ACL表中的唯一标识，该ID决定了规则在表中的顺序，范围1~2147483644。

permit：允许匹配该规则的包通过。

deny：禁止匹配该规则的包通过。

<*source*>：源IP地址。

<*source-wildcard*>：源IP地址的反掩码。

any：表示任意源IP地址。

3.设置MED属性值。

步骤	命令	功能
1	inspur(config)#**route-map** <*map-tag*>[**permit** | **deny**][<*sequence-number*>]	进入路由映射配置模式
2	inspur(config-route-map)#**set ip metric** [+ | -]<*metric-value*>	设置路由选择协议的度量值

+：表示增加度量值。

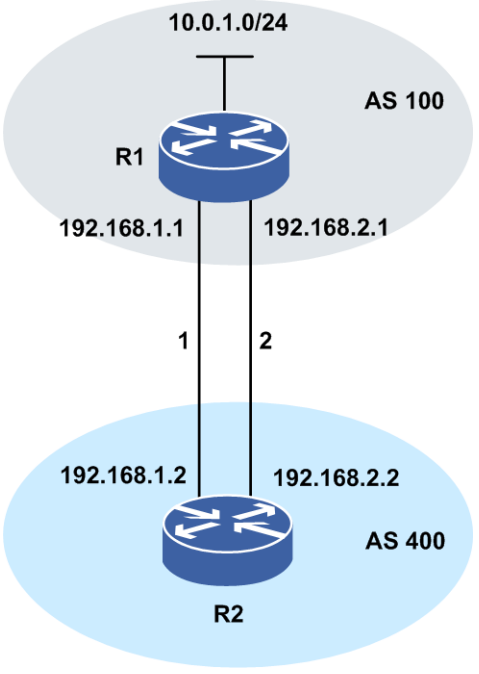
-：表示减少度量值。

<*metric-value*>：尺度值，范围0~4294967295。

举例

如*图 4-55*所示，AS100和AS400分别都有两条链路各自相连。通过在AS100中的配置来影响AS400，使得AS400优选其中一条链路1到达AS100。

图 4-55 利用 BGP MED 属性选择路由拓扑图



R1上的配置如下（端口配置和IGP配置略）：

```
R1(config)#router bgp 100
```

```
R1(config-bgp)#network 10.0.1.0 255.255.255.0
R1(config-bgp)#neighbor 192.168.1.2 remote-as 400
R1(config-bgp)#neighbor 192.168.1.2 activate
R1(config-bgp)#neighbor 192.168.1.2 route-map Med1 out
R1(config-bgp)#neighbor 192.168.1.2 send-med
R1(config-bgp)#neighbor 192.168.2.2 remote-as 400
R1(config-bgp)#neighbor 192.168.2.2 activate
R1(config-bgp)#neighbor 192.168.2.2 route-map Med2 out
R1(config-bgp)#neighbor 192.168.1.2 send-med
R1(config-bgp)#exit
R1(config)#ipv4-access-list 1
R1(config-ipv4-acl)#rule 1 permit any
R1(config-ipv4-acl)#exit
R1(config)#route-map Med1 permit 10
R1(config-route-map)#match ip address 1
R1(config-route-map)#set ip metric 50
R1(config-route-map)#exit
R1(config)#route-map Med2 permit 10
R1(config-route-map)#match ip address 1
R1(config-route-map)#set ip metric 100
R1(config-route-map)#exit
```

AS400中路由器R2上的配置如下：

```
R2(config)#router bgp 400
R2(config-bgp)#neighbor 192.168.1.1 remote-as 100
R2(config-bgp)#neighbor 192.168.1.1 activate
R2(config-bgp)#neighbor 192.168.2.1 remote-as 100
R2(config-bgp)#neighbor 192.168.2.1 activate
R2(config-bgp)#exit
```

查看配置结果，用**show ip bgp route**命令查看路由器R2上的BGP路由表情况。

```
R2(config-bgp)#show ip bgp route
Status codes: *valid, >best, i-internal
Origin codes: i-IGP, e-EGP, ?-incomplete
Network            NextHop     Metric   LocPrf    RtPrf  Path
*>10.0.1.0/24     192.168.2.1   50              20     100 i
 *10.0.1.0/24     192.168.1.1   100             20     100 i
*>10.0.2.0/24     0.0.0.0                       0     i

R2(config)#show ip bgp route detail 10.0.1.0 255.255.255.0
BGP routing table entry for 10.0.1.0/24
  01:44:13 received from 192.168.2.1 (10.0.1.1)
   origin i,nexthop 192.168.2.1,metric 50,
   as path [100]
  01:47:25 received from 192.168.1.1 (10.0.1.1)
   origin i,nexthop 192.168.1.1,metric 100,
   as path [100]
```

从上面的输出来看，通过对MED值的修改，路由器R2优选了MED值较小的50的链路1作为达到AS100的链路。

4.6.4.7 设置 BGP 团体串属性

本节介绍设置BGP团体串（community）属性的配置步骤和命令。

相关信息

BGP团体串属性属于BGP的任选可传递属性。团队属性是一组路由前缀共享有一个或多个相同的特性，有4个字节，前面两个字节的AS号，后面两个字节的管理上定义表示符。当对团体路由进行聚合时，聚合路由继承了所有路由的全部团体属性。

下面是几种已知公认的community属性定义：

·**no-export**：禁止向EBGP邻居通告

·**no-advertise**：禁止向任何BGP邻居通告

·**no-export-subconfed**：禁止向联盟外通告带有该属性的路由

·**local-AS**：只通告给本AS域内的BGP邻居路由器

·**Internet**：通告给所有其他路由器

除了这些被公认的团体属性以外，私有的团体属性可以被定义用作一些特殊用途。

1.创建路由图。

命令	功能
inspur(config)#**route-map** <*map-tag*>[**permit** | **deny**][<*sequence-number*>]	创建路由图

<*map-tag*>：路由映射的名称，长度为1~31个字符。

permit：如果路由映射符合匹配条件，允许再分配或被策略路由标志。

deny：如果路由映射符合匹配条件，不允许再分配或不被策略路由标志。

<*sequence-number*>：序列号，范围0~65535。

2.配置地址前缀列表。

命令	功能
inspur(config)#**ip prefix-list** <*prefix-list-name*>{[**seq** <*seq-number*>]{**permit** | **deny**}<*network-num*><*len*>[**ge** <*value*>| **le** <*value*>]|**description** <*prefix-list-description*>}	用于配置一条地址前缀列表，目前主要用于路由的通告过滤

<*prefix-list-name*>：prefix-list的名称，长度为1~31个字符。

seq <*seq-number*>：prefix-list表项索引值，值小的优先进行匹配；范围1~4294967294。

permit：如果待过滤的IP地址在该表项的前缀范围内，通过该表项的过滤并不再进行后续的匹配。若待过滤的IP地址不在该表项的前缀范围内则继续进行后续表项的匹配查找。

deny：如果待过滤的IP地址在该表项的前缀范围内，表示通不过该表项的过滤并且不在进行后续表项的匹配。若待过滤的IP地址不在该表项的前缀范围内则继续进行后续表项的匹配。

<*network-num*>：指定IP地址前缀范围。

<*len*>：指定IP地址的掩码长度，范围 0~32。

ge <*value*>：指定IP地址前缀的匹配范围后还需要该匹配的地址前缀长度大于该值，该值范围1~32。

le <*value*>：指定IP地址前缀的匹配范围后还需要该匹配的地址前缀长度小于该值，该值范围1~32。

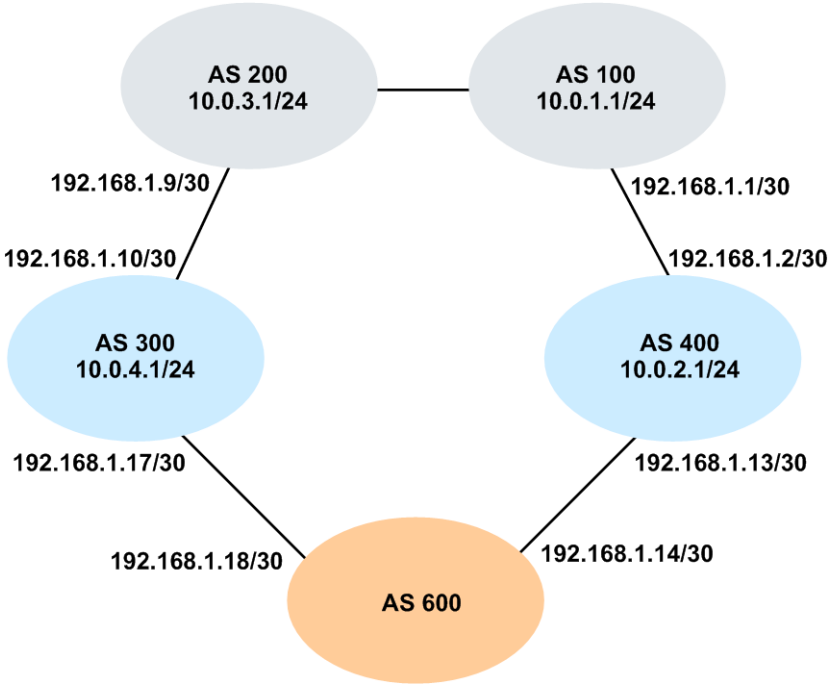
3.设置BGP路由COMMUNITY属性。

步骤	命令	功能
1	inspur(config)#**route-map** *<map-tag>*[**permit** | **deny**][*<sequence-number>*]	进入路由映射配置模式
2	inspur(config-route-map)#**set community** {**none** |[**additive**]{**internet** | **no-advertise** | **no-export** | **no-export-subconfed** |*<aa:nn>*|*<nn>*}[{**no-advertise** | **no-export** | **no-export-subconfed** |*<aa:nn>*|*<nn>*}]}	设置BGP路由COMMUNITY属性

举例1：对Community的路由进行标记

如*图 4-56*所示的网络中，AS600想要为来自不同AS的路由设置不一样的属性值。要求为AS300的路由标记300:1，为AS400的路由标记400:1。

图 4-56 用团体串属性来控制大量路由拓扑图



AS300中路由器的配置如下（端口配置和IGP配置略）：

```
inspur_AS300(config)#router bgp 300
inspur_AS300(config-bgp)#network 10.0.4.0 255.255.255.0
inspur_AS300(config-bgp)#neighbor 192.168.1.9 remote-as 200
inspur_AS300(config-bgp)#neighbor 192.168.1.9 activate
inspur_AS300(config-bgp)#neighbor 192.168.1.18 remote-as 600
inspur_AS300(config-bgp)#neighbor 192.168.1.18 activate
inspur_AS300(config-bgp)#neighbor 192.168.1.18 route-map Community out
inspur_AS300(config-bgp)#neighbor 192.168.1.18 send-community
inspur_AS300(config-bgp)#exit
inspur_AS300(config)#ip prefix-list AS200 seq 5 permit 10.0.3.0 24
inspur_AS300(config)#route-map Community permit 10
inspur_AS300(config-route-map)#match ip address prefix-list AS200
inspur_AS300(config-route-map)#set community 300:1
inspur_AS300(config-route-map)#exit
```

AS400中路由器的配置如下（端口配置和IGP配置略）：

```
inspur_AS400(config)#router bgp 300
```

```
inspur_AS400(config-bgp)#network 10.0.2.0 255.255.255.0
inspur_AS400(config-bgp)#neighbor 192.168.1.1 remote-as 100
inspur_AS400(config-bgp)#neighbor 192.168.1.1 activate
inspur_AS400(config-bgp)#neighbor 192.168.1.14 remote-as 600
inspur_AS400(config-bgp)#neighbor 192.168.1.14 activate
inspur_AS300(config-bgp)#network 10.0.2.0 255.255.255.0
inspur_AS400(config-bgp)#neighbor 192.168.1.14 route-map Community out
inspur_AS400(config-bgp)#neighbor 192.168.1.14 send-community
inspur_AS400(config-bgp)#exit
inspur_AS400(config)#ipv4-access-list 1
inspur_AS400(config-ipv4-acl)#rule 1 permit any
inspur_AS400(config-ipv4-acl)#exit
inspur_AS400(config)#route-map Community permit 10
inspur_AS400(config-route-map)#match ip address 1
inspur_AS400(config-route-map)#set community 400:1
inspur_AS400(config-route-map)#exit
```

查看配置结果，用**show ip bgp route**命令查看AS600上的BGP路由表情况。

```
inspur_AS600(config)#show ip bgp route
Status codes: *valid, >best, i-internal
Origin codes: i-IGP, e-EGP, ?-incomplete
Network          NextHop    Metric    LocPrf   RtPrf  Path
*>10.0.1.0/24    192.168.1.13          20    400 100 i
*>10.0.2.0/24    192.168.1.13          20    400 i
*>10.0.3.0/24    192.168.1.17          20    300 200 i
*10.0.3.0/24     192.168.1.13          20    400 100 200 i
*>10.0.4.0/24    192.168.1.13          20    400 100 200 300 i

inspur_AS600(config)#show ip bgp route detail 10.0.3.0 255.255.255.0
BGP routing table entry for 10.0.3.0/24
  00:28:52 received from 192.168.1.17 (10.0.4.1)
   origin i,nexthop 192.168.1.17,
   community 300:1
   as path [300 200]
  00:28:54 received from 192.168.1.13 (10.0.2.1)
   origin i,nexthop 192.168.1.13,
   community 400:1
   as path [400 100 200]
```

在AS600的设备上接收到的BGP路由已经根据来源分别做了标记：从AS300来的路由标记为300：1；从AS400来的路由标记为400：1。

举例2：利用对Community的路由进行标记来对大量路由进行过滤

配置要求：在AS600上根据Community属性，对路由进行Local_Pref设置来选择路由。

配置AS600（端口配置和IGP配置略）：

```
inspur_AS600(config)#router bgp 600
inspur_AS600(config-bgp)#neighbor 192.168.1.13 remote-as 400
inspur_AS600(config-bgp)#neighbor 192.168.1.13 activate
inspur_AS600(config-bgp)#neighbor 192.168.1.13 route-map Local_Pref in
inspur_AS600(config-bgp)#neighbor 192.168.1.17 remote-as 300
inspur_AS600(config-bgp)#neighbor 192.168.1.17 activate
inspur_AS600(config-bgp)#exit
inspur_AS600(config)#route-map Local_Pref permit 10
inspur_AS600(config-route-map)#match community-list 1
inspur_AS600(config-route-map)#set local-preference 200
inspur_AS600(config-route-map)#exit
inspur_AS600(config)#ip community-list 1 permit 400:1
```

查看配置结果，用**show ip bgp route**命令查看AS600上的BGP路由表情况，如下：

```
inspur_AS600(config)#show ip bgp route
Status codes: *valid, >best, i-internal
Origin codes: i-IGP, e-EGP, ?-incomplete
Network          NextHop  Metric  LocPrf   RtPrf  Path
*>10.0.1.0/24   192.168.1.13       200     20    400 100 i
```

```
*>10.0.2.0/24   192.168.1.13        200     20    400 i
*>10.0.3.0/24   192.168.1.13        200     20   400 100 200 i
*10.0.3.0/24   192.168.1.17                20    300 200 i
*>10.0.4.0/24   192.168.1.13       200   20  400 100 200 300 i
```

经上面的两次设置，BGP优先选择了Local_Pref值大的路由。在本例中，优先选择了从AS400到达目的网段10.0.3.0/24。

4.6.5 配置大型网络中 BGP 的应用功能

对于同一个AS内部的BGP路由器，要求两两之间必须建立邻居关系，构成全互连。这样，随着IBGP路由器的增加，邻居数将以n（n-1）/2数目递增（n为IBGP路由器的数量）。为了减少维护和配置的工作量，可以配置和使用路由反射器和联盟。

4.6.5.1 配置 BGP 路由反射器

本节介绍BGP路由反射器的配置步骤和命令。

相关信息

对于网络庞大的AS，为了减少复杂性，在其内部运行IBGP的路由器中选择一台作为路由反射器（RR），所有其它IBGP路由器作为其客户端，只与RR对等化，多个RR之间再对等化。这样所有客户端通过RR反射路由，这样邻居数就降为n-1。客户端是指与此路由反射器建立全连接的IBGP邻居，构成一个群。此路由反射器的其它不属于这个群的IBGP邻居就是非客户端。

当一条路由被RR接收后，将根据不同的对等体类型进行反射：

- 如果更新消息来自EBGP邻居，则反射给所有的非客户端和客户端。
- 如果更新消息来自非客户端，则仅反射给客户端。
- 如果更新消息来自某客户端，则反射给所有的客户端及非客户端，除了这条路由的始发者。

当一个AS内部存在多个RR时，可以把一个AS内部的多个RR划归为一个组群（cluster）。一个AS内部可以有多个cluster，一个cluster至少包含多于一个RR。

1.进入BGP路由配置模式。

命令	功能
inspur(config)#**router bgp** *<as-number>*	启动BGP进程并指定本路由器所在的AS号

2.设置路由反射器的簇ID。

命令	功能
inspur(config-bgp)#**bgp cluster-id** {*<value>*|*<ip-address>*}	设置路由反射器的簇ID，范围1~4294967295，缺省将Router-ID作为群ID号

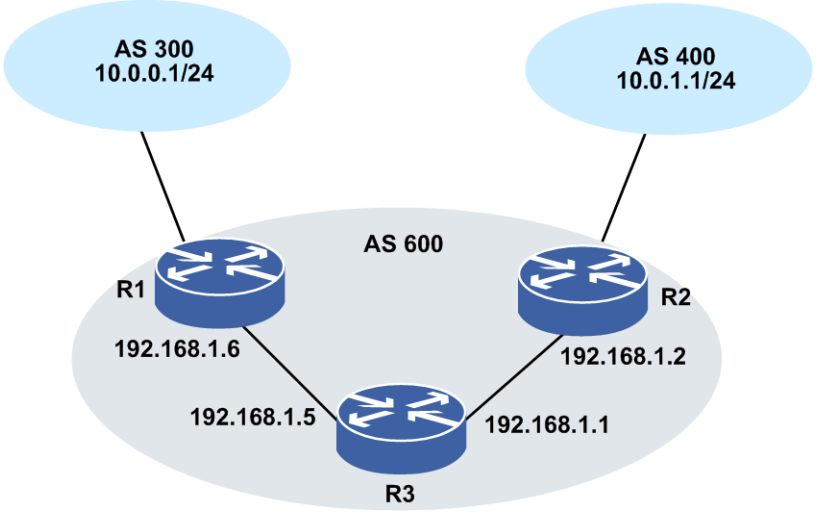
3.设置路由反射器客户对等体。

命令	功能
inspur(config-bgp)#**neighbor** [<*ipv4-address*>|<*peer-group-name*>] **router-refletor-client**	将邻居或邻居对等体组设置为路由反射器客户对等体

举例

如*图 4-57*所示的网络中，路由器R1、R2和R3之间是IBGP，但是没有全连接。现在为了打破IBGP必须是全连接的连接规则，配置路由反射器，使得R3能够将IBGP邻居接收到的路由，转发给另外一个IBGP邻居。鉴于AS600中的IBGP不是全连接，可以配置路由反射器来避免全连接。

图 4-57 BGP 路由反射器配置拓扑图



R1上的配置如下（端口配置和IGP配置略）：

```
R1(config)#router bgp 600
R1(config-bgp)#no synchronization
R1(config-bgp)#neighbor 172.16.1.2 remote-as 300
R1(config-bgp)#neighbor 172.16.1.2 activate
R1(config-bgp)#neighbor 192.168.1.5 remote-as 600
R1(config-bgp)#neighbor 192.168.1.5 activate
R1(config-bgp)#neighbor 192.168.1.5 next-hop-self
R1(config-bgp)#exit
```

R2上的配置如下（端口配置和IGP配置略）：

```
R2(config)#router bgp 600
R2(config-bgp)#no synchronization
R2(config-bgp)#neighbor 172.16.0.2 remote-as 400
R2(config-bgp)#neighbor 172.16.0.2 activate
R2(config-bgp)#neighbor 192.168.1.1 remote-as 600
R2(config-bgp)#neighbor 192.168.1.1 activate
R2(config-bgp)#neighbor 192.168.1.1 next-hop-self
R2(config-bgp)#exit
```

R3上的配置如下：

```
R3(config)#router bgp 600
R3(config-bgp)#no synchronization
R3(config-bgp)#bgp cluster-id 3.3.3.3
R3(config-bgp)#neighbor 192.168.1.2 remote-as 600
R3(config-bgp)#neighbor 192.168.1.2 activate
```

```
R3(config-bgp)#neighbor 192.168.1.2 route-reflector-client
R3(config-bgp)#neighbor 192.168.1.6 remote-as 600
R3(config-bgp)#neighbor 192.168.1.6 activate
R3(config-bgp)#neighbor 192.168.1.6 route-reflector-client
R3(config-bgp)#exit
```

用**show ip bgp route**命令来查看R1路由器上的BGP路由表情况。

```
R1(config)#show ip bgp route
Status codes: *valid, >best, i-internal
Origin codes: i-IGP, e-EGP, ?-incomplete

Network            NextHop     Metric   LocPrf    RtPrf   Path
*> 10.0.0.0/24     172.16.1.2                    20      300 i
*>i 10.0.1.0/24    192.168.1.2           100      200     400 i

R1#show ip bgp route detail 10.0.1.0 255.255.255.0
BGP routing table entry for 10.0.1.0/24
  05:04:45 received from 192.168.1.5 (192.168.1.1)
   origin i,nexthop 192.168.1.2,localpref 100, originator_id 172.16.0.1
cluster_list 3.3.3.3
   as path [400]
```

用**show ip bgp route**命令来查看R2路由器上的BGP路由表情况。

```
R2#show ip bgp route
Status codes: *valid, >best, i-internal
Origin codes: i-IGP, e-EGP, ?-incomplete

Network             NextHop     Metric   LocPrf    RtPrf   Path
*>i 10.0.0.0/24     192.168.1.6           100     200     300 i
*>  10.0.1.0/24     172.16.0.2                    20      400 i

R2#show ip bgp route detail 10.0.0.0 255.255.255.0
BGP routing table entry for 10.0.0.0/24
  05:05:19 received from 192.168.1.1 (192.168.1.1)
   origin i,nexthop 192.168.1.6,localpref 100, originator_id 172.16.1.1
   cluster_list 3.3.3.3
   as path [300]
```

从BGP路由的输出可以看到，R1和R2已经分别学习到了对端的路由。

4.6.5.2 配置 BGP 联盟

本节介绍BGP联盟的配置步骤和命令。

相关信息

路由联盟（confederation）的作用与路由反射器相同，目的是为了减少同一AS内部建立IBGP邻居的连接数量。路由联盟是将一个AS划分为多个子AS，AS内部的多个IBGP路由器分属各子AS，子AS内部建立IBGP，子AS之间建立EBGP。对于AS外部而言，子AS不可见。

1.进入BGP路由配置模式。

命令	功能
inspur(config)#**router bgp** *<as-number>*	启动BGP进程并指定本路由器所在的AS号

2.设置BGP联盟ID。

命令	功能
inspur(config-bgp)#**bgp confederation identifier** <*value*>	设置联盟ID号，范围1~65535；目前也支持4字节的 AS，其范围为1~4294967295

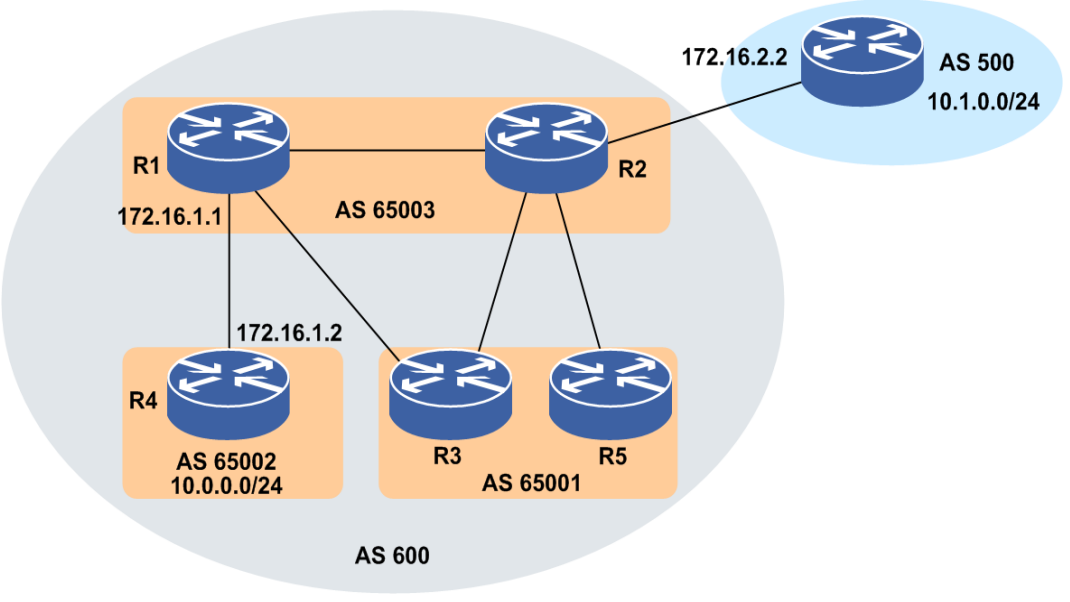
3.设置联盟对等端AS号。

命令	功能
inspur(config-bgp)#**bgp confederation peers** <*value*>[<*value*>]	设置联盟对等端AS号，范围1~65535；目前也支持4字节的AS，其范围为1~4294967295

举例

如*图 4-58*所示，要在AS600内使用联盟配置来避免IBGP全连接。

图 4-58 配置 BGP 联盟的拓扑图



路由器R2上的配置如下（端口配置和IGP配置略）：

```
R2(config)#router bgp 65003
R2(config-bgp)#bgp confederation identifier 600
R2(config-bgp)#no synchronization
R2(config-bgp)#bgp confederation peers 65001 65002
R2(config-bgp)#neighbor 172.16.0.2 remote-as 65001
R2(config-bgp)#neighbor 172.16.0.2 activate
R2(config-bgp)#neighbor 192.168.1.10 remote-as 65003
R2(config-bgp)#neighbor 192.168.1.10 activate
R2(config-bgp)#neighbor 192.168.1.1 remote-as 65001
R2(config-bgp)#neighbor 192.168.1.1 activate
R2(config-bgp)#neighbor 172.16.2.2 remote-as 500
R2(config-bgp)#neighbor 172.16.2.2 activate
R2(config-bgp)#exit
```

路由器R4上的配置如下（端口配置和IGP配置略）：

```
R4(config)#router bgp 65002
R4(config-bgp)#bgp confederation identifier 600
R4(config-bgp)#no synchronization
```

```
R4(config-bgp)#network 10.0.0.0 255.255.255.0
R4(config-bgp)#bgp confederation peers 65003
R4(config-bgp)#neighbor 172.16.1.1 remote-as 65003
R4(config-bgp)#neighbor 172.16.1.1 activate
R4(config-bgp)#exit
```

用**show ip bgp route**命令来查看路由器R2上的BGP路由表情况。

```
R2(config)#show ip bgp route
Status codes: *valid, >best, i-internal
Origin codes: i-IGP, e-EGP, ?-incomplete

Network          NextHop     Metric   LocPrf    RtPrf   Path
*>i 10.0.0.0/24   172.16.1.2          100       200     65002 i
*> 10.1.0.0/24    172.16.2.2                    20      500 i
```

以上输出可见在路由器R2上有去往R4的路由。

用**show ip bgp route**命令来查看路由器R4上的BGP路由表情况。

```
R4#show ip bgp route
Status codes: *valid, >best, i-internal
Origin codes: i-IGP, e-EGP, ?-incomplete

Network          NextHop    Metric    LocPrf    RtPrf  Path
*>10.0.0.0/24     0.0.0.0                       0      i
*>10.1.0.0/24     172.16.2.2          100       200    65003 500 i

R4#show ip bgp route detail 10.1.0.0 255.255.255.0
BGP routing table entry for 10.1.0.0/24
  06:27:14 received from 172.16.1.1 (172.16.1.1)
   origin i,nexthop 172.16.2.2,localpref 100,
   as path (65003) [500]
```

以上输出可见在路由器R4上有去往AS500的路由。

在联盟中，一个自治系统被划分为小的子自治系统，这些小的子自治系统治将通过EBGP实现连接。每个子自治系统作为一个独立的BGP自治系统在内部运行IBGP。

在完整的自治系统中只运行一个IGP协议，每个子自治系统含有其他所有子AS的IGP路由信息。

4.6.5.3 配置 BGP 路由抑制

本节介绍BGP路由抑制的配置步骤和命令。

相关信息

BGP提供了一种路由抑制（Route dampening，又叫路由阻尼）机制来减少由于路由波动（flap）造成的网络不稳定性。因为在路由波动发生时，路由的更新和撤消消息在网络中不断传播，会占用很大的带宽和路由器处理资源，这种情况对网络是不利的，要尽量避免。

BGP路由抑制的原理是：路由每波动一次赋予一个惩罚值（penalty）1000，当penalty达到一个抑制线（suppress-limit）时，该路由被抑制通告。每过一个半衰期（half-life-time），惩罚值将几何递减，当降到再次重用线（reuse-limit）时，路由通告抑制被取消。

在BGP路由抑制中会用到的几个值：

•半衰期（half-life-time）：范围1~45分钟，缺省15分钟

•再次使用值（reuse-value）：范围1~20000，缺省750

·抑制门限（suppress-value）：范围1~20000，缺省2000

·最大抑制时间（max-suppress-time）：范围1~255分钟，缺省4倍的half-life-time

1.进入BGP路由配置模式。

命令	功能
inspur(config)#**router bgp** <*as-number*>	启动BGP进程并指定本路由器所在的AS号

2.配置BGP路由抑制。

命令	功能
inspur(config-bgp)#**bgp dampening** [<*half-life*><*reuse*><*suppress*><*max-suppress-time*>| **route-map** <*map-tag*>]	使能BGP路由抑制以及修改各种路由抑制因素

<*half-life*>：改变路由阻尼因素的半衰期，范围1~45，缺省为15，单位：分钟。

<*reuse*>：改变路由阻尼因素的重新使用值，范围1~20000，缺省为750。

<*suppress*>：改变路由阻尼因素的路由抑制值，范围1~20000，缺省为2000。

<*max-suppress-time*>：改变路由阻尼因素的最大抑制时间，通常路由抑制时间到达该值以后，惩罚值不再增加，设置范围是1~255，缺省为60，单位：分钟。

<*map-tag*>：可使用的路由映射标识，长度为1~31个字符，只有在该映射中设置的路由振荡值将应用于当时的路由振荡。

举例

在本路由器上开启BGP路由抑制功能，且设置路由阻尼因素的半衰期为30分钟、重新使用值为500、阻尼因素的路由抑制值为2000、路由阻尼因素的最大抑制时间为120分钟。

```
inspur(config)#router bgp 100
inspur(config-bgp)#bgp dampening 30 500 2000 120
inspur(config-bgp)#network 203.250.15.0 255.255.255.0
inspur(config-bgp)#neighbor 192.208.10.5 remote-as 300
inspur(config-bgp)#exit
```

在路由器上用**show ip bgp protocol**命令可以查看关于路由抑制的配置情况。

```
inspur#show ip bgp protocol
BGP router ID is 1.1.1.2, Local as is 1
  Hold time is 180 seconds, KeepAlive time is 60 seconds
  Default local preference is 100
  Default export metric is 0
  IPv4 IGP synchronization is disabled
  IPv6 IGP synchronization is disabled
  Default information advertise is disabled
  Always compare med is disabled
  Fast fallover is enabled
  Client-to-client reflection is enabled
  Enforce-first-as is enabled
  IPv4 unicast is activated
  BGP FRR is disabled
  BGP IPv6 frr is disabled
  Router target is filtered
  Route dampening is enabled, halflife-time is 30, reuse is 500, suppress is
```

```
200
0, max-suppress-time is 120
  Graceful restart is disabled
  As-path ignore is disabled
  Router-id ignore is disabled
  BGP advertise-active-only is disabled
  BGP VPNv4 advertise-active-only is disabled
  BGP IPv4 rib-only is disabled
  BGP IPv6 rib-only is disabled
  Distance : external 20 internal 200
```

从上面的输出可以看到，路由抑制机制已经激活，并且半衰期为30分钟，重用值为500，路由抑制值为2000，最大抑制时间为120分钟。

4.6.5.4 配置 BGP 对等体组

本节介绍BGP对等体组的配置步骤和命令。

相关信息

BGP对等体组（peer group）的主要功能是用来对BGP 对等体进行集群管理。通过将对等体加入统一的等体组中，对其进行统一的属性配置及其他操作，这样可以减少对等体配置的工作量，简化配置过程，同时将对等体进行分类管理，提高维护的可靠性和方便性。

1.进入BGP路由配置模式。

命令	功能
inspur(config)#**router bgp** <*as-number*>	启动BGP进程并指定本路由器所在的AS号

2.配置BGP对等体组。

步骤	命令	功能
1	inspur(config-bgp)#**neighbor** <*word*> **peer-group**	创建一个BGP对等体组，对等体组的名称长度为1~31个字符
2	inspur(config-bgp)#**neighbor** <*word*> **remote-as** <*as-number*>	配置一个邻居对等体组的自治系统号
3	inspur(config-bgp)#**neighbor** <*ip-address*> **peer-group** <*word*>	将邻居加入BGP对等体组中

举例

创建一个BGP对等体组，等体组的名称为Inspur，在AS100中，将邻居192.168.0.2和192.168.0.3加入到此BGP对等体组中：

```
inspur(config)#router bgp 100
inspur(config-bgp)#neighbor Inspur peer-group
inspur(config-bgp)#neighbor Inspur remote-as 100
inspur(config-bgp)#neighbor 192.168.0.2 peer-group Inspur
inspur(config-bgp)#neighbor 192.168.0.3 peer-group Inspur
```

4.6.5.5 配置 BGP IPv6 VRF 对等体组

本节介绍在IPv6 VRF地址族下使用对等体组管理邻居的配置步骤和命令。

1.进入BGP路由配置模式。

命令	功能
inspur(config)#**router bgp** <*as-number*>	启动BGP进程并指定本路由器所在的AS号

2.进入BGP-IPv6-VRF模式。

命令	功能
inspur(config-bgp)#**address-family ipv6 vrf** <*vrf-name*>	创建并进入BGP-IPv6-VRF模式，VRF名称长度为1~32个字符

3.配置BGP对等体组。

步骤	命令	功能
1	inspur(config-bgp-af-ipv6-vrf)#**neighbor** <*word*> **peer-group**	创建一个BGP对等体组，对等体组的名称长度为1~31个字符
2	inspur(config-bgp-af-ipv6-vrf)#**neighbor** <*word*> **remote-as** <*as-number*>	配置一个邻居对等体组的自治系统号
3	inspur(config-bgp-af-ipv6-vrf)#**neighbor** <*ipv6-address*> **peer-group** <*word*>	将邻居加入BGP对等体组中

4.6.5.6 配置 BGP 对等体组路由策略

本节介绍BGP对等体组路由策略的配置步骤和命令。

相关信息

BGP对等体组支持的地址族路由有：BGP IPv4 unicast地址族、BGP IPv4 VRF unicast地址族、BGP VPNv4 unicast地址族、BGP IPv6 unicast地址族、BGP IPv6 VRF unicast地址族、BGP VPNv6 unicast地址族。

1.进入BGP路由配置模式。

命令	功能
inspur(config)#**router bgp** <*as-number*>	启动BGP进程并指定本路由器所在的AS号

2.创建BGP对等体组并设置路由策略生效规则。

步骤	命令	功能
1	inspur(config-bgp)#**neighbor** <*peer-group-name*> **peer-group**	创建一个BGP对等体组，对等体组的名称长度为1~31个字符
2	inspur(config-bgp)#**neighbor** <*peer-group-name*> **route-map** <*rmp-name*>{**in**|**out**}	设置对等体组路由策略在路由in方向或out方向生效

<*rmp-name*>：路由策略的名称。

in：表示路由策略在in方向的路由生效。

out：表示路由策略在out方向的路由生效。

3.设置对等体组路由策略。

步骤	命令	功能
1	inspur(config)#**route-map** <*rmp-name*>[{**deny**|**permit**}][<*routemap-sequence*>]	创建（删除）路由策略，并进入route-map配置模式
2	inspur(config-route-map)#**match interface *(**<*interface-name*>**)**	在route-map下设置match三层接口名称 只有下一跳与设置的match接口匹配的路由才能被发送/接收

permit：如果路由映射符合匹配条件，允许再分配策略路由标志。

deny：如果路由映射符合匹配条件，不允许再分配策略路由标志。

<*routemap-sequence*>：序列号，范围：0~65535。

4.验证配置结果。

命令	功能
inspur(config-bgp)#**show route-map**	显示路由策略

4.6.5.7 配置 Route-Map In 方向改变下一跳

本节介绍Route-Map In方向改变下一跳的配置步骤和命令。

1.创建Route-Map，配置下一跳。

步骤	命令	功能

步骤	命令	功能
1	inspur(config)#**route-map** <*rmp-name*>	创建Route-Map，并进入Route-Map配置模式
2	inspur(config-route-map)#**set next-hop** <*ip-address*>	在Route-Map配置模式下配置下一跳

2.在邻居入方向上应用Route-Map。

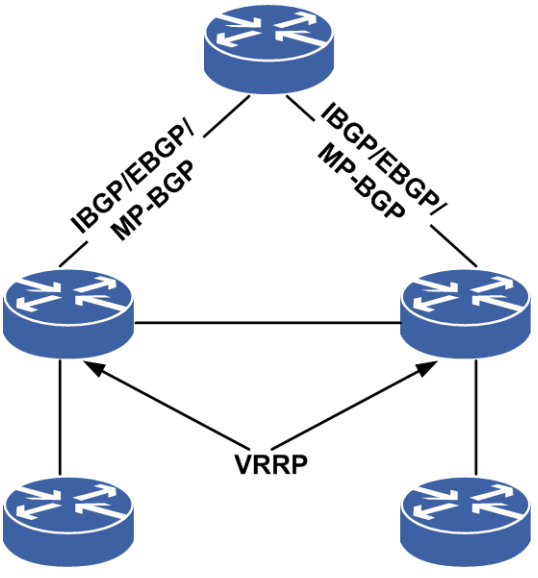
命令	功能
inspur(config-bgp)#**neighbor** <*peer*> **route-map** <*rmp-name*> **in**	在BGP模式下应用Route-Map在邻居入方向上
inspur(config-bgp-af-ipv4-vrf)#**neighbor** <*peer*> **route-map** <*rmp-name*> **in**	在VRF地址族模式下应用Route-Map在邻居入方向上
inspur(config-bgp-af-ipv4-multi)#**neighbor** <*peer*> **route-map** <*rmp-name*> **in**	在IPv4组播地址族模式下应用Route-Map在邻居入方向上

4.6.5.8 配置 BGP 与 VRRP 联动

本节介绍BGP与VRRP联动的配置步骤和命令。

如*图 4-59*所示，在下联接口上配置VRRP，虚地址作为接入设备的网关，上联通过BGP（IBGP/EBGP/MP-BGP）相连，为了保证上下行流量一致，需要VRRP的主设备的BGP路由优先级也为最优路由。

图 4-59 BGP 与 VRRP 联动典型组网图



目前BGP路由的优先级可以通过两种方法配置，一种方法是配置local preference值，另一种方法是配置metric值。

·local preference值改变只能在IBGP协议有效，对于跨域的BGP没有意义。

·metric值改变，对于IBGP或EBGP都有效。

1.BGP-UNICAST模式下配置BGP与VRRP联动。

步骤	命令	功能
1	inspur(config-vrrp)#**interface** <*interface-name*> inspur(config-vrrp-if)#**vrrp** <*vrid*> **ipv4** <*vr-ipaddress*>	在VRRP下创建与接口名关联的VRRP对象
2	inspur(config)#**samgr** inspur(config-samgr)#**track** <*track-name*> **vrrp interface** <*interface-name*> **vrid** <*vrid*>	在samgr下创建与VRRP对象关联的track对象
3	inspur(config)#**router bgp** <*as-number*> inspur(config-bgp)#**track** <*track-name*> **adjust-priority** <*priority-value*><*interface-name*>	在BGP下配置local preference/metric与VRRP联动

步骤1中的参数描述如下：

参数	描述
<*interface-name*>	接口名称。
<*vrid*>	VRRP对象id，范围1-255。
<*vr-ipaddress*>	虚拟IP地址。

步骤2中的参数描述如下：

参数	描述
<*track-name*>	VRRP类型track对象，长度1-31个字符。
<*interface-name*>	与track的VRRP对象关联的接口名称。
<*vrid*>	Track的VRRP对象id，范围1-255。

步骤3中的参数描述如下：

参数	描述
<*as-number*>	自治系统号。
<*track-name*>	VRRP类型track对象，长度1-31个字符。
<*priority-value*>	调整路由优先级，范围为1-100。
<*interface-name*>	与track的VRRP对象关联的接口名称。

2.BGP-IPV4-VRF模式下配置BGP与VRRP联动。

步骤	命令	功能

步骤	命令	功能
1	inspur(config-vrrp)#**interface** <*interface-name*> inspur(config-vrrp-if)#**vrrp** <*vrid*> **ipv4** <*vr-ipaddress*>	在VRRP下创建与接口名关联的VRRP对象
2	inspur(config)#**samgr** inspur(config-samgr)#**track** <*track-name*> **vrrp interface** <*interface-name*> **vrid** <*vrid*>	在samgr下创建与VRRP对象关联的track对象
3	inspur(config)#**router bgp** <*as-number*> inspur(config-bgp)#**address-family ipv4 vrf** <*vrf-name*> inspur(config-bgp-if)#**track** <*track-name*> **adjust-priority** <*priority-value*><*interface-name*>	在BGP下配置local preference/metric与VRRP联动

步骤1中的参数描述如下：

参数	描述
<*interface-name*>	接口名称。
<*vrid*>	VRRP对象id，范围1-255。
<*vr-ipaddress*>	虚拟IP地址。

步骤2中的参数描述如下：

参数	描述
<*track-name*>	VRRP类型track对象，长度1-31个字符。
<*interface-name*>	与track的VRRP对象关联的接口名称。
<*vrid*>	Track的VRRP对象id，范围1-255。

步骤3中的参数描述如下：

参数	描述
<*as-number*>	自治系统号。
<*vrf-name*>	VRF名称，长度1-31个字符。
<*track-name*>	VRRP类型track对象，长度1-31个字符。
<*priority-value*>	调整路由优先级，范围为1-100。
<*interface-name*>	与track的VRRP对象关联的接口名称。

4.6.5.9 配置 BGP 下一跳的迭代策略控制

在MPLS/MPLS VPN网络中，BGP采用嵌套查询，通过BGP查询路由下一跳时，若存在两条链路（直连口、环回口都建立邻居），优先匹配到32子网掩码的下一跳。

1.配置下一跳的迭代策略控制。

步骤	命令	功能
1	inspur(config)#**ip vrf** <*vrf-name*>	创建一个VRF实例，实例名称长度1~32个字符
2	inspur(config-vrf-name)#**rd** <*route-distinguisher*>	定义VRF的路由标识符
3	inspur(config-vrf-name)#**address-family ipv4**	激活IPv4地址族
4	inspur(config-vrf-name-af-ipv4)#**next-hop host-only**	配置下一跳的迭代策略控制

<*route-distinguisher*>：VRF的路由标识符，有三种格式。

- <0~65535>:<0~4294967295>
- A.B.C.D:<0~65535>
- <1-65535>.<0-65535>:<0-65535>

2.验证配置结果。

命令	功能
inspur(config)#**show ip vrf detail** [<*vrf-name*>]	查看VRF的信息

4.6.6 配置 BGP 动态组

本节介绍BGP动态组的配置步骤和命令。

相关信息

BGP动态组功能默认是开启的。

1.配置BGP动态组。

步骤	命令	功能
1	inspur(config)#**router bgp** <*as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**neighbor** {<*ipv4-address*>|<*ipv6-address*>|<*peer-group-name*>} **split-update-group**	表示该邻居不再和其他邻居共享动态组，独自占用一个动态组

2.查看BGP动态组配置。

命令	功能
inspur#**show ip bgp update-group** [<*ipv4-address*>|<*ipv6-address*>|<*index*>]	显示BGP邻居所在的动态组信息
inspur#**show bgp vpnv4 mcast update-group** [<*ipv4-address*>|<*ipv6-address*>|<*index*>]	显示VPN地址族下mcast的动态组信息
inspur#**show bgp vpnv4 multicast** [**vrf** <*vrf-name*>] **update-group** [<*ipv4-address*>|<*ipv6-address*>|<*index*>]	显示VPN地址族下组播的动态组信息
inspur#**show bgp vpnv4 unicast update-group** [**vrf** <*vrf-name*>][<*ipv4-address*>|<*ipv6-address*>|<*index*>]	显示VPN地址族下单播的动态组信息
inspur#**show bgp vpnv6 unicast update-group** [**vrf** <*vrf-name*>][<*ipv4-address*>|<*ipv6-address*>|<*index*>]	显示VPNv6地址族下单播的动态组信息
inspur#**show bgp** {**ipv4** | **ipv6**} **multicast update-group** [<*ipv4-address*>|<*ipv6-address*>|<*index*>]	显示IPv4或IPv6地址族组播的动态组信息
inspur#**show bgp** {**ipv4** | **ipv6**} **unicast update-group** [<*ipv4-address*>|<*ipv6-address*>|<*index*>]	显示IPv4或IPv6地址族下单播的动态组信息

3.清除BGP动态组信息。

命令	功能
inspur#**clear ip bgp update-group** [<*ipv4-address*>|<*ipv6-address*>|<*index*>]	清除BGP邻居所在的动态组信息
inspur#**clear ip bgp ipv4** [**vrf** <*vrf-name*>] **multicast update-group** [<*ipv4-address*>|<*ipv6-address*>|<*index*>]	清除IPv4地址族下组播的动态组信息
inspur#**clear ip bgp ipv4** [**vrf** <*vrf-name*>] **unicast update-group** [<*ipv4-address*>|<*ipv6-address*>|<*index*>]	清除IPv4地址族下单播的动态组信息
inspur#**clear ip bgp ipv6** [**vrf** <*vrf-name*>] **unicast update-group** [<*ipv4-address*>|<*ipv6-address*>|<*index*>]	清除IPv6地址族下单播的动态组信息
inspur#**clear ip bgp ipv6 multicast update-group** [<*ipv4-address*>|<*ipv6-address*>|<*index*>]	清除IPv6地址族下组播的动态组信息
inspur#**clear ip bgp vpnv4 mcast update-group** [<*ipv4-address*>|<*ipv6-address*>|<*index*>]	清除VPN地址族下mcast的动态组信息
inspur#**clear ip bgp vpnv4 multicast update-group** [<*ipv4-address*>|<*ipv6-address*>|<*index*>]	清除VPN地址族下组播的动态组信息
inspur#**clear ip bgp vpnv4 unicast update-group** [<*ipv4-address*>|<*ipv6-address*>|<*index*>]	清除VPN地址族下单播的动态组信息

命令	功能
inspur#**clear ip bgp vpnv6 unicast update-group** [<*ipv4-address*>|<*ipv6-address*>|<*index*>]	清除VPNv6地址族下单播的动态组信息

4.6.7 验证及维护 BGP

验证BGP配置结果

IR12000提供了以下命令查看BGP相关信息：

命令	功能
inspur#**show ip bgp protocol**	显示本地BGP协议模块的配置信息
inspur#**show ip bgp neighbor** [<*ipv4-address*>]	查看BGP邻接关系，显示当前邻居状态
inspur#**show ip bgp route** [**network** <*ip-address*>[**mask** <*net-mask*>]|**detail** <*ip-address*>[<*net-mask*>]	显示BGP路由信息表中的条目
inspur#**show ip bgp summary**	显示所有BGP邻居连接的状态

维护BGP

IR12000提供了debug命令对BGP协议进行调试，跟踪相关信息：

命令	功能
inspur#**debug ip bgp in**	跟踪显示BGP接收的notification报文，并列出错误号和子错误号
inspur#**debug ip bgp out**	跟踪显示BGP发出的notification报文，并列出错误号和子错误号
inspur#**debug ip bgp dampening**	BGP路由抑制情况
inspur#**debug ip bgp keepalieves**	BGP KeepAlieve消息处理情况
inspur#**debug ip bgp updates**	BGP Update消息处理情况；可以具体到只对某个对等体相关的Update消息处理情况进行跟踪打印
inspur#**debug ip bgp events**	跟踪显示BGP连接的状态机迁移
inspur#**debug bgp all**	跟踪显示所有BGP的debug命令的相关信息
inspur#**show debug bgp**	显示debug命令配置信息

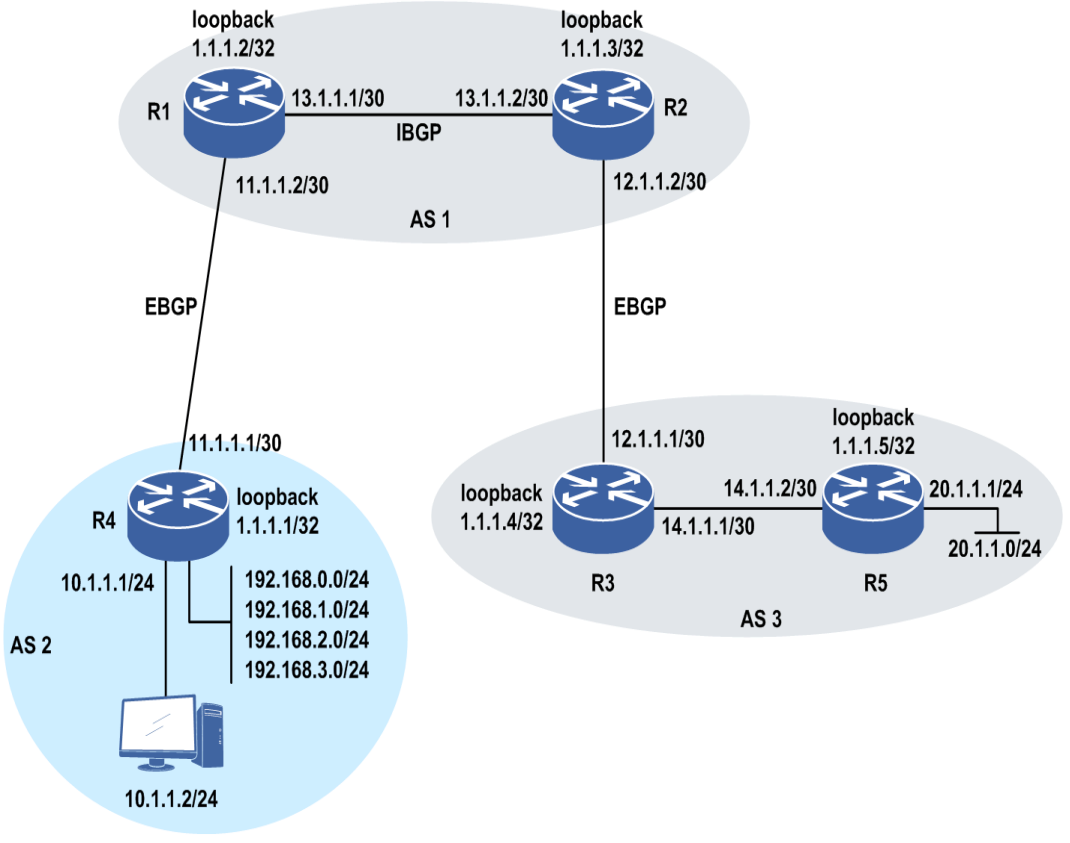
4.6.8 BGP 综合配置实例一（Loopback 接口创建 BGP）

配置说明

如*图 4-60*所示的网络拓扑中，R1与R2同在AS1中，R4在AS2中，R3和R5在AS3中。每台路由器的Loopback地址参见下表。

路由器	Loopback地址
R1	1.1.1.2/32
R2	1.1.1.3/32
R3	1.1.1.4/32
R4	1.1.1.1/32
R5	1.1.1.5/32

图 4-60 BGP 综合配置实例一拓扑图



1.R1与R2建立IBGP邻居；R1与R4建立EBGP邻居；R2与R3建立EBGP邻居。

2.R3与R5之间通过静态路由和OSPF连通。

3.R3将OSPF路由导入BGP中，且设置导入BGP的OSPF路由的Metric为122。

4.R4 上 有 192.168.0.0/24 、 192.168.1.0/24 、 192.168.2.0/24 、 192.168.3.0/24 、 192.168.100.0/24、10.1.1.0/24网段的静态路由。

5.R4将其静态路由分发到BGP中去，且将Metric置为33，但需要将192.168.100.0/24网

段的路由信息过滤掉。

6.在R4上进行路由聚合，同时发布明细路由。

7.保证在AS2中的PC机能和R5上的20.1.1.0/24网段互通。

8.所有路由器均采用Loopback1口BGP建链的源地址，互联地址掩码是30位。

配置思路

1.R1上建立BGP邻居和静态路由。

2.R2上建立BGP邻居和静态路由。

3.R3上建立BGP邻居和静态路由、OSPF。

4.R4上建立BGP邻居并配置地址聚合和路由过滤。

5.R5上配置IGP（OSPF）。

配置过程

R1上的配置：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ip address 11.1.1.2 255.255.255.252
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#ip address 13.1.1.1 255.255.255.252
R1(config-if-gei-1/2)#exit

R1(config)#router bgp 1
R1(config-bgp)#no synchronization
R1(config-bgp)#redistribute connected/*重分发直连路由*/
R1(config-bgp)#neighbor 1.1.1.1 remote-as 2
R1(config-bgp)#neighbor 1.1.1.1 activate
R1(config-bgp)#neighbor 1.1.1.1 ebgp-multihop ttl 5
R1(config-bgp)#neighbor 1.1.1.1 update-source loopback1/*通过loopback地址建立
EBGP邻居*/
R1(config-bgp)#neighbor 1.1.1.3 remote-as 1
R1(config-bgp)#neighbor 1.1.1.3 activate
R1(config-bgp)#neighbor 1.1.1.3 next-hop-self
R1(config-bgp)#neighbor 1.1.1.3 update-source loopback1/*通过loopback地址建立
IBGP邻居*/
R1(config-bgp)#exit

R1(config)#ip route 1.1.1.1 255.255.255.255 11.1.1.1
R1(config)#ip route 1.1.1.3 255.255.255.255 13.1.1.2
```

R2上的配置：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.3 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 13.1.1.2 255.255.255.252
```

```
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#ip address 12.1.1.2 255.255.255.252
R2(config-if-gei-1/2)#exit

R2(config)#router bgp 1
R2(config-bgp)#no synchronization
R2(config-bgp)#redistribute connected
R2(config-bgp)#neighbor 1.1.1.2 remote-as 1
R2(config-bgp)#neighbor 1.1.1.2 activate
R2(config-bgp)#neighbor 1.1.1.2 next-hop-self
R2(config-bgp)#neighbor 1.1.1.2 update-source loopback1/*通过loopback地址建立
IBGP邻居*/
R2(config-bgp)#neighbor 1.1.1.4 remote-as 3
R2(config-bgp)#neighbor 1.1.1.4 activate
R2(config-bgp)#neighbor 1.1.1.4 ebgp-multihop ttl 5/*配置多跳*/
R2(config-bgp)#neighbor 1.1.1.4 update-source loopback1/*通过loopback地址建立
EBGP邻居*/
R2(config-bgp)#exit

R2(config)#ip route 1.1.1.4 255.255.255.255 12.1.1.1
R2(config)#ip route 1.1.1.2 255.255.255.255 13.1.1.1
```

R3上的配置：

```
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 1.1.1.4 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-1/1
R3(config-if-gei-1/1)#no shutdown
R3(config-if-gei-1/1)#ip address 12.1.1.1 255.255.255.252
R3(config-if-gei-1/1)#exit
R3(config)#interface gei-1/2
R3(config-if-gei-1/2)#no shutdown
R3(config-if-gei-1/2)#ip address 14.1.1.1 255.255.255.252
R3(config-if-gei-1/2)#exit

R3(config)#router bgp 3
R3(config-bgp)#redistribute connected/*重分发直连路由*/
R3(config-bgp)#redistribute ospf-int 1 metric 122/*重分发OSPF路由*/
R3(config-bgp)#neighbor 1.1.1.3 remote-as 1
R3(config-bgp)#neighbor 1.1.1.3 activate
R3(config-bgp)#neighbor 1.1.1.3 ebgp-multihop ttl 5
R3(config-bgp)#neighbor 1.1.1.3 send-med/*通告路由时发送MED属性*/
R3(config-bgp)#neighbor 1.1.1.3 update-source loopback1/*通过loopback地址建立
EBGP邻居*/
R3(config-bgp)#exit

R3(config)#ip route 1.1.1.3 255.255.255.255 12.1.1.2

R3(config)#router ospf 1
R3(config-ospf-1)#area 0
R3(config-ospf-1-area-0)#network 14.1.1.0 0.0.0.3
```

R4上的配置：

```
R4(config)#interface loopback1
R4(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
R4(config-if-loopback1)#exit
R4(config)#interface gei-1/1
R4(config-if-gei-1/1)#no shutdown
R4(config-if-gei-1/1)#ip address 11.1.1.1 255.255.255.252
R4(config-if)#exit
R4(config)#interface gei-1/2
R4(config-if-gei-1/2)#no shutdown
R4(config-if-gei-1/2)#ip address 10.1.1.1 255.255.255.0
R4(config-if-gei-1/2)#exit
```

```
R4(config)#router bgp 2
R4(config-bgp)#redistribute connected
R4(config-bgp)#redistribute static /*配置重分发*/
R4(config-bgp)#network 10.1.1.0 255.255.255.0
R4(config-bgp)#aggregate-address 192.168.0.0 255.255.252.0 count 0
as-set/*配置地址聚合*/
R4(config-bgp)#neighbor 1.1.1.2 remote-as 1
R4(config-bgp)#neighbor 1.1.1.2 activate
R4(config-bgp)#neighbor 1.1.1.2 ebgp-multihop ttl 5
R4(config-bgp)#neighbor 1.1.1.2 send-med
R4(config-bgp)#neighbor 1.1.1.2 update-source loopback1/*通过loopback地址建立
EBGP邻居*/
R4(config-bgp)#neighbor 1.1.1.2 route-map test-static out/*配置路由过滤*/
R4(config-bgp)#exit

R4(config)#ip route 1.1.1.2 255.255.255.255 11.1.1.2
R4(config)#ip route 192.168.100.0 255.255.255.0 10.1.1.2
R4(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.2
R4(config)#ip route 192.168.0.0 255.255.255.0 10.1.1.2
R4(config)#ip route 192.168.3.0 255.255.255.0 10.1.1.2
R4(config)#ip route 192.168.2.0 255.255.255.0 10.1.1.2/*配置静态路由*/

R4(config)#ipv4-access-list 1
R4(config-ipv4-acl)#rule 1 permit 192.168.0.0 0.0.3.255
R4(config-ipv4-acl)#rule 2 permit 10.1.1.0 0.0.0.255
R4(config-ipv4-acl)#exit

R4(config)#route-map test-static permit 10/*以下配置路由图过滤条件*/
R4(config-route-map)#match ip address 1
R4(config-route-map)#set ip metric 33
R4(config-route-map)#exit
```

R5上的配置：

```
R5(config)#interface loopback1
R5(config-if-loopback1)#ip address 1.1.1.5 255.255.255.255
R5(config-if-loopback1)#exit
R5(config)#interface gei-1/1
R5(config-if-gei-1/1)#no shutdown
R5(config-if-gei-1/1)#ip address 20.1.1.1 255.255.255.0
R5(config-if-gei-1/1)#exit
R5(config)#interface gei-1/2
R5(config-if-gei-1/2)#no shutdown
R5(config-if-gei-1/2)#ip address 14.1.1.2 255.255.255.252
R5(config-if-gei-1/2)#exit

R5(config)#router ospf 1 /*以下配置IGP*/
R5(config-ospf-1)#area 0
R5(config-ospf-1-area-0)#network 14.1.1.0 0.0.0.3
R5(config-ospf-1-area-0)#network 20.1.1.0 0.0.0.255
R5(config-ospf-1-area-0)#exit

R5(config)#ip route 0.0.0.0 0.0.0.0 14.1.1.1
```

配置验证

查看R1上的BGP路由表和路由转发表。

```
R1#show ip bgp route
Status codes: *-valid, >-best, i-internal,s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete
Network          NextHop    Metric   LocPrf   RtPrf    Path
*>1.1.1.2/32      1.1.1.2                     0     ?
*>10.1.1.0/24     1.1.1.1      33             20    2 i
*>11.1.1.0/30     11.1.1.2                    0     ?
*>i 12.1.1.0/30    1.1.1.3             100     200   ?
```

```
*>13.1.1.0/30      13.1.1.1                    0     ?
 *i 13.1.1.0/30    1.1.1.3            100      200   ?
*>i 14.1.1.0/30    1.1.1.3      0     100      200   3 ?
*>i 20.1.1.0/24    1.1.1.3      122   100      200   3 ?
*>192.168.0.0/22   1.1.1.1      33             20    2 i
*>192.168.0.0/24   1.1.1.1      33             20    2 ?
*>192.168.1.0/24   1.1.1.1      33             20    2 ?
*>192.168.2.0/24   1.1.1.1      33             20    2 ?
*>192.168.3.0/24   1.1.1.1      33             20    2 ?

R1#show ip forwarding route
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest           Gw         Interface       Owner     pri  metric
1.1.1.1        11.1.1.1   gei-1/1          Static    1   0
1.1.1.2        1.1.1.2    loopback1        Address   0   0
1.1.1.3        13.1.1.2   gei-1/2          Static    1   0
10.1.1.0       11.1.1.1   gei-1/1          BGP      20   33
11.1.1.0       11.1.1.2   gei-1/1          Direct    0    0
11.1.1.2       11.1.1.2   gei-1/1          Address   0    0
12.1.1.0       13.1.1.2   gei-1/2          BGP      200  0
13.1.1.0       13.1.1.1   gei-1/2          Direct    0    0
13.1.1.1       13.1.1.1   gei-1/2          Address   0   0
14.1.1.0       13.1.1.2   gei-1/2          BGP      200   0
20.1.1.0       13.1.1.2   gei-1/2          BGP      200  122
192.168.0.0    11.1.1.1   gei-1/1          BGP       20   33
192.168.0.0    11.1.1.1   gei-1/1          BGP       20   33
192.168.1.0    11.1.1.1   gei-1/1          BGP       20   33
192.168.2.0    11.1.1.1   gei-1/1          BGP       20   33
192.168.3.0    11.1.1.1   gei-1/1          BGP       20   33
```

查看R2上的BGP路由表和路由转发表：

```
R2#show ip bgp route
Status codes: * valid, > best, i-internal,s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete
 Network          NextHop     Metric    LocPrf    RtPrf    Path
*>1.1.1.3/32      1.1.1.3                          0      ?
*>i 10.1.1.0/24    1.1.1.2     33       100       200    2 i
*>i 11.1.1.0/30    1.1.1.2              100       200    ?
*> 12.1.1.0/30     12.1.1.2                         0      ?
 * 12.1.1.0/30     1.1.1.4       0                  20     3 ?
*> 13.1.1.0/30     13.1.1.2                         0      ?
 *i  13.1.1.0/30   1.1.1.2              100       200    ?
*>14.1.1.0/30      1.1.1.4       0                  20     3 ?
*>20.1.1.0/24      1.1.1.4      122                 20     3 ?
*>i 192.168.0.0/22  1.1.1.2    33       100       200    2 i
*>i 192.168.0.0/24  1.1.1.2    33       100       200    2 ?
*>i 192.168.1.0/24  1.1.1.2    33       100       200    2 ?
*>i 192.168.2.0/24  1.1.1.2    33       100       200    2 ?
*>i 192.168.3.0/24  1.1.1.2    33       100       200    2 ?

R2#show ip forwarding route
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest           Gw         Interface       Owner     pri  metric
1.1.1.2        13.1.1.1   gei-1/1          Static    1    0
1.1.1.3        1.1.1.3    loopback1        Address   0    0
```

```
1.1.1.4         12.1.1.1    gei-1/2        Static     1    0
10.1.1.0        13.1.1.1    gei-1/1        BGP        200  33
11.1.1.0        13.1.1.1    gei-1/1        BGP        200  0
12.1.1.0        12.1.1.2    gei-1/2        Direct     0    0
12.1.1.2        12.1.1.2    gei-1/2        Address    0    0
13.1.1.0        13.1.1.2    gei-1/1        Direct     0    0
13.1.1.2        13.1.1.2    gei-1/1        Address    0    0
14.1.1.0        12.1.1.1    gei-1/2        BGP        20   0
20.1.1.0        12.1.1.1    gei-1/2        BGP        20   122
192.168.0.0      13.1.1.1    gei-1/1        BGP        200  33
192.168.0.0      13.1.1.1    gei-1/1        BGP        200  33
192.168.1.0      13.1.1.1    gei-1/1        BGP        200  33
192.168.2.0      13.1.1.1    gei-1/1        BGP        200  33
192.168.3.0      13.1.1.1    gei-1/1        BGP        200  33
```

查看R3上的BGP路由表、OSPF路由表和路由转发表：

```
R3#show ip bgp route
Status codes: * valid, > best, i-internal,s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete
 Network          NextHop   Metric  LocPrf     RtPrf    Path
*>1.1.1.4/32      1.1.1.4                      0      ?
*>10.1.1.0/24     1.1.1.3                      20     1 2 i
*>11.1.1.0/30     1.1.1.3                      20     1 ?
*>12.1.1.0/30     12.1.1.1                     0      ?
 *12.1.1.0/30     1.1.1.3                      20     1 ?
*>13.1.1.0/30     1.1.1.3                      20     1 ?
*>14.1.1.0/30     14.1.1.1                      0      ?
*>20.1.1.0/24     14.1.1.2    122               110    ?
*>192.168.0.0/22   1.1.1.3                     20     1 2 ?
*>192.168.0.0/24   1.1.1.3                     20     1 2 ?
*>192.168.1.0/24   1.1.1.3                     20     1 2 ?
*>192.168.2.0/24   1.1.1.3                     20     1 2 ?
*>192.168.3.0/24   1.1.1.3                     20     1 2 ?

R3#show ip forwarding route
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-Static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest           Gw          Interface      Owner     pri  metric
1.1.1.3         12.1.1.2     gei-1/1        Static    1    0
1.1.1.4         1.1.1.4      loopback1      Address   0    0
10.1.1.0        12.1.1.2     gei-1/1        BGP       20   0
11.1.1.0        12.1.1.2     gei-1/1        BGP       20   0
12.1.1.0        12.1.1.1     gei-1/1        Direct    0    0
12.1.1.1        12.1.1.1     gei-1/1        Address   0    0
13.1.1.0        12.1.1.2     gei-1/1        BGP       20   0
14.1.1.0        14.1.1.1     gei-1/2        Direct    0    0
14.1.1.1        14.1.1.1     gei-1/2        Address   0    0
20.1.1.0        14.1.1.2     gei-1/2        ospf      110  2
192.168.0.0      12.1.1.2     gei-1/1        BGP       20   0
192.168.0.0      12.1.1.2     gei-1/1        BGP       20   0
192.168.1.0      12.1.1.2     gei-1/1        BGP       20   0
192.168.2.0      12.1.1.2     gei-1/1        BGP       20   0
192.168.3.0      12.1.1.2     gei-1/1        BGP       20   0

R3#show ip forwarding route ospf
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
```

```
Dest          Gw          Interface      Owner    pri   metric
20.1.1.0       14.1.1.2     gei-1/2        OSPF     110   2
```

查看R4上的BGP路由表和路由转发表：

```
R4#show ip bgp route
Status codes: *-valid, >-best, i-internal,s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete
 Network         NextHop    Metric    LocPrf    RtPrf   Path
*>1.1.1.1/32     1.1.1.1                        0      ?
*>1.1.1.2/32     11.1.1.2                       1      ?
*>10.1.1.0/24    10.1.1.1                       0      i
*>11.1.1.0/30    11.1.1.1                       0      ?
*11.1.1.0/30     1.1.1.2                       20     1 ?
*>12.1.1.0/30    1.1.1.2                      20     1 ?
*>13.1.1.0/30    1.1.1.2                      20     1 ?
*>14.1.1.0/30    1.1.1.2                      20     1 3 ?
*>20.1.1.0/24    1.1.1.2                      20     1 3 ?
*>192.168.0.0/22   0.0.0.0                     254    i
*>192.168.0.0/24   10.1.1.2                    1      ?
*>192.168.1.0/24   10.1.1.2                    1      ?
*>192.168.2.0/24   10.1.1.2                    1      ?
*>192.168.3.0/24    10.1.1.2                   1      ?
*>192.168.100.0/24  10.1.1.2                    1      ?

R4#show ip forwarding route
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest          Gw          Interface      Owner     pri  metric
1.1.1.1        1.1.1.1     loopback1      Address    0    0
1.1.1.2        11.1.1.2    gei-1/1        Static     1    0
10.1.1.0       10.1.1.1    gei-1/2        Direct     0    0
10.1.1.1       10.1.1.1    gei-1/2        Address    0    0
11.1.1.0       11.1.1.1    gei-1/1        Direct     0    0
11.1.1.1       11.1.1.1    gei-1/1        Address    0    0
12.1.1.0       11.1.1.2    gei-1/1        BGP       20   0
13.1.1.0       11.1.1.2    gei-1/1        BGP       20   0
14.1.1.0       11.1.1.2    gei-1/1        BGP       20   0
20.1.1.0       11.1.1.2    gei-1/1        BGP       20   0
192.168.0.0     10.1.1.2    gei-1/2        Static     1    0
192.168.1.0     10.1.1.2    gei-1/2        Static     1    0
192.168.2.0     10.1.1.2    gei-1/2        Static     1    0
192.168.3.0     10.1.1.2    gei-1/2        Static     1    0
192.168.100.0   10.1.1.2    gei-1/2        Static     1    0
```

在R4和R5上测试网络的连通性：

```
R4#ping 20.1.1.1
sending 5,100-byte ICMP echos to 20.1.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 0/4/20 ms.
R4#trace 20.1.1.1
 tracing the route to 20.1.1.1
1  11.1.1.2  20 ms  <20ms  <20ms
2  13.1.1.2  <20ms  <20ms  <20ms
3  12.1.1.1  <20ms  <20ms  <20ms
4  14.1.1.2  <20ms  <20ms  <20ms
 [finished]

R5#ping 10.1.1.2
sending 5,100-byte ICMP echos to 10.1.1.2,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 0/0/0 ms.
R5#trace 10.1.1.2
```

```
 tracing the route to 10.1.1.2
1  14.1.1.1  <20ms  <20ms  <20ms
2  12.1.1.2  <20ms  <20ms  <20ms
3  13.1.1.1  <20ms  <20ms  <20ms
4  11.1.1.1  <20ms  <20ms  <20ms
5    *  *  *
[finished]
```

在IP为10.1.1.2 255.255.255.0 的PC机上测试：

```
C:\Documents and Settings\Administrator>ping 20.1.1.1
Pinging 20.1.1.1 with 32 bytes of data:
Reply from 20.1.1.1: bytes=32 time=1ms TTL=251
Reply from 20.1.1.1: bytes=32 time=1ms TTL=251
Reply from 20.1.1.1: bytes=32 time=1ms TTL=251
Reply from 20.1.1.1: bytes=32 time=1ms TTL=251
Ping statistics for 20.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\Administrator>tracert 20.1.1.1
Tracing route to 20.1.1.1 over a maximum of 30 hops
  1    <1 ms     6 ms    <1 ms  10.1.1.1
  2     1 ms     1 ms     1 ms  11.1.1.2
  3     1 ms     1 ms     1 ms  13.1.1.2
  4     1 ms     1 ms     1 ms  12.1.1.1
  5     1 ms     1 ms     1 ms  20.1.1.1
Trace complete.
```

第5、6步的测试说明AS2与AS3之间的指定网段通信正常。

4.6.9 BGP 综合配置实例二（物理接口创建 BGP）

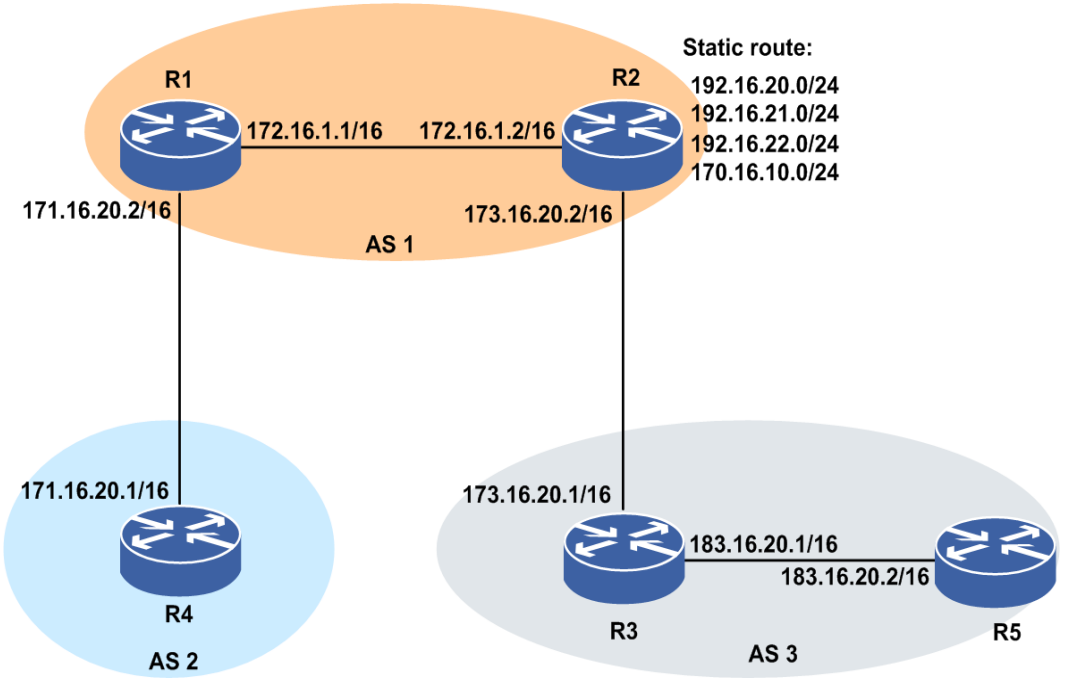
配置说明

下面是一个BGP综合实例，其中涉及到路由聚合、静态路由的再分配等BGP功能的实际应用。

如*图 4-61*所示，R4和R1建立EBGP，R1和R2建立IBGP，R2和R5建立多跳EBGP邻居。其中，假设R2中存在图中右上角标注的四条静态路由。

在R2的配置中，仅聚合通告192.16.0.0/16网段，并且通过路由图禁止通过BGP对外通告170.16.10.0/24网段。R2与R5之间通过R3建立EBGP多跳关系，此时在配置BGP之前需要保证该两台路由器建立邻居的地址能够互通。

图 4-61 BGP 综合配置实例二拓扑图



配置思路

1.R1上建立BGP邻居。

2.R2上建立BGP邻居，并配置多跳。

3.R4上建立BGP邻居，并配置路由聚合、路由过滤。

4.R5上建立BGP邻居，并配置多跳。

配置过程

本实例接口IP地址配置省略，可以参考“Loopback接口地址建立邻居BGP综合配置实例 （重分发、聚合、过滤）”

R1上的配置如下：

```
R1(config)#router bgp 1
R1(config-bgp)#no synchronization
R1(config-bgp)#neighbor 172.16.1.2  remote-as 1  /*建立IBGP邻居*/
R1(config-bgp)#neighbor 172.16.1.2  next-hop-self
R1(config-bgp)#neighbor 171.16.20.1  remote-as 2  /*建立EBGP邻居*/
```

R2上的配置如下：

```
R2(config)#ip route 183.16.0.0 255.255.0.0 173.16.20.1
R2(config)#router bgp 1
R2(config-bgp)#neighbor 172.16.1.1 remote-as 1  /*建立IBGP邻居*/
R2(config-bgp)#neighbor 172.16.1.1 next-hop-self
R2(config-bgp)#neighbor 183.16.20.2 remote-as 3   /*建立EBGP邻居*/
R2(config-bgp)#neighbor 183.16.20.2 ebgp-multihop ttl 2
/*配置多跳*/
R2(config-bgp)#exit
```

R4上的配置如下：

```
R4(config)#router bgp 2
R4(config-bgp)#redistribute static
R4(config-bgp)#neighbor 171.16.20.2 remote-as 1
R4(config-bgp)#aggregate-address 192.16.0.0 255.255.0.0 count 0
as-set summary-only  /*配置路由聚合*/
R4(config-bgp)#neighbor 171.16.20.2 route-map torouter1 out
/*配置路由过滤*/
R4(config-bgp)#exit
R4(config)#ipv4-access-list 1
R4(config-ipv4-acl)#rule 1 deny  170.16.10.0 0.0.0.255
R4(config-ipv4-acl)#rule 2 permit any
R4(config-ipv4-acl)#exit
R4(config)#route-map torouter1 permit 10   /*配置路由图过滤条件*/
R4(config-route-map)#match ip address 1
R4(config-route-map)#exit
```

R5上的配置如下：

```
R5(config)#ip route 173.16.0.0 255.255.0.0 183.16.20.1
R5(config)#router bgp 3
R5(config-bgp)#neighbor 173.16.20.2 remote-as 1  /*建立EBGP邻居*/
R5(config-bgp)#neighbor 173.16.20.2 ebgp-multihop ttl 2
/*配置多跳*/
```

配置验证

R4上**show ip bgp summary**查看邻居关系：

```
R4(config)#show ip bgp summary
Neighbor        Ver  As    MsgRcvd    MsgSend    Up/Down(s)   State/PfxRcd
171.16.20.2      4    1     46         140        00:22:35     0
```

R4上**show ip bgp route**查看bgp协议路由表：

```
R4(config)#show ip bgp route
Status codes: * valid, > best, i-internal, s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete
    Network          NextHop     Metric    LocPrf    RtPrf    Path
*> 192.16.0.0/16      0.0.0.0                          254      i
*> 192.16.20.0/24     171.16.20.2                        1      ?
*> 192.16.21.0/24     171.16.20.2                        1      ?
*> 192.16.22.0/24     171.16.20.2                        1      ?
*> 170.16.10.0/24     171.16.20.2                        1      ?
```

R1上用**show ip bgp summary**命令查看邻居关系：

```
R1(config)#show ip bgp summary
Neighbor      Ver  As   MsgRcvd   MsgSend   Up/Down(s)   State/PfxRcd
171.16.20.1    4    2    46        140       00:22:35     1
172.16.1.2     4    1    46        140       00:22:35     0
```

R1上查看BGP协议路由表：

```
R1(config)#show ip bgp route
Status codes: * valid, > best, i-internal, s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete
    Network          NextHop     Metric    LocPrf    RtPrf  Path
 *>  192.16.0.0/16    172.16.20.1                      20     i 2
```

R2上用**show ip bgp summary**命令查看邻居关系：

```
R2(config)#show ip bgp summary
Neighbor      Ver  As   MsgRcvd   MsgSend   Up/Down(s)   State/PfxRcd
183.16.20.2    4    3    46        140       00:22:35     0
172.16.1.1     4    1    46        140       00:22:35     1
```

R2上查看BGP协议路由表：

```
R2(config)#show ip bgp route
Status codes: * valid, > best, i-internal, s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete
    Network          NextHop     Metric    LocPrf    RtPrf  Path
*>i  192.16.0.0/16    172.16.1.1                     200    i 2
```

R5上用**show ip bgp summay**命令查看邻居关系：

```
R5(config)#show ip bgp summary
Neighbor      Ver  As   MsgRcvd   MsgSend   Up/Down(s)   State/PfxRcd
173.16.20.2   4    1    46        140       00:22:35     1
```

在R5上查看BGP协议路由表：

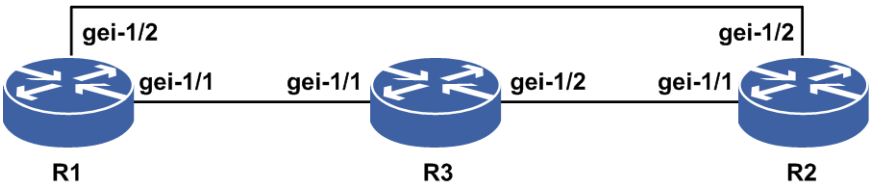
```
R5(config)#show ip bgp route
Status codes: * valid, > best, i-internal, s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete
   Network          NextHop       Metric    LocPrf    RtPrf  Path
*>  192.16.0.0/16     173.16.20.2                     20     i 1 2
```

4.6.10 BGP FRR 配置实例

配置说明

BGP FRR配置实例组网如*图 4-62*所示。

图 4-62 BGP FRR 典型组网示意图



配置思路

1.R1、R2和R3两两建立EBGP邻居。在R1上将从R2学来的路由设置本地优先属性为200。

2.在R1上启用BGP FRR功能。

配置过程

具体协议配置信息如下：

以*图 4-171*中的BGP协议为例，先两两通过实接口建立EBGP邻居，再在R1上启用FRR功能，举例通过设置本地优先属性为200，使R3通告过来的路由1.1.1.150/32通过R1→R2→R3的路径最优。

R1的配置：

```
R1(config)#router bgp 1
R1(config-bgp)#neighbor 172.16.1.2  remote-as 2
```

```
R1(config-bgp)#neighbor 171.16.20.2  remote-as 3
/*分别建立EBGP邻居*/
R1(config-bgp)#bgp frr  /*启用FRR功能*/
R1(config-bgp)#exit
R1(config)#route-map lt  /*配置路由图*/
R1(config-route-map)#set local-preference 200
R1(config-route-map)#exit
R1(config)#router bgp 1
R1(config-bgp)#neighbor 172.16.1.2  route-map lt in
R1(config-bgp)#exit
```

R2的配置：

```
R2(config)#router bgp 2
R2(config-bgp)#neighbor 172.16.1.1 remote-as 1
R2(config-bgp)#neighbor 183.16.20.2 remote-as 3
R2(config-bgp)#exit
```

R3的配置：

```
R3(config)#router bgp 3
R3(config-bgp)#neighbor 171.16.20.1 remote-as 1
R3(config-bgp)#neighbor 183.16.20.1 remote-as 2
R3(config-bgp)#exit
```

配置验证

用**show ip forwarding backup route**验证配置结果是否使FRR最终生效。

R1上BGP的FRR生效情况查看：

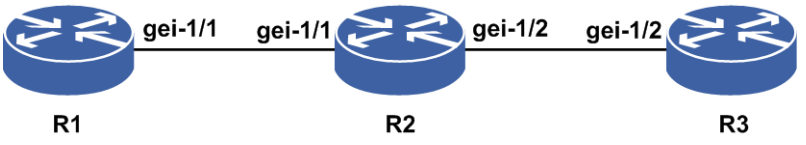
```
R1#show ip forwarding backup route
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority,  M/S: Master/Slave,
         Sta: Status;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best, M: Master, S: Slave, I: Inuse, U: Unuse;
   Dest        Gw           Interface     Owner   Pri Metric M/S Sta
1.1.1.150/32   172.16.1.2   gei-1/1       BGP     20   0      M   I
1.1.1.150/32   171.16.20.2  gei-1/2       BGP     20   0      S   U
```

4.6.11 BGP 路由反射器配置实例

配置说明

BGP路由反射器可在客户端之间进行路由通告，在客户端和非客户端之间进行路由通告，在客户端和EBGP之间进行路由通告。如*图 4-63*所示的例子是路由反射器在客户端之间进行路由通告。

图 4-63 BGP 路由反射器配置实例示意图



配置思路

1.R1、R2和R3之间建立IBGP邻居。

2.把R2配置成RR，R1和R3分别为R2的客户端。

3.在R1上重分发直连路由，通告给R2。

4.R2把这条路由反射给R3，R3能通过IGP学习到这条路由下一跳。

配置过程

R1的配置如下（接口地址配置省略）：

```
R1(config)#router bgp 100
R1(config-bgp)#neighbor 1.1.1.2 remote-as 100
R1(config-bgp)#redistribute connected  /*重分发直连路由，方便配置验证查看路由*/
R1(config-bgp)#exit
```

R2的配置如下（接口地址配置省略）：

```
R2(config)#router bgp 100
R2(config-bgp)#neighbor 1.1.1.1 remote-as 100
R2(config-bgp)#neighbor 2.1.1.2 remote-as 100
R2(config-bgp)#neighbor 1.1.1.1 route-reflector-client
R2(config-bgp)#neighbor 2.1.1.2 route-reflector-client
R2(config-bgp)#exit
```

R3的配置如下（接口地址配置和IGP配置配置省略）：

```
R3(config)#router bgp 100
R3(config-bgp)#neighbor 2.1.1.1 remote-as 100
R3(config-bgp)#exit
```

配置验证

```
R1(config-bgp)#show ip bgp route
Status codes: *-valid, >-best, i-internal, s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete

Network          NextHop       Metric    LocPrf    RtPrf  Path
*>   1.1.1.0/24      1.1.1.1       0                 0     ?
```

R3上收到R2反射的路由：

```
R3(config-bgp)#show ip bgp route
Status codes: *-valid, >-best, i-internal, s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete

    Network          NextHop       Metric    LocPrf    RtPrf  Path
*>i  1.1.1.0/24       1.1.1.1                 100       200    ?
```

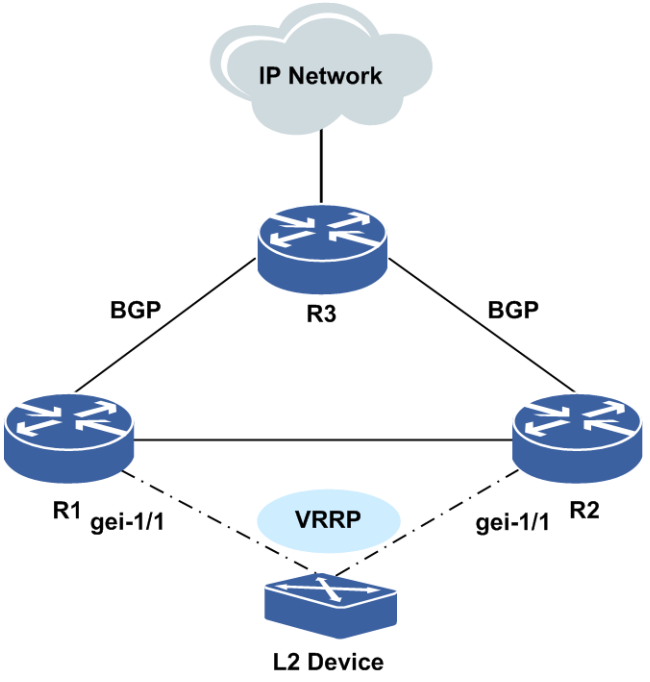
4.6.12 BGP 与 VRRP 联动配置实例

配置说明

如*图 4-64*所示，在下联接口上配置VRRP，虚地址作为接入设备的网关，上联通过BGP（IBGP、EBGP、MP-IBGP、MP-EBGP）相连。为了保证上下行流量一致，需要VRRP

的master报文所在的路由器的BGP路由优先级也为最优路由。

图 4-64 BGP 与 VRRP 联动配置实例组网图



配置思路

1.R1与R3，R2与R3建立BGP邻居。

2.R1，R2做VRRP检测主备。

3.BGP模式下配置track samgr对象。

配置步骤

R1和R3，R2和R3建立BGP邻居，参考“BGP综合配置实例”。

R1和R2配VRRP检测主备，参见可靠性的VRRP章节，本实例略。

R1上配置：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ip address 13.13.13.1 255.255.255.0
/* Vrrp模式下配置vrrp检查接口，vrrp虚地址是13.13.13.66*/
R1(config-if-gei-1/1)#exit
R1(config)#vrrp
R1(config-vrrp)#interface gei-1/1
R1(config-vrrp-if-gei-1/1)#vrrp 66 ipv4 13.13.13.66
R1(config-vrrp-if-gei-1/1)#exit
R1(config-vrrp)#exit
/* samgr模式下配置track vrrp对象*/
R1(config)#samgr
R1(config-samgr)#track Inspur vrrp interface gei-1/1 vrid 66
/* bgp地址族模式下配置track samgr对象*/
R1(config-samgr)#exit
```

```
R1(config)#router bgp 66.66
R1(config-bgp)#track Inspur adjust-priority 67
```

R2上配置：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 13.13.13.3 255.255.255.0
 /* Vrrp模式下配置vrrp检查接口，vrrp虚地址是13.13.13.66*/
R2(config-if-gei-1/1)#exit
R2(config)#vrrp
R2(config-vrrp)#interface gei-1/1
R2(config-vrrp-if-gei-1/1)#vrrp 66 ipv4 13.13.13.66
R2(config-vrrp-if-gei-1/1)#exit
R2(config-vrrp)#exit
 /* samgr模式下配置track vrrp对象*/
R2(config)#samgr
R2(config-samgr)#track Inspur vrrp interface gei-1/1 vrid 66
 /* bgp地址族模式下配置track samgr对象*/
R2(config-samgr)#exit
R2(config)#router bgp 66.66
R2(config-bgp)#track Inspur adjust-priority 67
```

配置验证

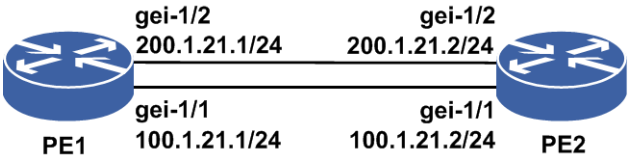
R1为主的情况下，转发流量从R1→R3转发，R1链路中断的情况下，流量自动切换到R2→R3转发。

4.6.13 BGP 路由负荷分担配置实例

配置说明

负荷分担可使超出单个接口带宽的流量均分到多条链路上，实现流量在各条链路上的负载均衡。如*图 4-65*所示，采用BGP路由的负荷分担实现负载均衡。

图 4-65 BGP 路由负荷分担配置实例



配置思路

1.配置接口地址， PE2路由器上配置一个loopback地址，为1.1.1.2/32。

2.PE1 和 PE2 上启用 BGP 协议（如 EBGP），通告各接口地址，并配置 **maxinum-paths**，使负荷分担生效。

3.可以更改负荷分担方式即逐包或者逐流。

配置过程

PE1上的配置如下：

```
PE1(config)#interface gei-1/1
PE1(config-if-gei-1/1)#no shutdown
PE1(config-if-gei-1/1)#ip address 100.1.21.1 255.255.255.0
PE1(config-if-gei-1/1)#exit
PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#no shutdown
PE1(config-if-gei-1/2)#ip address 200.1.21.1 255.255.255.0
PE1(config-if-gei-1/2)#exit

PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 100.1.21.2 remote-as 200
PE1(config-bgp)#neighbor 200.1.21.2 remote-as 200
PE1(config-bgp)#maximum-paths 2     /*负荷分担支持路由数目为2*/
PE1(config-bgp)#exit

PE1(config)#interface gei-1/1
PE1(config-if-gei-1/1)#ip load-sharing per-packet   /*选择逐包方式*/
PE1(config-if-gei-1/1)#exit
PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#ip load-sharing per-packet   /*选择逐包方式*/
PE1(config-if-gei-1/2)#exit
```

PE2上的配置如下：

```
PE2(config)#interface gei-1/1
PE2(config-if-gei-1/1)#no shutdown
PE2(config-if-gei-1/1)#ip address 100.1.21.2 255.255.255.0
PE2(config-if-gei-1/1)#exit
PE2(config)#interface gei-1/2
PE2(config-if-gei-1/2)#no shutdown
PE2(config-if-gei-1/2)#ip address 200.1.21.2 255.255.255.0
PE2(config-if-gei-1/2)#exit
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
PE2(config-if-loopback1)#exit

PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 100.1.21.1 remote-as 100
PE2(config-bgp)#neighbor 200.1.21.1 remote-as 100
PE2(config-bgp)#network 1.1.1.2 255.255.255.255
PE2(config-bgp)#exit
```

配置验证

在PE1上用**show ip forwarding route**命令验证配置结果：

```
PE1#show ip forwarding route
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;

Dest        Gw           Interface     Owner    pri  metric
1.1.1.2      200.1.21.2     gei-1/2       BGP      20   0
1.1.1.2      100.1.21.2     gei-1/1       BGP      20   0
```

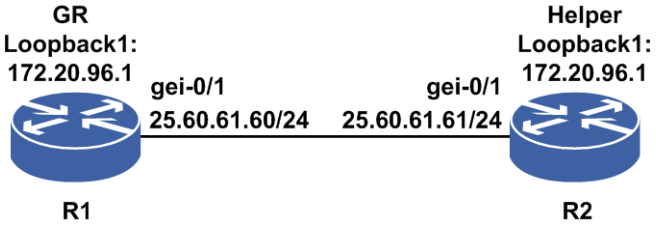
可以看到，到达同一目的地有两条路由，分别走不同的出接口，负荷分担配置成功。

4.6.14 BGP Graceful Restart 配置实例

配置说明

如*图 4-66*所示，路由器R1、R2是BGP邻居，现在R1和R2上开启Graceful Restart功能，一台路由器做GR，一台路由做helper。路由不多的情况下，默认配置即可，使得在R1或R2主备倒换时仍然能够正常转发数据报文。

图 4-66 BGP Graceful Restart 配置实例



配置思路

1.配置路由器R1、R2形成BGP邻居

2.在R1、R2上开启Graceful Restart功能

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 172.20.96.1 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-0/1
R1(config-if-gei-0/1)#no shutdown
R1(config-if-gei-0/1)#ip address 25.60.61.60  255.255.255.252
R1(config-if-gei-0/1)#exit
R1(config)#router bgp 18004
R1(config-bgp)#neighbor 172.20.96.2 remote-as 18004
R1(config-bgp)#neighbor 172.20.96.2 update-source loopback1
R1(config-bgp)#bgp graceful-restart
```

R2上的配置如下：

```
R2 (config)#interface loopback1
R2(config-if-loopback1)#ip address 172.20.96.2 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-0/1
R2(config-if-gei-0/1)#no shutdown
R2(config-if-gei-0/1)#ip address 25.60.61.61  255.255.255.252
R2(config-if-gei-0/1)#exit
R2(config)#router bgp 18004
R2(config-bgp)#neighbor 172.20.96.1 remote-as 18004
R2(config-bgp)#neighbor 172.20.96.1 update-source loopback1
R2(config-bgp)#bgp graceful-restart
/*loopback地址之间的路由学习，可以配置IGP，配置略*/
```

配置验证

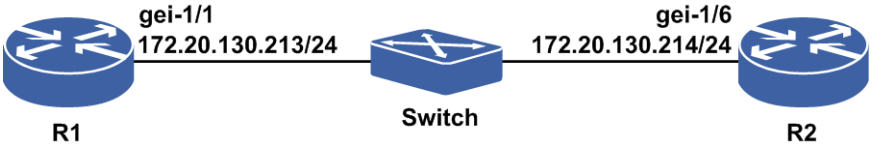
主备倒换R1后，流量仍然能够正常转发。

4.6.15 BGP 单跳 BFD 配置实例

配置说明

如*图 4-67*所示，R1、R2之间运行BGP 协议，R1、R2协议接口下使能BFD。

图 4-67 BGP 单跳 BFD 配置实例



配置思路

1.R1、R2之间运行BGP 协议。

2.R1、R2协议进程下使能BFD。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 172.20.130.213 255.255.255.0
R1(config-if-gei-1/1)#exit

R1(config)#router bgp 18004
R1(config-bgp)#neighbor 172.20.130.214 remote-as 18004
R1(config-bgp)#neighbor 172.20.130.214 fall-over bfd
R1(config-bgp)#exit
```

R2的配置如下：

```
R2(config)#interface gei-1/6
R2(config-if-gei-1/6)#ip address 172.20.130.214 255.255.255.0
R2(config-if-gei-1/6)#exit

R2(config)#router bgp 18004
R2(config-bgp)#neighbor 172.20.130.213 remote-as 18004
R2(config-bgp)#neighbor 172.20.130.213 fall-over bfd
R2(config-bgp)#exit
```

配置验证

正确配置后，BGP BFD会话应该能够成功建立，可以用如下命令查看结果：

用**show bfd neighbors [ip brief|ip detail]**来查看验证BGP BFD是否生效。

R1上BGP BFD生效情况查看：

```
R1(config-bgp)#show bfd neighbors ip brief
LocalAddr       PeerAddr       LD     RD     Hold   State    Interface
172.20.130.213  172.20.130.214   4      25     150    UP       gei-1/1

R1(config-bgp)#show bfd neighbors ip detail
------------------------------------------------------------------------------
-
LocalAddr:172.20.130.213
PeerAddr :172.20.130.214
Local Discr:1              Remote Discr:3          State:UP

Holdown(ms):150           Interface: gei-1/1
Vpnid:0                   VRF Name:---
BFD Type:SingleHop
Instance Name:
------------------------------------------------------------------------------
--
Version:1               Dest UDP Port:3784       Final Bit:1
Local Diag:0             Demand Mode:0           Poll Bit:1
MinTxInt:50              MinRxInt:50             Multiplier:3
Received MinTxInt:50      Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24         Max BFD Length:24

Rx Count:0              Rx Interval (ms) min/max/avg:0     /0     /0
Tx Count:0              Tx Interval (ms) min/max/avg:0     /0     /0
Registered Protocols:BGP
Uptime:0 day(s),0 hour(s),0 minute(s)
Control Plane Rcv Phy Interface Name: gei-1/1
==============================================================================
```

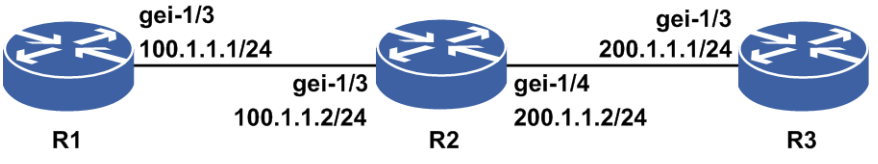
4.6.16 BGP 多跳 BFD 配置实例

配置说明

BFD旨在当远端链路发生失效后，本端能快速检测到远端的失效情况。

多跳BFD典型组网如*图 4-68*所示：

图 4-68 多跳 BFD 典型组网示意图



配置思路

1.配置各个路由协议。

2.协议接口下或在指定的目的路由上启用BFD。

配置过程

具体配置信息如下：

多跳BFD的配置

R1的配置：

```
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#ip address 100.1.1.1 255.255.255.0
R1(config-if-gei-1/3)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.211 255.255.255.255
R1(config-if-loopback1)#exit

R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 100.1.1.0 0.0.0.255
R1(config-ospf-1-area-0)#network 1.1.1.211 0.0.0.0
R1(config-ospf-1-area-0)#exit

R1(config)#router bgp 100
R1(config-bgp)#neighbor 1.1.1.213 remote 200
R1(config-bgp)#neighbor 1.1.1.213 update-source loopback1
R1(config-bgp)#neighbor 1.1.1.213 ebgp-multihop
R1(config-bgp)#neighbor 1.1.1.213 fall-over bfd
R1(config-bgp)#exit
```

R2的配置：

```
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#ip address 100.1.1.2 255.255.255.0
R2(config-if-gei-1/3)#exit
R2(config)#interface gei-1/4
R2(config-if-gei-1/4)#ip address 200.1.1.2 255.255.255.0
R2(config-if-gei-1/4)#exit

R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 100.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#network 200.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#exit
```

R3的配置：

```
R3(config)#interface gei-1/3
R3(config-if-gei-1/3)#ip address 200.1.1.1 255.255.255.0
R3(config-if-gei-1/3)#exit
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 1.1.1.213 255.255.255.255
R3(config-if-loopback1)#exit

R3(config)#router ospf 1
R3(config-ospf-1)#area 0
R3(config-ospf-1-area-0)#network 200.1.1.0 0.0.0.255
R3(config-ospf-1-area-0)#network 1.1.1.213 0.0.0.0
R3(config-ospf-1-area-0)#exit

R3(config)#router bgp 200
R3(config-bgp)#neighbor 1.1.1.211 remote 100
R3(config-bgp)#neighbor 1.1.1.211 update-source loopback1
R3(config-bgp)#neighbor 1.1.1.211 ebgp-multihop
R3(config-bgp)#exit
R3(config)#bfd
R3(config-bfd)#session 1 peer-bfd ipv4 1.1.1.213 1.1.1.211
```

```
R3(config-bfd)#exit
```

配置验证

正确配置后，BFD会话应该能够成功建立，可以用如下命令查看结果：

用**show bfd neighbors** [**ip brief** | **ip detail**]来查看验证配置结果是否使BFD最终生效。

R1上多跳BFD生效情况查看：

```
R1#show bfd neighbors ip brief
LocalAddr     PeerAddr        LD      RD      Hold   State     Interface
1.1.1.211     1.1.1.213       56      57      150    UP        gei-1/3

R1#show bfd neighbors ip detail
------------------------------------------------------------------------------
--

LocalAddr:1.1.1.211
PeerAddr :1.1.1.213
Local Discr: 56          Remote Discr:57          State:UP

Holdown(ms):150           Interface:---
Vpnid:0                  VRF Name:---
BFD Type:MultiHop
Instance Name:1
------------------------------------------------------------------------------
--
Version:1               Dest UDP Port:4784       Final Bit:1
Local Diag:0            Demand Mode:0            Poll Bit:1
MinTxInt:50             MinRxInt:50             Multiplier:3
Received MinTxInt:50      Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24        Max BFD Length:24

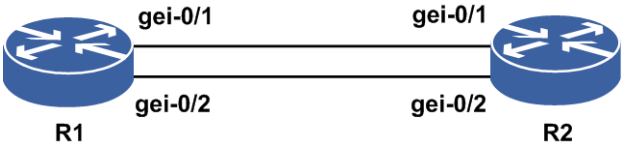
Rx Count:50             Rx Interval (ms) min/max/avg:50     /60     /50
Tx Count:40             Tx Interval (ms) min/max/avg:48    /48    /46
Registered Protocols:BGP INSTANCE
Uptime:0 day(s),0 hour(s),0 minute(s)
Control Plane Rcv Phy Interface Name:gei-1/3
==============================================================================
```

4.6.17 BGP 动态组配置实例

配置说明

如*图 4-69*所示，R1和R2通过gei-0/1互联并建立BGP邻居。设备默认开启BGP动态组功能。

图 4-69 BGP 动态组配置实例示意图



配置思路

1.R1和R2的gei-0/1先建立BGP邻居。

2.新邻居通过R1和R2的gei-0/2的接口加入。

3.如想让该邻居独自占用一个动态组，可以配置**split-update-group**命令。

配置过程

1.R1和R2的gei-0/1建立BGP邻居。

R1的配置如下：

```
R1(config)#router bgp 65530
R1(config-bgp)#neighbor 10.1.1.3 remote-as 1
R1(config-bgp)#exit
```

R2上配置如下：

```
R2(config)#router bgp 1
R2(config-bgp)#neighbor 10.1.1.1  remote-as 65530
R2(config-bgp)#exit
```

2.R1和R2通过gei-0/1、gei-0/2接口建立BGP邻居。

R1上的配置如下：

```
R1(config)#router bgp 65530
R1(config-bgp)#neighbor 10.1.1.3 remote-as 1
R1(config-bgp)#neighbor 20.1.1.3 remote-as 1
R1(config-bgp)#exit
```

R2上的配置如下：

```
R2(config)#router bgp 1
R2(config-bgp)#neighbor 10.1.1.1 remote-as 65530
R2(config-bgp)#neighbor 20.1.1.1 remote-as 65530
R2(config-bgp)#exit
```

3.要使R1和R2通过gei-0/2接口建立的BGP邻居处于独立的BGP动态组，则进行如下配置。

R1上的配置如下：

```
R1(config)#router bgp 65530
R1(config-bgp)#neighbor 10.1.1.3 remote-as 1
R1(config-bgp)#neighbor 20.1.1.3 remote-as 1
R1(config-bgp)#neighbor 10.1.1.3 activate
R1(config-bgp)#neighbor 20.1.1.3 activate
R1(config-bgp)#neighbor 20.1.1.3 split-update-group
R1(config-bgp)#exit
```

R2上的配置如下：

```
R2(config)#router bgp 1
R2(config-bgp)#neighbor 10.1.1.1 remote-as 65530
R2(config-bgp)#neighbor 20.1.1.1 remote-as 65530
R2(config-bgp)#neighbor 10.1.1.1 activate
R2(config-bgp)#neighbor 20.1.1.1 activate
R2(config-bgp)#exit
```

配置验证

1.步骤1配置完成配置验证。

在R1上执行命令**show ip bgp summary**看到BGP邻居正常建立：

```
R1#show ip bgp summary
Neighbor     Ver  As      MsgRcvd    MsgSend    Up/Down     State/PfxRcd
10.1.1.3     4    1       3          0          00:08:22          1
```

在R1上执行命令**show ip bgp update-group**看到组已创建，并且邻居已经加入了该BGP动态组：

```
R1#show ip bgp update-group
Index: 1
Number of static caches: 10 use 0
Has 1 members:
Normal peer:
10.1.1.3
```

2.步骤2配置完成后配置验证。

在R1上执行命令**show ip bgp summary**显示BGP邻居正常建立：

```
R1#show ip bgp summary
Neighbor     Ver  As      MsgRcvd    MsgSend    Up/Down     State/PfxRcd
10.1.1.3     4    1       3          1          00:04:55          1
20.1.1.3     4    1       3          1          00:01:59          1
```

在R1上执行命令**show ip bgp update-group**显示邻居20.1.1.3已经加入了该BGP动态组中：

```
R1(config-bgp)#show ip bgp update-group
Index: 1
Number of static caches: 10 use 0
Has 2 members:
Normal peer:
10.1.1.3        20.1.1.3
```

3.步骤3配置完成后配置验证。

改变邻居的输出策略后，在R1上查看BGP邻居的状态是正常的：

```
R1(config-bgp)#show ip bgp summary
Neighbor     Ver  As      MsgRcvd    MsgSend    Up/Down     State/PfxRcd
10.1.1.3     4    1       3          2          00:28:45          1
20.1.1.3     4    1       3          3          00:25:49          1
```

在R1上执行命令**show ip bgp update-group**可以看到10.1.1.3 和20.1.1.3 分别属于不同的BGP动态组中：

```
R1(config-bgp)#show ip bgp update-group
Index: 1
Number of static caches: 10 use 0
Has 1 members:
Normal peer: 20.1.1.3

Index: 2
Number of static caches: 10 use 0
Has 1 members:
Normal peer:
10.1.1.3
```

在R1上执行命令**no neighbor 20.1.1.3 split-update-group**后，用命令**show ip bgp update-group**可以看到10.1.1.3 和20.1.1.3又恢复到同一个BGP动态组中：

```
R1(config-bgp)#show ip bgp update-group
```

```
Index: 1
Number of static caches: 10 use 0
Has 2 members:
Normal peer: 10.1.1.3         20.1.1.3
```

5 IPv4 组播

5.1 组播

组播是一种点到多点或多点到多点的通信方式，即多个接收者同时接收一个源发送的相同信息。基于组播的应用有视频会议、远程教学、软件分发等。

组播协议包括组成员管理协议和组播路由协议，组成员管理协议用于管理组播组成员的加入和离开，组播路由协议负责在路由器之间交互信息来建立组播树。

组播路由协议负责在路由器之间交互信息来建立组播树。不同的组播路由协议，使用的方法也不同，为适应网络中组播用户分布情况的需要，组播路由协议被分为两类：密集模式和稀疏模式。

- 密集模式组播路由协议通过阶段性的将组播数据包洪泛至整个网络来建立和维护组播树。运行组播路由协议的路由器，将收到的组播数据包在所有其他的接口上扩散。

  密集模式组播路由协议包括DVMRP、MOSPF、PIM-DM。

- 稀疏模式组播路由协议适用于网络中组播接收者分布比较稀疏的情况，此时如果使用与密集模式相同的洪泛法来构建组播路由树，对带宽是极大的浪费。

  稀疏模式组播路由协议包括CBT、PIM-SM。

静态组播是一种特殊的组播路由协议，提供用户直接配置组播路由表的出接口和入接口，并根据用户的这种配置形成组播转发表。如果同时存在静态组播路由和动态组播路由，静态组播路由优先。静态组播的逻辑地位同PIM-SM和PIM-DM。

5.1.1 配置组播

本节介绍组播功能的配置步骤和命令。

1.启用基本的公共组播功能。

步骤	命令	功能
1	`inspur(config)#`**ip multicast-routing**	启用IP组播路由功能
2	`inspur(config-mcast)#`**router pim**	启用PIM-SM协议
3	`inspur(config-mcast)#`**vrf** *<vrf-name>*	进入组播VRF模式
4	`inspur(config-mcast-vrf-name)#`**mtunnel** *<interface-name>*	将某接口配置成mtunnel接口
5	`inspur(config-mcast-vrf-name)#`**mdt**	配置组播某实例的mdt default

步骤	命令	功能
	default <*group-address*>	group
6	inspur(config-mcast-vrf-name)#**mdt data** <*group-address*><*group-mask*>[<*acl-name*>]	配置组播某实例的mdt data group
7	inspur(config-mcast)#**forwarding-policy** {**per-packet**|**per-user**|**per-stream**}[**group-list** <*acl-name*>]	配置组播转发策略区分为逐包、逐用户和逐流，默认为逐流

2.配置组播监控的接口和路由。

步骤	命令	功能
1	inspur(config)#**ip multicast-routing**	启用IP组播路由功能
2	inspur(config-mcast)#**monitor-interface** <*interface-name*>	配置监控的接口，每次只配置一个监控接口，允许最多配置20个监控接口
3	inspur(config-mcast)#**monitor-mroute** <*source-address*><*group-address*>[**interface** <*interface-name*>]	配置组播监控路由，检查该命令中的接口参数和配置的监控接口是否一致，如果接口一致，就中断该接口经过的流量。

3.配置组播全局过滤的接口或指定组播路由过滤的接口。

步骤	命令	功能
1	inspur(config-mcast)#**filter-policy monitor-interface** <*interface-name*>< *interface-mode* >< *interface-type* >	配置全局过滤的接口，每次只配置一个过滤接口，配置该接口的全局过滤模式(include/exclude)和接口的过滤类型(add/delete)，允许最多配置20个过滤接口。所有过滤接口的全局过滤模式必须统一
2	inspur(config-mcast)#**filter-policy monitor-mroute-interface** <*source-address*><*group-address*><*interface-name*>< *interface-type* >	配置指定路由过滤的接口，根据过滤接口类型决定该路由下该出接口的过滤类型(add/delete)，每次只配置一条路由和一个过滤的接口，某条路由允许最多配置22个过滤接口
3	inspur(config-mcast)#**filter-policy monitor-mroute-mode** <*source-address*><*group-address*>< *route-mode* >	配置指定路由过滤的模式(include/exclude)，根据过滤模式决定指定路由每个出接口的过滤类型，一条路由只能配置一个过滤模式，最多配置1000个路由的过滤模式

4.配置组播Damping。

步骤	命令	功能
1	inspur(config-mcast)#**damping-enable**	使能组播Damping
2	inspur(config-mcast)#**damping-threshold** < *threshold*>	对路由下发次数的阈值限制，超过阈值路由下发将启动Damping功能，抑制下发，最少等10s最多等60秒下发

5.配置组播Nexthop。

步骤	命令	功能
1	inspur(config-mcast)#**nexthop** < *dest-address*>< *net-mask*>< *interface-name*>< *nexthop-address*>	配置静态组播，指定目的地址、下一跳接口和下一跳地址
2	inspur(config-mcast-nexthop)#**select-mroute** <*source-address*><*group-address*>	进入Nexthop模式，负荷分担时，指定某条特定路由不参与负荷分担，固定选该Nexthop

6.配置组播转发范围。

命令	功能
inspur(config-mcast)#**multicast-boundary** <*access-list-name*><*interface-name*>	在接口上配置组播转发边界
inspur(config-mcast)#**multicast-ttl** <*ttl-value*><*interface-name*>	在接口上配置组播转发TTL阈值，限定组播报文被转发的距离 接口只转发TTL不小于阈值的报文，若报文TTL值小于阈值，则丢弃该报文
inspur(config-mcast)#**reject-inbound-data** <*interface-name*>	配置禁止转发面接收组播数据报文，组播路由器不能在指定接口上接收组播数据报文

7.配置组播转发表项限制参数。

命令	功能
inspur(config-mcast)#**mroute-limit** <*limit*>	配置对组播转发表中的表项数量进行限制，缺省情况下，采用系统允许的最大值
inspur(config-mcast)#**mroute-downstrem-limit** <*limit*>	限制组播转发表中单条表项的下行节点数目

8.配置PIM组播安全。

步骤	命令	功能

步骤	命令	功能
1	inspur(config-mcast)#**router pim**	启用PIM协议
2	inspur(config-mcast)#**interface** <*interface-name*>	进入接口配置模式
3	inspur(config-mcast-pim-if-interface-name)#**pim-silent**	启用**pim-silent**功能，该接口不接收和处理PIM协议报文

9.配置MSDP MD5认证功能和MSDP GTSM功能。

步骤	命令	功能
1	inspur(config-mcast)#**router msdp**	启用MSDP协议
2	inspur(config-mcast-msdp)#**peer** <*peer-address*>	配置MSDP邻居，参数为邻居地址
3	inspur(config-mcast-msdp-peer)#**password** {**encryped** <*encryped-password*>|**clear** <*password*>|<*password*>}	配置MD5认证密码
4	inspur(config-mcast-msdp-peer)#**ttl-security-hops** <*number*>	配置限制本地接收邻居的TTL，范围1~254

10.验证配置结果。

命令	功能
inspur#**show ip mroute** [**vrf** <*vrf-name*>][{[**group** <*group-address*>][**source** <*source-address*>]][**source** <*source-address*>]}][**iif** <*in-interface-name*>][**oif** <*out-interface-name*>]	显示IP组播路由表的内容
inspur#**show ip mdt**	显示组播MDT信息
inspur#**show ip mroute summary** [**vrf** <*vrf-name*>]	显示IP组播路由表的具体数目
inspur#**show ip mroute brief** [**vrf** <*vrf-name*>]	显示IP组播路由表的简明信息

11.维护组播。

命令	功能
inspur#**clear ip mroute** [**vrf** <*vrf-name*>][**group-address** <*group-address*>][**source-address** <*source-address*>]]	清除组播路由

5.1.2 配置静态组播

本节介绍配置静态组播功能，用于期望组播按照指定的路径进行转发的情况。

1.配置静态组播。

步骤	命令	功能
1	inspur(config-mcast)#**ip multicast-static-start**	启用静态组播
2	inspur(config-mcast)#**ip multicast-static-limit xg** *<xg-limit>* **sg** *<sg-limit>*	配置静态组播路由条目数最大值
3	inspur(config-mcast)#**ip multicast-static-route** *<source-address><group-address>*[{[**iif** *<iif-name>*],[**oif** *<oif-index>*]}]	配置静态组播路由条目
4	inspur(config-mcast)#**ip multicast-static-interface index** *<index>* **interface** *<interface-name>*	配置静态组播出接口集合

<xg-limit>：允许配置的静态组播(*,G)路由条目数，默认为0。

<sg-limit>：允许配置的静态组播(S,G)路由条目数，默认为0。

<group-address>：指定的组播组地址。

<source-address>：指定的组播源地址。

<iif-name>：组播路由条目入接口名称。

<oif-index>：组播路由条目出接口集合序号。

<index>：配置出接口集合的序号。

< interface-name>：加入出接口集合的接口名。

2.验证配置结果。

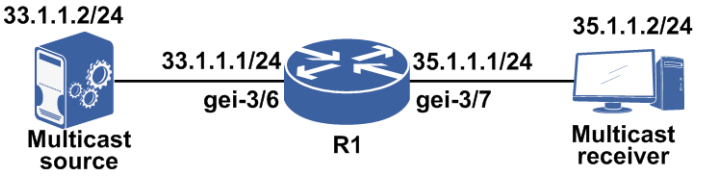
命令	功能
inspur#**show ip multicast-static-interface**[**index***<index>*]	显示出接口集合中所有的接口
inspur#**show ip multicast-static-route** [**group** *<group-address>*|[**source** *<source-address>*]]|[**source** *<source-address>*]	显示静态组播路由表内容
inspur#**show ip multicast-static-route summary**	显示静态组播路由表的内容统计信息

5.1.3 静态组播配置实例

配置说明

如*图 5-1*所示，配置一条源为33.1.1.2，目的为225.10.0.1的静态组播路由，使组播流可以正常转发。

图 5-1 静态组播配置实例组网图



配置思路

1.配置接口IP地址。

2.进入组播模式。

3.启动静态组播。

4.配置静态组播（*,G）、(S,G)最大条目数。

5.配置静态组播出接口列表。

6.配置具体静态组播路由。

配置过程

R1的配置如下：

```
R1(config)#ip multicast-routing
R1(config-mcast)#ip multicast-static-start
R1(config-mcast)#ip multicast-static-limit xg 1024 sg 1024
R1(config-mcast)#ip multicast-static-interface index 2 interface gei-3/7
R1(config-mcast)#ip multicast-static-route 33.1.1.2 225.10.1.2 iif gei-3/6 oif
2
R1(config-mcast)#end
```

配置验证

在R1上通过**show ip multicast-static-interface**命令查看端口静态组播信息：

```
R1(config)#show ip multicast-static-interface
STATIC-MULTICAST OUT PORT INDEX 2:
Outgoing Interface:
              gei-3/7

R1(config)#show ip multicast-static-route
The Capability of Static Multicast Route
(*, g) 1024, (s, g) 1024
(33.1.1.2, 225.10.1.2)
```

```
Incoming interface: gei-3/6  A
Outgoing interface list:
          gei-3/7  F

R1(config)#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(33.1.1.2, 225.10.1.2), TYPE: STATIC, FLAGS:
   Incoming interface: gei-3/6, flags:
   Outgoing interface list:
     gei-3/7, flags:F/S
```

5.2 IGMP

若一个主机想要接收一个特定组的组播数据包，需要监听发往该组的所有数据包。为解决Internet上组播数据包的路径选择，主机需要通知其网络上的组播路由器主机所加入或离开的组。

组播中采用Internet组管理协议（IGMP）来完成组播数据包的路径选择任务。通过IGMP，组播路由器就可以知道网络上是否存在组播组的成员，并由此决定是否向该网络转发组播数据包。当一个组播路由器收到一个组播数据包时，检查数据包的组播目的地址，向所有存在该组的成员的接口或下游路由器转发数据包。

目前IGMP有以下三个版本：

•IGMPv1中定义了基本的组成员查询和报告过程。

•IGMPv2在IGMPv1的基础上添加了组成员的离开机制等。

•IGMPv3中增加了成员对组播源的选择能力，以实现对SSM模型的支持。

5.2.1 配置 IGMP

本节介绍IGMP功能的配置步骤和命令。

相关信息

以下配置是在非VRF模式下的接口配置，VRF模式下命令操作完全相同，开启VRF模式命令具体见“配置组播”。

1.配置IGMP基本功能。

步骤	命令	功能
1	inspur(config-mcast)#**router igmp**	进入IGMP配置模式
2	inspur(config-mcast-igmp)#**interface** <*interface-name*>	进入IGMP接口配置模式
3	inspur(config-mcast-igmp-interface-name)#**immediate-leave** {**group-list** <*access-list-name*>| **all**}	配置允许成员立即离开的组范围

<*access-list-name*>：ACL名，范围1~31字符。

all：所有组播组有效。

IR12000智能路由器的IGMP功能是基于PIM接口的，所有启动PIM的接口都自动启用IGMP功能。

2.配置IGMP查询者规避功能。

命令	功能
inspur(config-mcast-igmp-interface-name)# **querier-election disable**	在IGMP接口模式下配置不进行查询者选举，即设备认为自己就是查询者
inspur(config-mcast-igmp-interface-name)# **querier-election connect**	在IGMP接口模式下配置查询者选举限制在同一网段内，非同一网段不选举

3.配置Require-alert-options选项。

命令	功能
inspur(config-mcast-igmp)#**require-alert-options**	在IGMP配置模式下配置设备上只接收IP头中包含**Router_Alert_Options**选项的报文，否则丢弃

4.配置限制IGMP join的报文速率。

步骤	命令	功能
1	inspur(config-mcast-igmp)#**shaping packets-number** <*number*>	在IGMP配置模式下，限制所有接口收到报文的总和，范围：1~4294967295
2	inspur(config-mcast-igmp-if-interface-name)#**shaping-packets-number** <*number*>	在IGMP接口配置模式下，限制一个接口收到报文的数量，范围：1~4294967295
	inspur(config-mcast-igmp-if-interface-name)#**maximum-joins** <*number*>	限制一个查询周期中IGMP接口允许的最大组加入数，范围：1~40000

5.配置SSM-Mapping功能。

命令	功能
inspur(config-mcast-igmp)#**ssm-map static** {**default** | **group-list** <*access-list-name*>}<*source-address*>	在IGMP配置模式下，配置ssm-mapping映射功能，实现IGMPv1和IGMPv2的指定组源查询

default映射的是default组，是指232.0.0.0~232.255.255.255。

6.配置IGMP组加入访问列表。

命令	功能
inspur(config-mcast-igmp-if-interface-name)#**access-group** <*access-list-name*>	在IGMP接口配置模式下，配置允许IGMP加入的组范围，缺省没有IGMP加入组限制

7.配置IGMP版本。

目前IGMP有v1、v2和v3三种，缺省为v2，可以根据情况使用命令**version** <*version*>调整。基于安全考虑，IR12000智能路由器要求同一网段上的网元都是IGMP v1 v2或都是IGMP v3。

IGMP版本的配置是基于接口的，不同的接口可以配置为不同的版本。

命令	功能
inspur(config-mcast-igmp-if-interface-name)#**version** {**1** | **2** | **3**}	在IGMP接口配置模式下，配置IGMP协议版本号

8.配置接口上的IGMP组。

步骤	命令	功能
1	inspur(config-mcast-igmp-if-interface-name)#**static-group** <*group-address*>[**source**{**ssm-map** |<*source-address*>}|[{**include** | **exclude**}]]	配置IGMP接口上的静态组成员
2	inspur(config-mcast-igmp-if-interface-name)#**immediate-leave** {**all** | **group-list** <*access-list-name*>}	配置允许成员立即离开的组范围

9.配置IGMP定时器功能。

在连接共享网段的组播设备接口上启用IGMP后，选举出一个最优的充当该网段上的查询者（querier），负责发送查询消息来获取组成员的信息。查询者发送出查询消息后，会在一段时间内等待接收主机的成员报告，时长为发送查询消息时携带的最大响应时间（max response time）值，缺省为10秒。

网段上的主机成员在收到查询消息后，会在最大响应时间的基础上减去一个随机偏差值，将结果作为自己的响应时间。在此期间若收到其它主机成员的报告则取消，若没有则到时发出主机报告。所以提高最大响应时间则相应增加了网段上组成员的等待机会，可以减少网段上多个主机报告的突发性。根据网络实际情况，可以适当调整与查询者相关的几个定时器的参数值。

命令	功能
inspur(config-mcast-igmp-if-interface-name)#**query-interval** <*seconds*>	配置IGMP查询时间间隔，单位：秒，范围1~65535，缺省为125秒
inspur(config-mcast-igmp-if-interface-name)#**query-max-response-time** <*seconds*>	配置IGMP协议发送查询消息时携带的**max response time**时间值，仅对IGMP v2和IGMP v3接口有效，单位：秒，范围1~25，缺省为10秒

命令	功能
inspur(config-mcast-igmp-if-interface-name)#**querier-timeout** <*seconds*>	配置IGMP查询器超时时间，单位：秒，范围60~300，缺省值按下式计算：<*query-interval*>*<*robustness-count*>+<*query-max-response-time*>/2秒
inspur(config-mcast-igmp-if-interface-name)#**last-member-query-interval** <*seconds*>	配置IGMP特定组查询间隔，单位：秒，范围1~25，缺省为1秒
inspur(config-mcast-igmp-if-interface-name)#**robustness-count** <*times*>	配置IGMP查询器健壮系数，即发送查询报文的次数，范围：2~7
inspur(config-mcast-igmp-if-interface-name)#**shaping-packets-number** <*number*>	抑制接口报文上送数量，范围从1到该接口允许的最大数
inspur(config-mcast-igmp-if-interface-name)#**unsolicited-report-interval** <*seconds*>	在上游接口上，配置主机侧初始发送report报文的间隔（单位：秒），范围：1~25
inspur(config-mcast-igmp-if-interface-name)#**older-version-querier-present** <*seconds*>	配置在上游接口上，在收到低版本查询以后，配置等待可以发送高版本report消息的时间间隔（单位：秒），范围：60-32000

10.配置对收到的report或者leave报文是否是同一网段进行过滤。

命令	功能
inspur(config-mcast-igmp-if-interface-name)#**ip-source-check**	配置在IGMP接口模式下，对收到的report或者leave报文是否是同一网段进行过滤，缺省不过滤

11.验证配置结果。

命令	功能
inspur#**show ip igmp interface** [**vrf** <*vrf-name*>][<*interface-name*>]	查看接口IGMP配置
inspur#**show ip igmp groups** [**vrf** <*vrf-name*>][{[<*interface-name*>],[<*group-address*>]}][**deatil**]	查看接口上IGMP组加入情况
inspur#**show ip igmp packet-count** [**vrf** <*vrf-name*>][<*interface-name*>]	查看IGMP协议报文接收和发送的统计计数
inspur#**show ip igmp groups summary** [**vrf** <*vrf-name*>]	查看接口上IGMP组数目总和

12.维护IGMP。

命令	功能
inspur#**clear ip igmp groups** [**vrf** <*vrf-name*>][<*interface-name*>]	删除动态加入的组播组

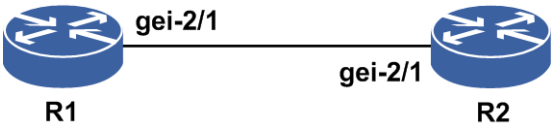
命令	功能
inspur#**clear ip igmp packet-count** [**vrf** <*vrf-name*>][<*interface-name*>]	清除IGMP接收和发送的报文统计计数

5.2.2 IGMP 查询路由器选举配置实例

配置说明

如*图 5-2*所示，R1和R2上启用PIM-SM协议，IGMP协议版本启用v2，IGMPv2通过常规查询报文进行选举，最低IP地址的IGMPv2路由器成为查询路由器。

图 5-2 IGMP 查询路由器选举配置实例



配置思路

1.接口模式下，配置两台路由器接口地址，使R1地址小于R2地址。

2.打开组播模块的总开关ip multicast-routing。

3.进入PIM路由模式，再进入所要配置的接口。

4.接口模式下，开启PIM-SM协议。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/1
R1(config-if-gei-2/1)#ip address 10.0.0.1 255.255.255.0
R1(config-if-gei-2/1)#no shutdown
R1(config-if-gei-2/1)#exit
R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-2/1
R1(config-mcast-pim-if-gei-2/1)#pimsm
```

R2上的配置如下：

```
R2(config)#interface gei-2/1
R2(config-if-gei-2/1)#ip address 10.0.0.2 255.255.255.0 /*比R1的接口IP地址大*/
R2(config-if-gei-2/1)#no shutdown
R2(config-if-gei-2/1)#exit
R2(config)#ip multicast-routing
R2(config-mcast)#router pim
R2(config-mcast-pim)#interface gei-2/1
R2(config-mcast-pim-if-gei-2/1)#pimsm
```

配置验证

R1上查看生效性：

```
R1#show ip igmp interface gei-2/1
gei-2/1
  Internet address is 10.0.0.1, subnet mask len is 24
  IGMP is enabled on interface
  Current IGMP version is 2              /*IGMP版本信息*/
  IGMP query interval is 125 seconds            /*查询间隔时间*/
  IGMP last member query interval is 1 seconds   /*最后成员查询间隔*/
  IGMP query max response time is 10 seconds     /*最大响应时间*/
  IGMP querier timeout period is 255 seconds     /*查询者超时时间*/
  IGMP robustness variable is 2
  IGMP querier is 10.0.0.1, never expire
  /*查询者信息，本端接口IP地址小，为查询者则显示never expire */
  Inbound IGMP access group is not set
  IGMP immediate leave control is not set
  IGMP shaping packets number is not set
  IGMP maximum joins is not set
```

R2上查看生效性：

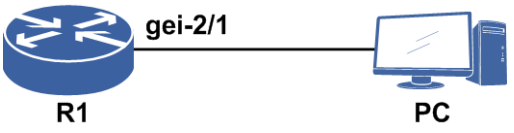
```
R2#show ip igmp interface gei-2/1
gei-2/1
  Internet address is 10.0.0.2, subnet mask len is 24
  IGMP is enabled on interface
  Current IGMP version is 2              /*IGMP版本信息*/
  IGMP query interval is 125 seconds            /*查询间隔时间*/
  IGMP last member query interval is 1 seconds   /*最后成员查询间隔*/
  IGMP query max response time is 10 seconds     /*最大响应时间*/
  IGMP querier timeout period is 255 seconds     /*查询者超时时间*/
  IGMP robustness variable is 2
  IGMP querier is 10.0.0.1, expire timer: 00:04:06
/*显示查询者信息，本端为非查询者，显示查询者目前的超时时间
为00:04:06，表示再过4分06秒查询者超时 */
  Inbound IGMP access group is not set
  IGMP immediate leave control is not set
  IGMP shaping packets number is not set
  IGMP maximum joins is not set
```

5.2.3 IGMP 动态组、静态组加入配置实例

配置说明

如*图 5-3*所示，R1上启用PIM-SM协议，IGMP协议版本默认为v2，在R1上配置静态组加入225.1.1.2 ，并通过测试机配置动态组加入225.1.1.1。

图 5-3 IGMP 动态组、静态组加入配置实例



配置思路

1.接口模式下，配置路由器接口地址。

2.打开组播模块的总开关**ip multicast-routing**。

3.进入PIM路由模式，再进入所要配置的接口。

4.接口模式下，开启PIM-SM协议。

5.组播模式下，进入IGMP路由模式，再进入所要配置的接口。

6.在R1的gei-2/1接口上配置静态组加入。

7.在测试机上发送IGMP组加入报文。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/1
R1(config-if-gei-2/1)#ip address 10.0.0.1 255.255.255.0
R1(config-if-gei-2/1)#no shutdown
R1(config-if-gei-2/1)#exit
R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-2/1
R1(config-mcast-pim-if-gei-2/1)#pimsm
R1(config-mcast-pim-if-gei-2/1)#exit
R1(config-mcast-pim)#exit
R1(config-mcast)#router igmp
R1(config-mcast-igmp)#interface gei-2/1
R1(config-mcast-igmp-if-gei-2/1)#static-group 225.1.1.2 /*静态组配置*/
```

配置验证

R1上查看IGMP接口信息：

```
R1#show ip igmp interface gei-2/1
  gei-2/1
  Internet address is 10.0.0.1, subnet mask len is 24 /*IGMP接口IP地址*/
  IGMP is enabled on interface
  Current IGMP version is 2  /*IGMP版本信息*/
  IGMP query interval is 125 seconds  /*查询间隔时间*/
  IGMP last member query interval is 1 seconds  /*最后成员查询间隔*/
  IGMP query max response time is 10 seconds  /*最大响应时间*/
  IGMP querier timeout period is 255 seconds /*查询者超时时间*/
  IGMP robustness variable is 2        /*IGMP版本信息*/
  IGMP querier is 10.0.0.1, never expire
  /*查询者信息，为查询者则显示never expire */
  Inbound IGMP access group is not set
  IGMP immediate leave control is not set
  IGMP shaping packets number is not set
  IGMP maximum joins is not set
```

R1上查看对应接口的组的详细信息：

```
R1#show ip igmp groups gei-2/1 detail
Flags: S - Static Group, SSM - SSM Group, M - MDT Group
Interface:    gei-2/1
Group:        225.1.1.1
```

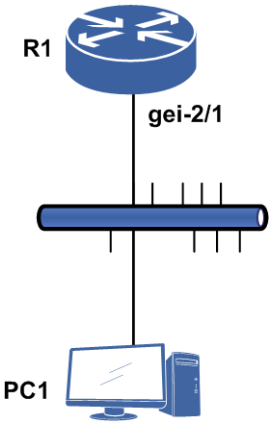
```
Flags:
Uptime:        00:05:12
Group mode:     EXCLUDE（(Expires:00:04:13） /*动态组超时时间*/
Last reporter:  10.0.0.10
Group source list is empty
Interface:      gei-2/1
Group:         225.1.1.2
Flags:         S   /*静态组标志*/
Uptime:        00:01:16
Group mode:     EXCLUDE (Expires: never)
Last reporter:  10.0.0.1
Group source list is empty
```

5.2.4 IGMP 对所有组的快速离开配置实例

配置说明

如*图 5-4*所示，路由器与组播用户直连，通过PC1动态组加入225.0.0.0。

图 5-4 IGMP 对所有组的快速离开配置组网图



配置思路

1.进入组播配置模式，使能接口IGMP功能。

2.配置接口对所有组快速离开。

配置过程

R1上的配置如下：

```
R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-2/1
R1(config-mcast-pim-if-gei-2/1)#pimsm
R1(config-mcast-pim-if-gei-2/1)#exit
R1(config-mcast-pim)#exit
R1(config-mcast)#router igmp
R1(config-mcast-igmp)#interface gei-2/1
R1(config-mcast-igmp-if-gei-2/1)#immediate-leave all
```

```
R1(config-mcast-igmp-if-gei-2/1)#version 2
R1(config-mcast-igmp-if-gei-2/1)#exit
R1(config-mcast-igmp)#exit
R1(config-mcast)#exit
```

配置验证

在接口gei-2/1上进行组加入和组离开，并打开debug信息，查看处理过程。

```
R1#show running-config multicast
!<multicast>
ip multicast-routing
  router pim
    interface gei-2/1
      pimsm
    $
  $
  router igmp
    interface gei-2/1
      immediate-leave  all
      version 2
    $
  $
$
!</multicast>

R1#debug ip igmp gei-2/1
IGMP permit interface (gei-2/1) debugging is on
R1#terminal monitor
R1 MPFU-8/0 2010-7-27 17:18:14
IGMP : Receive packet from 33.33.0.12 on interface gei-2/1
R1 MPFU-8/0 2010-7-27 17:18:14
IGMP : Received packet is IGMPv2 membership report for group 225.0.0.0
R1 MPFU-8/0 2010-7-27 17:18:14
IGMP : Create group (225.0.0.0) on gei-2/1
R1 MPFU-8/0 2010-7-27 17:18:14
IGMP : Switching to EXCLUDE mode for group(225.0.0.0)
R1 MPFU-8/0 2010-7-27 17:18:14
IGMP : Switching to EXCLUDE mode for group(225.0.0.0)
R1 MPFU-8/0 2010-7-27 17:18:14
IGMP : Updating EXCLUDE group timer for 225.0.0.0 timer to 260 seconds
R1 MPFU-8/0 2010-7-27 17:18:20
IGMP : Receive packet from 33.33.0.12 on interface gei-2/1
R1 MPFU-8/0 2010-7-27 17:18:20
IGMP : Received packet is IGMPv2 membership report for group 225.0.0.0
R1 MPFU-8/0 2010-7-27 17:18:20
IGMP : Updating EXCLUDE group timer for 225.0.0.0 timer to 260 seconds

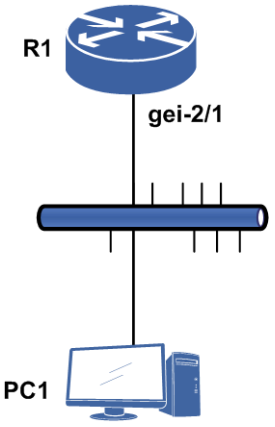
R1#show ip igmp group
Total: 1 groups
Group addr      Interface          Present     Expire      Last Reporter
225.0.0.0       gei-2/1           00:00:06    00:04:14    33.33.0.12
R1 MPFU-8/0 2010-7-27 17:19:42
IGMP : Receive packet from 33.33.0.12 on interface gei-2/1
R1 MPFU-8/0 2010-7-27 17:19:42
IGMP : Received packet is IGMPv2 leave message (225.0.0.0)
R1 MPFU-8/0 2010-7-27 17:19:42
IGMP : Membership (225.0.0.0) immediately leaves on gei-2/1
R1 MPFU-8/0 2010-7-27 17:19:42
IGMP : Delete group 225.0.0.0 on gei-2/1
R1#show ip igmp group
Total: 0 groups
Group addr      Interface          Present     Expire     Last Reporter
```

5.2.5 IGMP 对指定组的快速离开配置实例

配置说明

如*图 5-5*所示，路由器与组播用户直连， 通过PC1动态组加入225.0.0.0和225.0.0.1。

图 5-5 IGMP 对特定组的快速离开配置组网图



配置思路

1.配置组过滤规则。

2.进入组播配置模式，使能接口IGMP功能。

3.配置接口对指定组快速离开。

配置过程

R1上的配置如下：

```
R1(config)#ipv4-access-list groupfilter
R1(config-ipv4-acl)#rule 1 permit 225.0.0.0
R1(config-ipv4-acl)#rule 2 deny any
R1(config-ipv4-acl)#exit

R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-2/1
R1(config-mcast-pim-if-gei-2/1)#pimsm
R1(config-mcast-pim-if-gei-2/1)#exit
R1(config-mcast-pim)#exit
R1(config-mcast)#router igmp
R1(config-mcast-igmp)#interface gei-2/1
R1(config-mcast-igmp-if-gei-2/1)#immediate-leave groupfilter
R1(config-mcast-igmp-if-gei-2/1)#version 2
R1(config-mcast-igmp-if-gei-2/1)#exit
R1(config-mcast-igmp)#exit
R1(config-mcast)#exit
```

配置验证

在接口gei-2/1上进行组加入和组离开，并打开debug信息，查看处理过程。

```
R1(config)#show running-config ipv4-acl
!<ipv4-acl>
ipv4-access-list groupfilter
  rule 1 permit 225.0.0.0 0.0.0.0
  rule 2 deny any
$
!</ipv4-acl>

R1(config)#show running-config multicast
!<multicast>
ip multicast-routing
  router pim
    interface gei-2/1
      pimsm
    $
  $
  router igmp
    interface gei-2/1
      immediate-leave groupfilter
      version 2
    $
  $
$
!</multicast>
R1 MPFU-8/0 2010-7-27 09:58:18
igmp : Receive IGMP packet from 33.33.0.12 on interface gei-2/1
R1 MPFU-8/0 2010-7-27 09:58:18
igmp : Received packet is IGMP v2 membership report for group 225.0.0.0
R1 MPFU-8/0 2010-7-27 09:58:18
igmp : Create group (225.0.0.0) on gei-2/1
R1 MPFU-8/0 2010-7-27 09:58:18
igmp : Updating EXCLUDE group timer for 225.0.0.0 timer to 260 seconds
R1#
R1 MPFU-8/0 2010-7-27 09:58:23
igmp : Receive IGMP packet from 33.33.0.12 on interface gei-2/1
R1 MPFU-8/0 2010-7-27 09:58:23
igmp : Received packet is IGMP v2 membership report for group 225.0.0.1
R1 MPFU-8/0 2010-7-27 09:58:23
igmp : Create group (225.0.0.1) on gei-2/1
R1 MPFU-8/0 2010-7-27 09:58:23
igmp : Updating EXCLUDE group timer for 225.0.0.1 timer to 260 seconds

R1#show ip igmp group
Total: 2 groups
Group addr      Interface          Present     Expire      Last Reporter
225.0.0.0       gei-2/1           00:00:11    00:04:09    33.33.0.12
225.0.0.1       gei-2/1           00:00:06    00:04:14    33.33.0.12
R1#
R1 MPFU-8/0 2010-7-27 17:23:01
IGMP : Receive packet from 33.33.0.12 on interface gei-2/1
R1 MPFU-8/0 2010-7-27 17:23:01
IGMP : Received packet is IGMPv2 leave message (225.0.0.0)
R1 MPFU-8/0 2010-7-27 17:23:01
IGMP : Membership (225.0.0.0) immediately leaves on gei-2/1
R1 MPFU-8/0 2010-7-27 17:23:01
IGMP : Delete group 225.0.0.0 on gei-2/1
R1 MPFU-8/0 2010-7-27 17:23:01
IGMP : Receive packet from 33.33.0.12 on interface gei-2/1
R1 MPFU-8/0 2010-7-27 17:23:01
IGMP : Received packet is IGMPv2 leave message (225.0.0.1)
R1 MPFU-8/0 2010-7-27 17:23:01
IGMP : Send IGMPv2 specific query(225.0.0.1) on gei-2/1
R1 MPFU-8/0 2010-7-27 17:23:03
IGMP : Send IGMPv2 specific query(225.0.0.1) on gei-2/1
```

```
R1 MPFU-8/0 2010-7-27 17:23:04
IGMP : Delete group 225.0.0.1 on gei-2/1

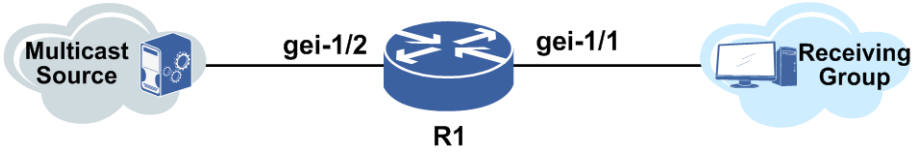
R1#show ip igmp group
Total: 0 groups
Group addr      Interface     Present     Expire      Last Reporter
```

5.2.6 组播接口限制配置实例

配置说明

如*图 5-6*所示，R1上配置了组播抑制功能，接收者发送大量加入组播的report，只能有抑制数量的组播组加入。

图 5-6 组播接口限制配置实例示意图



配置思路

1.R1上使能组播。

2.配置接口允许的最大加入数。

3.接口启用PIMSM协议。

配置过程

```
R1(config)#ip multicast-routing
R1(config-mcast)#router igmp
R1(config-mcast-igmp)#interface gei-1/1
R1(config-mcast-igmp-if-gei-1/1)#maximum-joins 100    /*接口允许的最大加入数*/
R1(config-mcast-igmp-if-gei-1/1)#exit
R1(config-mcast-igmp)#exit

R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-1/1
R1(config-mcast-pim-if-gei-1/1)#pimsm
R1(config-mcast-pim)#interface gei-1/2
R1(config-mcast-pim-if-gei-1/2)#pimsm
```

配置验证

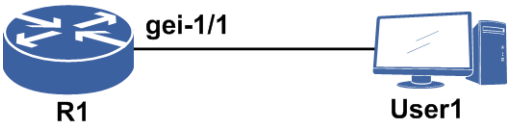
接收端发送加入大量组播组的请求，只有在抑制范围之内的数量报文被上送，只能加入一部分组播组。使用**show ip igmp groups**命令可以看到结果只加入了100条。

5.2.7 IP-Source-Check 功能配置实例

配置说明

开启IGMP report和leave报文的源地址过滤功能，只有收到的报文和当前接口地址在同一网段才进行处理。示例组网如*图 5-7*所示。

图 5-7 IP-Source-Check 功能配置组网示意图



配置思路

1.接口模式下，配置路由器接口地址。

2.打开组播模块的总开关**ip multicast—routing**。

3.进入PIM路由模式，再进入所要配置的接口。

4.接口模式下，开启PIM-SM协议。

5.组播模式下，进入IGMP路由模式，再进入所要配置的接口。

6.在R1的gei-1/1接口上配置**ip-source-check**。

7.在用户设备上发送和接口IP地址不是同一网段的地址报文，则成员无法成功加入。

8.修改用户设备的IP地址和接口为同一网段，发送加入报文，则成员加入成功。

配置过程

R1的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 10.0.0.1 255.255.255.0
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-1/1
R1(config-mcast-pim-if-gei-1/1)#pimsm
R1(config-mcast-pim-if-gei-1/1)#exit
R1(config-mcast-pim)#exit
R1(config-mcast)#router igmp
R1(config-mcast-igmp)#interface gei-1/1
R1(config-mcast-igmp-if-gei-1/1)#ip-source-check
R1(config-mcast-igmp-if-gei-1/1)#exit
```

配置验证

用户设备发送源IP地址为20.0.0.2的IGMP加入报文，在R1上**show ip igmp group**，此时显示表项为空，加入失败。用户设备修改IP地址为10.0.0.2，再次发送IGMP加入报文并查看表项，显示加入成功。

```
R1(config)#show ip igmp groups

Total:1 groups
Group addr      Interface       Present/Expire    Last Reporter
225.0.0.1       gei-1/1         03:17:56/00:04:20  10.0.0.2
```

5.3 PIM-DM

PIM-DM协议适用于密集模式，即网络中组播接收者较多的应用场景。PIM-DM协议机制相对较为简单，采用PUSH方式，将组播流量周期性扩散到网络中所有设备，建立和维护SPT转发树。

5.3.1 配置 PIM-DM

本节介绍PIM-DM功能的配置步骤和命令。

1.配置PIM-DM。

步骤	命令	功能
1	inspur(config-mcast)#**router pim**	启用PIM协议
2	inspur(config-mcast-pim)#**interface** <*interface-name*>	进入PIM接口配置模式
3	inspur(config-mcast-pim-if-interface-name)#**pimdm**	接口启用IP组播协议PIM-DM

2.验证配置结果。

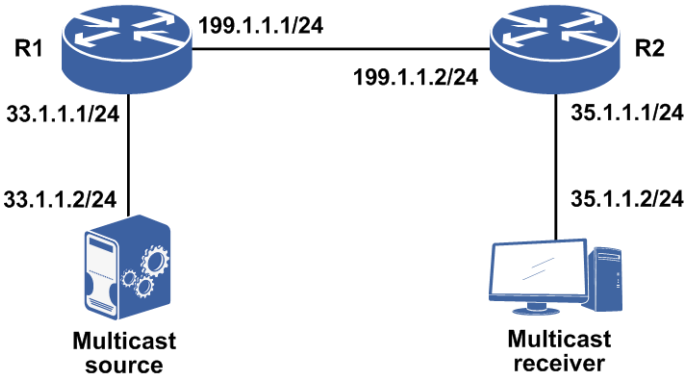
命令	功能
inspur#**show ip pim interface** [**vrf** <*vrf-name*>][<*interface-name*>]	查看配置的PIM接口情况
inspur#**show ip pim mroute** [**vrf** <*vrf-name*>][**group** <*group-address*>|[**source** <*source-address*>]]	显示PIM组播路由表的内容
inspur#**show ip pim mroute summary** [**vrf** <*vrf-name*>]	显示IP组播PIM路由表的内容统计信息
inspur#**show ip pim neighbor** [**vrf** <*vrf-name*>][<*interface-name*>]	查看PIM接口的邻居情况

5.3.2 PIM-DM 邻居建立配置实例

配置说明

如*图 5-8*所示，R1和R2建立PIM-DM邻居。

图 5-8 PIM-DM 配置实例



配置思路

1.配置相应接口的IP地址。

2.进入组播模式。

3.进入PIM模式。

4.在相应接口下使能PIM-DM。

配置过程

R1的配置实例：

```
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#ip address 199.1.1.1 255.255.255.0
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#exit
R1(config)#interface gei-1/4
R1(config-if-gei-1/4)#ip address 33.1.1.1  255.255.255.0
R1(config-if-gei-1/4)#no shutdown
R1(config-if-gei-1/4)#exit

R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-1/3
R1(config-mcast-pim-if-gei-1/3)#pimdm
R1(config-mcast-pim-if-gei-1/3)#exit
R1(config-mcast-pim)#interface gei-1/4
R1(config-mcast-pim-if-gei-1/4)#pimdm
R1(config-mcast-pim-if-gei-1/4)#exit
```

R2的配置如下：

```
R2(config)#interface gei-1/7
R2(config-if-gei-1/7)#ip address 199.1.1.2 255.255.255.0
```

```
R2(config-if-gei-1/7)#no shutdown
R2(config-if-gei-1/7)#exit
R2(config)#interface gei-1/8
R2(config-if-gei-1/8)#ip address 35.1.1.1 255.255.255.0
R2(config-if-gei-1/8)#no shutdown
R2(config-if-gei-1/8)#exit

R2(config)#ip multicast-routing
R2(config-mcast)#router pim
R2(config-mcast-pim)#interface gei-1/7
R2(config-mcast-pim-if-gei-1/7)#pimdm
R2(config-mcast-pim-if-gei-1/7)#exit
R2(config-mcast-pim)#interface gei-1/8
R2(config-mcast-pim-if-gei-1/8)#pimdm
R2(config-mcast-pim-if-gei-1/8)#end
R2#configure terminal
R2(config)#ip route 33.1.1.0 255.255.255.0 199.1.1.1  /*到源的单播路由*/
```

配置验证

在R1上通过**show ip pim neighbor**查看邻居状态：

```
R1(config)#show ip pim neighbor
Neighbor Address  Interface      DR Priority   Uptime    Expires   Ver
199.1.1.2        gei-1/3    1           00:09:14   00:01:36  V2
```

在R1上通过**show ip pim interface**查看接口状态：

```
R1(config)#show ip pim interface
Address    Interface     State Nbr   Hello  DR        DR         PIM       Mode
                           Count Period Priority            Silent
199.1.1.1  gei-1/3       Up    1     30     1         199.1.1.2   Disabled   D
33.1.1.1   gei-1/4       Up    1     30     1         33.1.1.1    Disabled   D
```

接收组加入组播组，组播源发送组播流，在R1上通过**show ip mroute**查看IP组播路由表状态：

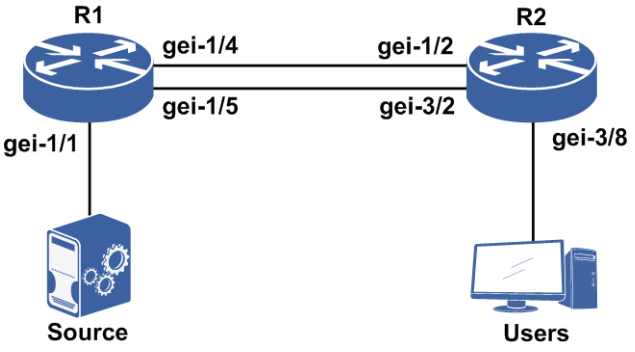
```
R1#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(33.1.1.2, 225.10.0.1), TYPE: DYNAMIC, FLAGS:
   Incoming interface: gei-1/4, flags:
   Outgoing interface list:
     gei-1/3, flags:F/S
```

5.3.3 PIM-DM 组播负荷分担配置实例

配置说明

当源到最后一跳路由器之间存在多条等价路径时，可以通过配置组播负荷分担，使流量沿不同路径到达用户。如*图 5-9*所示，源S向用户发送多个组的组播流量；且最后一跳路由器（Last-hop Router）R2到源S存在两条路径。

图 5-9 组播负荷分担配置实例示意图



路由器上各个接口的地址如下。

路由器	接口	IP地址	掩码
R1	gei-1/1	172.1.3.44	255.255.255.0
R1	gei-1/4	172.1.7.44	255.255.255.0
R1	gei-1/5	172.1.13.44	255.255.255.0
R2	gei-3/2	172.1.13.46	255.255.255.0
R2	gei-3/8	172.1.5.46	255.255.255.0
R2	gei-1/2	172.1.7.46	255.255.255.0

对于R2，这两条路径的代价是相等的，即这两条路径是最后一跳路由器R2和源之间的等价路径，可以通过在R2上配置组播负荷分担使不同组的组播流量沿着两条路径到达用户。

配置思路

1.各路由器接口配置PIM-DM协议，使用户可以正常接收从源发送的组播流量。

2.在R2路由器上配置组播负荷分担。

配置过程

R1的配置（各接口启用PIM-DM协议）如下：

```
R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-1/1
R1(config-mcast-pim-if-gei-1/1)#pimdm
R1(config-mcast-pim-if-gei-1/1)#exit
R1(config-mcast-pim)#interface gei-1/4
R1(config-mcast-pim-if-gei-1/4)#pimdm
R1(config-mcast-pim-if-gei-1/4)#exit
R1(config-mcast-pim)#interface gei-1/5
R1(config-mcast-pim-if-gei-1/5)#pimdm
R1(config-mcast-pim-if-gei-1/5)#exit
```

R2的配置（各接口使能PIM-DM协议）如下：

```
R2(config-mcast-pim)#interface gei-3/2
R2(config-mcast-pim-if-gei-3/2)#pimdm
R2(config-mcast-pim-if-gei-3/2)#exit
R2(config-mcast-pim)#interface gei-3/8
R2(config-mcast-pim-if-gei-3/8)#pimdm
R2(config-mcast-pim-if-gei-3/8)#exit
R2(config-mcast-pim)#interface gei-1/2
R2(config-mcast-pim-if-gei-1/2)#pimdm
R2(config-mcast-pim-if-gei-1/2)#exit

R2(config)#ip route 172.1.3.0 255.255.255.0 172.1.7.44
R2(config)#ip route 172.1.3.0 255.255.255.0 172.1.13.44
/*如果使用OSPF等协议，也要满足单播负荷分担*/

/*最后在R2配置启用负荷分担，以s-g-hash为例*/
R2(config)#ip multicast-routing
R2(config-mcast)#multipath s-g-hash basic
R2(config-mcast)#exit
```

配置验证

当用户开始接收源S发送的组播流量时，查看R1和R2上的组播路由表及形成的邻居。

R1的组播路由表如下：

```
R1#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(172.1.3.2, 225.0.0.1), TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-1/1, flags:
  Outgoing interface list:
    gei-1/4, flags: F/S
(172.1.3.2, 225.0.0.2), TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-1/1, flags:
  Outgoing interface list:
    gei-1/5, flags: F/S
(172.1.3.2, 225.0.0.3), TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-1/1, flags:
  Outgoing interface list:
    gei-1/4, flags: F/S
(172.1.3.2, 225.0.0.4), TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-1/1, flags:
  Outgoing interface list:
    gei-1/5, flags: F/S
```

查看R1的邻居形成情况：

```
R1#show ip pim neighbor
Neighbor Address  Interface  DR Priority   Uptime    Expires   Ver
172.1.7.46       gei-1/4    1           00:13:36   00:01:25  V2
172.1.13.46      gei-1/5    1           00:18:38   00:01:18  V2
```

R2的组播路由表如下：

```
R2#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(*, 225.0.0.1), RP: 0.0.0.0, TYPE: DYNAMIC, FLAGS:
  Incoming interface: NULL, flags:
  Outgoing interface list:
    gei-3/8, flags: F/S
(172.1.3.2, 225.0.0.1), TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-1/2, flags:
  Outgoing interface list:
    gei-3/8, flags: F/S
```

```
(*, 225.0.0.2), RP: 0.0.0.0, TYPE: DYNAMIC, FLAGS:
  Incoming interface: NULL, flags:
  Outgoing interface list:
    gei-3/8, flags: F/S
(172.1.3.2, 225.0.0.2), TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-3/2, flags:
  Outgoing interface list:
    gei-3/8, flags: F/S
(*, 225.0.0.3), RP: 0.0.0.0, TYPE: DYNAMIC, FLAGS:
  Incoming interface: NULL, flags:
  Outgoing interface list:
    gei-3/8, flags: F/S
(172.1.3.2, 225.0.0.3), TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-1/2, flags:
  Outgoing interface list:
    gei-3/8, flags: F/S
(*, 225.0.0.4), RP: 0.0.0.0, TYPE: DYNAMIC, FLAGS:
  Incoming interface: NULL, flags:
  Outgoing interface list:
    gei-3/8, flags: F/S
(172.1.3.2, 225.0.0.4), TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-3/2, flags:
  Outgoing interface list:
    gei-3/8, flags: F/S
```

5.4 PIM-SM

PIM-SM主要适用于组成员分布相对分散、范围较广、网络带宽资源有限的应用场景，不依赖于特定的单播路由协议。

PIM-SM通过设置RP向所有支持PIM-SM的路由器通告组播信息。在PIM-SM中，路由器显式地加入和退出组播组，可以减少数据报文和控制报文占用的网络带宽。

5.4.1 配置 PIM-SM

本节介绍PIM-SM功能的配置步骤和命令。

1.启用PIM协议并配置RP和BSR。

步骤	命令	功能
1	inspur(config-mcast)#**router pim**	启用PIM协议
2	inspur(config-mcast-pim)#**static-rp** <*ip-address*>[{[**group-list** <*prefix-list-name*>],[**priority** <*priority*>]}]	配置静态RP <*priority*>：优先级，缺省为192，范围为0~255
	inspur(config-mcast-pim)#**static-rp override**	配置静态RP优先
	inspur(config-mcast-pim)#**bsr-candidate** <*interface-name*>[{[**hash-mask-length** <*hash-mask-length*>],[**priority** <*priority*>]}]	配置候选BSR <*priority*>：优先级，缺省为0，范围为0~255
	inspur(config-mcast-pim)#**rp-candidate** <*interface-name*>[{[**group-list**	配置候选RP <*priority*>：优先级，缺省为

步骤	命令	功能
	<*prefix-list-name*>],[**priority** <*priority*>]}]	192，范围为0~255
	inspur(config-mcast-pim)#**accept-rp** <*access-list-name*>	对BSR消息中通告的候选RP地址进行过滤
3	inspur(config-mcast-pim)#**data-filter**< *access-list-name* >	配置源数据过滤（可选）

<*prefix-list-name*>：组范围，该范围是被通告RP服务范围。

<*hash-mask-length*>：哈希掩码长度，范围0~32，缺省为30。

<*access-list-name*>：ACL名，范围1~31个字符。

2.在接口模式下启用PIM协议并配置接口的DR优先级。

步骤	命令	功能
1	inspur(config-mcast-pim)#**interface**<*interface-name*>	进入PIM接口模式
2	inspur(config-mcast-pim-if-interface-name)#**pimsm**	接口上启动组播路由协议PIM-SM
	inspur(config-mcast-pim-if-interface-name)#**dr-priority** <*priority*>	设置PIM接口DR优先级，范围：0~4294967295，缺省为1

3.配置PIM安全控制功能。

步骤	命令	功能
1	inspur(config-mcast)#**router pim**	启用PIM协议
2	inspur(config-mcast-pim)#**register-holdtime** <*seconds*>	设置路由器收不到注册停止报文保持注册状态的时间
3	inspur(config-mcast-pim)#**join-prune-interval** <*seconds*>	设置发送Join/Prune报文的周期

4.配置组播MoFRR功能。

命令	功能
inspur(config-mcast-pim)#**mofrr** <*access-list-name*>	启用MoFRR功能

5.验证配置结果。

命令	功能
inspur#**show ip pim mroute** [**vrf** <*vrf-name*>][**group** <*group-address*>|[**source**	显示组播PIM路由表的内容

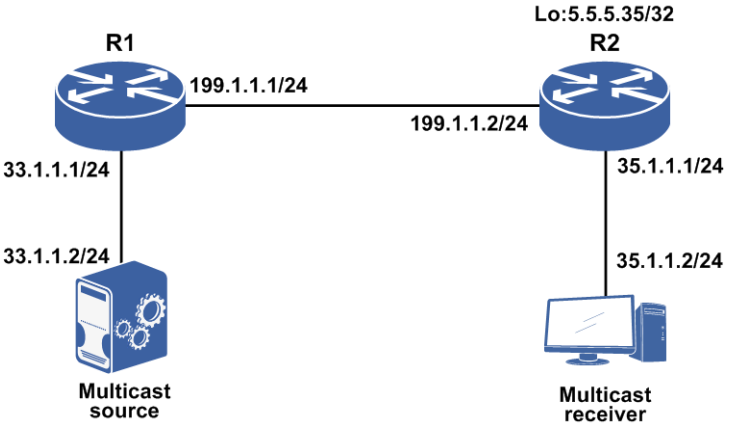
命令	功能
<*source-address*>]]	
inspur#**show ip pim mroute summary** [**vrf** <*vrf-name*>]	显示PIM路由表的内容统计信息
inspur#**show ip pim bsr** [**vrf** <*vrf-name*>]	显示引导路由器（BSR）的信息
inspur#**show ip pim rp mapping** [**vrf** <*vrf-name*>]	显示本路由器上的RP集信息
inspur#**show ip pim rp hash** [**vrf** <*vrf-name*>]<*group-address*>	显示特定组播组选择的RP信息
inspur#**show ip pim interface** [**vrf** <*vrf-name*>][<*interface-name*>]	查看配置的PIM接口情况
inspur#**show ip pim neighbor** [**vrf** <*vrf-name*>][<*interface-name*>]	查看PIM接口的邻居情况
inspur#**show ip pim nexthop** [**vrf** <*vrf-name*>][**dest-address** <*ip-address*>]	查看PIM下一跳的信息
inspur#**show ip pim bfd**[**vrf** <*vrf-name*>][<*interface-name*>]	查看PIM BFD邻居的信息

5.4.2 PIM-SM 转发组播流（使用动态 RP）配置实例

配置说明

如*图 5-10*所示，R2端IGMP组加入，R1端组播源加入，配置BSR和CRP。

图 5-10 使用 PIM-SM 转发组播流（使用动态 RP）配置实例



配置思路

1.配置相应接口地址。

2.进入组播配置模式。

3.进入PIM配置模式。

4.配置R2的loopback5接口为CRP 和BSR。

5.进入接口启动PIM-SM。

6.在R1上配置到RP的单播路由，在R2上配置到组播源的单播路由（本例使用静态路由配置也可以使用IGP打通路由）。

配置过程

R1的配置如下：

```
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#ip address 199.1.1.1 255.255.255.0
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#exit
R1(config)#interface gei-1/7
R1(config-if-gei-1/7)#ip address 33.1.1.1 255.255.255.0
R1(config-if-gei-1/7)#no shutdown
R1(config-if-gei-1/7)#exit

R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-1/3
R1(config-mcast-pim-if-gei-1/3)#pimsm
R1(config-mcast-pim-if-gei-1/3)#exit
R1(config-mcast-pim)#interface gei-1/7
R1(config-mcast-pim-if-gei-1/7)#pimsm
R1(config-mcast-pim-if-gei-1/7)#dr-priority 20
R1(config-mcast-pim-if-gei-1/7)#exit

R1(config)#ip route 5.5.5.35 255.255.255.255 199.1.1.2  /*配置到RP的静态路由*/
```

R2的配置如下：

```
R2(config)#interface gei-3/8
R2(config-if-gei-3/8)#ip address 199.1.1.2 255.255.255.0
R2(config-if-gei-3/8)#no shutdown
R2(config-if-gei-3/8)#exit
R2(config)#interface gei-3/7
R2(config-if-gei-3/7)#ip address 35.1.1.1 255.255.255.0
R2(config-if-gei-3/7)#no shutdown
R2(config-if-gei-3/7)#exit
R2(config)#interface loopback5
R2(config-if-loopback5)#ip address 5.5.5.35 255.255.255.255
R2(config-if-loopback5)#exit

R2(config)#ip multicast-routing
R2(config-mcast)#router pim
R2(config-mcast-pim)#rp-candidate loopback5
R2(config-mcast-pim)#bsr-candidate loopback5
R2(config-mcast-pim)#interface gei-3/8
R2(config-mcast-pim-if-gei-3/8)#pimsm
R2(config-mcast-pim-if-gei-3/8)#exit
R2(config-mcast-pim)#interface gei-3/7
R2(config-mcast-pim-if-gei-3/7)#pimsm
R2(config-mcast-pim-if-gei-3/7)#dr-priority 20
R2(config-mcast-pim-if-gei-3/7)#exit

R2(config)#ip route 33.1.1.0 255.255.255.0 199.1.1.1
/*配置到组播源的静态路由*/
```

配置验证

在R1上通过**show ip pim interface**查看接口状态：

```
R1(config)#show ip pim interface
Address      Interface      State  Nbr    Hello   DR          DR           PIM
Mode
                            Count  Period Priority             Silent
33.1.1.1    gei-1/7       Up    0     30     20        33.1.1.1    Disabled   S
199.1.1.1   gei-1/3       Up    1     30     1         199.1.1.2   Disabled   S
```

在R1上通过**show ip pim neighbor**查看邻居状态：

```
R1(config)#show ip pim neighbor
Neighbor Address  Interface      DR Priority   Uptime    Expires   Ver
199.1.1.2        gei-1/3        1            00:07:48   00:01:23  V2
```

在R1上通过**show ip pim bsr**查看BSR状态：

```
R1(config)#show ip pim bsr
BSR address: 5.5.5.35
Uptime: 00:00:40, BSR Priority :0, Hash mask length:30
Expires:00:01:30
No candidate RP information!
```

在R1上通过**show ip pim rp mapping**查看RP状态：

```
R1(config)#show ip pim rp mapping
Group(s): 224.0.0.0/4(SM)
  RP: 5.5.5.35, v2, Priority:192
  BSR: 5.5.5.35, via bootstrap
      Uptime: 00:00:43, expires: 00:01:47
Group(s): 0.0.0.0/0(NOUSED)
```

在R2上通过**show ip mroute**命令查看：

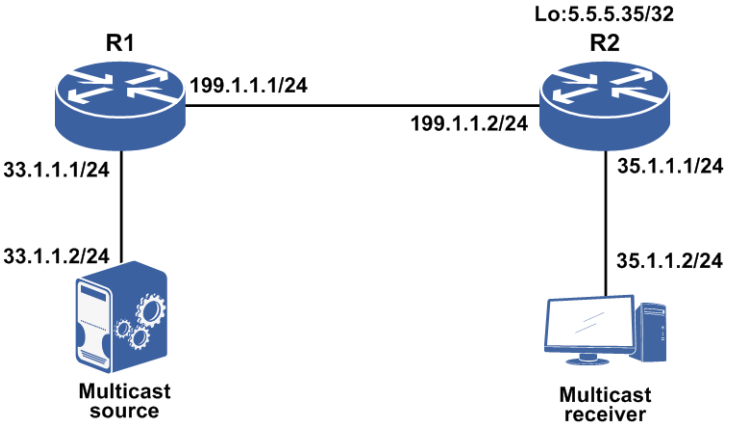
```
R2(config)#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(*, 225.10.0.1), RP: 5.5.5.35, TYPE: DYNAMIC, FLAGS:
   Incoming interface: NULL, flags:
   Outgoing interface list:
     gei-3/7, flags: F/S
(33.1.1.2, 225.10.0.1), TYPE: DYNAMIC, FLAGS:
   Incoming interface: gei-3/8, flags:
   Outgoing interface list:
     gei-3/7, flags: F/S
```

5.4.3 PIM-SM 转发组播流（使用静态 RP）配置实例

配置说明

如*图 5-11*所示，R2端IGMP组加入，R1端组播源加入，配置PIM-SM邻居和静态RP 。

图 5-11 使用 PIM-SM 转发组播流（使用静态 RP）配置实例



配置思路

1.进入组播配置模式。

2.进入PIM配置模式。

3.配置5.5.5.35 为**static-rp**。

4.进入接口启动PIM-SM。

5.在R1上配置到RP的单播路由，在R2上配置到组播源的单播路由（本例使用静态路由配置）。

配置过程

R1的配置如下：

```
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#ip address 199.1.1.1 255.255.255.0
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#exit
R1(config)#interface gei-1/7
R1(config-if-gei-1/7)#ip address 33.1.1.1 255.255.255.0
R1(config-if-gei-1/7)#no shutdown
R1(config-if-gei-1/7)#exit

R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-1/3
R1(config-mcast-pim-if-gei-1/3)#pimsm
R1(config-mcast-pim-if-gei-1/3)#exit
R1(config-mcast-pim)#interface gei-1/7
R1(config-mcast-pim-if-gei-1/7)#pimsm
R1(config-mcast-pim-if-gei-1/7)#dr-priority 20
R1(config-mcast-pim)#exit
R1(config-mcast-pim)#static-rp 5.5.5.35
R1(config-mcast-pim)#exit
R1(config)#ip route 5.5.5.35 255.255.255.255 199.1.1.2
```

R2的配置如下：

```
R2(config)#interface gei-3/8
R2(config-if-gei-3/8)#ip address 199.1.1.2 255.255.255.0
R2(config-if-gei-3/8)#no shutdown
```

```
R2(config-if-gei-3/8)#exit
R2(config)#interface gei-3/7
R2(config-if-gei-3/7)#ip address 35.1.1.1 255.255.255.0
R2(config-if-gei-3/7)#no shutdown
R2(config-if-gei-3/7)#exit
R2(config)#interface loopback5
R2(config-if-loopback5)#ip address 5.5.5.35 255.255.255.255
R2(config-if-loopback5)#exit

R2(config)#ip multicast-routing
R2(config-mcast)#router pim
R2(config-mcast-pim)#static-rp 5.5.5.35
R2(config-mcast-pim)#interface gei-3/8
R2(config-mcast-pim-if-gei-3/8)#pimsm
R2(config-mcast-pim-if-gei-3/8)#exit
R2(config-mcast-pim)#interface gei-3/7
R2(config-mcast-pim-if-gei-3/7)#pimsm
R2(config-mcast-pim-if-gei-3/7)#dr-priority 20
R2(config-mcast-pim-if-gei-3/7)#exit

R2(config)#ip route 33.1.1.0 255.255.255.0 199.1.1.1
```

配置验证

在R1上通过**show ip pim interface**查看接口状态：

```
R1(config)#show ip pim interface
Address    Interface     State Nbr   Hello  DR        DR         PIM       Mode
                           Count Period Priority            Silent
33.1.1.1   gei-1/7       Up    0     30     20        33.1.1.1   Disabled   S
199.1.1.1  gei-1/3       Up    1     30     1         199.1.1.2  Disabled   S
```

在R1上通过**show ip pim neighbor**查看邻居状态：

```
R1(config)#show ip pim neighbor
Neighbor Address  Interface       DR Priority   Uptime     Expires    Ver
199.1.1.2         gei-1/3         1             00:07:48   00:01:23   V2
```

在R1上通过**show ip pim rp mapping**查看RP状态：

```
R1(config)#show ip pim rp mapping
Static RP is overriding in group-set!
Group(s): 224.0.0.0/4(SM)
  RP: 5.5.5.35, Static, Priority:192
Group(s): 0.0.0.0/0(NOUSED)
```

在R2上通过**show ip mroute**命令查看：

```
R2(config)#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(*, 225.10.0.1), RP: 5.5.5.35, TYPE: DYNAMIC, FLAGS:
   Incoming interface: NULL, flags:
   Outgoing interface list:
     gei-3/7, flags: F/S
(33.1.1.2, 225.10.0.1), TYPE: DYNAMIC, FLAGS:
   Incoming interface: gei-3/8, flags:
   Outgoing interface list:
     gei-3/7, flags: F/S
```

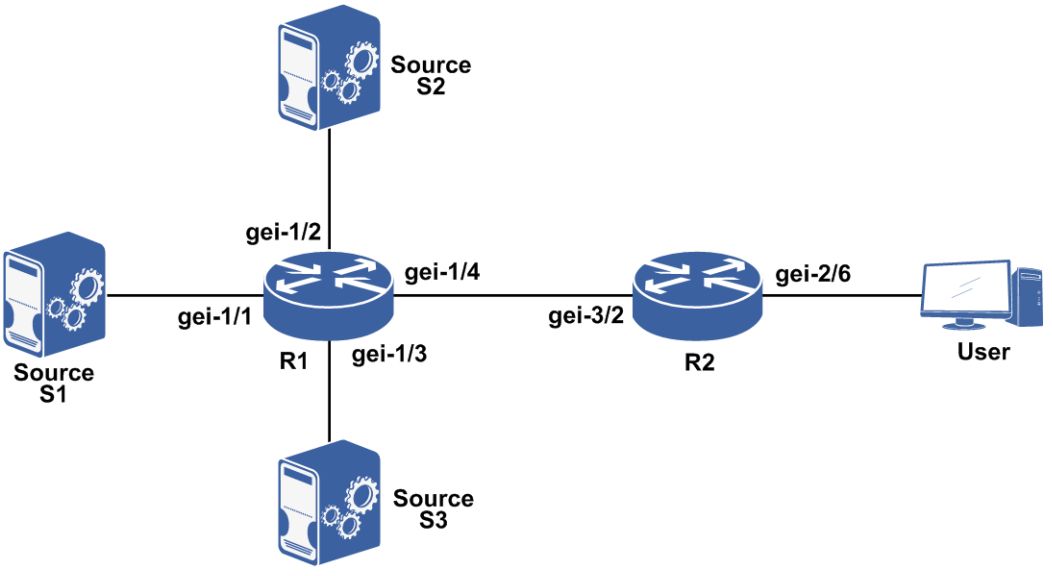
5.4.4 非法组播源控制配置实例

配置说明

组播协议规范中没有对组播源的合法性提供控制，任何用户都可以作为组播源向网络发送组播流量。可以通过配置非法组播源过滤来阻止未授权组播源向网络发送组播数据流。

如*图 5-12*所示，源S1在向用户发送组播数据；另外在网络中还存在两个非法组播源S2和S3向网络发送组播数据。为阻止S2和S3的数据在网络上传播，需要在第一跳路由器和RP配置非法源控制策略。

图 5-12 非法组播源控制配置实例示意图



非法源控制策略包括在第一跳路由器（first-hop router）上配置源过滤和在RP上配置源注册过滤：

- 在第一跳路由器配置源过滤可以尽早阻止非法源向网络发送组播数据。
- 在RP配置源注册过滤可以阻止非法源向RP注册。这种方式较为简便，且容易管理，但非法源的流量仍在第一跳与RP之间传递，且第一跳上的用户仍然可以接收到非法组播数据。

在实际应用中，应当结合使用这两种方式，将RP与第一跳路由器的职责做恰当分工，达到提高管理效率与控制网络安全性的目的。

配置思路

1.在第一跳路由器R1（first-hop router）上配置源过滤。

2.在RP上配置源注册过滤。

配置过程

按下表为R1、R2配置接口IP地址，确保IP连通性：

路由器	接口	IP地址	掩码
R1	gei-1/1	172.1.3.44	255.255.255.0
R1	gei-1/2	172.2.3.44	255.255.255.0
R1	gei-1/3	172.3.3.44	255.255.255.0
R1	gei-1/4	172.1.7.44	255.255.255.0
R2	gei-2/6	172.1.5.46	255.255.255.0
R2	gei-3/2	172.1.7.46	255.255.255.0
R2	loopback63	46.63.1.1	255.255.255.255

在R1-R2配置组播协议，以建立从源到用户的组播分发树，配置以PIM-SM为例。

R1的配置（在各接口使能PIM-SM协议）：

```
R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-1/1
R1(config-mcast-pim-if-gei-1/1)#pimsm
R1(config-mcast-pim-if-gei-1/1)#exit
R1(config-mcast-pim)#interface gei-1/2
R1(config-mcast-pim-if-gei-1/2)#pimsm
R1(config-mcast-pim-if-gei-1/2)#exit
R1(config-mcast-pim)#interface gei-1/3
R1(config-mcast-pim-if-gei-1/3)#pimsm
R1(config-mcast-pim-if-gei-1/3)#exit
R1(config-mcast-pim)#interface gei-1/4
R1(config-mcast-pim-if-gei-1/4)#pimsm
R1(config-mcast-pim-if-gei-1/4)#exit
R1(config-mcast-pim)#exit

R1(config)#router ospf 1
R1(config-ospf-1)#router-id 1.1.1.1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 172.1.3.0 0.0.0.255
R1(config-ospf-1-area-0)#network 172.2.3.0 0.0.0.255
R1(config-ospf-1-area-0)#network 172.3.3.0 0.0.0.255
R1(config-ospf-1-area-0)#network 172.1.7.0 0.0.0.255
R1(config-ospf-1-area-0)#exit
```

R2的配置（在各接口使能PIM-SM协议，并在loopback63接口配置BSR和RP）：

```
R2(config)#ip multicast-routing
R2(config-mcast)#router pim
R2(config-mcast-pim)#interface gei-3/2
R2(config-mcast-pim-if-gei-3/2)#pimsm
R2(config-mcast-pim-if-gei-3/2)#exit
R2(config-mcast-pim)#interface gei-2/6
R2(config-mcast-pim-if-gei-2/6)#pimsm
R2(config-mcast-pim-if-gei-2/6)#exit
R2(config-mcast-pim)#interface loopback63
R2(config-mcast-pim-if-loopback63)#pimsm
R2(config-mcast-pim-if-loopback63)#exit
R2(config-mcast-pim)#rp-candidate loopback63
R2(config-mcast-pim)#bsr-candidate loopback63
```

```
R2(config-mcast-pim)#exit
R2(config-mcast)#exit

R2(config)#router ospf 1
R2(config-ospf-1)#router-id 1.1.1.2
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 172.1.7.0 0.0.0.255
R2(config-ospf-1-area-0)#network 46.63.1.1 0.0.0.0
R2(config-ospf-1-area-0)#exit
```

在R1-R2配置非法源控制策略。

在R1配置源过滤策略：

```
R1(config)#ipv4-access-list aclUnwantedSource
R1(config-ipv4-acl)#rule deny ip 172.2.3.0 0.0.0.255 any
R1(config-ipv4-acl)#rule permit ip any any
R1(config-ipv4-acl)#exit
R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#data-filter aclUnwantedSource
```

在R2上配置源注册过滤策略：

```
R2(config)#ipv4-access-list aclWantedSource
R2(config-ipv4-acl)#rule deny ip 172.3.3.0 0.0.0.255 any
R2(config-ipv4-acl)#rule permit ip any any
R2(config-ipv4-acl)#exit
R2(config)#ip multicast-routing
R2(config-mcast)#router pim
R2(config-mcast-pim)#accept-register aclWantedSource
```

配置验证

在R1和R2上使用**show ip mroute**查看形成的组播路由条目。可以看到，由于在R1和R2上配置了非法源控制策略，使得只有合法源的组播数据可以转发到用户。查看用户接收到的组播流量，应该不包含非法源发送的组播数据。

根据以上配置，R1上仍然存在非法源S3的路由条目，但是因为RP配置了针对非法源S3的源注册过滤策略，因此S3的组播流量也不会到达最终用户。

R1上的路由条目：

```
R1#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(172.3.3.49, 234.254.254.255), RP: 46.63.1.1, TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-1/3, flags:
  Outgoing interface list:
    gei-1/4, flags: F/S
(172.1.3.49, 234.255.255.255), RP: 46.63.1.1, TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-1/1, flags:
  Outgoing interface list:
    gei-1/4, flags: F/S
```

R2上的路由条目：

```
R2#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(*, 234.254.254.255), RP: 46.63.1.1, TYPE: DYNAMIC, FLAGS:
  Incoming interface: NULL, flags:
  Outgoing interface list:
    gei-2/6, flags: F/S
(*, 234.255.254.255), RP: 46.63.1.1, TYPE: DYNAMIC, FLAGS:
```

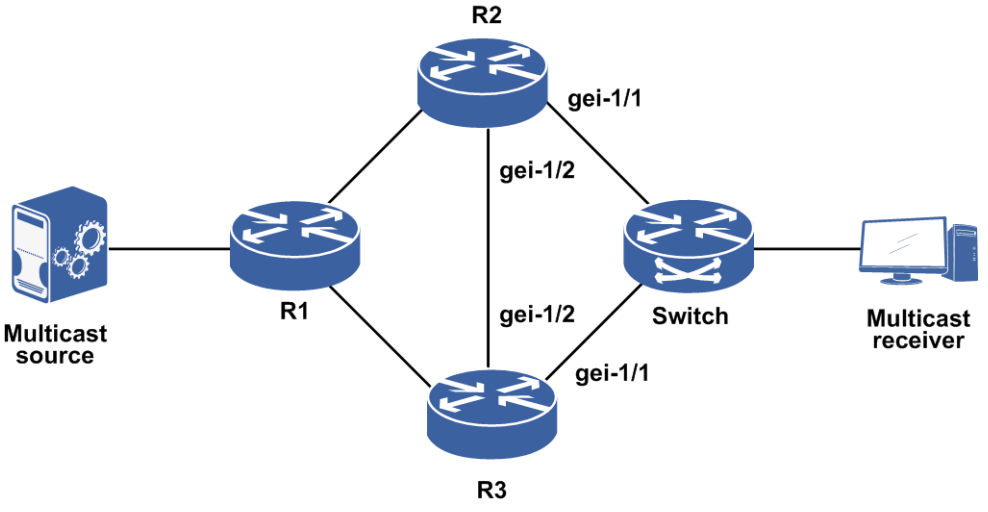
```
   Incoming interface: NULL, flags:
   Outgoing interface list:
     gei-2/6, flags: F/S
(*, 234.255.255.255), RP: 46.63.1.1, TYPE: DYNAMIC, FLAGS:
   Incoming interface: NULL, flags:
   Outgoing interface list:
     gei-2/6, flags: F/S
(172.1.3.49, 234.255.255.255), RP: 46.63.1.1, TYPE: DYNAMIC, FLAGS:
   Incoming interface: gei-3/2, flags:
   Outgoing interface list:
     gei-2/6, flags: F/S
```

5.4.5 anycast-rp 配置实例

配置说明

如*图 5-13*所示，在路由器R1、R2、R3上启用OSFP协议，配置anycast-rp。

图 5-13 anycast-rp 配置实例



配置思路

1.路由器R1、R2、R3上配置OSPF路由，单播R1和R2，R1和R3之间互通。

2.路由器R2和R3上配置PIM-SM协议，并且配置**anycast-rp**。

配置过程

R2上配置：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 11.1.1.2 255.255.255.0
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 12.1.1.2 255.255.255.0
R2(config-if-gei-1/2)#no shutdown
```

```
R2(config-if-gei-1/2)#exit
R2(config)#interface loopback64
R2(config-if-loopback64)#ip address 64.1.1.1 255.255.255.255
R2(config-if-loopback64)#exit

R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 11.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#network 12.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#exit

R2(config)#ip multicast-routing
R2(config-mcast)#router pim
R2(config-mcast-pim)#rp-candidate loopback64
R2(config-mcast-pim)#bsr-candidate loopback64
R2(config-mcast-pim)#anycast-rp-local gei-1/2    /*配置anycast-rp*/
R2(config-mcast-pim)#anycast-rp-peer 12.1.1.1
R2(config-mcast-pim)#interface gei-1/2
R2(config-mcast-pim-if-gei-1/2)#pimsm
R2(config-mcast-pim-if-gei-1/2)#exit
R2(config-mcast-pim)#interface gei-1/1
R2(config-mcast-pim-if-gei-1/1)#pimsm
R2(config-mcast-pim-if-gei-1/1)#exit
```

R3上配置如下：

```
R3(config)#interface gei-1/1
R3(config-if-gei-1/1)#ip address 11.1.1.1 255.255.255.0
R3(config-if-gei-1/1)#no shutdown
R3(config-if-gei-1/1)#exit
R3(config)#interface gei-1/2
R3(config-if-gei-1/2)#ip address 12.1.1.1 255.255.255.0
R3(config-if-gei-1/2)#no shutdown
R3(config-if-gei-1/2)#exit
R3(config)#interface loopback64
R3(config-if-loopback64)#ip address 64.1.1.1 255.255.255.255
R3(config-if-loopback64)#exit

R3(config)#router ospf 1
R3(config-ospf-1)#area 0
R3(config-ospf-1-area-0)#network 11.1.1.0 0.0.0.255
R3(config-ospf-1-area-0)#network 12.1.1.0 0.0.0.255
R3(config-ospf-1-area-0)#exit

R3(config)#ip multicast-routing
R3(config-mcast)#router pim
R3(config-mcast-pim)#rp-candidate loopback64
R3(config-mcast-pim)#bsr-candidate loopback64
R3(config-mcast-pim)#anycast-rp-local gei-1/2
R3(config-mcast-pim)#anycast-rp-peer 12.1.1.2  /*配置anycast-rp*/
R3(config-mcast-pim)#interface gei-1/2
R3(config-mcast-pim-if-gei-1/2)#pimsm
R3(config-mcast-pim-if-gei-1/2)#exit
R3(config-mcast-pim)#interface gei-1/1
R3(config-mcast-pim-if-gei-1/1)#pimsm
R3(config-mcast-pim-if-gei-1/1)#exit
```

交换机接口上参考路由器2、3 都启用PIM-SM协议。

配置验证

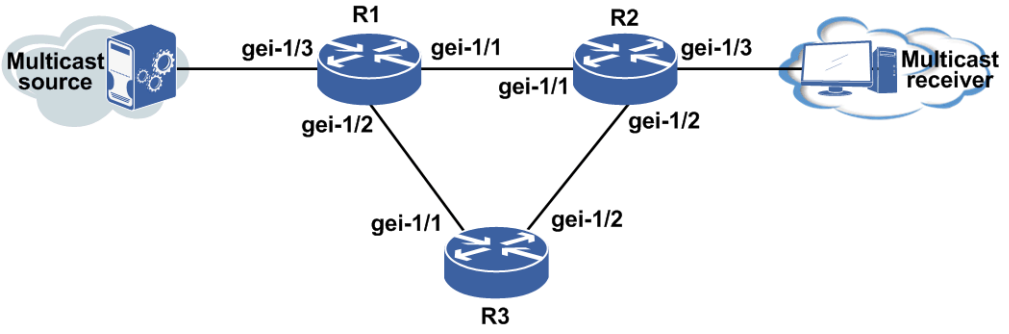
接收者加入组播组，从R2和R3中随机选择一个作为RP来转发注册报文，如果被选择的链路断链，流量从另一条链路上转发。

5.4.6 RPT-SPT 切换配置实例

配置说明

如*图 5-14*所示，实现RPT-SPT切换的组网。

图 5-14 RPT-SPT 切换配置实例示意图



配置思路

1.搭建环境，配置接口IP地址。

2.在所有接口下启用PIM-SM协议。

3.R3上将Loopback1接口配置为BSR和CRP。

4.R2上配置到源的单播路由，下一跳为gei-1/1，到RP的单播路由下一跳为接口gei-1/2。

5.R3上配置到源的单播路由，下一跳为gei-1/1。

6.R2上配置**spt-threshold infinity**。

7.接收端加入10个IGMP组。

8.组播源向这10个IGMP组发送组播流量。

9.查看各路由器上组播路由表生成情况。

10.R2上删除**spt-threshold infinity**。

11.查看各路由器上组播路由表生成情况。

配置过程

R1上接口IP配置：

```
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#ip address 1.1.1.1 255.255.255.0
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip address 2.1.1.1 255.255.255.0
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#exit
R1(config)#interface gei-1/3
```

```
R1(config-if-gei-1/3)#ip address 3.1.1.1 255.255.255.0
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#exit
```

R2上接口IP配置：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 1.1.1.2 255.255.255.0
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 4.1.1.1 255.255.255.0
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#exit
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#ip address 5.1.1.1 255.255.255.0
R2(config-if-gei-1/3)#no shutdown
R2(config-if-gei-1/3)#exit
```

R3上接口IP配置：

```
R3(config)#interface gei-1/1
R3(config-if-gei-1/1)#ip address 2.1.1.2 255.255.255.0
R3(config-if-gei-1/1)#no shutdown
R3(config-if-gei-1/1)#exit
R3(config)#interface gei-1/2
R3(config-if-gei-1/2)#ip address 4.1.1.2 255.255.255.0
R3(config-if-gei-1/2)#no shutdown
R3(config-if-gei-1/2)#exit
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 1.1.1.32 255.255.255.255
R3(config-if-loopback1)#exit
```

R2上配置到直连源和RP的单播路由：

```
R2(config)#ip route 3.1.1.0 255.255.255.0 1.1.1.1
R2(config)#ip route 1.1.1.32 255.255.255.255 4.1.1.2
```

R1上配置到RP的单播路由：

```
R1(config)#ip route 1.1.1.32 255.255.255.255 2.1.1.2
```

R3上配置到源的单播路由：

```
R3(config)#ip route 3.1.1.0 255.255.255.0 2.1.1.1
```

R1接口下启用PIMSM协议：

```
R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-1/3
R1(config-mcast-pim-if-gei-1/3)#pimsm
R1(config-mcast-pim-if-gei-1/3)#exit
R1(config-mcast-pim)#interface gei-1/2
R1(config-mcast-pim-if-gei-1/2)#pimsm
R1(config-mcast-pim-if-gei-1/2)#exit
R1(config-mcast-pim)#interface gei-1/3
R1(config-mcast-pim-if-gei-1/3)#pimsm
R1(config-mcast-pim-if-gei-1/3)#exit
```

R2接口下启用PIMSM协议，并配置**spt-threshold infinity**：

```
R2(config)#ip multicast-routing
R2(config-mcast)#router pim
R2(config-mcast-pim)#interface gei-1/1
R2(config-mcast-pim-if-gei-1/1)#pimsm
R2(config-mcast-pim-if-gei-1/1)#exit
R2(config-mcast-pim)#interface gei-1/2
R2(config-mcast-pim-if-gei-1/2)#pimsm
R2(config-mcast-pim-if-gei-1/2)#exit
R2(config-mcast-pim)#interface gei-1/3
R2(config-mcast-pim-if-gei-1/3)#pimsm
R2(config-mcast-pim-if-gei-1/3)#exit
```

```
R2(config-mcast-pim)#spt-threshold infinity
```

R3接口下启用PIMSM协议，并配置Loopback1为BSR和RP：

```
R3(config)#ip multicast-routing
R3(config-mcast)#router pim
R3(config-mcast-pim)#interface gei-1/1
R3(config-mcast-pim-if-gei-1/1)#pimsm
R3(config-mcast-pim-if-gei-1/1)#exit
R3(config-mcast-pim)#interface gei-1/2
R3(config-mcast-pim-if-gei-1/2)#pimsm
R3(config-mcast-pim-if-gei-1/2)#exit
R3(config-mcast-pim)#bsr-candidate loopback1
R3(config-mcast-pim)#rp-candidate loopback1
```

R2上删除**spt-threshold infinity**：

```
R2(config-mcast-pim)#no spt-threshold
```

配置验证

配置完成后，查看R1、R3上生成(S,G)，R2上只生成(*,G)。

当R2上删除**spt-threshold infinity**之后，查看R2上生成(S,G)：

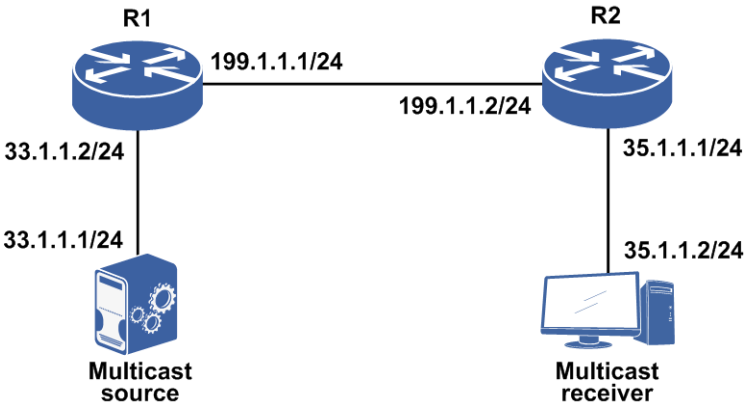
```
R2#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(*, 225.0.0.1), RP: 1.1.1.32, TYPE: DYNAMIC, FLAGS: NS
  Incoming interface: gei-1/2, flags: NS
  Outgoing interface list:
    gei-1/3, flags: F/S
(3.1.1.2, 225.0.0.1), TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-1/1, flags:
  Outgoing interface list:
    gei-1/3, flags: F/S
```

5.4.7 PIM-SM 与 PIM-DM 混合运行配置实例

配置说明

如*图 5-15*所示，R1和R2搭建PIM-SM和PIM-DM混合运行环境（使用静态RP和静态指定源加入）。

图 5-15 PIM-SM 与 PIM-DM 混合运行配置实例示意图



配置思路

1.配置相应接口地址。

2.进入组播模式。

3.进入PIM模式。

4.在相应接口下使能PIM-SM。

5.进入IGMP模式。

6.在相应接口下配置静态指定源组加入。

配置过程

R1上的配置：

```
R1(config)#interface gei-2/3
R1(config-if-gei-2/3)#ip address 199.1.1.1 255.255.255.0
R1(config-if-gei-2/3)#no shutdown
R1(config-if-gei-2/3)#exit
R1(config)#interface gei-2/4
R1(config-if-gei-2/4)#ip address 33.1.1.2  255.255.255.0
R1(config-if-gei-2/4)#no shutdown
R1(config-if-gei-2/4)#exit
R1(config)#interface loopback11
R1(config-if-loopback11)#ip address 1.1.1.11 255.255.255.255
R1(config-if-loopback11)#exit

R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#static-rp 1.1.1.11
R1(config-mcast-pim)#interface gei-2/3
R1(config-mcast-pim-if-gei-2/3)#pimsm
R1(config-mcast-pim-if-gei-2/3)#pimdm
R1(config-mcast-pim-if-gei-2/3)#exit
R1(config-mcast-pim)#interface gei-2/4
R1(config-mcast-pim-if-gei-2/4)#pimsm
R1(config-mcast-pim-if-gei-2/4)#pimdm
R1(config-mcast-pim-if-gei-2/4)#exit
R1(config-mcast-pim)#interface loopback11
R1(config-mcast-pim-if-loopback11)#pimsm
R1(config-mcast-pim-if-loopback11)#exit
R1(config-mcast-pim)#exit
```

R2的配置如下：

```
R2(config)#interface gei-2/7
R2(config-if-gei-2/7)#ip address 199.1.1.2 255.255.255.0
R2(config-if-gei-2/7)#no shutdown
R2(config-if-gei-2/7)#exit
R2(config)#interface gei-2/8
R2(config-if-gei-2/8)#ip address 35.1.1.1 255.255.255.0
R2(config-if-gei-2/8)#no shutdown
R2(config-if-gei-2/8)#exit

R2(config)#ip multicast-routing
R2(config-mcast)#router pim
R2(config-mcast-pim)#static-rp 1.1.1.11
R2(config-mcast-pim)#interface gei-2/7
R2(config-mcast-pim-if-gei-2/7)#pimsm
R2(config-mcast-pim-if-gei-2/7)#pimdm
R2(config-mcast-pim-if-gei-2/7)#exit
R2(config-mcast-pim)#interface gei-2/8
R2(config-mcast-pim-if-gei-2/8)#pimsm
R2(config-mcast-pim-if-gei-2/8)#pimdm
R2(config-mcast-pim-if-gei-2/8)#exit
R2(config-mcast-pim)#exit
R2(config-mcast)#router igmp
R2(config-mcast-igmp)#interface gei-2/8
R2(config-mcast-igmp-if-gei-2/8)#static-group 225.1.1.1 source 33.1.1.1
R2(config-mcast-igmp-if-gei-2/8)#exit
R2(config-mcast-igmp)#end

R2(config)#ip route 1.1.1.11 255.255.255.255 199.1.1.1
R2(config)#ip route 33.1.1.1 255.255.255.255 199.1.1.1
```

配置验证

在R1上通过**show ip pim mroute**查看PIM-SM路由条目：

```
R1(config)#show ip pim mroute
PIM Multicast Routing Table
Flags: T- SPT-bit set,A- Forward,J- Join SPT,U- Upsend,S- PIM-SM,D- PIM-DM,
Macro state: Ind- Pim Include Macro,Exd- Pim Exclude Macro,
     Jns- Pim Joins Macro,LAst- Pim Lost_assert Macro,
     Imo- Pim Immediate_olist Macro,Ino- Pim Inherited_olist Macro,
     Lcd- Pim Local_receiver_include Macro
Timers:Uptime/Expires(Upstream State)
(33.1.1.1, 225.1.1.1), 00:59:00/00:00:00(JOINED)/00:00:00,
 Reg:NO INFO; RP:1.1.1.11; RT:NULL;
MSDP: TO BE ADV ;
   Ind:0/Exd:0/Jns:1/LAst:0/Imo:1/Ino:1
   Iif:gei-2/4, RPF nbr:0.0.0.0(S); AT
     RPF nbr:0.0.0.0(D); 00:00:00(FORWARD);
    Oif:
    gei-2/3 ,   JoinsSG  /  InoSG  /  DenseOlist
```

在R1上通过**show ip mroute**查看MR路由条目：

```
R1(config)#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(33.1.1.1, 225.1.1.1), TYPE: DYNAMIC, FLAGS:
   Incoming interface: gei-2/4, flags:
   Outgoing interface list:
     gei-2/3, flags: F/S
```

在R2上通过**show ip pim mroute**查看PIM路由条目：

```
R2(config)#show ip pim mroute
PIM Multicast Routing Table
```

```
Flags: T- SPT-bit set,A- Forward,J- Join SPT,U- Upsend,S- PIM-SM,D- PIM-DM,
Macro state: Ind- Pim Include Macro,Exd- Pim Exclude Macro,
     Jns- Pim Joins Macro,LAst- Pim Lost_assert Macro,
     Imo- Pim Immediate_olist Macro,Ino- Pim Inherited_olist Macro,
     Lcd- Pim Local_receiver_include Macro
Timers:Uptime/Expires(Upstream State)
(33.1.1.1, 225.1.1.1), 01:05:41/00:00:52(JOINED)/00:00:00,
 Reg:NO INFO; RP: 1.1.1.11; RT:NULL;
  Ind:1/Exd:0/Jns:0/LAst:0/Imo:0/Ino:0
  Iif: gei-2/7 , RPF nbr:199.1.1.1(S); AT
      RPF nbr: 199.1.1.1 (D); 00:00:00(FORWARD);
  Oif:
    gei-2/8,   LocalInSG  /  DenseOlist  /  DenseAstWSG
```

在R2上通过**show ip mroute**查看MR路由条目：

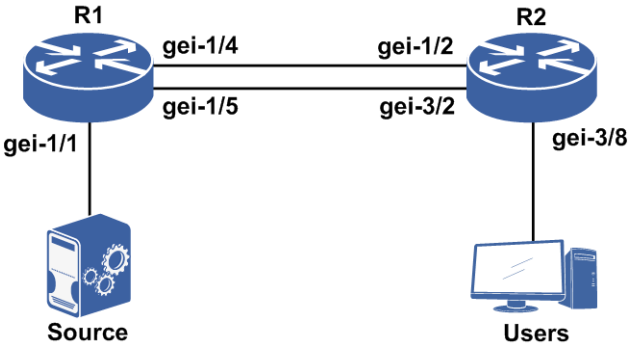
```
R2(config)#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(33.1.1.1, 225.1.1.1), TYPE: DYNAMIC, FLAGS:
   Incoming interface: gei-2/7, flags:
   Outgoing interface list:
     gei-2/8, flags: F/S
```

5.4.8 PIM-SM 组播负荷分担配置实例

配置说明

源到最后一跳路由器之间存在多条等价路径时，可以通过配置组播负荷分担，使流量沿不同路径到达用户（接受端）。如*图 5-16*所示，源S向用户发送多个组的组播流量；且最后一跳路由器（Last-hop Router）R2到源S存在两条路径。

图 5-16 组播负荷分担配置实例示意图



路由器上各个接口的地址如下。

路由器	接口	IP地址	掩码
R1	gei-1/1	172.1.3.44	255.255.255.0
R1	gei-1/4	172.1.7.44	255.255.255.0
R1	gei-1/5	172.1.13.44	255.255.255.0
R1	loopback63	44.63.1.1	255.255.255.255

路由器	接口	IP地址	掩码
R2	gei-3/2	172.1.13.46	255.255.255.0
R2	gei-3/8	172.1.5.46	255.255.255.0
R2	gei-1/2	172.1.7.46	255.255.255.0

假设对于R2，这两条路径的代价是相等的，即这两条路径是最后一跳路由器R2和源之间的等价路径，即可以通过在R2上配置组播负荷分担使不同组的组播流量沿着两条路径到达用户。

配置思路

1.各路由器配置PIM-SM协议及BSR、RP，使用户可以正常接收源下发的组播流量。

2.在R2路由器上配置组播负荷分担。

配置过程

在R1和R2上配置组播协议，以建立从源到用户的组播分发树。

R1的配置（在各接口使能PIM-SM协议，并在loopback63接口配置BSR与CRP）如下：

```
R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-1/1
R1(config-mcast-pim-if-gei-1/1)#pimsm
R1(config-mcast-pim-if-gei-1/1)#exit
R1(config-mcast-pim)#interface gei-1/4
R1(config-mcast-pim-if-gei-1/4)#pimsm
R1(config-mcast-pim-if-gei-1/4)#exit
R1(config-mcast-pim)#interface gei-1/5
R1(config-mcast-pim-if-gei-1/5)#pimsm
R1(config-mcast-pim-if-gei-1/5)#exit

R1(config-mcast-pim)#bsr-candidate loopback63
R1(config-mcast-pim)#rp-candidate loopback63
```

R2的配置（在各接口使能PIM-SM协议，并配置到BSR、CRP的路由，使其可以正确接收BSR消息、建立组播路由表；配置到源的路由，使源与最后一跳路由器R2之间存在两条等代价路径）如下：

```
R2(config-mcast-pim)#interface gei-1/2
R2(config-mcast-pim-if-gei-1/2)#pimsm
R2(config-mcast-pim-if-gei-1/2)#exit
R2(config-mcast-pim)#interface gei-3/8
R2(config-mcast-pim-if-gei-3/8)#pimsm
R2(config-mcast-pim-if-gei-3/8)#exit
R2(config-mcast-pim)#interface gei-3/2
R2(config-mcast-pim-if-gei-3/2)#pimsm
R2(config-mcast-pim-if-gei-3/2)#exit

R2(config)#ip route 44.63.1.1 255.255.255.255 172.1.7.44
R2(config)#ip route 172.1.3.0 255.255.255.0 172.1.7.44
R2(config)#ip route 172.1.3.0 255.255.255.0 172.1.13.44

/*最后在R2配置启用负荷分担，以s-g-hash为例*/
```

```
R2(config)#ip multicast-routing
R2(config-mcast)#multipath s-g-hash basic
R2(config-mcast)#exit
```

配置验证

当用户开始接收源S发送的组播流量时，查看R1和R2上的组播路由表，注意路由条目的出入接口。

R1的组播路由表如下：

```
R1#show ip mroute
   IP Multicast Routing Table
(*, 238.255.255.0), RP: 44.63.1.1, TYPE: DYNAMIC, FLAGS:
   Incoming interface: NULL, flags:
   Outgoing interface list:
     gei-1/4, flags: F
(172.1.3.49, 238.255.255.0), RP: 44.63.1.1, TYPE: DYNAMIC, FLAGS:
   Incoming interface: gei-1/1, flags:
   Outgoing interface list:
     gei-1/5, flags: F
(*, 238.255.255.1), RP: 44.63.1.1, TYPE: DYNAMIC, FLAGS:
   Incoming interface: NULL, flags:
   Outgoing interface list:
     gei-1/4, flags: F
(172.1.3.49, 238.255.255.1), RP: 44.63.1.1, TYPE: DYNAMIC, FLAGS:
   Incoming interface: gei-1/1, flags:
   Outgoing interface list:
     gei-1/5, flags: F
```

查看R2的组播路由表如下：

```
R2#show ip mroute

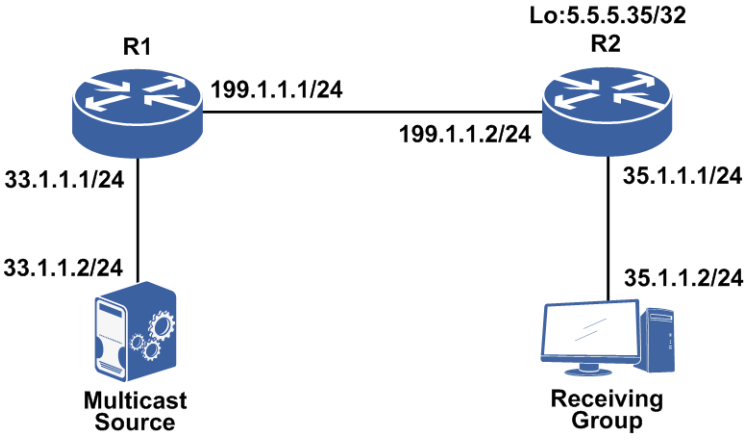
IP Multicast Routing Table
(*, 238.255.255.0), RP: 44.63.1.1, TYPE: DYNAMIC, FLAGS: NS
   Incoming interface: gei-3/2, flags: NS
   Outgoing interface list:
     gei-2/8, flags: F
(172.1.3.49, 238.255.255.0), RP: 44.63.1.1, TYPE: DYNAMIC, FLAGS:
   Incoming interface: gei-1/2, flags:
   Outgoing interface list:
     gei-2/8, flags: F
(*, 238.255.255.1), RP: 44.63.1.1, TYPE: DYNAMIC, FLAGS: NS
   Incoming interface: gei-3/2, flags: NS
   Outgoing interface list:
     gei-2/8, flags: F
(172.1.3.49, 238.255.255.1), RP: 44.63.1.1, TYPE: DYNAMIC, FLAGS:
   Incoming interface: gei-1/2, flags:
   Outgoing interface list:
     gei-2/8, flags:
```

5.4.9 PIM-SM BFD 配置实例

配置说明

如*图 5-17*所示，配置BFD关联PIM。

图 5-17 PIM BFD 配置实例拓扑图



配置思路

1.配置相应接口地址。

2.进入组播配置模式。

3.进入PIM配置模式。

4.配置R2的loopback5接口为CRP和BSR。

5.进入接口启动PIM-SM。

6.在组播PIM模式的接口下，启用BFD。

配置过程

R1的配置如下：

```
R1(config)#interface gei-2/3
R1(config-if-gei-2/3)#ip address 199.1.1.1 255.255.255.0
R1(config-if-gei-2/3)#no shutdown
R1(config-if-gei-2/3)#exit
R1(config)#interface gei-2/7
R1(config-if-gei-2/7)#ip address 33.1.1.1 255.255.255.0
R1(config-if-gei-2/7)#no shutdown
R1(config-if-gei-2/7)#exit

R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-2/3
R1(config-mcast-pim-if-gei-2/3)#pimsm
R1(config-mcast-pim-if-gei-2/3)#bfd-enable
R1(config-mcast-pim-if-gei-2/3)#exit
R1(config-mcast-pim)#interface gei-2/7
R1(config-mcast-pim-if-gei-2/7)#pimsm
R1(config-mcast-pim-if-gei-2/7)#dr-priority 20
R1(config-mcast-pim-if-gei-2/7)#exit
```

R2的配置如下：

```
R2(config)#interface gei-3/8
R2(config-if-gei-3/8)#ip address 199.1.1.2 255.255.255.0
R2(config-if-gei-3/8)#no shutdown
```

```
R2(config-if-gei-3/8)#exit
R2(config)#interface gei-3/7
R2(config-if-gei-3/7)#ip address 35.1.1.1 255.255.255.0
R2(config-if-gei-3/7)#no shutdown
R2(config-if-gei-3/7)#exit
R2(config)#interface loopback5
R2(config-if-loopback5)#ip address 5.5.5.35 255.255.255.255
R2(config-if-loopback5)#exit

R2(config)#ip multicast-routing
R2(config-mcast)#router pim
R2(config-mcast-pim)#interface gei-3/8
R2(config-mcast-pim-if-gei-3/8)#pimsm
R2(config-mcast-pim-if-gei-3/8)#bfd-enable
R2(config-mcast-pim-if-gei-3/8)#exit
R2(config-mcast-pim)#interface gei-3/7
R2(config-mcast-pim-if-gei-3/7)#pimsm
R2(config-mcast-pim-if-gei-3/7)#dr-priority 20
R2(config-mcast-pim-if-gei-3/7)#exit
```

配置验证

在R1上通过**show ip pim interface**查看接口状态：

```
R1(config)#show ip pim interface
Address      Interface   State Nbr   Hello  DR        DR       PIM     Mode
                               Count  Period    Priority  Silent
33.1.1.1     gei-2/7      Up    0     30     20       33.1.1.1  Disabled S
199.1.1.1    gei-2/3      Up    1     30     1        199.1.1.2 Disabled S
```

在R1上通过**show ip pim neighbor**查看邻居状态：

```
R1(config)#show ip pim neighbor
Neighbor Address   Interface      DR Priority    Uptime    Expires   Ver
199.1.1.2         gei-2/3        1             00:07:48   00:01:23  V2
```

在R1上通过**show ip pim bfd**查看BFD邻居状态：

```
R1 config)#show ip pim bfd
Interface    BFD Local_Addr   BFD Peer_Addr    State
gei-2/3     199.1.1.1(BDR)    199.1.1.2DR)     UP
```

在R1上通过**show bfd neighbor ip brief**查看BFD状态：

```
R1(config)#show bfd neighbor ip brief
LocalAddr       PeerAddr       LD       RD       Hold   State    Interface
199.1.1.1       199.1.1.2      2053      2054     150    UP       gei-2/3

R1(config)#show bfd neighbor ip detail
------------------------------------------------------------------------------
LocalAddr: 199.1.1.1
PeerAddr : 199.1.1.2
Local Discr:2053          Remote Discr:2054           State:UP
Holdown(ms):150           Interface: gei-2/3
Vpnid:0                  VRF Name:---
BFD Type:SingleHop
Instance Name:
------------------------------------------------------------------------------
Version:1               Dest UDP Port:3784       Final Bit:1
Local Diag:0            Demand Mode:0            Poll Bit:0
MinTxInt:50             MinRxInt:50              Multiplier:3
Received MinTxInt:50     Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24        Max BFD Length:24
```

```
Rx Count:4352           Rx Interval (ms) min/max/avg:30    /100   /59
Tx Count:4159           Tx Interval (ms) min/max/avg:50    /120   /59
Registered Protocols:PIM
Uptime:0 day(s),0 hour(s),6 minute(s)
Control Plane Rcv Phy Interface Name: gei-2/3
============================================================================
```

在R2上通过**show ip pim neighbor**查看邻居状态：

```
R2(config)#show ip pim neighbor
Neighbor Address  Interface       DR Priority    Uptime    Expires   Ver
199.1.1.1        gei-3/8         1             00:07:48   00:01:23  V2
```

在R2上通过**show ip pim bfd**查看BFD邻居状态：

```
R2config)#show ip pim bfd
Interface     BFD Local_Addr   BFD Peer_Addr    State
gei-3/8     199.1.1.2(DR)     199.1.1.1BDR)     UP
```

在R2上通过**show bfd neighbor ip brief**查看BFD状态：

```
R2(config)#show bfd neighbor ip brief
LocalAddr       PeerAddr       LD       RD       Hold   State     Interface
199.1.1.2       199.1.1.1       2055     2054     150    UP        gei-3/8

R2(config)#show bfd neighbor ip detail
----------------------------------------------------------------------------
LocalAddr: 199.1.1.2
PeerAddr : 199.1.1.1
Local Discr:2055          Remote Discr:2054           State:UP
Holdown(ms):150           Interface: gei-3/8
Vpnid:0                  VRF Name:---
BFD Type:SingleHop
Instance Name:
----------------------------------------------------------------------------
Version:1               Dest UDP Port:3784       Final Bit:1
Local Diag:0             Demand Mode:0           Poll Bit:0
MinTxInt:50             MinRxInt:50             Multiplier:3
Received MinTxInt:50     Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24        Max BFD Length:24

Rx Count:804            Rx Interval (ms) min/max/avg:40    /100   /59
Tx Count:813            Tx Interval (ms) min/max/avg:40    /80    /59
Registered Protocols:PIM
Uptime:0 day(s),0 hour(s),1 minute(s)
Control Plane Rcv Phy Interface Name: gei-3/8
============================================================================
```

5.5 PIM-SSM

PIM-SSM具有PIM–SM协议的所有优点，只是不建立共享树，只建立基于源的最短路径树。在收到某个特定的源到组的成员关系报告消息时直接建立最短路径树。

PIM-SSM是PIM-SM的一个子集，PIM-SSM适合于well known源，在域内和域间都有效。PIM-SM使用域间组播路由协议MSDP，而PIM-SSM不需要使用。

5.5.1 配置 PIM-SSM

本节介绍PIM-SSM功能的配置步骤和命令。

1.配置启用PIM-SSM协议。

命令	功能
inspur(config-mcast-pim)#**ssm enable**	启用SSM协议

2.配置SSM组地址范围。

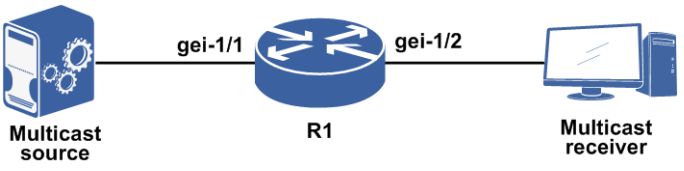
命令	功能
inspur(config-mcast-pim)#**ssm range** {**default** | **group-list** <*access-list-name*>}	配置SSM组地址范围

5.5.2 PIM-SSM 配置实例

配置说明

如*图 5-18*所示，R1上启用PIM协议，并且使能ssm，配置ssm组的范围（默认为232.0.0.0/8），IGMP协议版本启用v3，发送指定源动态组加入，组播源向多个指定源的组播组发流，只有源地址和组播组地址都匹配的流量能通。

图 5-18 PIM-SSM 配置实例



配置思路

1.接口模式下，配置路由器的gei-1/1、gei-1/2接口地址。

2.打开组播模块的总开关**ip multicast-routing**。

3.进入PIM路由模式，配置**ssm enable**和**ssm range default**。

4.进入接口gei-1/1和gei-1/2，开启PIM-SM协议。

5.进入IGMP路由模式，再进入所要配置的接口。

6.在接收组上发送指定源的动态组加入。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 10.0.0.1 255.255.255.0
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip address 30.0.0.1 255.255.255.0
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#exit

R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-1/1
R1(config-mcast-pim-if-gei-1/1)#pimsm
R1(config-mcast-pim-if-gei-1/1)#exit
R1(config-mcast-pim)#interface gei-1/2
R1(config-mcast-pim-if-gei-1/2)#pimsm
R1(config-mcast-pim-if-gei-1/2)#exit

R1(config-mcast-pim)#ssm enable
R1(config-mcast-pim)#ssm range default
R1(config-mcast-pim)#exit
R1(config-mcast)#router igmp
R1(config-mcast-igmp)#interface gei-1/2
R1(config-mcast-igmp-if-gei-1/2)#version 3
R1(config-mcast-igmp-if-gei-1/2)#exit
```

配置验证

R1上查看配置信息：

```
R1#show running-config multicast
!<multicast>
ip multicast-routing
  router pim
    ssm enable
    ssm range default
    interface gei-1/2
      pimsm
    $
    interface gei-1/1
      pimsm
    $
  $
  router igmp
    interface gei-1/1
      version 3
    $
  $
$
!</multicast>
```

R1上查看生效情况：

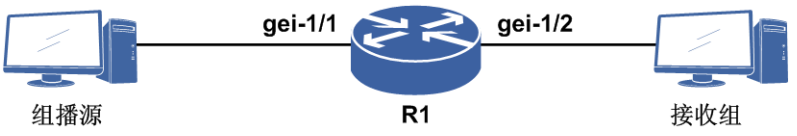
```
R1#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(10.0.0.2, 232.0.0.1), RP: 0.0.0.0, TYPE: DYNAMIC, FLAGS: NS
   Incoming interface: gei-1/1, flags: NS
   Outgoing interface list:
     gei-1/2, flags: F   /*生成（S,G）条目*/
```

5.5.3 SSM-Mapping 配置实例

配置说明

如*图 5-19*所示，R1上启用PIM协议、启用SSM功能，配置SSM组的范围（默认为232.0.0.0/8）。IGMP协议版本启用v2，同时配置**ssm-mapping**，指定特定范围组向源地址的映射，发送指定源动态组加入，只有**ssm-mapping**中配置的组可以直接形成（S，G）表项。

图 5-19 SSM-Mapping 功能组网示意图



配置思路

1.配置ACL，指定特定组。

2.接口模式下，配置R1的gei-1/1、gei-1/2接口地址。

3.打开组播模块的总开关**ip multicast-routing**。

4.进入PIM路由模式，配置**ssm enable**和**ssm range group-list ssm**。

5.进入接口gei-1/1和gei-1/2，开启PIM-SM协议。

6.进入IGMP路由模式，再进入所要配置的接口。

7.配置**ssm-mapping**功能。

配置过程

R1的配置如下：

```
/*ACL相关配置*/
R1(config)#ipv4-access-list ssm
R1(config-ipv4-acl)#rule 1 permit 225.0.0.1  /*配置特定组，ACL名称为ssm*/
R1(config-ipv4-acl)#!
/*接口相关配置*/
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 10.0.0.1 255.255.255.0
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip address 30.0.0.1 255.255.255.0
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#exit
R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-1/1
R1(config-mcast-pim-if-gei-1/1)#pimsm
R1(config-mcast-pim-if-gei-1/1)#exit
R1(config-mcast-pim)#interface gei-1/2
R1(config-mcast-pim-if-gei-1/2)#pimsm
```

```
R1(config-mcast-pim-if-gei-1/2)#exit
R1(config-mcast-pim)#ssm enable
R1(config-mcast-pim)#ssm range group-list ssm
R1(config-mcast-pim)#exit
R1(config-mcast)#router igmp
R1(config-mcast-igmp)#interface gei-1/2
R1(config-mcast-igmp-if-gei-1/2)#ssm-map static group-list ssm 30.0.0.2
/*配置 acl ssm中制定的组对应的源地址为3.3.3.3*/
R1(config-mcast-igmp-if-gei-1/2)#exit
```

配置验证

从接受组发送IGMPv2的组加入，组为225.0.0.1和225.0.0.2。在R1设备上查看组播路由表项，此时只有225.0.0.1生成了（S，G）表项没有（*，G）表，而225.0.0.2组只生成了（*，G），因为没有指定源信息。

R1上查看IGMP接口信息：

```
R1(config)#show ip mroute

IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(30.0.0.2, 225.0.0.1)
  TYPE: DYNAMIC, FLAGS: F
  Incoming interface: gei-1/2, flags: F
  Outgoing interface list:
   gei-1/1, flags: F/S  /*只有制定的组生成了SG表项，而没有*G表项*/

(*, 225.0.0.2)
  TYPE: DYNAMIC, FLAGS:
  RP: 100.0.5.1
  Incoming interface: NULL, flags:
  Outgoing interface list:
gei-1/1, flags: F/S
```

5.6 组播负荷分担

路由设备IP报文转发的依据是IP路由表，路由表中的一个目的前缀（prefix）可能具有多条路径时，这些路径的优先级可能相同或不同。路由设备总是选择到具有最高优先级的路由作为活动路径，当有多条路径都具有最高优先级时，则可以将到该目的前缀的流量均衡地分配在多条路径上，以达到负荷分担地目的。

在组播应用中，三层组播负荷分担的原理同普通路由负荷分担类似

5.6.1 配置组播负荷分担

本节介绍组播负荷分担功能的配置步骤和命令。

1.配置组播负荷分担。

步骤	命令	功能

步骤	命令	功能
1	inspur(config-mcast)#**multipath**	启用负荷分担，使用基于源地址的哈希算法
2	inspur(config-mcast)#**multipath s-g-hash basic**	启用负荷分担，使用基于源地址、组播地址的哈希算法
	inspur(config-mcast)#**multipath s-g-hash next-hop-based**	启用负荷分担，使用基于下一跳的哈希算法

2.验证配置结果。

命令	功能
inspur#**show ip mroute nexthop** [**vrf** <*vrf-name*>][<*destination-address*>]	显示组播下一跳及ECMP信息

5.6.2 组播负荷分担配置实例

参见PIM-DM和PIM-SM中的负荷分担配置实例。

5.7 MSDP

MSDP是一种用于连接多个PIM域的协议，工作在TCP协议之上，为PIM-SM提供PIM域外的组播源信息。

5.7.1 配置 MSDP

本节介绍配置MSDP功能，用于组播源的邻居发现。

1.启用MSDP。

命令	功能
inspur(config-mcast)#**router msdp**	启用IP组播协议MSDP

2.配置MSDP邻居。

步骤	命令	功能
1	inspur(config-mcast-msdp)#**peer** <*peer-address*>	配置MSDP邻居，执行后进入PEER配置模式
2	inspur(config-mcast-msdp)#**default-peer** <*peer-address*>[**list** <*access-list-name*>]	定义一个默认MSDP邻居，本地路由器将接收来自这个邻居的所

步骤	命令	功能
		有SA消息
3	inspur(config-mcast-msdp-peer)#**mesh-group** <*mesh-name*>	配置指定的MSDP邻居为某**mesh group**成员，缺省MSDP邻居不属于任何**mesh group**

3.配置MSDP扩展功能。

命令	功能
inspur(config-mcast-msdp)#**originator-id** <*interface-name*>	把指定接口的IP地址用作SA消息中的RP地址
inspur(config-mcast-msdp-peer)#**description** <*desc-text*>	给MSDP邻居添加说明性描述
inspur(config-mcast-msdp-peer)#**sa-limit** <*sa-limit*>	限制SA cache表中来自于指定MSDP邻居的SA消息数量，范围1~2147483646，缺省为没有限制
inspur(config-mcast-msdp-peer)#**ttl-threshold** <*ttl-value*>	限制组播数据包封装在SA报文中发送给MSDP邻居的范围，TTL值的范围1~255

4.配置MSDP策略。

命令	功能
inspur(config-mcast-msdp)#**connect-source** <*interface-name*>	配置TCP连接的源IP地址
inspur(config-mcast-msdp)#**redistribute** [**list** <*access-list-name*>]	配置ACL规则，满足该规则的（S，G）组播路由条目才会出现在由MSDP邻居产生的SA消息中
inspur(config-mcast-msdp-peer)#**sa-filter in** [**list** <*access-list-name*>]	配置对来自指定MSDP邻居的SA消息进行过滤
inspur(config-mcast-msdp-peer)#**sa-filter out** [**list** <*access-list-name*>]	配置对向指定MSDP邻居发送的SA消息进行过滤

5.验证配置结果。

命令	功能
inspur#**show ip msdp peer** [<*peer-address*>]	显示MSDP邻居的详细信息
inspur#**show ip msdp sa-cache** [<*group-address*>|[<*source-address*>]]	显示来自各MSDP邻居的（S，G）状态
inspur#**show ip msdp summary**	显示MSDP邻居状态
inspur#**show ip msdp count**	显示SA消息产生的源/组播组数量和SA cache中来自每个MSDP

命令	功能
	邻居的SA消息数量

6.维护MSDP。

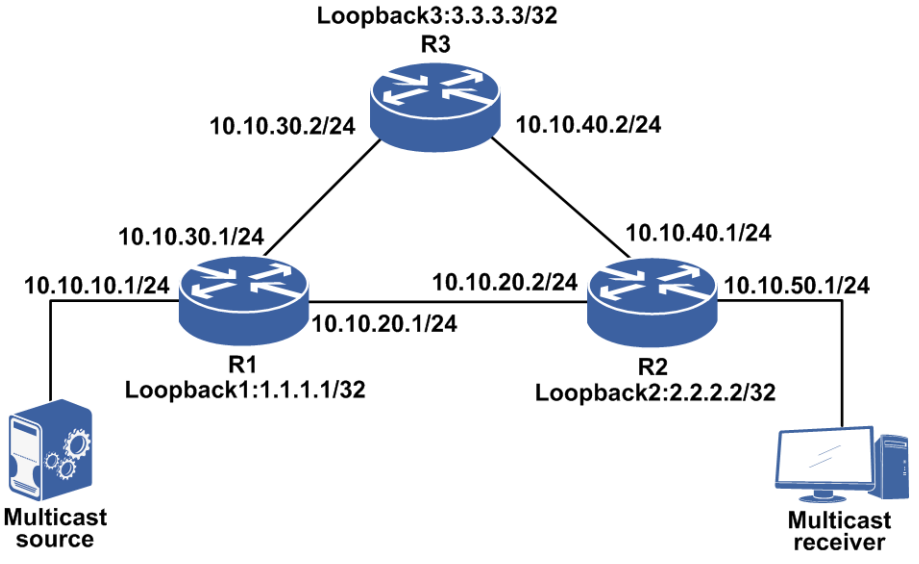
命令	功能
inspur#**clear ip msdp peer** [<*peer-address*>]	清除与所有或指定MSDP邻居建立的TCP连接
inspur#**clear ip msdp sa-cache** [<*group-address*>]	清除MSDP SA cache项
inspur#**clear ip msdp statistics** [<*peer-address*>]	清除MSDP邻居的统计数据，但并不重置MSDP会话

5.7.2 MSDP 基本配置实例

配置说明

如*图 5-20*所示，配置R1、R3在同一PIM-SM组播域，R2属于另一PIM-SM组播域，通过MSDP实现两个PIM-SM域组播数据流互通。

图 5-20 MSDP 基本配置实例



配置思路

1.启用PIM-SM组播功能并配置候选BSR、RP。

2.运用OSPF等单播路由导通互相之间的路由。

3.使能MSDP并建立对等体，组播源发送组播流，当组播接收者发相应的组播组加入

消息时，流量互通。

配置过程

R1的配置：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
R1(config-if-loopback1)#exit

R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#rp-candidate loopback1 priority 10
R1(config-mcast-pim)#bsr-candidate loopback1 priority 10
R1(config-mcast-pim)#interface loopback1
R1(config-mcast-pim-if-loopback1)#pimsm
R1(config-mcast-pim-if-loopback1)#exit
R1(config-mcast-pim)#exit
R1(config-mcast)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 10.10.10.1 255.255.255.0
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip address 10.10.20.1 255.255.255.0
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#exit
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#ip address 10.10.30.1 255.255.255.0
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#exit

R1(config)#router ospf 1
R1(config-ospf-1)#router-id 1.1.1.1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 10.10.10.0 0.0.0.255
R1(config-ospf-1-area-0)#network 10.10.20.0 0.0.0.255
R1(config-ospf-1-area-0)#network 10.10.30.0 0.0.0.255
R1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
R1(config-ospf-1-area-0)#exit

R1(config)#ip multicast-routing
R1(config-mcast)#router msdp
R1(config-mcast-msdp)#peer 10.10.20.2
R1(config-mcast-msdp-peer)#connect-source gei-1/2
R1(config-mcast-msdp-peer)#exit

R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-1/1
R1(config-mcast-pim-if-gei-1/1)#pimsm
R1(config-mcast-pim-if-gei-1/1)#exit
R1(config-mcast-pim)#interface gei-1/2
R1(config-mcast-pim-if-gei-1/2)#pimsm
R1(config-mcast-pim-if-gei-1/2)#bsr-border
R1(config-mcast-pim-if-gei-1/2)#exit
R1(config-mcast-pim)#interface gei-1/3
R1(config-mcast-pim-if-gei-1/3)#pimsm
R1(config-mcast-pim-if-gei-1/3)#exit
R1(config-mcast-pim)#exit
R1(config-mcast)#exit
```

R2的配置：

```
R2(config)#interface loopback2
R2(config-if-loopback2)#ip address 2.2.2.2 255.255.255.255
R2(config-if-loopback2)#exit
```

```
R2(config)#ip multicast-routing
R2(config-mcast)#router pim
R2(config-mcast-pim)#rp-candidate loopback2 priority 20
R2(config-mcast-pim)#bsr-candidate loopback2 priority 20
R2(config-mcast-pim)#interface loopback2
R2(config-mcast-pim-if-loopback2)#pimsm
R2(config-mcast-pim-if-loopback2)#exit
R2(config-mcast-pim)#exit
R2(config-mcast)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 10.10.20.2 255.255.255.0
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#exit
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#ip address 10.10.40.1 255.255.255.0
R2(config-if-gei-1/3)#no shutdown
R2(config-if-gei-1/3)#exit
R2(config)#interface gei-1/4
R2(config-if-gei-1/4)#ip address 10.10.50.1 255.255.255.0
R2(config-if-gei-1/4)#no shutdown
R2(config-if-gei-1/4)#exit

R2(config)#router ospf 1
R2(config-ospf-1)#router-id 2.2.2.2
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 10.10.20.0 0.0.0.255
R2(config-ospf-1-area-0)#network 10.10.40.0 0.0.0.255
R2(config-ospf-1-area-0)#network 10.10.50.0 0.0.0.255
R2(config-ospf-1-area-0)#network 2.2.2.2 0.0.0.0
R2(config-ospf-1-area-0)#exit

R2(config)#ip multicast-routing
R2(config-mcast)#router msdp
R2(config-mcast-msdp)#peer 10.10.20.1
R2(config-mcast-msdp-peer)#connect-source gei-1/2
R2(config-mcast-msdp-peer)#exit

R2(config-mcast)#router pim
R2(config-mcast-pim)#interface gei-1/2
R2(config-mcast-pim-if-gei-1/2)#pimsm
R2(config-mcast-pim-if-gei-1/2)#bsr-border
R2(config-mcast-pim-if-gei-1/2)#exit
R2(config-mcast-pim)#interface gei-1/3
R2(config-mcast-pim-if-gei-1/3)#pimsm
R2(config-mcast-pim-if-gei-1/3)#bsr-border
R2(config-mcast-pim-if-gei-1/3)#exit
R2(config-mcast-pim)#interface gei-1/4
R2(config-mcast-pim-if-gei-1/4)#pimsm
R2(config-mcast-pim-if-gei-1/4)#exit
R2(config-mcast-pim)#exit
R2(config-mcast)#exit
```

R3的配置：

```
R3(config)#interface loopback3
R3(config-if-loopback3)#ip address 3.3.3.3 255.255.255.255
R3(config-if-loopback3)#exit

R3(config)#ip multicast-routing
R3(config-mcast)#router pim
R3(config-mcast-pim)#interface loopback3
R3(config-mcast-pim-if-loopback3)#pimsm
R3(config-mcast-pim-if-loopback3)#exit
R3(config-mcast-pim)#exit
R3(config-mcast)#exit
R3(config)#interface gei-3/1
R3(config-if-gei-3/1)#ip address 10.10.30.2 255.255.255.0
R3(config-if-gei-3/1)#no shutdown
R3(config-if-gei-3/1)#exit
```

```
R3(config)#interface gei-3/2
R3(config-if-gei-3/2)#ip address 10.10.40.2 255.255.255.0
R3(config-if-gei-3/2)#no shutdown
R3(config-if-gei-3/2)#exit

R3(config)#router ospf 1
R3(config-ospf-1)#router-id 3.3.3.3
R3(config-ospf-1)#area 0
R3(config-ospf-1-area-0)#network 10.10.30.0 0.0.0.255
R3(config-ospf-1-area-0)#network 10.10.40.0 0.0.0.255
R3(config-ospf-1-area-0)#network 3.3.3.3 0.0.0.0
R3(config-ospf-1-area-0)#exit

R3(config)#ip multicast-routing
R3(config-mcast)#router pim
R3(config-mcast-pim)#interface gei-3/1
R3(config-mcast-pim-if-gei-3/1)#pimsm
R3(config-mcast-pim-if-gei-3/1)#exit
R3(config-mcast-pim)#interface gei-3/2
R3(config-mcast-pim-if-gei-3/2)#pimsm
R3(config-mcast-pim-if-gei-3/2)#bsr-border
R3(config-mcast-pim-if-gei-3/2)#exit
```

配置验证

在R1上通过**show ip msdp summary**命令查看MSDP Peer的建立：

```
R1#show ip msdp summary
MSDP Peer Status Summary
Peer Address       State     Uptime/        Reset      SA
                             Downtime       Count      Count
10.10.20.2          up       00:05:34         0          0

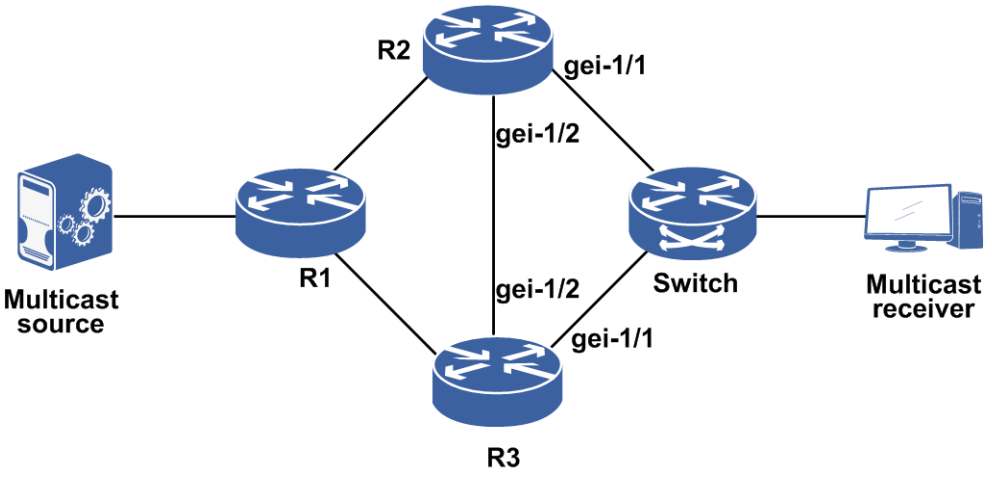
R2#show ip msdp summary
MSDP Peer Status Summary
Peer Address       State     Uptime/        Reset      SA
                             Downtime       Count      Count
*10.10.20.1         up       00:07:34         0          0
```

5.7.3 MSDP 实现 anycast-rp 配置实例

配置说明

如*图 5-21*所示，在路由器R2、R3上配置MSDP以实现anycast-rp。

图 5-21 MSDP 实现 anycast-rp 配置实例



配置思路

1.配置OSPF使得路由器R1和R2，R1和R3之间互通。

2.启PIM协议配置RP。

3.R2和R3之间配置MSDP。

4.接收者加入组播组，组播源发流。

配置过程

路由器R2上配置：

```
R2(config)interface gei-1/1
R2(config-if-gei-1/1)#ip address 11.1.1.2 255.255.255.0
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#ip address 12.1.1.2 255.255.255.0
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#exit
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 64.1.1.1 255.255.255.255
R2(config-if-loopback1)exit
R2(config)#interface loopback2
R2(config-if-loopback2)#ip address 64.1.1.10 255.255.255.255
R2(config-if-loopback2)#exit
R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 11.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#network 12.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#network 64.1.1.1 0.0.0.0
R2(config-ospf-1-area-0)#network 64.1.1.10 0.0.0.0
R2(config-ospf-1-area-0)#exit

R2(config)#ip multicast-routing
R2(config-mcast)#router pim
R2(config-mcast-pim)#bsr-candidate loopback1
R2(config-mcast-pim)#rp-candidate loopback1   /*loopback1做rp*/
R2(config-mcast-pim)#interface loopback1
R2(config-mcast-pim-if-loopback1)#pimsm
```

```
R2(config-mcast-pim-if-loopback1)#exit
R2(config-mcast-pim)#exit
R2(config-mcast)#router msdp
R2(config-mcast-msdp)#originator-id loopback2
R2(config-mcast-msdp)#peer 64.1.1.11
R2(config-mcast-msdp-peer)#connect-source loopback2   /*配置MSDP*/
R2(config-mcast-msdp-peer)#exit
R2(config-msdp-peer)#mesh-group inspur
/*配置mesh-group,mesh-group不需要事先定义，取消对peer SA消息的RPF检查*/
```

路由器R3上配置：

```
R3(config)#interface gei-1/1
R3(config-if-gei-1/1)#ip address 11.1.1.1 255.255.255.0
R3(config-if-gei-1/1)#no shutdown
R3(config-if-gei-1/1)#exit
R3(config)#interface gei-1/2
R3(config-if-gei-1/2)#ip address 12.1.1.1 255.255.255.0
R3(config-if-gei-1/2)#no shutdown
R3(config-if-gei-1/2)#exit
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 64.1.1.1 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface loopback2
R3(config-if-loopback2)#ip address 64.1.1.11 255.255.255.255
R3(config-if-loopback2)#exit
R3(config)#router ospf 1
R3(config-ospf-1)#area 0
R3(config-ospf-1-area-0)#network 11.1.1.0 0.0.0.255
R3(config-ospf-1-area-0)#network 12.1.1.0 0.0.0.255
R3(config-ospf-1-area-0)#network 64.1.1.1 0.0.0.0
R3(config-ospf-1-area-0)#network 64.1.1.11 0.0.0.0
R3(config-ospf-1-area-0)#exit

R3(config)#ip multicast-routing
R3(config-mcast)#router pim
R3(config-mcast-pim)#bsr-candidate loopback1
R3(config-mcast-pim)#rp-candidate loopback1   /*loopback1做rp，地址和B上的一样
*/
R3(config-mcast-pim)#interface loopback1
R3(config-mcast-pim-if-loopback1)#pimsm
R3(config-mcast-pim-if-loopback1)#exit
R3(config-mcast-pim)#exit
R3(config-mcast)#router msdp
R3(config-mcast-msdp)#originator-id loopback2
R3(config-mcast-msdp)#peer 64.1.1.10
R3(config-mcast-msdp-peer)#connect-source loopback2   /*配置MSDP*/
R3(config-mcast-msdp-peer)#exit
R3(config-msdp-peer)#mesh-group inspur
/*配置mesh-group,mesh-group不需要事先定义，取消对peer SA消息的RPF检查*/
```

配置验证

接收侧加入组播组，本例中路由器中B的gei-1/1地址大，会选为DR。路由器R2是最后一跳DR，如果路由器R3节点down，流量从路由器R1转发。

6 MPLS

6.1 MPLS 简介

MPLS多协议标签交换技术是新一代的IP高速骨干网络交换标准，由IETF提出，结合了网络核心的交换技术和网络边缘的IP路由技术的优点。

MPLS协议的特点就是使用标签交换（Label Switching），网络路由设备只需要判别标签后即可进行转发处理。MPLS支持任意的网络层协议（IPv6、IPX、IP等）及数据链路层协议（如ATM、FR、PPP等）。

MPLS网络工作的机制就是在MPLS网络外部通过IP进行三层路由查找，在MPLS网络内部通过对标签的查找实现二层交换。

MPLS技术具有如下特点：

·MPLS为IP网络提供面向连接的服务。

·通过集成链路层（ATM、FR）与网络层路由技术，解决了Internet扩展、保证IP QoS传输的问题，提供了高服务质量的Internet服务。

·通过短小固定的标签，采用精确匹配寻径方式取代传统路由器的最长匹配寻径方式，提供了高速率的IP转发。

·在提供IP业务的同时，提供高可靠的安全和QoS保证。

·利用显式路由功能，同时通过带有QoS参数的信令协议，建立受限标签交换路径（CR-LSP），因而能够有效地实施流量工程。

·利用标签嵌套技术，MPLS能很好的支持VPN。

6.2 MPLS 基础配置

6.2.1 配置 MPLS

在设备上启用MPLS功能，在网络节点之间分发标签，建立LSP。

1.在全局和接口上启用MPLS。

步骤	命令	功能
1	inspur(config)#**mpls ldp instance** <*instance-id*>[**vrf** <*vrf-name*>]	启用LDP，实例号的范围是1~65535
2	inspur(config-ldp-instance-id)#**interface** <*interface-name*>	在LDP配置模式下添加接口，表示要在此接口上进行标签转发

在需要启用LDP功能时，执行**mpls ldp instance**命令，配置LDP实例，启用LDP功能，并进入LDP配置模式。在LDP配置模式下添加接口，表示要在哪些接口上进

行标签转发，LDP实例就开始在接口上周期地发送hello消息。当从该接口得到到达某目的网段的出标签后，到目的网段去的包将被打上该出标签并从该接口转发。

启用MPLS的实例如下：

```
inspur(config)#interface loopback1
inspur(config-if-loopback1)#ip address 210.210.210.1 255.255.255.255
inspur(config-if-loopback1)#exit
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ip address 190.190.190.2 255.255.255.0
inspur(config-if-gei-0/1)#exit
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip address 190.190.191.2 255.255.255.0
inspur(config-if-gei-0/2)#exit

inspur(config)#mpls ldp instance 1
inspur(config-ldp-1)#router-id loopback1
inspur(config-ldp-1)#interface gei-0/2
inspur(config-ldp-1-if-gei-0/2)#discovery transport-address interface
inspur(config-ldp-1-if-gei-0/2)#exit
inspur(config-ldp-1)#interface gei-0/1
inspur(config-ldp-1-if-gei-0/1)#discovery transport-address interface
inspur(config-ldp-1-if-gei-0/1)#exit
```

2.配置LDP的路由器标识。

命令	功能
inspur(config-ldp-instance-id)#**router-id** *<interface-name>*	配置LDP实例标识，可以使用此命令配置本VPN域中的某一接口地址为LDP实例的路由器标识 为了保证LDP连接的稳定性，推荐选用loopback接口地址作为LDP实例的路由器标识

缺省情况下自动选取的路由器ID有时会不可用，例如，路由协议可能没有向邻居通告选作路由器ID的IP地址。另外，路由器的配置可能导致LDP的路由器ID具有不确定性，使得邻居的控制策略失效。命令**router-id**提供了一个指定某个接口的IP地址作为路由器ID的手段。但是要注意，地址用作路由器ID的接口其状态必须是“Operational”。

命令**router-id**的效果取决于所指定接口的当前状态：

- 如果指定的接口处于UP（Operational）状态，而且其地址不是当前的路由器ID，路由器强制将LDP实例的路由器ID改变为指定值，同时中断LDP实例的所有当前的会话，释放由会话学习到的标签，中断与这些标签绑定有关的MPLS转发。
- 如果指定的接口处于down状态，一旦其变为UP状态，路由器强制将LDP实例的路由器ID改变为指定值，同时中断所有当前的会话，释放由会话学习到的标签，中断与这些标签绑定有关的MPLS转发。

3.控制标签的生成与分发。

通过配置，管理员可以控制为哪些网段生成标签、生成标签的范围以及控制LDP分发标签。

步骤	命令	功能
1	inspur(config)#**mpls ldp instance** *<instance-id>*[**vrf** *<vrf-name>*]	使能LDP沿着普通的逐跳路由路径建立LSP，并且进入

步骤	命令	功能
		LDP配置模式
2	inspur(config-ldp-instance-id)#**access-fec** { **ip-prefix** { **for** < *prefix-access-list*>| **host-route-only**}| **bgp**}	控制LDP可以为哪些网段生成标签，创建FEC
3	inspur(config-ldp-instance-id)#**label-advertise** {**disable** | **old-style** | **for** < *prefix-access-list*>[**to** < *prefix-access-list*>]}	控制本地分配的标签（入标签）通过LDP分发，这条命令控制哪些目的网段的标签向哪些邻居通告，缺省向所有邻居通告所有标签

host-route-only：指定仅为32位掩码的目的网段（即主机地址）创建FEC。

bgp：指定为通过BGP获得的路由网段创建FEC。

控制标签的生成与分发的配置实例如下：

```
inspur(config)#ipv4-access-list 2
inspur(config-ipv4-acl)#rule 10 deny 200.200.201.0 0.0.0.255
inspur(config-ipv4-acl)#rule 20 permit any
inspur(config-ipv4-acl)#exit
inspur(config)#mpls ldp instance 1
inspur(config-ldp-1)#access-fec for 2
inspur(config-ldp-1)#exit
```

按照实例中的配置，LDP实例将不为200.200.201.0/24网段的路由分配标签。

4.配置LDP邻居。

步骤	命令	功能
1	inspur(config)#**mpls ldp instance** <*instance-id*>[**vrf** <*vrf-name*>]	使能LDP实例沿着普通的逐跳路由路径建立LSP，并且进入LDP配置模式
2	inspur(config-ldp-instance-id)#**target-session** {<*ip-address*>| **ipv6** < *X:X::X:X* >}[**dod**]	配置非直连远端目标target-session的地址，建立target-session
3	inspur(config-ldp-instance-id)#**discovery hello** { **holdtime** <*holdtime*>| **interval** <*interval*>}	配置LDP实例hello发现消息发送间隔，及LDP邻居的保持时间
4	inspur(config-ldp-instance-id)#**discovery targeted-hello** {**holdtime** <*holdtime*>| **interval** <*interval*>}	配置非直连LSR间，LDP实例hello发现消息发送间隔，及发现的LDP邻居超时的时间

holdtime <*holdtime*>：指定LDP实例发现的邻居在收不到后续hello消息的情况下的状态保存时间，单位：秒，范围1~65535，缺省为15秒，targeted-hello缺省为45秒。

interval <*interval*>：指定LDP实例周期性发送hello消息的间隔，单位：秒，范围1~65535，缺省为5秒，targeted-hello缺省为15秒。

配置LDP邻居的使用实例如下：

```
inspur(config)#mpls ldp instance 1
```

```
inspur(config-ldp-1)#discovery hello holdtime 20
inspur(config-ldp-1)#show mpls ldp parameters instance 1
Protocol version: 1
Session holdtime: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 20 sec; interval: 5 sec
Discovery targeted hello: holdtime: 45 sec; interval: 15 sec
LDP for targeted sessions
Downstream on Demand max hop count: 255
LDP used lsp control mode: Independent
LDP configred lsp control mode: Independent
LDP used label retention mode: Liberal
LDP configred label retention mode: Liberal
LDP loop detection: off
LDP IGP sync delay: 5 sec
```

5.配置LDP其他功能。

步骤	命令	功能
1	inspur(config)#**mpls ldp instance** <*instance-id*>[**vrf** <*vrf-name*>]	使能LDP沿着普通的逐跳路由路径建立LSP，并且进入LDP配置模式
2	inspur(config-ldp-instance-id)#**egress** { **for** <*prefix-access-list*>| **nexthop** <*nexthop-access-list*>}	控制LDP为特定的非直连的目的网段分配弹出标签，即egress控制策略
3	inspur(config-ldp-instance-id)#**explicit-null** [**for** <*prefix-acl*>][**to** <*peer-acl*>]	要使LDP实例在本该通告隐式空标签的时候通告显式空标签，默认情况使用的是隐式空标签
4	inspur(config-ldp-instance-id)#**holdtime** <*seconds*>	配置LDP会话在收不到后续LDP消息的情况下的维持时间，单位：秒，范围15~65535，缺省为180秒
5	inspur(config-ldp-instance-id)#**neighbor** <*ip-address*> **password** {**sealed** <*sealed-password*>|<*password*>}	配置LDP与邻居建立TCP连接会话的MD5密钥
6	inspur(config-ldp-instance-id)#**label-request for** <*prefix-access-list*>	配置LDP需要发送request消息的前缀
7	inspur(config-ldp-instance-id)#**gtsm target-neighbor** < *ip-address* > **hop-count** <*hop-num*> inspur(config-ldp-instance-id-if-ifname)#**gtsm**	通过配置该命令使路由器启动检查对端发送来的LDP报文的ttl跳数，设置分针对直连和非直连会话
8	inspur(config-ldp-instance-id)#**filter packet for** <*word*>	配置报文过滤策略
9	inspur(config-ldp-instance-id)#**igp sync delay** <*para*>	设定LDP IGP同步延时定时器超时时间
10	inspur(config-ldp-instance-id)#**label-retention conservative**	控制LDP实例使能保守的标签保持模式
11	inspur(config-ldp-instance-id)#**longest-match** {**ipv4 for** <*acl-name*>|**ipv6 for**	配置最长匹配LSP的建立拆除等功能

步骤	命令	功能
	<*acl-name*>}	
12	inspur(config-ldp-instance-id)#**lsp-control ordered**	控制LDP实例使能有序的LSP控制模式
13	inspur(config-ldp-instance-id-if-ifname)#**label-distribution dod**	LDP接口配置模式下控制LDP接口使能下游按需标签分发

<*prefix-acl*>：指定用显式空标签通告代替隐式标签通告的前缀。

<*peer-acl*>：指定向哪些邻居通告显式空标签代替隐式标签。

<*ip-address*>：对端LSR地址。

<*hop-num*>：TTL跳数，取值为1-254。

<*word*>：acl名称，名称支持的最大长度为31个字符。

<*para*>：指定延迟时间，取值为1~65535。

<*acl-name*>：acl名称，名称支持的最大长度为31个字符。

6.配置LDP BFD。

步骤	命令	功能
1	inspur(config)#**mpls ldp instance** <*instance-id*>[**vrf** <*vrf-name*>]	使能LDP沿着普通的逐跳路由路径建立LSP，并且进入LDP配置模式
2	inspur(config-ldp-instance-id)#**bfd** <*FEC-address*><*mask-length*> **interval** <*interval*> **min_rx** <*min_rx*> **multiplier** <*multiplier*>	配置LDP LSP BFD相关参数，并触发创建LSP的BFD会话
3	inspur(config-ldp-instance-id)#**peer bfd remote-routerid** < *ip-address* >[**delay** [<*time*>]]	配置LDPPeerBFD相关参数，LDP会话up后，会触发创建与指定邻居的PeerBFD会话 当只配置**delay**时，LDP会话up后延迟60秒触发创建BFD会话，60秒为延迟默认值 当在**delay**后面配置具体延迟时间时，则LDP会话up后延迟所配置的时间，触发创建BFD会话

<*interval*>：指定期望的报文最小发送间隔时间，单位：ms，取值范围为10~990。

<*min_rx*>：指定期望的报文最小接收间隔时间，单位：ms，取值范围为10~990。

<*multiplier*>：指定检测超时的倍数，取值范围为3~50。

<*ip-address*>：指定建立BFD的邻居routerid地址。

<*time*>：LDP会话up后延迟时间，单位：秒，范围0~720。

7.LDP Graceful Restart。

步骤	命令	功能
1	inspur(config)#**mpls ldp instance** <*1-65535*>[**vrf** <*vrf-name*>]	创建LDP实例，进入LDP配置模式
2	inspur(config-ldp-instance-id)#**graceful-restart** [**timer** {**max-recovery** <*interval*>| **neighbor-liveness** <*interval*>}]	配置LDP Graceful Restart

max-recovery <*interval*>：LSR等待对端邻居进行标记恢复的最长时间，该参数需要协商，单位：秒，范围15~600，缺省120秒。

neighbor-liveness <*interval*>：LSR等待LDP session会话恢复的最长时间，该参数需要协商，单位：秒，范围5~300，缺省120秒。

8.配置LSP Ping/LSP Trace检测功能。

为了使互联网中的路由器报告MPLS LSP数据平面错误或提供有关意外情况的信息，提出了LSP Ping/LSP Trace的功能。

LSP Ping/LSP Trace是一种检测MPLS LSP数据平面故障的方法，这个方法简单有效，可以发现一些控制平面无法发现的故障，为用户提供了一种在短时间内发现和隔离路由黑洞或者路由丢失等故障的方法。

LSP Ping/LSP Trace的具体介绍参见本套手册“配置指导（系统管理）”中的“网络层检测”章节。

9.配置IGP同步：OSPF。

在IR12000智能路由器上使用以下命令配置OSPF的LDP IGP同步。

步骤	命令	功能
1	inspur(config)#**router ospf** <*1-65535*>[**vrf** <*vrf-name*>]	创建OSPF实例，进入OSPF配置模式
2	inspur(config-ospf-instance-id)#**mpls ldp sync** inspur(config-ospf-instance-id)#**area** <*0-4294967295*> **mpls ldp sync** inspur(config-ospf-instance-id-if-interface-name)#**mpls ldp sync**	配置LDP IGP同步。同时根据配置命令的不同确定IGP同步的作用域是整个OSPF实例，还是OSPF实例下的某个域，还是某个OSPF接口

area<*0-4294967295*>：OSPF area号。

10.配置IGP同步：IS-IS。

在IR12000智能路由器上使用以下命令配置IS-IS的LDP IGP同步。

步骤	命令	功能

步骤	命令	功能
1	inspur(config)#**router isis** <*1-65535*>[**vrf** <*vrf-name*>]	创建IS-IS实例，进入IS-IS配置模式
2	inspur(config-isis-instance-id)#**mpls ldp sync** inspur(config-isis-instance-id-if-interface-name)#**mpls ldp sync**	配置LDP IGP同步。同时根据配置命令的不同确定IGP同步的作用域是整个IS-IS实例，还是某个IS-IS接口

11.配置IGP同步延时定时器。

在IR12000智能路由器上使用以下命令配置LDP IGP同步延时定时器超时时间。

步骤	命令	功能
1	inspur(config)#**mpls ldp instance** <*1-65535*>[**vrf** <*vrf-name*>]	创建LDP实例，进入LDP配置模式
2	inspur(config-ldp-instance-id)#**igp sync delay** <*1-65535*>	设定LDP IGP同步延时定时器超时时间

igp sync delay <*1-65535*>：同步延时定时器时长，单位：秒，默认5秒。

12.配置LDP接口的自动配置功能。

步骤	命令	功能
1	inspur(config)#**mpls ldp instance** <*1-65535*>[**vrf** <*vrf-name*>]	创建LDP实例，进入LDP配置模式
2	inspur(config-ldp-instance-id)#**auto-config interface global** { **enable** | **disable** }	开启或者关闭LDP实例下的所有LDP IPv4接口的自动配置功能 该命令是全局的配置命令，在关闭LDP自动配置功能之后，将不会进行LDP接口的自动创建，所有接口上的LDP Hello收发、LDP会话创建将不再受该接口上的IGP状态影响，由LDP接口配置决定
3	inspur(config-ldp-instance-id)#**auto-config interface** <*interface-name*>{**enable** | **disable**}	开启或者关闭LDP实例下的特定LDP IPv4接口的自动配置功能 如果LDP实例下配置了全局的关闭自动配置功能，则不管接口是否有开启或关闭自动配置功能，都以全局的关闭配置为最高优先级。如果LDP实例下没有配置全局的关闭自动配置功能，也就是默认开启自动配置时，再检查单个接口是否关闭自动配置，有单个

步骤	命令	功能
		接口的关闭自动配置，则表示该接口不会被自动创建

enable：开启全局IPv4自动配置或者开启LDP实例下的特定LDP IPv4接口的自动配置。

disable：关闭全局IPv4自动配置或者关闭LDP实例下的特定LDP IPv4接口的自动配置。

<*interface-name*>：接口名称。

13.验证配置结果。

命令	功能
inspur#**show mpls ldp interface** [<*interface-name*>] **instance** <*instance id*>	显示LDP实例所在VPN域中启动了LDP的接口信息
inspur#**show mpls ldp backoff instance** <*instance-id*>	显示LDP实例的会话退避重建参数的配置，及处于退避重建状态的会话
inspur#**show mpls ldp bindings** [{**(X:X::X:X** <*0-128*> **)** | **(**<*ip-address*>{<*net-mask*>|<*length*>}[**longer-prefixes**]**)**}] [**local-label** <*label*>[<*label*>]][**remote-label** <*label*>[<*label*>]][**neighbor** <*ip-address*>][**detail**] **instance** <*instance-id*>	显示LDP实例学习到的标签绑定
inspur#**show mpls ldp bindings summary instance** <*instance-id*>	显示LDP实例学习到的标签绑定的简要信息
inspur#**show mpls ldp discovery** [**detail**] **instance** <*instance-id*>	显示LDP实例的发现信息
inspur#**show mpls ldp neighbor** [<*neighbor*>|<*interface-name*>][**detail**] **instance** <*instance-id*>	显示LDP实例的会话信息
inspur#**show mpls ldp parameters instance** <*instance-id*>	显示LDP实例的当前参数信息
inspur#**show debug ldp instance** <*instance-id*>	显示路由器当前LDP实例的debug信息开启情况
inspur#**show mpls ldp graceful-restart instance** <*1-65535*>	显示路由器当前的LDP Graceful Restart配置情况
inspur#**show mpls ldp neighbor** [[<*neighbor-ipaddress*>][**detail**]] **instance** <*instance-id*>	查看GR的邻居信息
inspur#**show mpls ldp igp sync** [**interface** <*interface-name*>] **instance** <*instance-id*>	显示LDP IGP同步状态信息

14.维护MPLS。

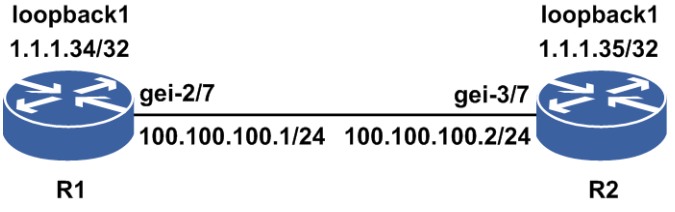
命令	功能
inspur#**debug ldp advertisements instance** *<instance-id>*	监视向LDP邻居通告的地址和标签，使用**no**命令取消监视
inspur#**debug ldp all** [**instance** < *instance-id*>]	打开LDP相关的所有debug开关
inspur#**debug ldp bindings instance** *<instanc-id>*	监视LDP邻居通告的地址和标签
inspur#**debug ldp messages** {**received** | **sent**} **instance** *<instance-id>*	监视向LDP邻居发送/从LDP邻居接收的消息
inspur#**debug ldp session** {**io** | **state-machine**} **instance** *<instance-id>*	监视LDP会话活动
inspur#**debug ldp transport** {**connections** | **events**} **instance** *<instance-id>*	监视LDP发现的信息

6.2.2 基本的 LDP 邻居会话配置实例

配置说明

如*图 6-1*所示是两台路由器建立LDP邻居，进行MPLS标签转发的基本配置实例。

图 6-1 建立基本的 LDP 邻居会话配置实例拓扑图



配置思路

在两台路由器R1和R2之间建立基本LDP邻居会话的配置思路如下：

1.使能R1和R2间的MPLS逐跳转发。

2.配置R1和R2间的LDP标签分发。

3.配置Loopback接口的IP地址作为LSR的路由器ID。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.34 255.255.255.255
R1(config-if-loopback1)#exit
```

```
R1(config)#interface gei-2/7
R1(config-if-gei-2/7)#no shutdown
R1(config-if-gei-2/7)#ip address 100.100.100.1 255.255.255.0
R1(config-if-gei-2/7)#exit

R1(config)#router isis
R1(config-isis-0)#area 00.0001
R1(config-isis-0)#system-id 0001.0002.0034
R1(config-isis-0)#interface gei-2/7
R1(config-isis-0-if-gei-2/7)#ip router isis
R1(config-isis-0-if-gei-2/7)#exit
R1(config-isis-0)#interface loopback1
R1(config-isis-0-if-loopback1)#ip router isis
R1(config-isis-0-if-loopback1)#exit
R1(config-isis-0)#exit

R1(config)#mpls ldp instance 1
/*配置LDP的Router-ID和接口*/
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-2/7
R1(config-ldp-1-if-gei-2/7)#exit
R1(config-ldp-1)#exit
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.35 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-3/7
R2(config-if-gei-3/7)#no shutdown
R2(config-if-gei-3/7)#ip address 100.100.100.2 255.255.255.0
R2(config-if-gei-3/7)#exit

R2(config)#router isis
R2(config-isis-0)#area 00.0002
R2(config-isis-0)#system-id 0002.0002.0035
R2(config-isis-0)#interface gei-3/7
R2(config-isis-0-if-gei-3/7)#ip router isis
R2(config-isis-0-if-gei-3/7)#exit
R2(config-isis-0)#interface loopback1
R2(config-isis-0-if-loopbck1)#ip router isis
R2(config-isis-0-if-loopbck1)#exit
R2(config-isis-0)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-3/7
R2(config-ldp-1-if-gei-3/7)#exit
R2(config-ldp-1)#exit
```

在以上的配置中，运行IS-IS动态路由协议的目的是为了通告各LSR的Router-ID即Loopback接口地址的路由。

使用Loopback接口地址作为LDP实例的路由器标识，有利于保证路由器的LDP ID的稳定，因为Loopback接口地址的状态是不会变的（除非手工关闭该接口）。

配置验证

在R2上查看邻居的建立情况：

```
R2(config)#show mpls ldp neighbor detail instance 1
Peer LDP Ident: 1.1.1.34:0; Local LDP Ident: 1.1.1.35:0
 TCP connection: 1.1.1.34.646 - 1.1.1.35.26408
 State: Oper; Msgs sent/rcvd: 31/31; Downstream
 Up Time: 00:24:57
 LDP discovery sources:
```

```
gei-3/7; Src IP addr: 100.100.100.1
holdtime: 15000 ms, hello interval: 5000 ms
Addresses bound to peer LDP Ident:
1.1.1.34 100.100.100.1
Session holdtime: 180000 ms; KA interval: 60000 ms
LDP Peer BFD not register.
LDP dynamic capability enable:
LDP send capability:
LDP dynamic capability
LDP Typed Wildcard FEC Cap
LDP Unrecognized Noti Cap
LDP received capability:
LDP dynamic capability negotiate success
LDP Typed Wildcard FEC Cap negotiate success
LDP Unrecognized Noti Cap negotiate success
```

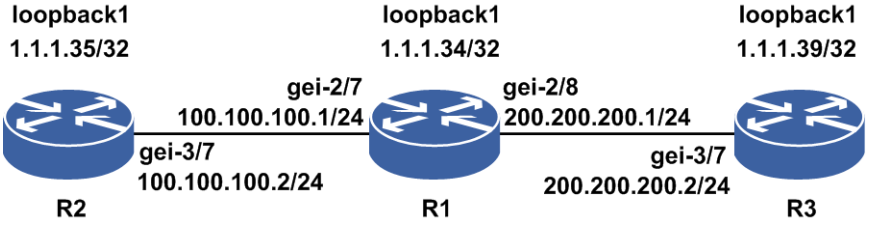
会话的状态是Oper（state: Oper），说明参数协商正确，和1.1.1.34（R1）的邻居关系已建立。

6.2.3 LDP 远端会话配置实例

配置说明

配置LDP会话组网如*图 6-2*所示，R1、R2和R3均支持MPLS。R1和R2、R1和R3之间建立直连LDP会话；R2和R3之间建立远端LDP会话。

图 6-2 LDP 远端会话配置实例拓扑图



配置思路

在路由器R2和R3之间建立LDP远端会话的配置思路如下：

1.R1和R2、R1和R3建立LDP邻居。

2.R2和R3建立LDP远端邻居。

3.配置Loopback接口的IP地址作为LSR的路由器ID。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.34 255.255.255.255
R1(config-if-loopback1)#exit
```

```
R1(config)#interface gei-2/7
R1(config-if-gei-2/7)#no shutdown
R1(config-if-gei-2/7)#ip address 100.100.100.1 255.255.255.0
R1(config-if-gei-2/7)#exit
R1(config)#interface gei-2/8
R1(config-if-gei-2/8)#no shutdown
R1(config-if-gei-2/8)#ip address 200.200.200.1 255.255.255.0
R1(config-if-gei-2/8)#exit

R1(config)#router isis
R1(config-isis-0)#area 00.0001
R1(config-isis-0)#system-id 0001.0002.0034
R1(config-isis-0)#interface gei-2/7
R1(config-isis-0-if-gei-2/7)#ip router isis
R1(config-isis-0-if-gei-2/7)#exit
R1(config-isis-0)#interface gei-2/8
R1(config-isis-0-if-gei-2/8)#ip router isis
R1(config-isis-0-if-gei-2/8)#exit
R1(config-isis-0)#interface loopback1
R1(config-isis-0-if-loopback1)#ip router isis
R1(config-isis-0-if-loopback1)#exit
R1(config-isis-0)#exit

R1(config)#mpls ldp instance 1
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-2/7
R1(config-ldp-1-if-gei-2/7)#exit
R1(config-ldp-1)#interface gei-2/8
R1(config-ldp-1-if-gei-2/8)#exit
R1(config-ldp-1)#exit
/*配置LDP的Router ID和接口*/
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.35 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-3/7
R2(config-if-gei-3/7)#no shutdown
R2(config-if-gei-3/7)#ip address 100.100.100.2 255.255.255.0
R2(config-if-gei-3/7)#exit

R2(config)#router isis
R2(config-isis-0)#area 00.0002
R2(config-isis-0)#system-id 0002.0002.0035
R2(config-isis-0)#interface gei-3/7
R2(config-isis-0-if-gei-3/7)#ip router isis
R2(config-isis-0-if-gei-3/7)#exit
R2(config-isis-0)#interface loopback1
R2(config-isis-0-if-loopback1)#ip router isis
R2(config-isis-0-if-loopback1)#exit
R2(config-isis-0)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-3/7
R2(config-ldp-1-if-gei-3/7)#exit
R2(config-ldp-1)#target-session 1.1.1.39
R2(config-ldp-1)#exit
```

R3上的配置如下：

```
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 1.1.1.39 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-3/7
R3(config-if-gei-3/7)#no shutdown
R3(config-if-gei-3/7)#ip address 200.200.200.2 255.255.255.0
R3(config-if-gei-3/7)#exit
```

```
R3(config)#router isis
R3(config-isis-0)#area 00.0003
R3(config-isis-0)#system-id 0003.0003.0039
R3(config-isis-0)#interface gei-3/7
R3(config-isis-0-if-gei-3/7)#ip router isis
R3(config-isis-0-if-gei-3/7)#exit
R3(config-isis-0)#interface loopback1
R3(config-isis-0-if-loopback1)#ip router isis
R3(config-isis-0-if-loopback1)#exit
R3(config-isis-0)#exit

R3(config)#mpls ldp instance 1
R3(config-ldp-1)#router-id loopback1
R3(config-ldp-1)#interface gei-3/7
R3(config-ldp-1-if-gei-3/7)#exit
R3(config-ldp-1)#target-session 1.1.1.35
R3(config-ldp-1)#exit
```

配置验证

用**show mpls ldp neighbor**命令在R3上查看邻居的建立情况：

```
R3(config)#show mpls ldp neighbor instance 1
Peer LDP Ident: 1.1.1.34:0; Local LDP Ident: 1.1.1.39:0
 TCP connection: 1.1.1.34.26406 - 1.1.1.2.646
 State: Oper; Msgs sent/rcvd: 10/10; Downstream
 Up Time: 00:01:38
 LDP discovery sources:
 gei-3/7; Src IP addr: 200.200.200.1
 Addresses bound to peer LDP Ident:
 1.1.1.34 100.100.100.1 200.200.200.1
Peer LDP Ident: 1.1.1.35:0; Local LDP Ident: 1.1.1.39:0
 TCP connection: 1.1.1.35.26412 - 1.1.1.2.646
 State: Oper; Msgs sent/rcvd: 9/9; Downstream
 Up Time: 00:00:39
 LDP discovery sources:
 Targeted Hello (1.1.1.6); Src IP addr: 1.1.1.6
 Addresses bound to peer LDP Ident:
 1.1.1.35 100.100.100.2
```

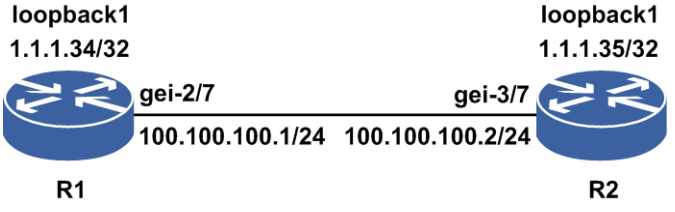
会话的状态是Oper（state: Oper），说明参数协商正确，和1.1.1.35（R2）的邻居关系已建立。

6.2.4 分配标签策略配置实例

配置说明

如*图 6-3*所示是为LSR配置标签分配策略配置示意图，要求在R1上配置标签分配策略，不为5.0.0.0/8和110.1.0.0/16网段分配FEC。

图 6-3 配置分配标签策略置实例拓扑图



配置思路

在R1上配置分配标签策略的配置思路如下：

1.使能R1和R2间的MPLS逐跳转发。

2.配置R1和R2间的LDP标签分发。

3.配置Loopback接口的IP地址作为LSR上LDP实例的路由器ID。

4.在R1上配置标签分配策略，不为5.0.0.0/8和110.1.0.0/16网段分配FEC。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.34 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-2/7
R1(config-if-gei-2/7)#no shutdown
R1(config-if-gei-2/7)#ip address 100.100.100.1 255.255.255.0
R1(config-if-gei-2/7)#exit

R1(config)#router isis
R1(config-isis-0)#area 00.0001
R1(config-isis-0)#system-id 0001.0002.0034
R1(config-isis-0)#interface gei-2/7
R1(config-isis-0-if-gei-2/7)#ip router isis
R1(config-isis-0-if-gei-2/7)#exit
R1(config-isis-0)#interface loopback1
R1(config-isis-0-if-loopback1)#ip router isis
R1(config-isis-0-if-loopback1)#exit
R1(config-isis-0)#exit

R1(config)#mpls ldp instance 1
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#access-fec ip-prefix for inspur
R1(config-ldp-1)#interface gei-2/7
R1(config-ldp-1-if-gei-2/7)#exit
R1(config-ldp-1)#exit
/*以下配置标签分配策略，不为5.0.0.0/8和110.1.0.0/16网段分配FEC*/
R1(config)#ipv4-access-list inspur
R1(config-ipv4-acl)#rule 10 deny 5.0.0.0 0.255.255.255
R1(config-ipv4-acl)#rule 20 deny 110.1.0.0 0.0.255.255
R1(config-ipv4-acl)#rule 30 permit any
R1(config-ipv4-acl)#exit
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.35 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-3/7
R2(config-if-gei-3/7)#no shutdown
R2(config-if-gei-3/7)#ip address 100.100.100.2 255.255.255.0
R2(config-if-gei-3/7)#exit

R2(config)#router isis
R2(config-isis-0)#area 00.0002
R2(config-isis-0)#system-id 0002.0002.0035
R2(config-isis-0)#interface gei-3/7
```

```
R2(config-isis-0-if-gei-3/7)#ip router isis
R2(config-isis-0-if-gei-3/7)#exit
R2(config-isis-0)#interface loopback1
R2(config-isis-0-if-loopback1)#ip router isis
R2(config-isis-0-if-loopback1)#exit
R2(config-isis-0)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-3/7
R2(config-ldp-1-if-gei-3/7)#exit
R2(config-ldp-1)#exit
```

配置验证

在R1上查看策略应用后的结果：

```
R1(config)#show mpls ldp bindings instance 1
 1.1.1.0/32
    local binding:  label: 4126
    remote binding: lsr: 1.1.1.35:0, label: imp-null(inuse)
    remote binding: lsr: 1.1.1.39:0, label: 51
 1.1.1.18/32
    local binding:  label: 4128
    remote binding: lsr: 1.1.1.35:0, label: 10175
    remote binding: lsr: 1.1.1.39:0, label: UnTag
 1.1.1.31/32 (no route)
    remote binding: lsr: 1.1.1.39:0, label: 54
 1.1.1.34/32
    local binding:  label: imp-null
    remote binding: lsr: 1.1.1.35:0, label: 10164
    remote binding: lsr: 1.1.1.39:0, label: 49
 1.1.1.35/32
    local binding:  label: 4101
    remote binding: lsr: 1.1.1.35:0, label: imp-null(inuse)
    remote binding: lsr: 1.1.1.39:0, label: 36
 1.1.1.39/32
    local binding:  label: 4119
    remote binding: lsr: 1.1.1.35:0, label: 10167
    remote binding: lsr: 1.1.1.39:0, label: imp-null
 60.0.2.0/24
    local binding:  label: 4108
    remote binding: lsr: 1.1.1.35:0, label: 4143(inuse)
    remote binding: lsr: 1.1.1.39:0, label: imp-null
 60.0.3.0/24
    local binding:  label: 4109
    remote binding: lsr: 1.1.1.35:0, label: 6149(inuse)
    remote binding: lsr: 1.1.1.39:0, label: 60
```

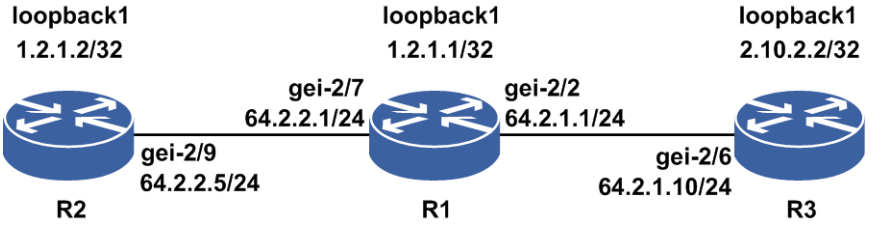
可以看到R1没有为5.0.0.0/8和110.1.0.0/16网段分配FEC。

6.2.5 LDP 多实例配置实例

配置说明

配置LDP会话组网如*图 6-4*所示，R1、R2和R3均支持MPLS。R1和R2建立公网会话，R1和R3之间建立私网会话。

图 6-4 LDP 多实例拓扑图



配置思路

在路由器R2和R3之间建立LDP多实例的配置思路如下：

1.R1和R2之间建立LDP公网邻居。

2.R1和R3之间建立LDP私网邻居。

配置过程

R1上的配置：

```
/*以下配置供LDP公网实例使用*/
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.2.1.1 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-2/7
R1(config-if-gei-2/7)#no shutdown
R1(config-if-gei-2/7)#ip address 64.2.2.1 255.255.255.0
R1(config-if-gei-2/7)#exit
R1(config)#router isis
R1(config-isis-0)#area 00.0001
R1(config-isis-0)#system-id 0001.0002.0034
R1(config-isis-0)#interface gei-2/7
R1(config-isis-0-if-gei-2/7)#ip router isis
R1(config-isis-0-if-gei-2/7)#exit
R1(config-isis-0)#interface loopback1
R1(config-isis-0-if-loopback1)#ip router isis
R1(config-isis-0-if-loopback1)#exit
R1(config-isis-0)#exit
R1(config)#mpls ldp instance 1
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-2/7
R1(config-ldp-1-if-gei-2/7)#exit
R1(config-ldp-1)#exit
/*以下配置供LDP私网实例使用*/
R1(config)#ip vrf  a
R1(config-vrf-a)#rd 1:1
R1(config-vrf-a)#address-family ipv4
R1(config-vrf-a-af-ipv4)#exit
R1(config-vrf-a)#exit
R1(config)#interface loopback2
R1(config-if-loopback2)#ip vrf forwarding a
R1(config-if-loopback2)#ip address 2.13.2.2 255.255.255.255
R1(config-if-loopback2)#exit
R1(config)#interface gei-2/2
R1(config-if-gei-2/2)#no shutdown
R1(config-if-gei-2/2)#ip vrf forwarding a
R1(config-if-gei-2/2)#ip address 64.2.1.1 255.255.255.0
R1(config-if-gei-2/2)#exit
R1(config)#router isis 1 vrf a
```

```
R1(config-isis-1)#area 00.0001
R1(config-isis-1)#system-id 1111.0002.0034
R1(config-isis-1)#interface gei-2/2
R1(config-isis-1-if-gei-2/2)#ip router isis
R1(config-isis-1-if-gei-2/2)#exit
R1(config-isis-1)#interface loopback2
R1(config-isis-1-if-loopback2)#ip router isis
R1(config-isis-1-if-loopback2)#exit
R1(config-isis-1)#exit
R1(config)#mpls ldp instance 2 vrf a
R1(config-ldp-2)#router-id loopback2
R1(config-ldp-2)#interface gei-2/2
R1(config-ldp-2-if-gei-2/2)#exit
R1(config-ldp-2)#exit
```

R2上的配置：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.2.1.2 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-2/9
R2(config-if-gei-2/9)#no shutdown
R2(config-if-gei-2/9)#ip address 64.2.2.5 255.255.255.0
R2(config-if-gei-2/9)#exit
R2(config)#router isis
R2(config-isis-0)#area 00.0002
R2(config-isis-0)#system-id 0002.0002.0035
R2(config-isis-0)#interface gei-2/9
R2(config-isis-0-if-gei-2/9)#ip router isis
R2(config-isis-0-if-gei-2/9)#exit
R2(config-isis-0)#interface loopback1
R2(config-isis-0-if-loopbck1)#ip router isis
R2(config-isis-0-if-loopbck1)#exit
R2(config-isis-0)#exit
R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-2/9
R2(config-ldp-1-if-gei-2/9)#exit
R2(config-ldp-1)#exit
```

R3上的配置：

```
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 2.10.2.2 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-2/6
R3(config-if-gei-2/6)#no shutdown
R3(config-if-gei-2/6)#ip address 64.2.1.10 255.255.255.0
R3(config-if-gei-2/6)#exit
R3(config)#router isis
R3(config-isis-0)#area 00.0003
R3(config-isis-0)#system-id 0003.0003.0039
R3(config-isis-0)#interface gei-2/6
R3(config-isis-0-if-gei-2/6)#ip router isis
R3(config-isis-0-if-gei-2/6)#exit
R3(config-isis-0)#interface loopback1
R3(config-isis-0-if-loopbck1)#ip router isis
R3(config-isis-0-if-loopbck1)#exit
R3(config-isis-0)#exit
R3(config)#mpls ldp instance 1
R3(config-ldp-1)#router-id loopback1
R3(config-ldp-1)#interface gei-2/6
R3(config-ldp-1-if-gei-2/6)#exit
R3(config-ldp-1)#exit
```

配置验证

在R1上查看公网和私网中邻居建立的结果：

```
R1(config)#show mpls ldp neighbor instance 1
Peer LDP Ident: 1.2.1.2:0; Local LDP Ident 1.2.1.1:0
       TCP connection: 1.2.1.2.1054 - 1.2.1.1.646
       state: Oper; Msgs sent/rcvd: 47/48; Downstream
       Up Time: 00:00:30
       LDP discovery sources:
         gei-2/7; Src IP addr: 64.2.2.5
       Addresses bound to peer LDP Ident:
         1.2.1.2 64.2.2.5
```

会话的状态是Oper（state: Oper），说明参数协商正确，和R2的公网邻居关系已建立。

```
R1(config)#show mpls ldp neighbor instance 2
Peer LDP Ident: 2.10.2.2:0; Local LDP Ident 1.1.1.39:0
       TCP connection: 2.10.2.2.646 - 2.13.2.2.1072
       state: Oper; Msgs sent/rcvd: 50/51; Downstream
       Up Time: 00:00:30
       LDP discovery sources:
         gei-2/2; Src IP addr: 64.2.1.10
       Addresses bound to peer LDP Ident:
         2.10.2.2 64.2.1.10
```

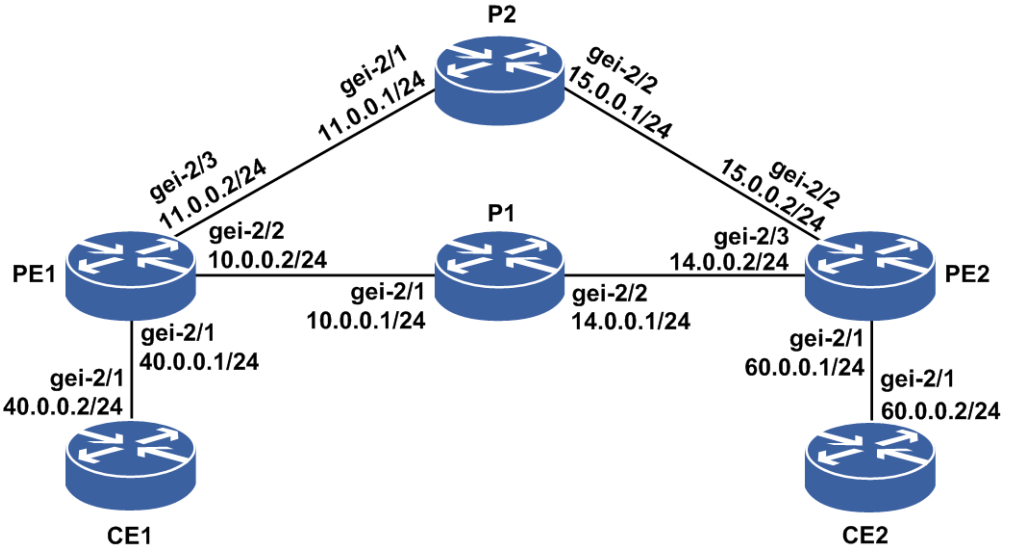
会话的状态是Oper（state: Oper），说明参数协商正确，和R3的私网邻居关系已建立。

6.2.6 LDP FRR 配置实例

配置说明

如*图* **6-5**所示，以L3VPN环境下，公网走LDP FRR组网为例。需要在PE间建立MP-BGP邻居，在公网上建立MPLS LDP邻居。

图 6-5 LDP FRR 配置实例示意图



配置思路

1.配置PE1与PE2间的IGP路由，保证互相能够互通。

2.配置MP-BGP邻居。

3.配置LDP邻居。

4.在PE1上启用路由协议的FRR。

配置过程

CE1上以OSPF协议接入，CE2以IS-IS协议接入，中间IGP路由以IS-IS协议为例，具体配置如下。

CE1的配置如下：

```
CE1(config)#interface gei-2/1
CE1(config-if-gei-2/1)#no shutdown
CE1(config-if-gei-2/1)#ip address 40.0.0.2 255.255.255.0
CE1(config-if-gei-2/1)#exit
CE1(config)#interface loopback1
CE1(config-if-loopback1)#ip address 12.1.2.1 255.255.255.255
CE1(config-if-loopack1)#exit

CE1(config)#router ospf 1
CE1(config-ospf-1)#router-id 12.1.2.1
CE1(config-ospf-1)#area 16
CE1(config-ospf-1-area-16)#network 40.0.0.0 0.0.0.255
CE1(config-ospf-1-area-16)#network 12.1.2.1 0.0.0.0
CE1(config-ospf-1-area-16)exit
```

CE2的配置如下：

```
E2(config)#interface gei-2/1
CE2(config-if-gei-2/1)#no shutdown
CE2(config-if-gei-2/1)#ip address 60.0.0.2 255.255.255.0
CE2(config-if-gei-2/1)#exit
CE2(config)#interface loopback1
CE2(config-if-loopback1)#ip address 12.1.2.5 255.255.255.255
CE2(config-if-loopback1)#exit

CE2(config)#router isis1
CE2(config-isis-1)#area 10
CE2(config-isis-1)#system-id 0000.0000.0001
CE2(config-isis-1)#interface loopback1
CE2(config-isis-1-if-loopback1)#ip router isis
CE2(config-isis-1)#exit
CE2(config-isis-1)#interface gei-2/1
CE2(config-isis-1-if-gei-2/1)#ip router isis
CE2(config-isis-1)#exit
```

PE1的配置如下：

```
PE1(config)#ip vrf inspur1
PE1(config-vrf-inspur1)#rd 100:1
PE1(config-vrf-inspur1)#route-target import 100:1
PE1(config-vrf-inspur1)#route-target export 100:1
PE1(config-vrf-inspur1)#exit

PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
PE1(config-if-loopback1)#exit
PE1(config)#interface gei-2/1
PE1(config-if-gei-2/1)#no shutdown
```

```
PE1(config-if-gei-2/1)#ip vrf forwarding inspur1
PE1(config-if-gei-2/1)#ip address 40.0.0.1 255.255.255.0
PE1(config-if-gei-2/1)#exit
PE1(config)#interface gei-2/2
PE1(config-if-gei-2/2)#no shutdown
PE1(config-if-gei-2/2)#ip address 10.0.0.2 255.255.255.0
PE1(config-if-gei-2/2)#exit
PE1(config)#interface gei-2/3
PE1(config-if-gei-2/3)#no shutdown
PE1(config-if-gei-2/3)#ip address 11.0.0.2 255.255.255.0
PE1(config-if-gei-2/3)#exit

PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#interface gei-2/2
PE1(config-ldp-1-if-gei-2/2)#exit
PE1(config-ldp-1)#interface gei-2/3
PE1(config-ldp-1-if-gei-2/3)#exit
PE1(config-ldp-1)#exit

PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 1.1.1.3 remote-as 100
PE1(config-bgp)#neighbor 1.1.1.3 update-source loopback1
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 1.1.1.3 activate
PE1(config-bgp-af)#exit
PE1(config-bgp)#address-family ipv4 vrf inspur1
PE1(config-bgp-af)#redistribute ospf-int
PE1(config-bgp-af)#exit
PE1(config-bgp)#exit

PE1(config)#router ospf 1 vrf inspur1
PE1(config-ospf-1)#area 16
PE1(config-ospf-1-area-16)#network 40.0.0.0 0.0.0.255
PE1(config-ospf-1-area-16)#exit

PE1(config)#router isis1
PE1(config-isis)#area 10
PE1(config-isis-1)#system-id 0000.70d0.c200
PE1(config-isis-1)#interface gei-2/2
PE1(config-isis-1-if-gei-2/2)#ip router isis
PE1(config-isis-1-if-gei-2/2)#exit
PE1(config-isis-1)#interfacegei-2/3
PE1(config-isis-1-if-gei-2/3)#ip router isis
PE1(config-isis-1-if-gei-2/3)#metric 20
PE1(config-isis-1-if-gei-2/3)#exit

PE1(config-isis-1)#fast-reroute lfa enable
PE1(config-isis-1)#interface loopback1
PE1(config-isis-1-if-loopback1)#ip router isis
PE1(config-isis-1-if-loopback1)#exit
PE1(config-isis-1)#exit
```

PE2的配置如下：

```
PE2(config)#ip vrf inspur1
PE2(config-vrf-inspur1)#rd 100:1
PE2(config-vrf-inspur1)#route-target import 100:1
PE2(config-vrf-inspur1)#route-target export 100:1
PE2(config-vrf-inspur1)#exit

PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 1.1.1.3 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#interface gei-2/1
PE2(config-if-gei-2/1)#no shutdown
PE2(config-if-gei-2/1)#ip vrf forwarding inspur1
PE2(config-if-gei-2/1)#ip address 60.0.0.1 255.255.255.0
PE2(config-if-gei-2/1)#exit
PE2(config)#interface gei-2/2
```

```
PE2(config-if-gei-2/2)#no shutdown
PE2(config-if-gei-2/2)#ip address 15.0.0.2 255.255.255.0
PE2(config-if-gei-2/2)#exit
PE2(config)#interface gei-2/3
PE2(config-if-gei-2/3)#no shutdown
PE2(config-if-gei-2/3)#ip address 14.0.0.2 255.255.255.0
PE2(config-if-gei-2/3)#exit

PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#interface gei-2/2
PE2(config-ldp-1-if-gei-2/2)#exit
PE2(config-ldp-1)#interface gei-2/3
PE2(config-ldp-1-if-gei-2/3)#exit
PE2(config-ldp-1)#exit

PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.2 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.2 update-source loopback1
PE2(config-bgp)#address-family ipv4 vrf inspur1
PE2(config-bgp-af)#redistribute isis-1-2
PE2(config-bgp-af)#exit
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 1.1.1.2 activate
PE2(config-bgp-af)#exit
PE2(config-bgp)#exit

PE2(config)#router isis vrf inspur1
PE2(config-isis-0)#area 10
PE2(config-isis-0)#system-id 0000.0000.0002
PE2(config-isis-0)#interface gei-2/1
PE2(config-isis-0-if-gei-2/1)#ip router isis
PE2(config-isis-0-if-gei-2/1)#exit
PE2(config-isis-0)#exit

PE2(config)#router isis1
PE2(config-isis-1)#area 10
PE2(config-isis-1)#system-id 0000.dd00.0002
PE2(config-isis-1)#interface gei-2/2
PE2(config-isis-1-if-gei-2/2)#ip router isis
PE2(config-isis-1-if-gei-2/2)#exit
PE2(config-isis-1)#interface gei-2/3
PE2(config-isis-1-if-gei-2/3)#ip router isis
PE2(config-isis-1-if-gei-2/3)#exit
PE2(config-isis-1)#interface loopback1
PE2(config-isis-1-if-loopback1)#ip router isis
PE2(config-isis-1-if-loopback1)#exit
PE2(config-isis-1)#exit
```

P1的配置如下：

```
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.4 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface gei-2/1
P1(config-if-gei-2/1)#no shutdown
P1(config-if-gei-2/1)#ip address 10.0.0.1 255.255.255.0
P1(config-if-gei-2/1)#exit
P1(config)#interface gei-2/2
P1(config-if-gei-2/2)#no shutdown
P1(config-if-gei-2/2)#ip address 14.0.0.1 255.255.255.0
P1(config-if-gei-2/2)#exit

P1(config)#router isis1
P1(config-isis-1)#area 10
P1(config-isis-1)#system-id 0000.dd00.1000
P1(config-isis-1)#interface gei-2/1
P1(config-isis-1-if-gei-2/1)#ip router isis
P1(config-isis-1-if-gei-2/1)#exit
P1(config-isis-1)#interface gei-2/2
```

```
P1(config-isis-1-if-gei-2/2)#ip router isis
P1(config-isis-1-if-gei-2/2)#exit
P1(config-isis-1)#interface loopback1
P1(config-isis-1-if-loopback1)#ip router isis
P1(config-isis-1-if-loopback1)#exit
P1(config-isis-1)#exit

P1(config)#mpls ldp instance 1
P1(config-ldp-1)#router-id loopback1
P1(config-ldp-1)#interface gei-2/1
P1(config-ldp-1-if-gei-2/1)#exit
P1(config-ldp-1)#interface gei-2/2
P1(config-ldp-1-if-gei-2/2)#exit
P1(config-ldp-1)#exit
```

P2的配置如下：

```
P2(config)#interface loopback1
P2(config-if-loopback1)#ip address 1.1.1.5 255.255.255.255
P2(config-if-loopback1)#exit
P2(config)#interface gei-2/1
P2(config-if-gei-2/1)#no shutdown
P2(config-if-gei-2/1)#ip address 11.0.0.1 255.255.255.0
P2(config-if-gei-2/1)#exit
P2(config)#interface gei-2/2
P2(config-if-gei-2/2)#no shutdown
P2(config-if-gei-2/2)#ip address 15.0.0.1 255.255.255.0
P2(config-if-gei-2/2)#exit

P2(config)#router isis1
P2(config-isis-1)#area 10
P2(config-isis-1)#system-id 0000.dd00.3000
P2(config-isis-1)#interface gei-2/1
P2(config-isis-1-if-gei-2/1)#ip router isis
P2(config-isis-1-if-gei-2/1)#exit
P2(config-isis-1)#interface gei-2/2
P2(config-isis-1-if-gei-2/2)#ip router isis
P2(config-isis-1-if-gei-2/2)#exit
P2(config-isis-1)#interface loopback1
P2(config-isis-1-if-loopback1)#ip router isis
P2(config-isis-1-if-loopback1)#exit
P2(config-isis-1)#exit

P2(config)#mpls ldp instance 1
P2(config-ldp-1)#router-id loopback1
P2(config-ldp-1)#interface gei-2/1
P2(config-ldp-1-if-gei-2/1)#exit
P2(config-ldp-1)#interface gei-2/2
P2(config-ldp-1-if-gei-2/2)#exit
P2(config-ldp-1)#exit
```

配置验证

使用**show ip forwarding backup route**命令验证配置结果是否使FRR最终生效。

PE1上IS-IS的FRR生效情况查看：

```
PE1#show isis fast-reroute-topology
IS-IS ipfrr paths to Level-1 routers
System id Interface Ipfrr interface Ipfrr type metric
0000.dd00.0002 gei-2/2 gei-2/3 node 30
IS-IS ipfrr paths to Level-2 routers
System id Interface Ipfrr interface Ipfrr type metric
0000.dd00.0002 gei-2/2 gei-2/3 node 30

PE1#show ip forwarding backup route
```

```
IPv4 Backup Routing Table:
status codes: *valid, >best, M:Master, S:Slave
   Dest     Gw       Interface     Owner       Pri  Metric M/S Status
1.1.1.3/32  10.0.0.2  gei-2/2       ISIS_LEVEL1  115  40     M   I
1.1.1.3/32  11.0.0.2  gei-2/3       ISIS_LEVEL1  115  40     S   U
```

查看LDP FRR生效情况：

```
PE1(config)#show mpls ldp bindings 1.1.1.3 32 detail instance 1
 1.1.1.3/32
    local binding:  label: 16399
      advertised to:
      1.1.1.4:0              1.1.1.5:0
 remote binding: lsr: 1.1.1.4:0, label: 16394(inuse)
 remote binding: lsr: 1.1.1.5:0, label: 16399(inuse_slv_ip)

PE1(config)#show mpls forwarding-table 1.1.1.3
Local     Outgoing  Prefix or    Outgoing      Next Hop     M/S
label     label     Tunnel Id    interface
16399     16394    1.1.1.3/32    gei-2/2       10.0.0.1     M
16399     16399    1.1.1.3/32    gei-2/3       11.0.0.1     S
```

查看PE1与PE2建立IBGP连接的情况：

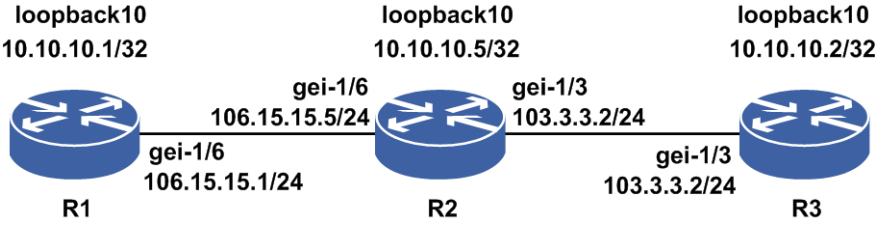
```
PE1#show ip bgp summary
Neighbor    Ver    As    MsgRcvd    MsgSend    Up/Down(s)   State
1.1.1.3     4     100     195        201       01:37:23     2
```

6.2.7 LDP Graceful Restart 配置实例

配置说明

如*图 6-6*所示，网络中三个节点R1、R2、R3都为双主控设备。三个节点间通过OSPF实现网络互通，并提供GR机制。在R1、R2、R3之间建立LDP会话，当R2的主板发生故障并切换时，需要通过LDP GR机制与邻居节点进行同步。

图 6-6 LDP Graceful Restart 配置实例图



配置思路

1.配置各节点接口的IP地址以及作为LSR ID的Loopback地址，并用OSPF协议通告各接口所连网段和LSR ID主机路由

2.在各节点上配置OSPF GR功能

3.各节点上的接口配置MPLS LDP，建立LDP邻居

4.在各节点上使能LDP GR能力

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/6
R1(config-if-gei-1/6)#no shutdown
R1(config-if-gei-1/6)#ip address 106.15.15.1 255.255.255.0
R1(config-if-gei-1/6)#exit
R1(config)#interface loopback10
R1(config-if-loopback10)#ip address 10.10.10.1 255.255.255.255
R1(config-if-loopback10)#exit

R1(config)#router ospf 2
R1(config-ospf-2)#router-id 10.10.10.1
R1(config-ospf-2)#area 0
R1(config-ospf-2-area-0)#network 106.15.15.0 0.0.0.255
R1(config-ospf-2-area-0)#network 10.10.10.1 0.0.0.0
R1(config-ospf-2-area-0)#exit
R1(config-ospf-2)#nsf
R1(config-ospf-2)#exit

R1(config)#mpls ldp instance 1
R1(config-ldp-1)#interface gei-1/6
R1(config-ldp-1-if-gei-1/6)#exit
R1(config-ldp-1)#router-id loopback10
R1(config-ldp-1)#graceful-restart
R1(config-ldp-1)#end
```

R2上的配置如下：

```
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#no shutdown
R2(config-if-gei-1/3)#ip address 103.3.3.2 255.255.255.0
R2(config-if-gei-1/3)#exit
R2(config)#interface gei-1/6
R2(config-if-gei-1/6)#no shutdown
R2(config-if-gei-1/6)#ip address 106.15.15.5 255.255.255.0
R2(config-if-gei-1/6)#exit
R2(config)#interface loopback10
R2(config-if-loopback10)#ip address 10.10.10.5 255.255.255.255
R2(config-if-loopback10)#exit

R2(config)#router ospf 2
R2(config-ospf-2)#router-id 10.10.10.5
R2(config-ospf-2)#area 0
R2(config-ospf-2-area-0)#network 103.3.3.0 0.0.0.255
R2(config-ospf-2-area-0)#network 106.15.15.0 0.0.0.255
R2(config-ospf-2-area-0)#network 10.10.10.5 0.0.0.0
R2(config-ospf-2-area-0)#exit
R2(config-ospf-2)#nsf
R2(config-ospf-2)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#interface gei-1/3
R2(config-ldp-1-if-gei-1/3)#exit
R2(config-ldp-1)#interface gei-1/6
R2(config-ldp-1-if-gei-1/6)#exit
R2(config-ldp-1)#router-id loopback10
R2(config-ldp-1)#graceful-restart
R2(config-ldp-1)#end
```

R3上的配置如下：

```
R3(config)#interface gei-1/3
R3(config-if-gei-1/3)#no shutdown
R3(config-if-gei-1/3)#ip address 103.3.3.2 255.255.255.0
R3(config-if-gei-1/3)#exit
R3(config)#interface loopback10
R3(config-if-loopback10)#ip address 10.10.10.2 255.255.255.255
```

```
R3(config-if-loopback10)#exit

R3(config)#router ospf 2
R3(config-ospf-2)#router-id 10.10.10.2
R3(config-ospf-2)#area 0
R3(config-ospf-2-area-0)#network 103.3.3.0 0.0.0.255
R3(config-ospf-2-area-0)#network 10.10.10.2 0.0.0.0
R3(config-ospf-2-area-0)#exit
R3(config-ospf-2)#nsf
R3(config-ospf-2)#exit

R3(config)#mpls ldp instance 1
R3(config-ldp-1)#interface gei-1/3
R3(config-ldp-1-if-gei-1/3)#exit
R3(config-ldp-1)#router-id loopback10
R3(config-ldp-1)#graceful-restart
R3(config-ldp-1)#exit
```

配置验证

在R2发生主备倒换或重启LDP之前，在R1、R2、R3上分别查看转发表和绑定信息。

查看R1上的信息：

```
R1#show mpls forwarding-table 10.10.10.2
Local     Outgoing  Prefix or         Outgoing       Next Hop       M/S
label     label     Tunnel Id         interface
16395     16388     10.10.10.2/32     gei-1/6     106.15.15.5     M

R1#show mpls ldp bindings 10.10.10.2 32 instance 1
 10.10.10.2/32
    local binding:  label: 16395
    remote binding: lsr: 10.10.10.5:0, label: 16388(inuse)

R1#show mpls ldp graceful-restart instance 1
 LDP Graceful Restart is enabled
 Neighbor Liveness Timer: 120 seconds
 Max Recovery Timer: 120 seconds
 Graceful Restart enabled Sessions:
  Peer LDP Ident: 10.10.10.5:0,State:Oper

R1#show mpls ldp neighbor graceful-restart instance 1
Peer LDP Ident: 10.10.10.5:0; Local LDP Ident: 10.10.10.1:0
       TCP connection: 10.10.10.5.6739 - 10.10.10.1.646
       State: Oper; Msgs sent/rcvd: 23/127; Downstream
       Up Time: 00:02:21
       LDP discovery sources:
         gei-1/6; Src IP addr: 106.15.15.5
       Addresses bound to peer LDP Ident:
         5.5.5.64  8.8.8.5  9.9.9.5  10.10.10.5
         13.13.13.5  14.14.14.5  15.15.15.5  16.16.16.5
         17.5.5.5  18.18.18.5  19.19.19.5  20.20.20.5
         21.21.21.5  23.23.23.5  24.24.24.5  25.25.25.5
         26.26.26.5  27.27.27.5  28.28.28.5  29.29.29.5
         31.31.31.1  32.32.32.5  33.33.33.5  34.34.34.5
         35.35.35.5  36.36.36.5  37.37.37.5  38.38.38.5
         39.39.39.5  40.40.40.5  41.41.41.5  42.42.42.5
         43.43.43.5  44.44.44.5  45.45.45.5  46.46.46.5
         47.47.47.5  48.48.48.5  49.49.49.5  50.50.50.5
         103.3.3.5  106.15.15.5
       Graceful Restart enabled; Peer reconnect time (msecs): 120000
```

查看R2上的信息：

```
R2#show mpls ldp graceful-restart instance 1
 LDP Graceful Restart is enabled
```

```
 Neighbor Liveness Timer: 120 seconds
 Max Recovery Timer: 120 seconds
 Graceful Restart enabled Sessions:
  Peer LDP Ident: 10.10.10.2:0,State:Oper
  Peer LDP Ident: 10.10.10.1:0,State:Oper

R2#show mpls ldp neighbor graceful-restart instance 1
Peer LDP Ident: 10.10.10.1:0; Local LDP Ident: 10.10.10.5:0
 TCP connection: 10.10.10.1.646 - 10.10.10.5.6739
 State: Oper; Msgs sent/rcvd: 127/22; Downstream
 Up Time: 00:02:15
 LDP discovery sources:
 gei-1/6; Src IP addr: 106.15.15.1
 Addresses bound to peer LDP Ident:
 1.1.1.64 10.10.10.1 106.15.15.1
 Graceful Restart enabled; Peer reconnect time (msecs): 120000
Peer LDP Ident: 10.10.10.2:0; Local LDP Ident: 10.10.10.5:0
       TCP connection: 10.10.10.2.646 - 10.10.10.5.6738
       State: Oper; Msgs sent/rcvd: 127/87; Downstream
       Up Time: 00:02:15
       LDP discovery sources:
         gei-1/3; Src IP addr: 103.3.3.2
       Addresses bound to peer LDP Ident:
         2.2.2.64  10.10.10.2  90.4.2.2  101.1.1.2
         103.3.3.2
       Graceful Restart enabled; Peer reconnect time (msecs): 120000
```

查看R3上的信息：

```
R3#show mpls ldp graceful-restart instance 1
 LDP Graceful Restart is enabled
 Neighbor Liveness Timer: 120 seconds
 Max Recovery Timer: 120 seconds
 Graceful Restart enabled Sessions:
  Peer LDP Ident: 10.10.10.5:0,State:Oper

R3#show mpls ldp neighbor graceful-restart instance 1
Peer LDP Ident: 10.10.10.5:0; Local LDP Ident: 10.10.10.2:0
       TCP connection: 10.10.10.5.6738 - 10.10.10.2.646
       State: Oper; Msgs sent/rcvd: 88/127; Downstream
       Up Time: 00:03:11
       LDP discovery sources:
         gei-1/3; Src IP addr: 103.3.3.5
       Addresses bound to peer LDP Ident:
         5.5.5.64  8.8.8.5  9.9.9.5  10.10.10.5
         13.13.13.5  14.14.14.5  15.15.15.5  16.16.16.5
         17.5.5.5  18.18.18.5  19.19.19.5  20.20.20.5
         21.21.21.5  23.23.23.5  24.24.24.5  25.25.25.5
         26.26.26.5  27.27.27.5  28.28.28.5  29.29.29.5
         31.31.31.1  32.32.32.5  33.33.33.5  34.34.34.5
         35.35.35.5  36.36.36.5  37.37.37.5  38.38.38.5
         39.39.39.5  40.40.40.5  41.41.41.5  42.42.42.5
         43.43.43.5  44.44.44.5  45.45.45.5  46.46.46.5
         47.47.47.5  48.48.48.5  49.49.49.5  50.50.50.5
         103.3.3.5  106.15.15.5
       Graceful Restart enabled; Peer reconnect time (msecs): 120000
```

R2作为Restarter方进行主备倒换或重启LDP时，R1作为Helper方感知到Restarter方进行主备倒换或LDP协议重启后，启动GR Reconnet定时器，在该定时器超时前保留Restarter方相关的转发表项。

如果在Helper方的GR Reconnect定时器超时前Restarter和Helper之间的LDP会话重建完成，则Helper方会删除GR Reconnect定时器，并启动GR Recovery定时器：

```
R1 MPU-0/4 2011-9-22 01:15:36 mpls_ldp_1:GR:
 down nbr 10.10.10.5:0:: wait for reconnecting
R1 MPU-0/4 2011-9-22 01:15:36 mpls_ldp_1:GR: GR session 10.10.10.5:0: lost
R1 MPU-0/4 2011-9-22 01:15:36 mpls_ldp_1:GR: down neighbor 10.10.10.5:0::
```

```
 reconnect timer started [120 secs]
R1 MPU-0/4 2011-9-22 01:15:36 mpls_ldp_1:GR: GR session 10.10.10.5:0::
 bindings retained
R1 MPU-0/4 2011-9-22 01:15:56 mpls_ldp_1:GR: Received FT Sess TLV from
 10.10.10.5:0 (rconn 120, rcov 120)
R1 MPU-0/4 2011-9-22 01:15:56 mpls_ldp_1:GR: Added FT Sess TLV
(Rconn 120000, Rcov 120000) to INIT msg to 10.10.10.5:0
R1 MPU-0/4 2011-9-22 01:15:59 mpls_ldp_1:GR: GR session 10.10.10.5:0::
 established
R1 MPU-0/4 2011-9-22 01:15:59 mpls_ldp_1:GR: ptcl_adj: 10.10.10.5:0::
 reconnect timer stopped
R1 MPU-0/4 2011-9-22 01:15:59 mpls_ldp_1:GR: GR session 10.10.10.5:0::
 state change (Reconnect-Wait -> Recovering)
R1 MPU-0/4 2011-9-22 01:15:59 mpls_ldp_1:GR: ptcl_adj: 10.10.10.5:0::
recovery timer started,120 secs
R1 MPU-0/4 2011-9-22 01:15:59 mpls_ldp_1:GR: 10.10.10.1/-1::
refreshing stale binding from 10.10.10.5:0
R1 MPU-0/4 2011-9-22 01:15:59 mpls_ldp_1:GR: 10.10.10.2/-1::
refreshing stale binding from 10.10.10.5:0
R1 MPU-0/4 2011-9-22 01:15:59 mpls_ldp_1:GR: 10.10.10.5/-1::
refreshing stale binding from 10.10.10.5:0
```

此时在R1上查看Graceful Restart实例：

```
R1#show mpls ldp neighbor graceful-restart instance 1
Peer LDP Ident: 10.10.10.5:0; Local LDP Ident: 10.10.10.1:0
       TCP connection: 10.10.10.5.6751 - 10.10.10.1.646
       State: Oper; Msgs sent/rcvd: 22/126; Downstream
       Up Time: 00:01:58
       LDP discovery sources:
         gei-1/6; Src IP addr: 106.15.15.5
       Addresses bound to peer LDP Ident:
         5.5.5.64  8.8.8.5  9.9.9.5  10.10.10.5
         13.13.13.5  14.14.14.5  15.15.15.5  16.16.16.5
         17.5.5.5  18.18.18.5  19.19.19.5  20.20.20.5
         21.21.21.5  23.23.23.5  24.24.24.5  25.25.25.5
         26.26.26.5  27.27.27.5  28.28.28.5  29.29.29.5
         31.31.31.1  32.32.32.5  33.33.33.5  34.34.34.5
         35.35.35.5  36.36.36.5  37.37.37.5  38.38.38.5
         39.39.39.5  40.40.40.5  41.41.41.5  42.42.42.5
         43.43.43.5  44.44.44.5  45.45.45.5  46.46.46.5
         47.47.47.5  48.48.48.5  49.49.49.5  50.50.50.5
         103.3.3.5  106.15.15.5
       Status: recovering (2 seconds left)
```

在R1上查看LDP标签情况：

```
R1#show mpls forwarding-table 10.10.10.2
Local    Outgoing  Prefix or        Outgoing      Next Hop      M/S
label    label    Tunnel Id        interface
16395    16388    10.10.10.2/32     gei-1/6    106.15.15.5    M
```

以上输出说明Graceful Restart前后的LDP的标签不会变化。

在R1上查看标签的LDP标签的详细信息：

```
R1#show mpls ldp bindings detail instance 1
10.10.10.2/32
    local binding:  label: 16395
      advertised to:
      10.10.10.5:0(deleting)
    remote binding: lsr: 10.10.10.5:0, label: 16388(inuse)(stale)
 10.10.10.5/32
    local binding:  label: 16388
      advertised to:
      10.10.10.5:0(deleting)
    remote binding: lsr: 10.10.10.5:0, label: exp-null(inuse)(stale)
```

以上输出说明Helper方把与GR Restarter相关的转发表项置上了**stale**标记。

在Helper方的GR Recovery定时器超时前，Helper会协助Restarter恢复转发表项，Restarter也会协助Helper恢复转发表项：

```
R1#show mpls ldp neighbor graceful-restart instance 1
Peer LDP Ident: 10.10.10.5:0; Local LDP Ident: 10.10.10.1:0
       TCP connection: 10.10.10.5.6751 - 10.10.10.1.646
       State: Oper; Msgs sent/rcvd: 23/126; Downstream
       Up Time: 00:01:59
       LDP discovery sources:
         gei-1/6; Src IP addr: 106.15.15.5
       Addresses bound to peer LDP Ident:
         5.5.5.64  8.8.8.5  9.9.9.5  10.10.10.5
         13.13.13.5  14.14.14.5  15.15.15.5  16.16.16.5
         17.5.5.5  18.18.18.5  19.19.19.5  20.20.20.5
         21.21.21.5  23.23.23.5  24.24.24.5  25.25.25.5
         26.26.26.5  27.27.27.5  28.28.28.5  29.29.29.5
         31.31.31.1  32.32.32.5  33.33.33.5  34.34.34.5
         35.35.35.5  36.36.36.5  37.37.37.5  38.38.38.5
         39.39.39.5  40.40.40.5  41.41.41.5  42.42.42.5
         43.43.43.5  44.44.44.5  45.45.45.5  46.46.46.5
         47.47.47.5  48.48.48.5  49.49.49.5  50.50.50.5
         103.3.3.5  106.15.15.5
       Graceful Restart enabled; Peer reconnect time (msecs): 120000

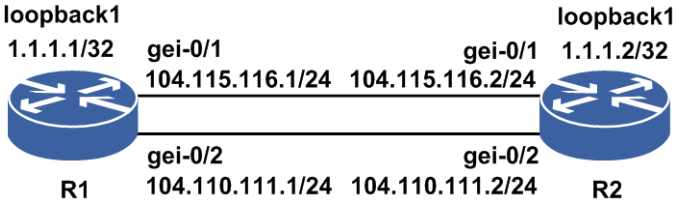
R1#show mpls ldp bindings 10.10.10.2 32 instance 1
 10.10.10.2/32
    local binding:  label: 16395
    remote binding: lsr: 10.10.10.5:0, label: 16388(inuse)
```

6.2.8 LDP 标签负荷分担配置实例

配置说明

如*图 6-7*所示，R1和R2之间启用OSPF协议并配置负荷分担。

图 6-7 LDP 标签负荷分担配置实例图



配置思路

1.R1和R2之间的OSPF协议启用负荷分担。

2.R1和R2之间的接口启用LDP。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
R1(config-if-loopback1)#exit

R1(config)#interface gei-0/2
R1(config-if-gei-0/2)#no shutdown
R1(config-if-gei-0/2)#ip address 104.110.111.1 255.255.255.0
R1(config-if-gei-0/2)#exit

R1(config)#interface gei-0/1
R1(config-if-gei-0/1)#no shutdown
R1(config-if-gei-0/1)#ip address 104.115.116.1 255.255.255.0
R1(config-if-gei-0/1)#exit

R1(config)#router ospf 1
R1(config-ospf-1)#router-id 1.1.1.1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 1.1.1.1  0.0.0.0
R1(config-ospf-1-area-0)#network 104.110.111.0 0.0.0.255
R1(config-ospf-1-area-0)#network 104.115.116.0 0.0.0.255
R1(config-ospf-1-area-0)#maximum-paths 2
R1(config-ospf-1-area-0)#exit

R1(config)#mpls ldp instance 1
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-0/2
R1(config-ldp-1-if-gei-0/2)#exit
R1(config-ldp-1)#interface gei-0/1
R1(config-ldp-1-if-gei-0/1)#exit
R1(config-ldp-1)#end
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.2  255.255.255.255
R2(config-if-loopback1)#exit

R2(config)#interface gei-0/2
R2(config-if-gei-0/2)#no shutdown
R2(config-if-gei-0/2)#ip address 104.110.111.2 255.255.255.0
R2(config-if-gei-0/2)#exit

R2(config)#interface gei-0/1
R2(config-if-gei-0/1)#no shutdown
R2(config-if-gei-0/1)#ip address 104.115.116.2 255.255.255.0
R2(config-if-gei-0/1)#exit

R2(config)#router ospf 1
R2(config-ospf-1)#router-id 1.1.1.2
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 1.1.1.2  0.0.0.0
R2(config-ospf-1-area-0)#network 104.110.111.0 0.0.0.255
R2(config-ospf-1-area-0)#network 104.115.116.0 0.0.0.255
R2(config-ospf-1-area-0)#maximum-paths 2
R2(config-ospf-1-area-0)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-0/2
R2(config-ldp-1-if-gei-0/2)#exit
R2(config-ldp-1)#interface gei-0/1
R2(config-ldp-1-if-gei-0/1)#exit
R2(config-ldp-1)#end
```

配置验证

在R1上查看配置情况：

```
R1(config)#show running-config ospfv2
!<ospfv2>
router ospf 1
 area 0
  maximum-paths 2
    network 1.1.1.1 0.0.0.0
    network 104.110.111.0 0.0.0.255
    network 104.115.116.0 0.0.0.255
  router-id 1.1.1.1
$
!</ospfv2>

R1(config)#show running-config ldp
!<LDP>
mpls ldp instance 1
  interface gei-0/2
  $
  interface gei-0/1
  $
  router-id loopback1
$
!</LDP>
```

在R1上查看配置情况OSPF邻居和LDP邻居情况：

```
R1(config)#show ip ospf neighbor
          OSPF Router with ID (1.1.1.1) (Process ID 1)
Neighbor ID     Pri State       DeadTime  Address         Interface
1.1.1.2         1   FULL/DR     00:00:36  104.110.111.2   gei-0/2

R1(config)#show mpls ldp nei instance 1
Peer LDP Ident: 1.1.1.2:0; Local LDP Ident: 1.1.1.1:0
       TCP connection: 1.1.1.2.26100 - 1.1.1.1.646
       State: Oper; Msgs sent/rcvd: 91/97; Downstream
       Up Time: 01:04:43
       LDP discovery sources:
         gei-0/1; Src IP addr: 104.115.116.2
         gei-0/2; Src IP addr: 104.110.111.2
       Addresses bound to peer LDP Ident:
         1.1.1.2  104.115.116.2  104.110.111.2
```

在R1上查看IGP负荷分担情况：

```
R1(config)#show ip forwarding route 1.1.1.2
IPv4 Routing Table:
status codes: *valid, >best
   Dest            Gw            Interface     Owner      Pri    Metric
*> 1.1.1.2/32      104.110.111.2   gei-0/2     ospf       110    1
*> 1.1.1.2/32      104.115.116.2   gei-0/1     ospf       110    1
```

在R1上查看LDP负荷分担表项情况：

```
R1(config)#show mpls forwarding-table
Local     Outgoing  Prefix or         Outgoing          Next Hop       M/S
label     label     Tunnel Id         interface
16384     Poptag    1.1.1.2/32        gei-0/2        104.110.111.2   M
16384     Poptag    1.1.1.2/32        gei-0/1        104.115.116.2   M

R1(config)#show mpls ldp binding instance 1
 1.1.1.1/32
    local binding:  label: imp-null
    remote binding: lsr: 1.1.1.2:0, label: 16386
 1.1.1.2/32
    local binding:  label: 16384
    remote binding: lsr: 1.1.1.2:0, label: imp-null(inuse:2)
 12.1.1.0/24
```

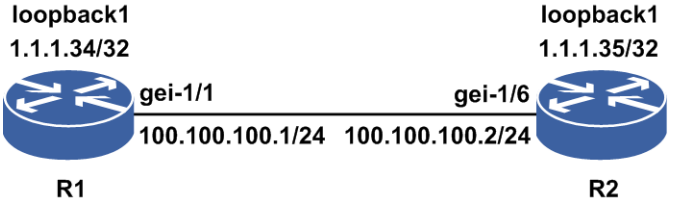
```
    local binding:  label: imp-null
    remote binding: lsr: 1.1.1.2:0, label: imp-null
17.1.1.0/24
    local binding:  label: imp-null
104.110.111.0/24
    local binding:  label: imp-null
    remote binding: lsr: 1.1.1.2:0, label: imp-null
104.115.116.0/24
    local binding:  label: imp-null
    remote binding: lsr: 1.1.1.2:0, label: imp-null
```

6.2.9 LDP BFD 配置实例

配置说明

如*图 6-8*所示是两台建立LDP邻居的路由器，要在两者之间配置LDP BFD功能。

图 6-8 LDP BFD配置实例拓扑图



配置思路

1.配置IGP路由，确保R1和R2的Loopback接口能互通。

2.在R1和R2间的直连接口上开启MPLS功能。

3.配置Loopback接口的IP地址作为LSR的Router-ID。

4.启用LDP BFD功能。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.34 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ip address 100.100.100.1 255.255.255.0
R1(config-if-gei-1/1)#exit

R1(config)#router isis 1
R1(config-isis-1)#area 00.0001
R1(config-isis-1)#system-id 0001.0002.0034
R1(config-isis-1)#interface gei-1/1
R1(config-isis-1-if-gei-1/1)#ip router isis
R1(config-isis-1-if-gei-1/1)#exit
R1(config-isis-1)#interface loopback1
```

```
R1(config-isis-1-if-loopback1)#ip router isis
R1(config-isis-1-if-loopback1)#exit
R1(config-isis-1)#exit

R1(config)#mpls ldp instance 1  /*配置LDP的Router-ID和接口*/
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-1/1
R1(config-ldp-1-if-gei-1/1)#exit
R1(config-ldp-1)#bfd 1.1.1.35 32 interval 100 min-rx 20 multiplier 5
R1(config-ldp-1)#exit
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.35 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/6
R1(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/6)#ip address 100.100.100.2 255.255.255.0
R2(config-if-gei-1/6)#exit

R2(config)#router isis 1
R2(config-isis-1)#area 00.0002
R2(config-isis-1)#system-id 0002.0002.0035
R2(config-isis-1)#interface gei-1/6
R2(config-isis-1-if-gei-1/6)#ip router isis
R2(config-isis-1-if-gei-1/6)#exit
R2(config-isis-1)#interface loopback1
R2(config-isis-1-if-loopbck1)#ip router isis
R2(config-isis-1-if-loopbck1)#exit
R2(config-isis-1)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-1/6
R2(config-ldp-1-if-gei-1/6)#exit
R2(config-ldp-1)#bfd 1.1.1.34 32 interval 100 min-rx 20 multiplier 5
R2(config-ldp-1)#exit
```

在以上配置中，运行IS-IS动态路由协议的目的是为了通告各LSR的Router-ID，即Loopback接口地址的路由。

使用Loopback接口地址作为LDP实例的路由器标识（Router-ID），有利于保证路由器LDP ID的稳定。因为Loopback接口地址的状态是稳定不变的（除非手工关闭该接口）。

配置验证

在R2上查看LDP邻居的建立情况：

```
R2(config)#show mpls ldp neighbor detail instance 1
Peer LDP Ident: 1.1.1.34:0; Local LDP Ident 1.1.1.35:0
       TCP connection: 1.1.1.34.646 - 1.1.1.35.1069
       state: Oper; Msgs sent/rcvd: 47/48; Downstream
       Up Time: 00:00:30
       LDP discovery sources:
         gei-1/6; Src IP addr: 100.100.100.1
           holdtime: 15000 ms, hello interval: 5000 ms
       Addresses bound to peer LDP Ident:
         1.1.1.34 100.100.100.1
       Session holdtime: 180000 ms; KA interval: 60000 ms
       LDP Peer BFD not register.
       LDP dynamic capability enable:
       LDP send capability:
         LDP dynamic capability
         LDP Typed Wildcard FEC Cap
         LDP Unrecognized Noti Cap
```

```
      LDP received capability:
        LDP dynamic capability negotiate success
        LDP Typed Wildcard FEC Cap negotiate success
        LDP Unrecognized Noti Cap negotiate success
```

以上输出中的“state: Oper”，表示会话的状态是**Oper**，说明参数协商正确，和1.1.1.34（R1）的邻居关系已建立。

在R1上查看LDP BFD邻居的建立情况：

```
R1(config)#show bfd neighbor ldp brief
PeerAddr       PrefixLen  LD      RD       Hold   State
1.1.1.35       32       2050     2050     60     UP
100.100.100.2   0        2049     2049     500    UP


R1(config)#show bfd neighbor ldp detail
------------------------------------------------------------------------------
--
PeerAddr :1.1.1.35
Prefixlen:32
Local Discr:2050          Remote Discr:2050          State:UP

Holdown(ms):60           Vpnid:0                   VRF Name:--
BFD Type:LDP[Active]
Instance Name:
------------------------------------------------------------------------------
--
Version:1               Dest UDP Port:3784       Final Bit:1
Local Diag:0            Demand Mode:0            Poll Bit:0
MinTxInt:100            MinRxInt:20             Multiplier:5
Received MinTxInt:10     Received MinRxInt:10     Received Multiplier:3
Length:24               Min Echo Interval:0

Rx Count:6393           Rx Interval (ms) min/max/avg:2    /18    /10
Tx Count:1457           Tx Interval (ms) min/max/avg:79   /79    /79
Registered Protocols:LDP LSP
Uptime:0 day(s),0 hour(s),2 minute(s)
Control Plane Rcv Phy Interface Name:gei-1/1
==============================================================================
==
------------------------------------------------------------------------------
--
PeerAddr :100.100.100.2
Prefixlen:0
Local Discr:2049          Remote Discr:2049          State:UP

Holdown(ms):500          Vpnid:0                   VRF Name:--
BFD Type:LDP[Passive]
Instance Name:
------------------------------------------------------------------------------
--
Version:1               Dest UDP Port:3784       Final Bit:1
Local Diag:0            Demand Mode:0            Poll Bit:0
MinTxInt:10             MinRxInt:10             Multiplier:3
Received MinTxInt:100    Received MinRxInt:20     Received Multiplier:5
Length:24               Min Echo Interval:0

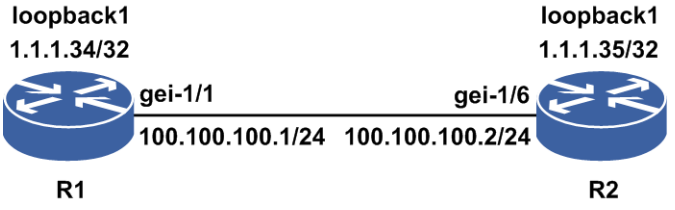
Rx Count:1983           Rx Interval (ms) min/max/avg:0    /78    /39
Tx Count:8586           Tx Interval (ms) min/max/avg:18   /18    /18
Registered Protocols:---
Uptime:0 day(s),0 hour(s),2 minute(s)
Control Plane Rcv Phy Interface Name:gei-1/1
==============================================================================
==
```

6.2.10 PEER BFD 配置实例

配置说明

如*图 6-9*所示，两台路由器建立LDP邻居，再在两者之间配置PEER BFD功能。

图 6-9 PEER BFD 配置实例拓扑图



配置思路

1.配置IGP路由，使R1和R2的Loopback接口能互通。

2.在R1和R2间的直连接口上启用MPLS功能。

3.配置Loopback接口的IP地址作为LSR的Router-ID。

4.启用PEER BFD功能。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.34 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ip address 100.100.100.1 255.255.255.0
R1(config-if-gei-1/1)#exit

R1(config)#router isis 1
R1(config-isis-1)#area 00.0001
R1(config-isis-1)#system-id 0001.0002.0034
R1(config-isis-1)#interface gei-1/1
R1(config-isis-1-if-gei-1/1)#ip router isis
R1(config-isis-1-if-gei-1/1)#exit
R1(config-isis-1)#interface loopback1
R1(config-isis-1-if-loopback1)#ip router isis
R1(config-isis-1-if-loopback1)#exit
R1(config-isis-1)#exit

R1(config)#mpls ldp instance 1
/*配置LDP的Router-ID和接口*/
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-1/1
R1(config-ldp-1-if-gei-1/1)#exit
R1(config-ldp-1)#peer bfd remote-routerid 1.1.1.35
R1(config-ldp-1)#exitt
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.35 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/6
R2(config-if-gei-1/6)#no shutdown
R2(config-if-gei-1/6)#ip address 100.100.100.2 255.255.255.0
R2(config-if-gei-1/6)#exit

R2(config)#router isis 1
R2(config-isis-1)#area 00.0002
R2(config-isis-1)#system-id 0002.0002.0035
R2(config-isis-1)#interface gei-1/6
R2(config-isis-1-if-gei-1/6)#ip router isis
R2(config-isis-1-if-gei-1/6)#exit
R2(config-isis-1)#interface loopback1
R2(config-isis-1-if-loopbck1)#ip router isis
R2(config-isis-1-if-loopbck1)#exit
R2(config-isis-1)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-1/6
R2(config-ldp-1-if-gei-1/6)#exit
R2(config-ldp-1)#peer bfd remote-routerid 1.1.1.34
R2(config-ldp-1)#exit
```

在以上配置中，运行IS-IS动态路由协议的目的是为了通告各LSR的Router-ID，即Loopback接口地址的路由。

使用Loopback接口地址作为LDP实例的路由器标识（Router-ID），有利于保证路由器LDP ID的稳定，因为Loopback接口地址的状态是稳定不变的（除非手工关闭该接口）。

配置验证

在R2上查看LDP邻居的建立情况：

```
R2(config)#show mpls ldp neighbor detail instance 1
Peer LDP Ident: 1.1.1.34:0; Local LDP Ident 1.1.1.35:0
       TCP connection: 1.1.1.34.646 - 1.1.1.35.1069
       state: Oper; Msgs sent/rcvd: 47/48; Downstream
       Up Time: 00:00:30
       LDP discovery sources:
         gei-1/6; Src IP addr: 100.100.100.1
           holdtime: 15000 ms, hello interval: 5000 ms
       Addresses bound to peer LDP Ident:
         1.1.1.34 100.100.100.1
       Session holdtime: 180000 ms; KA interval: 60000 ms
       LDP Peer BFD state up.
       LDP dynamic capability enable:
       LDP send capability:
         LDP dynamic capability
         LDP Typed Wildcard FEC Cap
         LDP Unrecognized Noti Cap
         LDP received capability:
         LDP dynamic capability negotiate success
         LDP Typed Wildcard FEC Cap negotiate success
         LDP Unrecognized Noti Cap negotiate success
```

在以上输出中“state: Oper”表示会话的状态是**Oper**，说明参数协商正确，和1.1.1.34（R1）的邻居关系已建立。

在R1上查看PEER BFD邻居的建立情况：

```
R1(config-ldp-1)#show bfd neighbors ip brief
LocalAddr     PeerAddr       LD       RD       Hold   State    Interface
```

```
1.1.1.34      1.1.1.35       2087     2085     150    UP          --

R1(config-ldp-1)#show bfd neighbors ip detail
------------------------------------------------------------------------------
--
LocalAddr:1.1.1.34
PeerAddr :1.1.1.35
Local Discr:2087          Remote Discr:2085          State:UP

Holdown(ms):150           Interface:---
Vpnid:0                  VRF Name:---
BFD Type:MultiHop
Instance Name:1
------------------------------------------------------------------------------
--
Version:1               Dest UDP Port:4784       Final Bit:1
Local Diag:0             Demand Mode:0           Poll Bit:0
MinTxInt:50              MinRxInt:50            Multiplier:3
Received MinTxInt:50      Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24         Max BFD Length:24

Rx Count:8746            Rx Interval (ms) min/max/avg:0     /49    /24
Tx Count:9124            Tx Interval (ms) min/max/avg:46    /46    /46
Registered Protocols:LDPINSTANCE
Uptime:0 day(s),0 hour(s),7 minute(s)
Control Plane Rcv Phy Interface Name:gei-1/1
==============================================================================
==
```

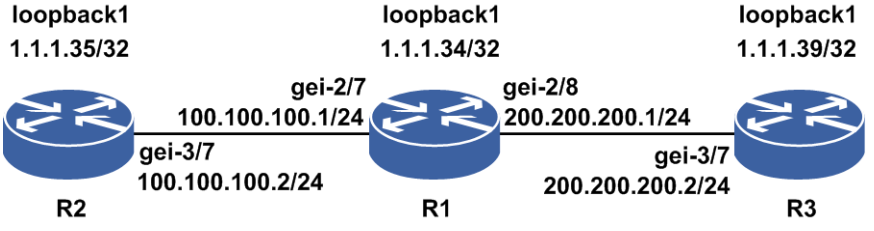
6.2.11 GTSM 配置实例

配置说明

如*图 6-10*所示：

- 配置非直连GTSM时，需在R2上配置非直连会话的GTSM跳数为1，使R2-R3之间的target会话不能建立。
- 配置直连GTSM时，需在R2上配置直连GTSM，R1上配置直连GTSM，使两端协商生效。

图 6-10 GTSM 配置实例拓扑图



配置思路

1.R1与R2建立直连会话。

2.R1与R3建立直连会话。

3.R2与R3建立target会话。

4.R2上配置非直连GTSM跳数为1，等待超时，R2-R3之间的非直连会话down。

5.R2上配置直连GTSM。

6.R1上配置直连GTSM。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.34 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-2/7
R1(config-if-gei-2/7)#no shutdown
R1(config-if-gei-2/7)#ip address 100.100.100.1 255.255.255.0
R1(config-if-gei-2/7)#exit
R1(config)#interface gei-2/8
R1(config-if-gei-2/8)#no shutdown
R1(config-if-gei-2/8)#ip address 200.200.200.1 255.255.255.0
R1(config-if-gei-2/8)#exit
R1(config)#router isis
R1(config-isis-0)#area 00.0001
R1(config-isis-0)#system-id 0001.0002.0034
R1(config-isis-0)#interface gei-2/7
R1(config-isis-0-if-gei-2/7)#ip router isis
R1(config-isis-0-if-gei-2/7)#exit
R1(config-isis-0)#interface gei-2/8
R1(config-isis-0-if-gei-2/8)#ip router isis
R1(config-isis-0-if-gei-2/8)#exit
R1(config-isis-0)#interface loopback1
R1(config-isis-0-if-loopback1)#ip router isis
R1(config-isis-0-if-loopback1)#exit
R1(config-isis-0)#exit

R1(config)#mpls ldp instance 1
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-2/7

/*配置直连GTSM */
R1(config-ldp-1-if-gei-2/7)#gtsm
R1(config-ldp-1-if-gei-2/7)#exit
R1(config-ldp-1)#interface gei-2/8
R1(config-ldp-1-if-gei-2/8)#exit
R1(config-ldp-1)#exit
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.35 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-3/7
R2(config-if-gei-3/7)#no shutdown
R2(config-if-gei-3/7)#ip address 100.100.100.2 255.255.255.0
R2(config-if-gei-3/7)#exit

R2(config)#router isis
R2(config-isis-0)#area 00.0002
R2(config-isis-0)#system-id 0002.0002.0035
R2(config-isis-0)#interface gei-3/7
R2(config-isis-0-if-gei-3/7)#ip router isis
R2(config-isis-0-if-gei-3/7)#exit
R2(config-isis-0)#interface loopback1
R2(config-isis-0-if-loopback1)#ip router isis
```

```
R2(config-isis-0-if-loopback1)#exit
R2(config-isis-0)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp)#interface gei-3/7

/*配置直连GTSM*/
R2(config-ldp-1-if-gei-3/7)#gtsm
R2(config-ldp-1-if-gei-3/7)#exit
R2(config-ldp-1)#target-session 1.1.1.39

/*等到R2-R3的target会话up后，配置GTSM跳数为1，邻居地址配置为R3的router-id*/
R2(config-ldp-1)#gtsm target-neighbor 1.1.1.39 hop-count 1
R2(config-ldp-1)#exit
```

R3上的配置如下：

```
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 1.1.1.39 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-3/7
R3(config-if-gei-3/7)#no shutdown
R3(config-if-gei-3/7)#ip address 200.200.200.2 255.255.255.0
R3(config-if-gei-3/7)#exit

R3(config)#router isis
R3(config-isis-0)#area 00.0003
R3(config-isis-0)#system-id 0003.0003.0039
R3(config-isis-0)#interface gei-3/7
R3(config-isis-0-if-gei-3/7)#ip router isis
R3(config-isis-0-if-gei-3/7)#exit
R3(config-isis-0)#interface loopback1
R3(config-isis-0-if-loopback1)#ip router isis
R3(config-isis-0-if-loopback1)#exit
R3(config-isis-0)#exit

R3(config)#mpls ldp instance 1
R3(config-ldp-1)#router-id loopback1
R3(config-ldp-1)#interface gei-3/7
R3(config-ldp-1-if-gei-3/7)#exit
R3(config-ldp-1)#target-session 1.1.1.35
R3(config-ldp-1)#exit
```

配置验证

使用**show mpls ldp neighbor**命令在R2上查看邻居的建立情况（配置GTSM后，会话超时down前）。

```
R2(config)#show mpls ldp neighbor instance 1
Peer LDP Ident: 1.1.1.39:0; Local LDP Ident 1.1.1.35:0
TCP connection: 1.1.1.39.1072 - 1.1.1.39.646
state: Oper; Msgs sent/rcvd: 50/46; Downstream
Up Time: 00:00:02
LDP discovery sources:
Targeted Hello (1.1.1.39); Src IP addr: 1.1.1.39
Addresses bound to peer LDP Ident:
1.1.1.39 100.100.100.2 200.200.200.2
LDP neighbor may be up to 1 hops away
```

等待keepalive超时，会话会down 。因为GTSM非直连会话跳数设置为1，R2-R3之间的跳数为2，R2不能收到R3的报文，导致会话down。将GTSM配置删除，会话会重新up。

使用**show mpls ldp neighbor**命令在R1上查看邻居的建立情况（R1，R2的直连

GTSM配置协商成功）。

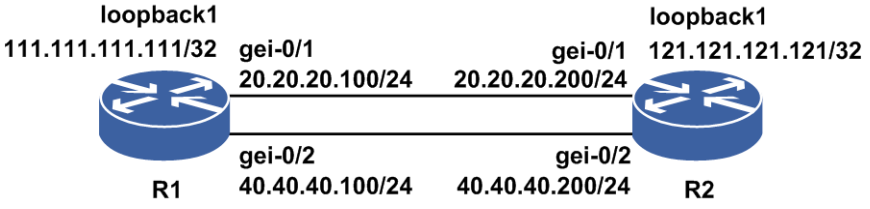
```
R1(config)#show mpls ldp neighbor instance 1
Peer LDP Ident: 1.1.1.35:0; Local LDP Ident 1.1.1.34:0
 TCP connection: 1.1.1.35.646 - 1.1.1.34.1072
 state: Oper; Msgs sent/rcvd: 46/50; Downstream
 Up Time: 00:00:02
 LDP discovery sources:
 gei-2/7; Src IP addr: 100.100.100.2
 Addresses bound to peer LDP Ident:
 1.1.1.35 100.100.100.2
 LDP neighbor may be up to 1 hops away
```

6.2.12 IGP 同步配置实例（OSPF）

配置说明

如*图6-8*所示，配置IGP同步，在R1上配置LDP IGP同步，R1节点的两个OSPF接口下开启IGP同步生效功能。

图 6-81 IGP 同步配置实例拓扑图



配置思路

1.R1与R2建立直连会话。

2.R1上配置OSPF实例，OSPF实例配置IGP同步。

3.R1上配置同步延时定时器时长为10秒。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 111.111.111.111 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-0/1
R1(config-if-gei-0/1)#ip address 20.20.20.100 255.255.255.0
R1(config-if-gei-0/1)#no shutdown
R1(config-if-gei-0/1)#exit
R1(config)#interface gei-0/2
R1(config-if-gei-0/2)#ip address 40.40.40.100 255.255.255.0
R1(config-if-gei-0/2)#no shutdown
R1(config-if-gei-0/2)#exit

R1(config)#router ospf 1
R1(config-ospf-1)#mpls ldp sync
```

```
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 0.0.0.0 255.255.255.255
R1(config-ospf-1-area-0)#exit

R1(config)#mpls ldp instance 1
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-0/1
R1(config-ldp-1)#interface gei-0/2
R1(config-ldp-1)#igp sync delay 10
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 121.121.121.121 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-0/1
R2(config-if-gei-0/1)#ip address 20.20.20.200 255.255.255.0
R2(config-if-gei-0/1)#no shutdown
R2(config-if-gei-0/1)#exit
R2(config)#interfacegei-0/2
R2(config-if-gei-0/2)#ip address 40.40.40.200 255.255.255.0
R2(config-if-gei-0/2)#no shutdown
R2(config-if-gei-0/2)#exit

R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 0.0.0.0 255.255.255.255
R2(config-ospf-1-area-0)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-0/1
R2(config-ldp-1)#interface gei-0/2
```

配置验证

使用**show mpls ldp neighbor**命令在R1上查看邻居的建立情况（两个接口收到的hello均维护该session）。

```
Peer LDP Ident: 121.121.121.121:0; Local LDP Ident: 111.111.111.111:0
 TCP connection: 121.121.121.121.26459 - 111.111.111.111.646
 State: Oper; Msgs sent/rcvd: 47/64; Downstream
 Up Time: 00:29:46
 LDP discovery sources:
 gei-0/1; Src IP addr: 20.20.20.200
 gei-0/2; Src IP addr: 40.40.40.200
 Addresses bound to peer LDP Ident:
 20.20.20.200 40.40.40.200 121.121.121.121
```

使用**show mpls ldp igp sync ins 1**命令查看R1上的LDP IGP同步信息和同步状态。

```
  gei-0/1:
 LDP configured; LDP-IGP Synchronization enabled.
 Sync status: Ready
 Peers:
 121.121.121.121:0 (Fully Operational)

gei-0/2:
 LDP configured; LDP-IGP Synchronization enabled.
 Sync status: Ready
 Peers:
 121.121.121.121:0 (Fully Operational)
```

用**show ip ospf interface**命令查看R1上OSPF接口的LDP IGP同步信息和同步状

态。

```
 OSPF Router with ID (20.20.20.100) (Process ID 1)

gei-0/2 is up
Track State is unknown
Internet Address 40.40.40.100 255.255.255.0 enable
Up for 01:00:28
In the area 0.0.0.0 DR
Cost 1, Priority 1, Network Type broadcast
Transmit Delay(sec) 1, Authentication Type null
TTL security disabled
LDP sync enabled
LDP sync state achieved
Sending max metric
Timer intervals(sec) : Hello 10, Dead 40, Retransmit 5
Designated Router (ID) 20.20.20.100, Interface address 40.40.40.100
Backup Designated router (ID) 22.22.22.22, Interface address 40.40.40.200
Number of Neighbors 1, Number of Adjacent neighbors 1
22.22.22.22 BDR
```

在R2上的gei-0/2接口下做**shutdown**操作，查看R1上gei-0/2接口的OSPF IGP同步状态以及路由的metric值。

使用**show mpls ldp igp sync ins 1**命令查看R1上的LDP IGP同步信息和同步状态，可以看到gei-0/2接口的IGP同步状态变为Not ready。

```
 gei-0/1:
 LDP configured; LDP-IGP Synchronization enabled.
 Sync status: Ready
 Peers:
 121.121.121.121:0 (Fully Operational)

 gei-0/2:
 LDP configured; LDP-IGP Synchronization enabled.
 Sync status: Not ready
    Peers:
```

使用**show ip ospf interface**命令查看R1上OSPF接口的LDP IGP同步信息和同步状态，可以看到gei-0/2接口下的LDP IGP同步状态为unachieved。

```
 OSPF Router with ID (20.20.20.100) (Process ID 1)

gei-0/2 is up
Track State is unknown
Internet Address 40.40.40.100 255.255.255.0 enable
Up for 01:37:22
In the area 0.0.0.0 DR
Cost 1, Priority 1, Network Type broadcast
Transmit Delay(sec) 1, Authentication Type null
TTL security disabled
LDP sync enabled
LDP sync state unachieved
Sending max metric
Timer intervals(sec) : Hello 10, Dead 40, Retransmit 5
Designated Router (ID) 20.20.20.100, Interface address 40.40.40.100
Backup Designated router (ID) 22.22.22.22, Interface address 40.40.40.200
Number of Neighbors 1, Number of Adjacent neighbors 1
22.22.22.22 BDR
```

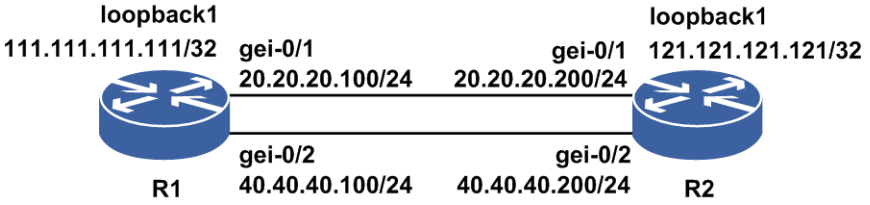
6.2.13 IGP 同步配置实例（IS-IS）

配置说明

如*图 6-92*所示，配置IGP同步，要求在R1上配置LDP IGP同步，R1节点的两个IS-IS

接口下开启IGP同步生效。

图 6-92 IGP 同步配置实例拓扑图



配置思路

1.R1与R2建立直连会话。

2.R1上配置IS-IS实例，IS-IS实例配置IGP同步。

3.R1上配置同步延时定时器时长为10秒。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 111.111.111.111 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-0/1
R1(config-if-gei-0/1)# ip address 20.20.20.100 255.255.255.0
R1(config-if-gei-0/1)# no shutdown
R1(config-if-gei-0/1)#exit
R1(config)#interface gei-0/2
R1(config-if-gei-0/2)# ip address 40.40.40.100 255.255.255.0
R1(config-if-gei-0/2)# no shutdown
R1(config-if-gei-0/2)#exit

R1(config)#router isis
R1(config-isis-0)#area 00.0001
R1(config-isis-0)#system-id 0001.0002.0034
R1(config-isis-0)#mpls ldp sync
R1(config-isis-0)#interface gei-0/1
R1(config-isis-0-if-gei-0/1)#ip router isis
R1(config-isis-0-if-gei-0/1)#exit
R1(config-isis-0)#interface gei-0/2
R1(config-isis-0-if-gei-0/2)#ip router isis
R1(config-isis-0-if-gei-0/2)#exit
R1(config-isis-0)#interface loopback1
R1(config-isis-0-if-loopback1)#ip router isis
R1(config-isis-0-if-loopback1)#exit
R1(config-isis-0)#exit

R1(config)#mpls ldp instance 1
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-0/1
R1(config-ldp-1)#interface gei-0/2
R1(config-ldp-1)#igp sync delay 10
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 121.121.121.121 255.255.255.255
```

```
R2(config-if-loopback1)#exit
R2(config)#interface gei-0/1
R2(config-if-gei-0/1)# ip address 20.20.20.200 255.255.255.0
R2(config-if-gei-0/1)# no shutdown
R2(config-if-gei-0/1)#exit
R2(config)#interface gei-0/2
R2(config-if-gei-0/2)# ip address 40.40.40.200 255.255.255.0
R2(config-if-gei-0/2)# no shutdown
R2(config-if-gei-0/2)#exit

R2(config)#router isis
R2(config-isis-0)#area 00.0002
R2(config-isis-0)#system-id 0002.0002.0035
R2(config-isis-0)#mpls ldp sync
R2(config-isis-0)#interface gei-0/1
R2(config-isis-0-if-gei-0/1)#ip router isis
R2(config-isis-0-if-gei-0/1)#exit
R2(config-isis-0)#interface gei-0/2
R2(config-isis-0-if-gei-0/2)#ip router isis
R2(config-isis-0-if-gei-0/2)#exit
R2(config-isis-0)#interface loopback1
R2(config-isis-0-if-loopbck1)#ip router isis
R2(config-isis-0-if-loopbck1)#exit
R2(config-isis-0)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-0/1
R2(config-ldp-1)#interface gei-0/2
```

配置验证

使用**show mpls ldp neighbor**命令在R1上查看邻居的建立情况（两个接口收到的hello均维护该session）。

```
Peer LDP Ident: 121.121.121.121:0; Local LDP Ident: 111.111.111.111:0
 TCP connection: 121.121.121.121.26469 - 111.111.111.111.646
 State: Oper; Msgs sent/rcvd: 22/21; Downstream
 Up Time: 00:14:03
 LDP discovery sources:
 gei-0/1; Src IP addr: 20.20.20.200
 gei-0/2; Src IP addr: 40.40.40.200
 Addresses bound to peer LDP Ident:
 20.20.20.200 40.40.40.200 121.121.121.121
```

使用**show mpls ldp igp sync ins 1**命令查看R1上的LDP IGP同步信息和同步状态。

```
 gei-0/1:
 LDP configured; LDP-IGP Synchronization enabled.
 Sync status: Ready
 Peers:
 121.121.121.121:0 (Fully Operational)

 gei-0/2:
 LDP configured; LDP-IGP Synchronization enabled.
 Sync status: Ready
 Peers:
 121.121.121.121:0 (Fully Operational)
```

使用**show isis circuits detail**命令查看R1上IS-IS接口的LDP IGP同步信息和同步状态为Achieved状态。

```
inspur(config-isis-0)#show isis circuits detail
Process ID: 0
 Interface:gei-0/1
```

```
Status:Up
Track Status:Unknown
Encapsulation:SAP
Circuit Type:Level-1-2
MPLS LDP Sync(L1/L2): Enable/Enable, Sync Status(L1/L2): Achieved/Achieved
Level-1 Metric:10 Priority:64 LAN ID:no found
Number of active adjacencies:0
Next hello in seconds:3
Level-2 Metric:10 Priority:64 LAN ID:IR12000.02
Number of active adjacencies:1
Next hello in seconds:3

Interface:gei-0/2
Status:Up
Track Status:Unknown
Encapsulation:SAP
Circuit Type:Level-1-2
MPLS LDP Sync(L1/L2): Enable/Enable, Sync Status(L1/L2): Achieved/Achieved
Level-1 Metric:10 Priority:64 LAN ID:no found
Number of active adjacencies:0
Next hello in seconds:8
Level-2 Metric:10 Priority:64 LAN ID:IR12000.03
Number of active adjacencies:1
Next hello in seconds:8

Interface:loopback11
Status:Up
Track Status:Unknown
Encapsulation:SAP
Circuit Type:Level-1-2
MPLS LDP Sync(L1/L2): Enable/Enable, Sync Status(L1/L2): Unknown/Unknown
Level-1 Metric:10 Level-2 Metric:10 Circuit ID:IR12000.00
Active Adj state:No adjacency
Next hello in seconds:0
```

在R2上的gei-0/2接口下做**shutdown**操作，查看R1上gei-0/2接口的IS-IS IGP同步状态以及路由的metric值。

使用**show mpls ldp igp sync ins 1**命令查看R1上的LDP IGP同步信息和同步状态，可以看到gei-0/2接口下的LDP IGP同步状态变为Not ready。

```
gei-0/1:
LDP configured; LDP-IGP Synchronization enabled.
Sync status: Ready
Peers:
121.121.121.121:0 (Fully Operational)

gei-0/2:
LDP configured; LDP-IGP Synchronization enabled.
Sync status: Not ready
  Peers:
```

使用**show isis circuits detail**命令查看R1上IS-IS接口的LDP IGP同步信息和同步状态，可以看到gei-0/2接口下的LDP IGP同步状态为unachieved。

```
Process ID: 0
 Interface:gei-0/1
 Status:Up
 Track Status:Unknown
 Encapsulation:SAP
 Circuit Type:Level-1-2
 MPLS LDP Sync(L1/L2): Enable/Enable, Sync Status(L1/L2): Achieved/Achieved
 Level-1 Metric:10 Priority:64 LAN ID:no found
 Number of active adjacencies:0
 Next hello in seconds:7
 Level-2 Metric:10 Priority:64 LAN ID:IR12000.02
 Number of active adjacencies:1
 Next hello in seconds:7
```

```
 Interface:gei-0/2
 Status:Up
 Track Status:Unknown
 Encapsulation:SAP
 Circuit Type:Level-1-2
 MPLS     LDP     Sync(L1/L2):     Enable/Enable,     Sync     Status(L1/L2):
UnAchieved/UnAchieved
 Level-1 Metric:63 Priority:64 LAN ID:no found
 Number of active adjacencies:0
 Next hello in seconds:2
 Level-2 Metric:63 Priority:64 LAN ID:no found
 Number of active adjacencies:0
 Next hello in seconds:2

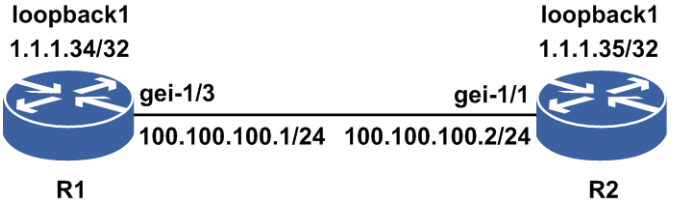
 Interface:loopback11
  Status:Up
 Track Status:Unknown
 Encapsulation:SAP
 Circuit Type:Level-1-2
 MPLS LDP Sync(L1/L2): Enable/Enable, Sync Status(L1/L2): Unknown/Unknown
 Level-1 Metric:10 Level-2 Metric:10 Circuit ID:IR12000.00
 Active Adj state:No adjacency
 Next hello in seconds:0
```

6.2.14 报文过滤配置实例

配置说明

如*图 6-10*所示，两台设备R1与R2建立LDP邻居，在R1上配置报文过滤功能。

图 6-103 报文过滤配置实例拓扑图



配置思路

1.配置IGP路由，使R1和R2的Loopback接口能互通。

2.在R1和R2间的直连接口上启用MPLS功能。

3.配置Loopback接口的IP地址作为LSR的Router-ID。

4.R1配置ACL规则。

5.R1启用报文过滤功能。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
```

```
R1(config-if-loopback1)#ip address 1.1.1.34 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#ip address 100.100.100.1 255.255.255.0
R1(config-if-gei-1/3)#exit

R1(config)#router isis 1
R1(config-isis-1)#area 00.0001
R1(config-isis-1)#system-id 0001.0002.0034
R1(config-isis-1)#interface gei-1/3
R1(config-isis-1-if-gei-1/3)#ip router isis
R1(config-isis-1-if-gei-1/3)#exit
R1(config-isis-1)#interface loopback1
R1(config-isis-1-if-loopback1)#ip router isis
R1(config-isis-1-if-loopback1)#exit
R1(config-isis-1)#exit

R1(config)#mpls ldp instance 1
/*配置LDP的Router-ID和接口*/
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-1/3
R1(config-ldp-1-if-gei-1/3)#exit
R1(config-ldp-1)#exit

R1(config)#ipv4-access-list 1
R1(config-ipv4-acl)#rule 1 deny tcp 1.1.1.35 0.0.0.0 any
R1(config-ipv4-acl)#rule 2 deny udp 100.100.100.2 0.0.0.0 any
R1(config-ipv4-acl)#rule 3 permit any

R1(config)#mpls ldp instance 1
R1(config-ldp-1)#filter packet for 1
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.35 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 100.100.100.2 255.255.255.0
R2(config-if-gei-1/1)#exit

R2(config)#router isis
R2(config-isis-1)#area 00.0002
R2(config-isis-1)#system-id 0002.0002.0035
R2(config-isis-1)#interface gei-1/1
R2(config-isis-1-if-gei-1/1)#ip router isis
R2(config-isis-1-if-gei-1/1)#exit
R2(config-isis-1)#interface loopback1
R2(config-isis-1-if-loopbck1)#ip router isis
R2(config-isis-1-if-loopbck1)#exit
R2(config-isis-1)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-1/1
R2(config-ldp-1-if-gei-1/1)#exit
R2(config-ldp-1)#exit
```

提示：

·在以上配置中，运行IS-IS动态路由协议的目的是为了通告各LSR的Router-ID，即Loopback接口地址的路由。

·报文过滤可以仅UDP报文过滤，也可仅TCP报文过滤，依靠ACL规则。

配置验证

在R2上查看LDP邻居的建立情况：

```
R2(config)#show mpls ldp neighbor detail instance 1
Peer LDP Ident: 1.1.1.34:0; Local LDP Ident 1.1.1.35:0
 TCP connection: 1.1.1.34.646 - 1.1.1.35.1069
 State: Sent; Msgs sent/rcvd: 1/0; Downstream
 Up Time: 00:00:30
 LDP discovery sources:
 gei-1/1; Src IP addr: 100.100.100.1
 holdtime: 15000 ms, hello interval: 5000 ms
 Addresses bound to peer LDP Ident:
 Session holdtime: 180000 ms; KA interval: 60000 ms
 LDP Peer BFD not register.
 LDP dynamic capability disable:
 LDP send capability:
 LDP dynamic capability
 LDP Typed Wildcard FEC Cap
 LDP Unrecognized Noti Cap
 LDP received capability:
```

在以上输出中"state: Sent"表示会话的状态是Sent，说明本端虽然发起了TCP链接，并且链接已建立，但对端R1启用了报文过滤，最终会话无法达到Oper状态。

在R1上查看邻居建立情况：

```
R1(config)#show mpls ldp neighbor detail instance 1
```

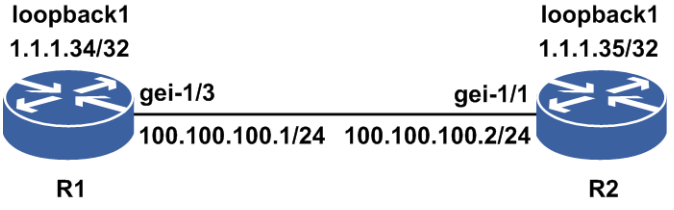
显示空内容，说明本端收到的UDP、TCP报文丢弃。

6.2.15 Label-distribution 配置实例

配置说明

如*图* **6-4**所示，两台设备R1与R2建立LDP邻居，在两者之间的直连接口上配置**label-distribution dod**功能。

图 6-14 Label-distribution dod 配置实例拓扑图



配置思路

1.配置IGP路由，使R1和R2的Loopback接口能互通。

2.在R1和R2间的直连接口上启用MPLS功能。

3.在R1和R2间的直连接口上配置**label-distribution dod**。

4.Reset MPLS实例。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.34 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#ip address 100.100.100.1 255.255.255.0
R1(config-if-gei-1/3)#exit

R1(config)#router isis 1
R1(config-isis-1)#area 00.0001
R1(config-isis-1)#system-id 0001.0002.0034
R1(config-isis-1)#interface gei-1/3
R1(config-isis-1-if-gei-1/3)#ip router isis
R1(config-isis-1-if-gei-1/3)#exit
R1(config-isis-1)#interface loopback1
R1(config-isis-1-if-loopback1)#ip router isis
R1(config-isis-1-if-loopback1)#exit
R1(config-isis-1)#exit

R1(config)#mpls ldp instance 1
/*配置LDP的Router-ID和接口*/
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-1/3
R1(config-ldp-1-if-gei-1/3)#label-distribution dod
R1(config-ldp-1-if-gei-1/3)#exit
R1(config-ldp-1)#exit
R1(config)#reset mpls ldp instance 1
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.35 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 100.100.100.2 255.255.255.0
R2(config-if-gei-1/1)#exit

R2(config)#router isis
R2(config-isis-1)#area 00.0002
R2(config-isis-1)#system-id 0002.0002.0035
R2(config-isis-1)#interface gei-1/1
R2(config-isis-1-if-gei-1/1)#ip router isis
R2(config-isis-1-if-gei-1/1)#exit
R2(config-isis-1)#interface loopback1
R2(config-isis-1-if-loopbck1)#ip router isis
R2(config-isis-1-if-loopbck1)#exit
R2(config-isis-1)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-1/1
R2(config-ldp-1-if-gei-1/3)#label-distribution dod
R2(config-ldp-1-if-gei-1/1)#exit
R2(config-ldp-1)#exit
R2(config)#reset mpls ldp instance 1
```

配置验证

在R2上查看LDP邻居的建立情况：

```
R2(config)#show mpls ldp neighbor detail instance 1
Peer LDP Ident: 1.1.1.34:0; Local LDP Ident 1.1.1.35:0
 TCP connection: 1.1.1.34.646 - 1.1.1.35.1069
 state: Oper; Msgs sent/rcvd: 47/48; Downstream on Demand
 Up Time: 00:00:30
 LDP discovery sources:
 gei-1/1; Src IP addr: 100.100.100.1
 holdtime: 15000 ms, hello interval: 5000 ms
 Addresses bound to peer LDP Ident:
 1.1.1.34 100.100.100.1
 Session holdtime: 180000 ms; KA interval: 60000 ms
 LDP Peer BFD not register.
 LDP dynamic capability enable:
 LDP send capability:
 LDP dynamic capability
 LDP Typed Wildcard FEC Cap
 LDP Unrecognized Noti Cap
 LDP received capability:
 LDP dynamic capability negotiate success
 LDP Typed Wildcard FEC Cap negotiate success
 LDP Unrecognized Noti Cap negotiate success
```

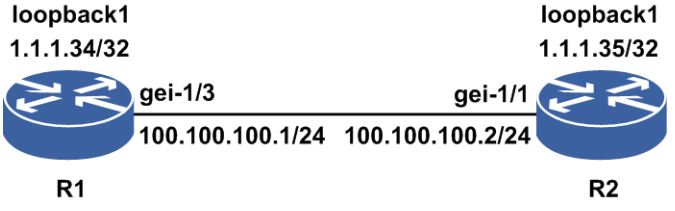
在以上输出中"state: Oper"表示会话的状态是Oper，说明参数协商正确，和1.1.1.34（R1）的邻居关系已建立。

6.2.16 Label-retention 配置实例

配置说明

如*图6-5*所示，两台设备R1与R2建立LDP邻居，在R2 LDP配置模式下配置**label-retention conservative**功能。

图 6-15 Label-retention conservative 配置实例拓扑图



配置思路

1.配置IGP路由，使R1和R2的Loopback接口能互通。

2.在R1和R2间的直连接口上启用MPLS功能。

3.在R1和R2的实例上配置**label-retention conservative**。

4.Reset MPLS实例。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.34 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#ip address 100.100.100.1 255.255.255.0
R1(config-if-gei-1/3)#exit

R1(config)#router isis 1
R1(config-isis-1)#area 00.0001
R1(config-isis-1)#system-id 0001.0002.0034
R1(config-isis-1)#interface gei-1/3
R1(config-isis-1-if-gei-1/3)#ip router isis
R1(config-isis-1-if-gei-1/3)#exit
R1(config-isis-1)#interface loopback1
R1(config-isis-1-if-loopback1)#ip router isis
R1(config-isis-1-if-loopback1)#exit
R1(config-isis-1)#exit

R1(config)#mpls ldp instance 1
/*配置LDP的Router-ID和接口*/
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-1/3
R1(config-ldp-1-if-gei-1/3)#exit
R1(config-ldp-1)#label-retention conservative
R1(config-ldp-1)#exit
R1(config)#reset mpls ldp instance 1
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.35 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 100.100.100.2 255.255.255.0
R2(config-if-gei-1/1)#exit

R2(config)#router isis
R2(config-isis-1)#area 00.0002
R2(config-isis-1)#system-id 0002.0002.0035
R2(config-isis-1)#interface gei-1/1
R2(config-isis-1-if-gei-1/1)#ip router isis
R2(config-isis-1-if-gei-1/1)#exit
R2(config-isis-1)#interface loopback1
R2(config-isis-1-if-loopbck1)#ip router isis
R2(config-isis-1-if-loopbck1)#exit
R2(config-isis-1)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-1/1
R2(config-ldp-1-if-gei-1/1)#exit
R1(config-ldp-1)#label-retention conservative
R2(config-ldp-1)#exit
R2(config)#reset mpls ldp instance 1
R2#debug ldp session io instance 1
R2#terminal monitor
```

配置验证

在R2上查看标签持有情况：

```
R2(config)#show mpls ldp bindings detail instance 1
1.1.1.34/32
 local binding: label: 16384
 remote binding: lsr: 1.1.1.34:0, label: imp-null(inuse)
1.1.1.35/32
 local binding: label: imp-null
 advertised to:
 1.1.1.34:0
```

在以上输出中1.1.1.34 FEC对应路由的下一跳指向R1，因此R1通告过来的标签被保留，但是1.1.1.35是本地标签没有有效下一跳，因此R1通告过来的标签没有被保存下来。

在R2上看到1.1.1.35 FEC对应出标签的Debug消息的交互。

```
mpls_ldp_1: Rcvd mapping msg from 1.1.1.34:0
baseMsg: uBit = 0; msgType = 0x400; msgLength = 24; msgId = 0x5
fecTlv:
 uBit = 0; fBit = 0; type = 0x100; length = 8
 with 1 FEC elements:
 1: type = 2, addFam = 0x1, preLen = 32, address = 0x1010123
genLblTlv:
 uBit = 0; fBit = 0; type = 0x200; length = 4
 label = 16385
Sent release msg to 1.1.1.34:0 with socket-id(0x00002ae7cf01ad10)
baseMsg: uBit = 0; msgType = 0x403; msgLength = 24; msgId = 0x6
fecTlv:
 uBit = 0; fBit = 0; type = 0x100; length = 8
 with 1 FEC elements:
 1: type = 2, addFam = 0x1, preLen = 32, address = 0x1010123
genLblTlv:
 uBit = 0; fBit = 0; type = 0x200; length = 4
 label = 16385
```

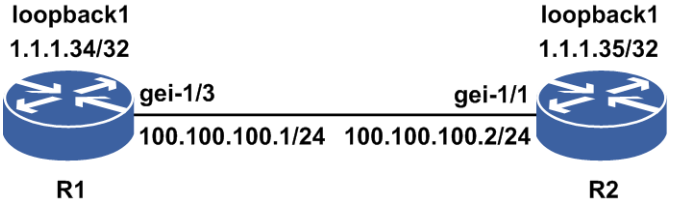
R2收到了R1发来的1.1.1.35的标签MAPPING消息，但是由于R2本地配置了保守的标签保持方式，因此R2回复了标签RELEASE消息。

6.2.17 Label-advertise 配置实例

配置说明

如*图 6-166*所示，两台设备R1与R2建立LDP邻居，在R2 LDP实例配置模式下配置**label-advertise**功能。

图 6-16 Label-advertise 配置实例拓扑图



配置思路

1.配置IGP路由，使R1和R2的Loopback接口能互通。

2.在R1和R2间的直连接口上启用MPLS功能。

3.R2上配置ACL策略"non"拒绝所有。

4.R2上配置ACL策略"all"接收所有。

5.R2的实例上配置"label-advertise for non"。

6.R2的实例上配置"label-advertise for all to non"。

配置时需要注意：

- 步骤5和6给出了两个可选配置方式，步骤5方式是按FEC的前缀进行过滤检查是否向邻居通告标签，步骤6方式按FEC前缀加邻居方式过滤检查是否要通告标签。
- 在前缀ACL相同的情况下只有最后一个配置生效例如先后输入"label-advertise for all"和"label-advertise for all to non"那么只有"label-advertise for all to non"这个配置生效。
- 如果前缀ACL不相同在系统可以配置多个通告组合策略，例如步骤5和步骤6的配置可以作为一个组合策略在设备R2上生效。
- 这个命令需要配合**label-advertise disable**才能生效。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.34 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#ip address 100.100.100.1 255.255.255.0
R1(config-if-gei-1/3)#exit

R1(config)#router isis 1
R1(config-isis-1)#area 00.0001
R1(config-isis-1)#system-id 0001.0002.0034
R1(config-isis-1)#interface gei-1/3
R1(config-isis-1-if-gei-1/3)#ip router isis
R1(config-isis-1-if-gei-1/3)#exit
R1(config-isis-1)#interface loopback1
R1(config-isis-1-if-loopback1)#ip router isis
R1(config-isis-1-if-loopback1)#exit
R1(config-isis-1)#exit

R1(config)#mpls ldp instance 1
/*配置LDP的Router-ID和接口*/
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-1/3
R1(config-ldp-1-if-gei-1/3)#exit
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.35 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
```

```
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 100.100.100.2 255.255.255.0
R2(config-if-gei-1/1)#exit

R2(config)#router isis
R2(config-isis-1)#area 00.0002
R2(config-isis-1)#system-id 0002.0002.0035
R2(config-isis-1)#interface gei-1/1
R2(config-isis-1-if-gei-1/1)#ip router isis
R2(config-isis-1-if-gei-1/1)#exit
R2(config-isis-1)#interface loopback1
R2(config-isis-1-if-loopbck1)#ip router isis
R2(config-isis-1-if-loopbck1)#exit
R2(config-isis-1)#exit

R2(config)#ipv4-access-list non
R2(config-ipv4-acl)#rule 1 deny any
R2(config-ipv4-acl)#exit
R2(config)#ipv4-access-list all
R2(config-ipv4-acl)#rule 1 permit any
R2(config-ipv4-acl)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-1/1
R2(config-ldp-1-if-gei-1/1)#exit

/*方式5的配置方法*/
R2(config-ldp-1)#label-advertise for non
R2(config-ldp-1)#label-advertise disable
R2(config-ldp-1)#exit

/*方式6的配置方法*/
R2(config-ldp-1)#label-advertise for all to non
R2(config-ldp-1)#label-advertise disable
R2(config-ldp-1)#exit
```

配置验证

在R2上查看标签持有情况：

```
R2(config)#show mpls ldp bindings detail instance 1
1.1.1.34/32
 local binding: label: 16384
 remote binding: lsr: 1.1.1.34:0, label: imp-null(inuse)
1.1.1.35/32
 local binding: label: imp-null
100.100.100.0/24
 local binding: label: imp-null
```

R2上看到所有FEC都没有标签通告信息，"advertised to:"信息找不到。

在R1上看到所有FEC都没有收到来自R2的标签"remote binding"信息显示，说明没有来自R2的标签。

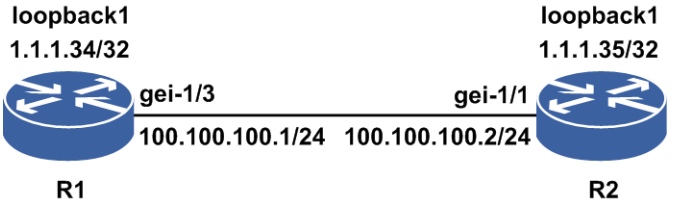
```
R2(config)#show mpls ldp neighbor detail instance 1
1.1.1.34/32
 local binding: label: imp-null
 advertised to:
 1.1.1.35:0
1.1.1.35/32
 local binding: label: 16384
 remote binding: lsr: 1.1.1.35:0, label: UnTag
100.100.100.0/24
 local binding: label: imp-null
```

6.2.18 Label-request 配置实例

配置说明

如*图 6-7*所示，两台设备R1与R2建立LDP邻居，在R2 LDP实例配置模式下配置"label-request"功能。

图 6-17 Label-request 配置实例拓扑图



配置思路

1.配置IGP路由，使R1和R2的Loopback接口能互通。

2.在R1和R2间的直连接口上启用MPLS功能。

3.在R2和R2的直接接口上配置**label-distribution dod**的会话协商为DOD模式。

4.R2上配置ACL策略"non"拒绝所有。

5.R2的实例上配置"label-request for non"。

提示：

会话工作在DOD模式下且没有配置label-request命令时，默认为FEC项所有有效下一跳发标签请求消息；当配置有label-request命令的时候才需要检查，如果不符合过滤规则不发送标签请求消息。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.34 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#ip address 100.100.100.1 255.255.255.0
R1(config-if-gei-1/3)#exit

R1(config)#router isis 1
R1(config-isis-1)#area 00.0001
R1(config-isis-1)#system-id 0001.0002.0034
R1(config-isis-1)#interface gei-1/3
R1(config-isis-1-if-gei-1/3)#ip router isis
R1(config-isis-1-if-gei-1/3)#exit
R1(config-isis-1)#interface loopback1
R1(config-isis-1-if-loopback1)#ip router isis
R1(config-isis-1-if-loopback1)#exit
R1(config-isis-1)#exit
```

```
R1(config)#mpls ldp instance 1
/*配置LDP的Router-ID和接口*/
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-1/3
R1(config-ldp-1-if-gei-1/3)#label-distribution dod
R1(config-ldp-1-if-gei-1/3)#exit
R1(config-ldp-1)#exit
R1(config)#reset mpls ldp instance 1
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.35 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 100.100.100.2 255.255.255.0
R2(config-if-gei-1/1)#exit

R2(config)#router isis
R2(config-isis-1)#area 00.0002
R2(config-isis-1)#system-id 0002.0002.0035
R2(config-isis-1)#interface gei-1/1
R2(config-isis-1-if-gei-1/1)#ip router isis
R2(config-isis-1-if-gei-1/1)#exit
R2(config-isis-1)#interface loopback1
R2(config-isis-1-if-loopbck1)#ip router isis
R2(config-isis-1-if-loopbck1)#exit
R2(config-isis-1)#exit

R2(config)#ipv4-access-list non
R2(config-ipv4-acl)#rule 1 deny any
R2(config-ipv4-acl)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-1/1
R2(config-ldp-1-if-gei-1/1)#label-distribution dod
R2(config-ldp-1-if-gei-1/1)#exit
R2(config-ldp-1)#label-request for non
R2(config-ldp-1)#exit
R2(config)#reset mpls ldp instance 1
```

配置验证

在R2上查看标签持有情况：

```
R2(config)#show mpls ldp bindings detail instance 1
1.1.1.34/32
 local binding: label: 16384
1.1.1.35/32
 local binding: label: imp-null
 advertised to:
 1.1.1.34:0
100.100.100.0/24
 local binding: label: imp-null
```

R2上看到1.1.1.34的有效下一跳是R1，本来在DOD模式下R2应该向R1发标签请求消息，最终形成如下"remote binding"信息项，但是由于配置了请求消息的ACL策略且是不允许发请求消息，因此1.1.1.34 FEC没有办法形成出标签表项。

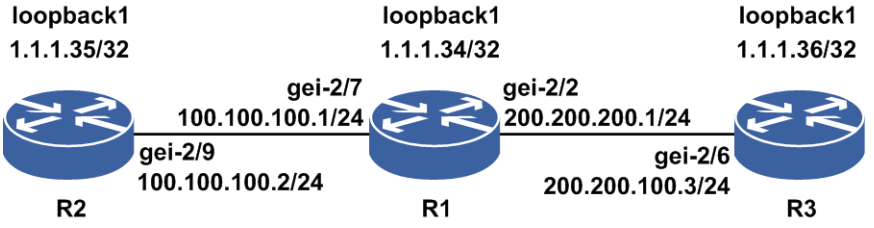
```
1.1.1.34/32
 local binding: label: 16384
 remote binding: lsr: 1.1.1.34:0, label: imp-null(inuse)
```

6.2.19 Lsp-control 配置实例

配置说明

如*图 6-8*所示，三台设备R1、R2与R3建立LDP邻居，在R1 LDP实例配置模式下配置**lsp-control ordered**功能。

图 6-18 Lsp-control ordered 配置实例拓扑图



配置思路

1.配置IGP路由，使R1、R2、R3的Loopback接口能互通。

2.在R1和R2、R1和R3间的直连接口上启用MPLS功能。

3.R1上配置lsp-control ordered模式。

4.R3的实例上配置label-advertise disable。

5.R3的实例上配置no label-advertise disable。

提示：

标签通告的有序模式不是很容易观察到，因此步骤4的目的是让下游先不通告标签，便于观察与配置步骤5后下游通告标签时R1和R2上1.1.1.36持有标签的区别。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.34 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-2/7
R1(config-if-gei-2/7)#ip address 100.100.100.1 255.255.255.0
R1(config-if-gei-2/7)#exit
R1(config)#interface gei-2/2
R1(config-if-gei-2/2)#no shutdown
R1(config-if-gei-2/2)#ip address 200.200.200.1 255.255.255.0
R1(config-if-gei-2/2)#exit

R1(config)#router isis 1
R1(config-isis-1)#area 00.0001
R1(config-isis-1)#system-id 0001.0002.0034
R1(config-isis-1)#interface gei-2/7
R1(config-isis-1-if-gei-2/7)#ip router isis
R1(config-isis-1-if-gei-2/7)#exit
R1(config-isis-1)#interface gei-2/2
```

```
R1(config-isis-1-if-gei-2/2)#ip router isis
R1(config-isis-1-if-gei-2/2)#exit
R1(config-isis-1)#interface loopback1
R1(config-isis-1-if-loopback1)#ip router isis
R1(config-isis-1-if-loopback1)#exit
R1(config-isis-1)#exit

R1(config)#mpls ldp instance 1
/*配置LDP的Router-ID和接口*/
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-2/7
R1(config-ldp-1-if-gei-2/7)#exit
R1(config-ldp-1)#interface gei-2/2
R1(config-ldp-1-if-gei-2/2)#exit
R1(config-ldp-1)#lsp-control ordered
R1(config-ldp-1)#exit
R1(config)#reset mpls ldp instance 1
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.35 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-2/9
R2(config-if-gei-2/9)#no shutdown
R2(config-if-gei-2/9)#ip address 100.100.100.2 255.255.255.0
R2(config-if-gei-2/9)#exit

R2(config)#router isis
R2(config-isis-1)#area 00.0002
R2(config-isis-1)#system-id 0002.0002.0035
R2(config-isis-1)#interface gei-2/9
R2(config-isis-1-if-gei-2/9)#ip router isis
R2(config-isis-1-if-gei-2/9)#exit
R2(config-isis-1)#interface loopback1
R2(config-isis-1-if-loopbck1)#ip router isis
R2(config-isis-1-if-loopbck1)#exit
R2(config-isis-1)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-2/9
R2(config-ldp-1-if-gei-2/9)#exit
R2(config-ldp-1)#exit
```

R3上的配置如下：

```
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 1.1.1.36 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-2/6
R3(config-if-gei-2/6)#ip address 200.200.100.3 255.255.255.0
R3(config-if-gei-2/6)#exit

R3(config)#router isis
R3(config-isis-1)#area 00.0003
R3(config-isis-1)#system-id 0003.0003.0036
R3(config-isis-1)#interface gei-2/6
R3(config-isis-1-if-gei-2/6)#ip router isis
R3(config-isis-1-if-gei-2/6)#exit
R3(config-isis-1)#interface loopback1
R3(config-isis-1-if-loopbck1)#ip router isis
R3(config-isis-1-if-loopbck1)#exit
R3(config-isis-1)#exit

R3(config)#mpls ldp instance 1
R3(config-ldp-1)#router-id loopback1
R3(config-ldp-1)#interface gei-2/6
R3(config-ldp-1-if-gei-2/6)#exit
```

```
/*步骤4操作*/
R3(config-ldp-1)#label-advertise disable

/*步骤5操作*/
R3(config-ldp-1)#label-advertise disable
```

配置验证

•R3执行到步骤4的结果。

在R1上查看标签持有情况：

```
R1(config)#show mpls ldp bindings 1.1.1.36 32 detail instance 1
1.1.1.36/32
 local binding: label: 16384
 remote binding: lsr: 1.1.1.36:0, label: UnTag
```

R1上看到FEC(1.1.1.36)的有效下一跳标签信息"remote binding"为"UnTag"，即邻居1.1.1.36没有通告标签，由于R1的LSP形成模式是有序的，因此表项中看不到"advertised to:"的标签通告信息。

在R2上查看标签持有情况：

```
R2(config)#show mpls ldp bindings 1.1.1.36 32 detail instance 1
1.1.1.36/32
 local binding: label: 16384
 remote binding: lsr: 1.1.1.34:0, label: UnTag
```

R2上看到的信息同R1所见，唯一的区别是R2发现R1没有通告FEC（1.1.1.36）的标签。

•R3执行到步骤5的结果。

在R1上查看标签持有情况：

```
R1(config)#show mpls ldp bindings 1.1.1.36 32 detail instance 1
1.1.1.36/32
 local binding: label: 16384
      advertised to:
 1.1.1.35:0 1.1.1.36:0
 remote binding: lsr: 1.1.1.36:0, label: imp-null(inuse)
```

R1上看到FEC（1.1.1.36）的有效下一跳R3发来有效标签，R1此时向R2和R3通告标签。

在R2上查看标签持有情况：

```
R2(config)#show mpls ldp bindings 1.1.1.36 32 detail instance 1
1.1.1.36/32
 local binding: label: 16384
 advertised to:
 1.1.1.34:0
 remote binding: lsr: 1.1.1.34:0, label: 16384 (inuse)
```

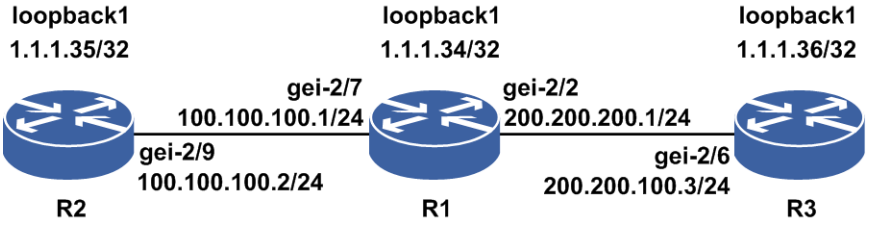
R2收到下游标签后开始向上游邻居通告标签。

6.2.20 Longest-match 配置实例

配置说明

如*图 6-119*所示，三台设备R1、R2与R3建立LDP邻居，在R1 LDP实例配置模式下配置**longest-match**功能。

图 6-119 Longest-match 配置实例拓扑图



配置思路

1.配置IGP路由，使R1、R2、R3的Loopback接口能互通。

2.在R1和R2、R1和R3间的直连接口上启用MPLS功能。

3.R2与R1间建立DOD模式的会话，R1与R3间建立DU模式的会话。

4.R1上配置ACL策略"acl12"允许1.2.0.0/16网段的路由。

5.R1上配置longest-match模式。

6.R1上配置静态聚合路由1.2.0.0/16下一跳地址指向R3。

7.R2上配置静态路由1.2.3.4/32下一跳指向R1。

8.R3上配置静态路由1.2.3.4/32下一跳指向R3自己。

9.R1上配置静态LDP 1.2.3.4/32静态入标签100。

提示：

步骤7、8、9分别可以单独触发R1上形成FEC（1.2.3.4/32）的最长匹配LSP，匹配结果同FEC（1.2.0.0/16）。

配置过程

R1上的配置如下：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.34 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-2/7
R1(config-if-gei-2/7)#no shutdown
R1(config-if-gei-2/7)#ip address 100.100.100.1 255.255.255.0
R1(config-if-gei-2/7)#exit
R1(config)#interface gei-2/2
R1(config-if-gei-2/2)#ip address 200.200.200.1 255.255.255.0
R1(config-if-gei-2/2)#exit
R1(config)#ip route 1.2.0.0 255.255.0.0 200.200.200.3
```

```
R1(config)#router isis 1
R1(config-isis-1)#area 00.0001
R1(config-isis-1)#system-id 0001.0002.0034
R1(config-isis-1)#interface gei-2/7
R1(config-isis-1-if-gei-2/7)#ip router isis
R1(config-isis-1-if-gei-2/7)#exit
R1(config-isis-1)#interface gei-2/2
R1(config-isis-1-if-gei-2/2)#ip router isis
R1(config-isis-1-if-gei-2/2)#exit
R1(config-isis-1)#interface loopback1
R1(config-isis-1-if-loopback1)#ip router isis
R1(config-isis-1-if-loopback1)#exit
R1(config-isis-1)#exit

R1(config)#ipv4-access-list acl12
R1(config-ipv4-acl)#rule 1 permit 1.2.0.0 0.0.255.255
R1(config-ipv4-acl)#exit

R1(config)#mpls ldp instance 1
/*配置LDP的Router-ID和接口*/
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-2/7
R1(config-ldp-1-if-gei-2/7)#label-distribution dod
R1(config-ldp-1-if-gei-2/7)#exit
R1(config-ldp-1)#interface gei-2/2
R1(config-ldp-1-if-gei-2/2)#exit
R1(config-ldp-1)#longest-match ipv4 for acl12
R1(config-ldp-1)#exit
R1(config)#reset mpls ldp instance 1
```

R2上的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 1.1.1.35 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-2/9
R2(config-if-gei-2/9)#no shutdown
R2(config-if-gei-2/9)#ip address 100.100.100.2 255.255.255.0
R2(config-if-gei-2/9)#exit

R2(config)#router isis
R2(config-isis-1)#area 00.0002
R2(config-isis-1)#system-id 0002.0002.0035
R2(config-isis-1)#interface gei-2/9
R2(config-isis-1-if-gei-2/9)#ip router isis
R2(config-isis-1-if-gei-2/9)#exit
R2(config-isis-1)#interface loopback1
R2(config-isis-1-if-loopbck1)#ip router isis
R2(config-isis-1-if-loopbck1)#exit
R2(config-isis-1)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-2/9
R2(config-ldp-1-if-gei-2/9)#label-distribution dod
R2(config-ldp-1-if-gei-2/9)#exit
R2(config-ldp-1)#exit
R2(config)#reset mpls ldp instance 1
```

R3上的配置如下：

```
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 1.1.1.36 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-2/6
R3(config-if-gei-2/6)#no shutdown
R3(config-if-gei-2/6)#ip address 200.200.100.3 255.255.255.0
R3(config-if-gei-2/6)#exit
```

```
R3(config)#router isis
R3(config-isis-1)#area 00.0003
R3(config-isis-1)#system-id 0003.0003.0036
R3(config-isis-1)#interface gei-2/6
R3(config-isis-1-if-gei-2/6)#ip router isis
R3(config-isis-1-if-gei-2/6)#exit
R3(config-isis-1)#interface loopback1
R3(config-isis-1-if-loopbck1)#ip router isis
R3(config-isis-1-if-loopbck1)#exit
R3(config-isis-1)#exit

R3(config)#mpls ldp instance 1
R3(config-ldp-1)#router-id loopback1
R3(config-ldp-1)#interface gei-2/6
R3(config-ldp-1-if-gei-2/6)#exit

/*步骤7操作，在R2上增加配置*/
R2(config)#ip route 1.2.3.4 255.255.255.255 100.100.100.1

/*步骤8操作，在R3上增加配置*/
R3(config)#ip route 1.2.3.4 255.255.255.255 loopback1

/*步骤9操作，在R1上增加配置*/
R1(config)#mpls static-lsp sta
R1(config-static-lsp-sta)#bind ipv4 1.2.3.4 255.255.255.255
R1(config-if-loopback2)#insegment inlabel 100
```

配置验证

•R2执行步骤7、或R1执行步骤9的结果。

在R1上查看标签持有情况：

```
R1(config)#show mpls ldp bindings 1.2.3.4 32 detail instance 1
1.2.3.4/32
 local binding: label: 16386
 remote binding: lsr: 1.1.1.36:0, label: 16385
```

此时R1上有R3发过来的出标签。

R1上现在看到的路由信息：

```
R1(config)#show ip forwarding route 1.2.3.4
------------------------------------------------------------------------
--

IPv4 Routing Table:
Headers: Dest - Destination,Gw - Gateway,Pri - Priority,M/S - Master/Slave,
 Sta - Status;
Codes : B - bgp,STAT - static, L1 - isis-l1, BROAD - broadcast, RSVP - rsvpte,
 O - ospf, IPsec - ipsec, L2 - isis-l2, DHCP-D - dhcp-dft, MART - martian,
 RIP - rip, VRRP - vrrp, ADDR - address, NAT64 - sl-nat64, DIRECT - direct,
 NAT - nat, SNMP - snmp, PS-U - ps-user, MULT - multicast, VPN-AS - asbr-vpn,
 PAT - pat, ICMP - icmp, PS-B - ps-busi, LDP-A - ldp-area, STATV - staticvrf,
 PPP - ppp, DHCP-S - dhcp-static, PerV-L - perVrf-label, U-NET - user-network,
 U-IP - user-ipaddr, U-SPEC - user-special;
Status codes: *valid, >best, M: Master, S: Slave;
   Dest       Gw            Interface   Owner    Pri  Metric
*> 1.2.3.4/32  100.100.100.2   gei-2/9     LDP-A    254  65534
*> 1.2.0.0/16  100.100.100.2   gei-2/9     STAT     1    0
```

从路由信息可以看出1.2.3.4/32是LDP协议根据路由1.2.0.0/16信息产生并形成的。1.2.3.4/32的路由出接口下一跳信息和1.2.0.0/16完全相同。

R1上现在看到转发表项信息：

```
R1(config)#show mpls forwarding-table 1.2.3.4
------------------------------------------------------------------------
--
Local   Outgoing   Prefix or    Outgoing     Next Hop M/S
label   label      Lspname      interface
16386   16385      1.2.3.4/32   loopback1    1.1.1.35 M
```

- R3执行步骤8的结果。

  在R1上查看标签持有情况：

```
R1(config)#show mpls ldp bindings 1.2.3.4 32 detail instance 1
1.2.3.4/32
 local binding: label: 16386
 remote binding: lsr: 1.1.1.36:0, label: 16385 (inuse)
```

  R1上现在看到的路由信息：

```
R1(config)#show ip forwarding route 1.2.3.4
------------------------------------------------------------------------
--
IPv4 Routing Table:
Headers: Dest - Destination, Gw - Gateway, Pri - Priority, M/S - Master/Slave,
 Sta - Status;
Codes : B - bgp,STAT - static, L1 - isis-l1, BROAD - broadcast, RSVP - rsvpte,
 O - ospf, IPsec - ipsec, L2 - isis-l2, DHCP-D - dhcp-dft, MART - martian,
 RIP - rip, VRRP - vrrp, ADDR - address, NAT64 - sl-nat64, DIRECT - direct,
 NAT - nat, SNMP - snmp, PS-U - ps-user, MULT - multicast, VPN-AS - asbr-vpn,
 PAT - pat, ICMP - icmp, PS-B - ps-busi, LDP-A - ldp-area, STATV - staticvrf,
 PPP - ppp, DHCP-S - dhcp-static, PerV-L - perVrf-label, U-NET - user-network,
 U-IP - user-ipaddr, U-SPEC - user-special;
Status codes: *valid, >best, M: Master, S: Slave;
   Dest        Gw            Interface   Owner    Pri  Metric
*> 1.2.3.4/32   100.100.100.2   gei-2/9     LDP-A    254  65534
*> 1.2.0.0/16   100.100.100.2   gei-2/9     STAT     1    0
```

  信息和步骤7、步骤9的操作结果一样。

  R1上现在看到的转发表项信息：

```
R1(config)#show mpls forwarding-table 1.2.3.4
------------------------------------------------------------------------
--
Local   Outgoing  Prefix or    Outgoing     Next Hop   M/S
label   label     Lspname      interface
16386   16385     1.2.3.4/32   loopback1    1.1.1.35   M
```

  此时转发表项有有效出标签。

6.3 MPLS TE 配置

6.3.1 RSVP

RSVP是一种为网络综合服务而设计，基于IP协议的资源预留协议。

用户通过RSVP协议向网络请求满足特殊服务质量要求的缓存和带宽，中间结点利用RSVP协议在数据传输通路上建立起资源预留并维护该通路，以实现相应的服务质量。

6.3.1.1 配置 RSVP

本节介绍采用RSVP-TE的方式来建立LSP隧道的配置步骤和命令。

1.创建tunnel接口。

命令	功能
inspur(config)#**interface te_tunnel**<*tunnel-number*>	创建tunnel接口

2.开启MPLS TE功能。

步骤	命令	功能
1	inspur(config)#**mpls traffic-eng**	开启MPLS TE功能，进入TE配置模式
2	inspur(config-mpls-te)#**interface** <*interface-name*>	配置接口启用TE
3	inspur(config-mpls-te-if)#**bandwidth** [{**static**|**dynamic**}]<*bandwidth value*>	配置TE接口带宽

bandwidth [{**static**|**dynamic**}]<*bandwidth value*>：TE接口支持流程工程的最大（静态预留类型或动态预留类型）带宽，范围：1~4294967295，单位：kbps。

3.配置隧道的显式路径。

步骤	命令	功能
1	inspur(config-mpls-te)#**explicit-path** {**identifier** <*identifier*>|**name** <*name*>}	配置隧道的显式路径名称或标记
2	inspur(config-mpls-te-expl-path-id-identifier)#**next-address** {**strict** | **loose**}<*A.B.C.D*>	配置隧道显式路径的下一跳
	inspur(config-mpls-te-expl-path-name)#**next-address** {**strict** | **loose**}<*A.B.C.D*>	配置隧道显式路径的下一跳
3	inspur(config-mpls-te-expl-path-id-identifier)#**exclude-address** {**interface**| **router-id**}<*A.B.C.D*>	配置排除路径

strict：严格路径。

loose：松散路径。

4.配置隧道目的地址。

步骤	命令	功能
1	inspur(config-mpls-te)#**tunnel te_tunnel**<*tunnel-number*>	进入tunnel配置模式
2	inspur(config-mpls-te-tunnel-te_tunnel-tunnel-number)#**tunnel destination ipv4** <*A.B.C.D*>	配置隧道的目的地

5.配置TE隧道名称。

步骤	命令	功能
1	inspur(config-mpls-te)#**tunnel te_tunnel**<*tunnel-number*>	进入tunnel配置模式
2	inspur(config-mpls-te-tunnel-te_tunnel-tunnel-number)#**tunnel mpls traffic-eng name** <*name*>	配置TE隧道的名称 通过RSVP-TE信令协议将此隧道名称携带至隧道经过的各个节点 通过显示命令查看不同的隧道名称，从而使相同tunnelID的隧道在中间节点更加容易区分

<*name*>：TE隧道名称，范围为1~63位字符串。

6.配置隧道的路径。

命令	功能
inspur(config-mpls-te-tunnel-te_tunnel-tunnel-number)#**tunnel mpls traffic-eng path-option** <*number*> **dynamic**	配置隧道的路径（动态）
inspur(config-mpls-te-tunnel-te_tunnel-tunnel-number)#**tunnel mpls traffic-eng path-option** <*number*> **explicit-path** {**identifier** <*identifier*>|**name** <*name*>}	配置隧道的路径（显式路径）

dynamic：使用动态计算路径方式。

7.配置RSVP的其他功能。

步骤	命令	功能
1	inspur(config-mpls-te-if-interface-name)#**bfd**	MPLS-TE的实接口模式下使能接口BFD
2	inspur(config-mpls-te-tunnel-te_tunnel-number)#**tunnel mpls traffic-eng bfd interval** <*interval*> **min-rx** < *min-rx* > **multiplier** <*multiplier*>	MPLS-TE的tunnel接口模式下使能tunnel LSP BFD
3	inspur(config-mpls-te-tunnel-te_tunnel-number)#**tunnel mpls traffic-eng hop limit** <*hop-num*>	配置隧道最大跳数限制，缺省为无限制

<*interval*>：指定BFD控制报文的最小发送间隔，单位：毫秒，范围：10~990。

<*min-rx*>：指定BFD控制报文的最小接收间隔，单位：毫秒，范围：10~990。

<*multiplier*>：指定BFD控制报文的检测倍数，范围：3~50。

<*hop-num*>：配置隧道的最大跳数，范围：1~32。

8.验证配置结果。

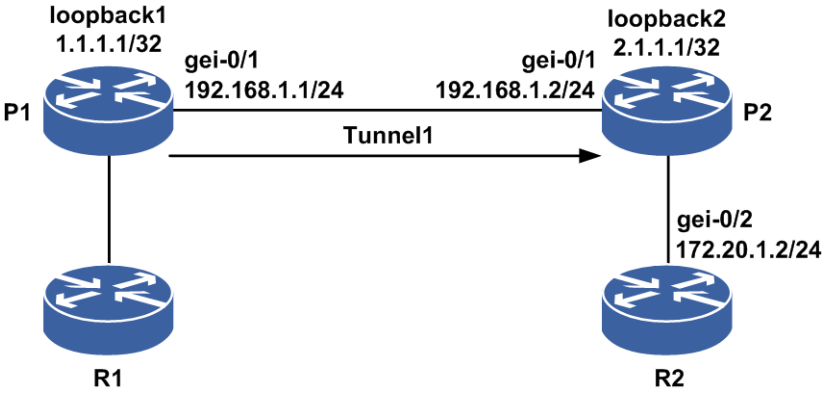
命令	功能
inspur#**show mpls traffic-eng tunnels te_tunnel** <*Tunnel ID*>	显示本地某条特定隧道信息
inspur#**show mpls traffic-eng tunnels remote-tunnel** [**tunnel-id** <*tunnel-id*> **lsp-id** <*lsp-id*> **ingress-id** <*ingress-id*> **egress-id** <*egress-id*>]	显示远程隧道信息
inspur#**show mpls traffic-eng tunnels brief**	查看TE隧道简略信息，可以查看TE隧道名是否生效
inspur#**show mpls traffic-eng interface brief**	显示开启了TE的接口简要信息
inspur#**show mpls traffic-eng interface detail**	显示开启了TE的接口详细信息

6.3.1.2 OSPF TE 配置实例

配置说明

如*图 6-20*所示为从P1到P2的RSVP普通隧道，采用OSPF TE进行动态选路的方式建立隧道。

图 6-20 OSPF TE 配置实例示意图



配置思路

1.P1、P2直连接口建立OSPF邻居，OSPF使能TE，所有接口在同一个OSPF域内建立RSVP隧道。

2.P1、P2直连接口使能TE，并在P1上配置Tunnel1的目的地和路径。

3.在P1上配置一条到目的地的静态路由，下一跳为Tunnel1，这样流量通过Tunnel来转发。

本实例中采用动态选路方式。

配置过程

P1的配置如下：

```
P1(config)#interface gei-0/1
P1(config-if-gei-0/1)#no shutdown
P1(config-if-gei-0/1)#ip address 192.168.1.1 255.255.255.0
P1(config-if-gei-0/1)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit
P1(config-ospf-1)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#interface gei-0/1
P1(config-mpls-te-if-gei-0/1)#exit
P1(config-mpls-te)#tunnel te_tunnel1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng path-option 1
dynamic
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#exit

P1(config)#ip route 172.20.1.2 255.255.255.255 te_tunnel1
```

P2的配置如下：

```
P2(config)#interface gei-0/1
P2(config-if-gei-0/1)#no shutdown
P2(config-if-gei-0/1)#ip address 192.168.1.2 255.255.255.0
P2(config-if-gei-0/1)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit
P2(config-ospf-1)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-0/1
P2(config-mpls-te-if-gei-0/1)#exit
P2(config-mpls-te)#exit
```

R2的配置如下：

```
R2(config)#interface gei-0/2
```

```
R2(config-if-gei-0/2)#ip address 172.20.1.2  255.255.255.0
R2(config-if-gei-0/2)#exit
```

提示：

MPLS TE中的Router-ID选用loopback接口，是为了防止Router-ID接口down影响隧道的建立，Loopback接口一直处于up状态（非手动改变）。

配置验证

在P1上查看隧道情况，处于up状态，且可以查看Tunnel1的详细信息：

```
P1(config)#show mpls traffic-eng tunnels brief
Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
TUNNEL NAME  DESTINATION UP IF   DOWN IF     STATE/PROT
tunnel_1     2.1.1.1     -      gei-0/1     up/up

P1(config)#show mpls traffic-eng tunnels te_tunnel 1

Name: tunnel_1               (Tunnel1) Destination: 2.1.1.1
  Status:
    Admin: up  Oper: up  Path:  valid  Signalling: connected
    Path option: 1, type dynamic (Basis for Setup)
    Hot-standby protection:
      no path options protected
  Config Parameters:
    Bandwidth: 0 kbps (Global) Priority: 7  7  Affinity: 0x0/0x0
    Resv-Style: SE
    Metric Type: IGP (default)   Upper Limit: 4294967295
    Facility Fast-reroute: disabled
    Detour Fast-reroute: disabled
    BFD: disabled
    Auto-bw: disabled
    Bidirect: disabled
    AutoRoute: disabled
    Forwarding-adjacency: disabled

  InLabel: -
  OutLabel: gei-0/1, 3
  RSVP Signalling Info :
    Src 1.1.1.1, Dst 2.1.1.1, Tun_Id 1, Tun_Instance 74
    RSVP Path Info:
      Explicit Route: 192.168.1.1 192.168.1.2  2.1.1.1
      Exclude Route: NULL
      Record Route: NULL
      Tspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits
    RSVP Resv Info:
      Record Route: NULL
      Fspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits

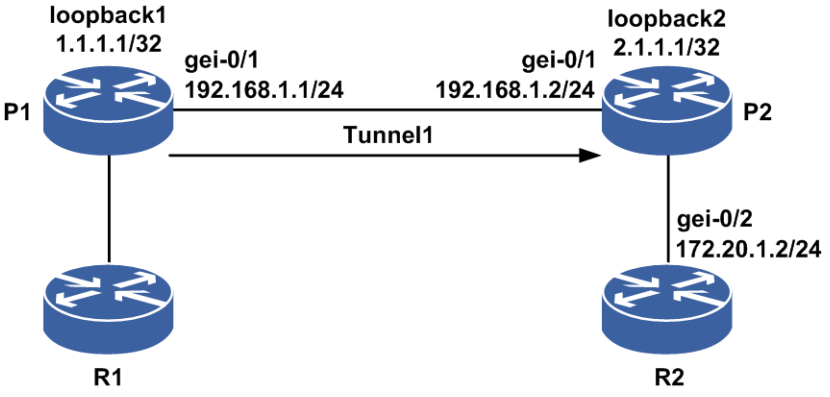
  History:
    Tunnel:
    Time since created: 0 days, 6 hours, 10 minutes
    Prior LSP: path option 1
    Current LSP: Uptime:0 days, 0 hours, 0 minutes
    Last lsp error information:
    None log record.
```

6.3.1.3 IS-IS TE 配置实例

配置说明

如*图* **6-**所示，从P1到P2的RSVP普通隧道建立采用IS-IS TE，进行严格选路的方式。

图 6-21 IS-IS TE 配置实例示意图



配置思路

1.P1、P2直连接口建立IS-IS邻居，IS-IS开启TE功能。

2.P1、P2直连接口使能TE，并在P1上配置Tunnel1的目的地和路径。

3.在P1上配置一条到目的地的静态路由，下一跳为Tunnel1，这样流量通过Tunnel来转发。

本实例中采用严格路径选路方式。

配置过程

P1的配置如下：

```
P1(config)#interface gei-0/1
P1(config-if-gei-0/1)#no shutdown
P1(config-if-gei-0/1)#ip address 192.168.1.1 255.255.255.0
P1(config-if-gei-0/1)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit

P1(config)#router isis 1
P1(config-isis-1)#area 00
P1(config-isis-1)#system-id AAAA.BBBB.1111
P1(config-isis-1)#interface gei-0/1
P1(config-isis-1-if-gei-0/1)#ip router isis
P1(config-isis-1-if-gei-0/1)#exit
P1(config-isis-1)#interface loopback1
P1(config-isis-1-if-loopback1)#ip router isis
P1(config-isis-1-if-loopback1)#exit
```

```
P1(config-isis-1)#metric-style wide
P1(config-isis-1)#mpls traffic-eng level-1
P1(config-isis-1)#mpls traffic-eng level-2
P1(config-isis-1)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#interface gei-0/1
P1(config-mpls-te-if-gei-0/1)#exit
P1(config-mpls-te)#explicit-path identifier 1
P1(config-mpls-te-expl-path-id-1)#next-address strict 192.168.1.2
P1(config-mpls-te-expl-path-id-1)#exit
P1(config-mpls-te)#tunnel te_tunnel1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng path-option 1
explicit-path identifier 1
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#exit

P1(config)#ip route 172.20.1.2 255.255.255.255 te_tunnel1
```

P2的配置如下：

```
P2(config)#interface gei-0/1
P2(config-if-gei-0/1)#no shutdown
P2(config-if-gei-0/1)#ip address 192.168.1.2 255.255.255.0
P2(config-if-gei-0/1)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router isis 1
P2(config-isis-1)#area 00
P2(config-isis-1)#system-id AAAA.BBBB.2222
P2(config-isis-1)#interface gei-0/1
P2(config-isis-1-if-gei-0/1)#ip router isis
P2(config-isis-1-if-gei-0/1)#exit
P2(config-isis-1)#interface loopback2
P2(config-isis-1-if-loopback2)#ip router isis
P2(config-isis-1-if-loopback2)#exit
P2(config-isis-1)#metric-style wide
P2(config-isis-1)#mpls traffic-eng level-1
P2(config-isis-1)#mpls traffic-eng level-2
P2(config-isis-1)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-0/1
P2(config-mpls-te-if-gei-0/1)#exit
P2(config-mpls-te)#exit
```

R2的配置如下：

```
R2(config)#interface gei-0/2
R2(config-if-gei-0/2)#no shutdown
R2(config-if-gei-0/2)#ip address 172.20.1.2  255.255.255.0
R2(config-if-gei-0/2)#exit
```

配置验证

在P1上查看隧道情况，处于up状态，且可以查看Tunnel 1的详细信息：

```
P1(config)#show mpls traffic-eng tunnels brief
Signalling Summary:
```

```
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
TUNNEL NAME   DESTINATION   UP IF   DOWN IF       STATE/PROT
tunnel_1      2.1.1.1       -       gei-0/1       up/up

P1(config-mpls-te)#show mpls traffic-eng tunnels te_tunnel 1

Name: tunnel_1               (Tunnel1) Destination: 2.1.1.1
  Status:
    Admin: up  Oper: up  Path:  valid  Signalling: connected
    Path option: 1, type explicit identifier: 1 (Basis for Setup)
    Hot-standby protection:
      no path options protected
  Config Parameters:
    Bandwidth: 0 kbps (Global) Priority: 7  7  Affinity: 0x0/0x0
    Resv-Style: SE
    Metric Type: IGP (default)   Upper Limit: 4294967295
    Facility Fast-reroute: disabled
    Detour Fast-reroute: disabled
    BFD: disabled
    Auto-bw: disabled
    Bidirect: disabled
    AutoRoute: disabled
    Forwarding-adjacency: disabled

  InLabel: -
  OutLabel: gei-0/1, 3
  RSVP Signalling Info :
    Src 1.1.1.1, Dst 2.1.1.1, Tun_Id 1, Tun_Instance 78
    RSVP Path Info:
      Explicit Route: 192.168.1.1 192.168.1.2 2.1.1.1
      Exclude Route: NULL
      Record Route: NULL
      Tspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits
    RSVP Resv Info:
      Record Route: NULL
      Fspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits

  History:
    Tunnel:
    Time since created: 0 days, 6 hours, 19 minutes
    Prior LSP: path option 1
    Current LSP: Uptime:0 days, 0 hours, 0 minutes
    Last lsp error information:
    None log record.
```

提示：

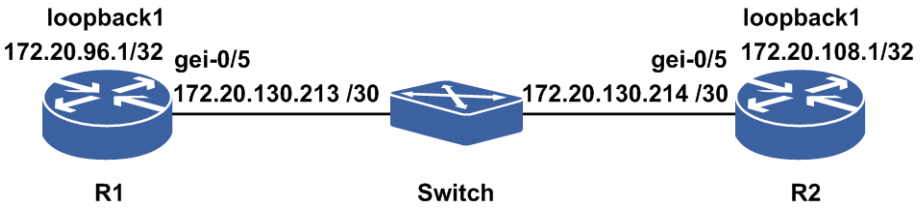
MPLS TE中的Router-ID选用Loopback接口，是为了防止Router-ID接口down影响隧道的建立，loopback接口一直处于up状态（非手动改变)。

6.3.1.4 RSVP 接口 BFD 配置实例

配置说明

如*图 6-222*所示，R1、R2之间建立IS-IS TE隧道，R1、R2上RSVP-TE接口开启BFD。

图 6-22 RSVP 接口 BFD 配置实例示意图



配置思路

1.R1、R2之间建立IS-IS TE的隧道。

2.R1、R2的TE模式接口下开启BFD。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-0/5
R1(config-if-gei-0/5)#ip address 172.20.130.213 255.255.255.252
R1(config-if-gei-0/5)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 172.20.96.1 255.255.255.255
R1(config-if-loopback1)#exit

R1(config)#router isis
R1(config-isis-0)#area 49.0172
R1(config-isis-0)#system-id 0020.0096.0001
R1(config-isis-0)#metric-style wide
R1(config-isis-0)#mpls traffic-eng level-2
R1(config-isis-0)#interface gei-0/5
R1(config-isis-0-if-gei-0/5)#ip router isis
R1(config-isis-0-if-gei-0/5)#end

R1(config)#interface te_tunnel1
R1(config-if-te_tunnel1)#ip unnumbered loopback1
R1(config-if-te_tunnel1)#exit
R1(config)#mpls traffic-eng
R1(config-mpls-te)#interface loopback1
R1(config-mpls-te-if-loopback1)#exit
R1(config-mpls-te)#router-id 172.20.96.1
R1(config-mpls-te)#tunnel te_tunnel 1
R1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 172.20.108.1
R1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
path-option 1 dynamic
R1(config-mpls-te-tunnel-te_tunnel1)#exit
R1(config-mpls-te)#interface gei-0/5
R1(config-mpls-te-if-gei-0/5)#bfd
```

R2上的配置如下：

```
R2(config)#interface gei-0/5
R2(config-if-gei-0/5)#ip address 172.20.130.214 255.255.255.252
R2(config-if-gei-0/5)#exit
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 172.20.108.1 255.255.255.255
R2(config-if-loopback1)#exit

R2(config)#router isis
R2(config-isis-0)#area 49.0172
```

```
R2(config-isis-0)#system-id 0020.0096.0002
R2(config-isis-0)#metric-style wide
R2(config-isis-0)#mpls traffic-eng level-2
R2(config-isis-0)#interface gei-0/5
R2(config-isis-0-if-gei-0/5)#ip router isis
R2(config-isis-0-if-gei-0/5)#end

R2(config)#mpls traffic-eng
R2(config-mpls-te)#interface loopback1
R2(config-mpls-te-if-loopback1)#exit
R2(config-mpls-te)#router-id 172.20.108.1
R2(config-mpls-te)#interface gei-0/5
R2(config-mpls-te-if-gei-0/5)#bfd
```

配置验证

正确配置后，R1上的RSVP 接口会话应该能够成功建立，可以用如下命令查看结果：

用**show bfd neighbors** [**ip brief**|**ip detail**]来查看验证RSVP 接口BFD是否生效。

R1上RSVP接口BFD生效情况查看：

```
R1(config)#show bfd neighbors ip brief
LocalAddr       PeerAddr        LD     RD     Hold   State   Interface
172.20.130.213   172.20.130.214   8      1     150    UP     gei-0/5

R1(config)#show bfd neighbors ip detail
------------------------------------------------------------
LocalAddr:172.20.130.213
PeerAddr :172.20.130.214
Local Discr:2050          Remote Discr:2049          State:UP

Holdown(ms):150           Interface: gei-0/5
Vpnid:0                  VRF Name:---
BFD Type:SingleHop
Instance Name:
------------------------------------------------------------------------
--
Version:1               Dest UDP Port:3784       Final Bit:1
Local Diag:0            Demand Mode:0            Poll Bit:1
MinTxInt:50             MinRxInt:50              Multiplier:3
Received MinTxInt:50     Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24        Max BFD Length:24

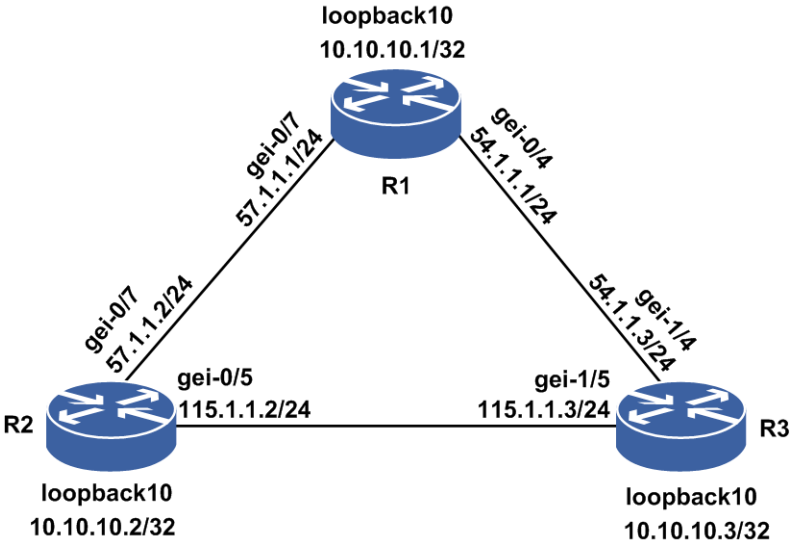
Rx Count:0              Rx Interval (ms) min/max/avg:0     /0     /0
Tx Count:66             Tx Interval (ms) min/max/avg:0     /0     /0
Registered Protocols:RSVP
Uptime:0 day(s),0 hour(s),0 minute(s)
Control Plane Rcv Phy Interface Name: gei-0/5
========================================================================
==
```

6.3.1.5 RSVP LSP BFD 配置实例

配置说明

如*图 6-123*所示，RSVP LSP BFD是采用BFD检测该RSVP隧道的LSP，当结合hotstandby功能时，且失效LSP为主LSP时，应先将隧道流量切换到备份LSP上。

图 6-123 RSVP LSP BFD 配置实例示意图



配置思路

1.R1、R2、R3之间使能OSPF-TE。

2.在R1上配置一条hotstandby隧道（R1-R3-R2），并在该隧道下配置BFD。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-0/4
R1(config-if-gei-0/4)#ip address 54.1.1.1 255.255.255.0
R1(config-if-gei-0/4)#exit
R1(config)#interface gei-0/7
R1(config-if-gei-0/7)#ip address 57.1.1.1 255.255.255.0
R1(config-if-gei-0/7)#exit
R1(config)#interface loopback10
R1(config-if-loopback10)#ip address 10.10.10.1 255.255.255.255
R1(config-if-loopback10)#exit

R1(config)#router ospf 100
R1(config-ospf-100)#area 0
R1(config-ospf-100-area-0)#network 54.1.1.0 0.0.0.255
R1(config-ospf-100-area-0)#network 57.1.1.0 0.0.0.255
R1(config-ospf-100-area-0)#network 10.10.10.1 0.0.0.0
R1(config-ospf-100-area-0)#mpls traffic-eng
R1(config-ospf-100-area-0)#exit

R1(config)#interface te_tunnel1
R1(config-if-te_tunnel1)#ip unnumbered loopback10
R1(config-if-te_tunnel1)#exit

R1(config)#mpls traffic-eng
R1(config-mpls-te)#interface loopback10
R1(config-mpls-te-if-loopback10)#exit
R1(config-mpls-te)#router-id 10.10.10.1
R1(config-mpls-te)#interface gei-0/4
R1(config-mpls-te-if-gei-0/4)#exit
R1(config-mpls-te)#interface gei-0/7
```

```
R1(config-mpls-te-if-gei-0/7)#exit
R1(config-mpls-te)#tunnel te_tunnel1
R1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 10.10.10.2
R1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng path-option 1
explicit-path identifier 1
R1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng record-route
R1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng hot-standby
protect 1 dynamic
R1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng bfd interval 30
min-rx 30 multiplier 5
R1(config-mpls-te-tunnel-te_tunnel1)#exit

R1(config-mpls-te)#explicit-path identifier 1
R1(config-mpls-te-expl-path-id-1)#next-address strict 54.1.1.3
R1(config-mpls-te-expl-path-id-1)#next-address strict 115.1.1.2
```

R2上的配置如下：

```
R2(config)#interface gei-0/7
R2(config-if-gei-0/7)#ip address 57.1.1.2 255.255.255.0
R2(config-if-gei-0/7)#exit
R2(config)#interface gei-0/5
R2(config-if-gei-0/5)#ip address 115.1.1.2 255.255.255.0
R2(config-if-gei-0/5)#exit
R2(config)#interface loopback10
R2(config-if-loopback10)#ip address 10.10.10.2 255.255.255.255
R2(config-if-loopback10)#exit

R2(config)#router ospf 100
R2(config-ospf-100)#area 0
R2(config-ospf-100-area-0)#network 115.1.1.0 0.0.0.255
R2(config-ospf-100-area-0)#network 57.1.1.0 0.0.0.255
R2(config-ospf-100-area-0)#network 10.10.10.2 0.0.0.0
R2(config-ospf-100-area-0)#mpls traffic-eng
R2(config-ospf-100-area-0)#exit

R2(config)#mpls traffic-eng
R2(config-mpls-te)#interface loopback10
R2(config-mpls-te-if-loopback10)#exit
R2(config-mpls-te)#router-id 10.10.10.2
R2(config-mpls-te)#interface gei-0/7
R2(config-mpls-te-if-gei-0/7)#exit
R2(config-mpls-te)#interface gei-0/5
R2(config-mpls-te-if-gei-0/5)#exit
```

R3上的配置如下：

```
R3(config)#interface gei-1/4
R3(config-if-gei-1/4)#ip address 54.1.1.3 255.255.255.0
R3(config-if-gei-1/4)#exit
R3(config)#interface gei-1/5
R3(config-if-gei-1/5)#ip address 115.1.1.3 255.255.255.0
R3(config-if-gei-1/5)#exit
R3(config)#interface loopback10
R3(config-if-loopback10)#ip address 10.10.10.3 255.255.255.255
R3(config-if-loopback10)#exit

R3(config)#router ospf 100
R3(config-ospf-100)#area 0
R3(config-ospf-100-area-0)#network 115.1.1.0 0.0.0.255
R3(config-ospf-100-area-0)#network 54.1.1.0 0.0.0.255
R3(config-ospf-100-area-0)#network 10.10.10.3 0.0.0.0
R3(config-ospf-100-area-0)#mpls traffic-eng
R3(config-ospf-100-area-0)#exit

R3(config)#mpls traffic-eng
R3(config-mpls-te)#interface loopback10
R3(config-mpls-te-if-loopback10)#exit
R3(config-mpls-te)#router-id 10.10.10.3
R3(config-mpls-te)#interface gei-1/4
```

```
R3(config-mpls-te-if-gei-1/4)#exit
R3(config-mpls-te)#interface gei-1/5
R3(config-mpls-te-if-gei-1/5)#exit
```

配置验证

正确配置后，R1上tunnel1 up，并且会生成一条hotstandby隧道，hotstandby关系为ready，并且R1上的RSVP LSP BFD会话应该能够成功建立。当R3-R2之间的链路失效后，LSP BFD会话down下再up，流量切换到hotstandby隧道上。

用**show bfd neighbors** [**rsvp brief**|**rsvp detail**]来查看验证RSVP 接口BFD是否生效。

R1上隧道up情况：

```
R1(config)#show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:           running
    RSVP Process:                 running
    Forwarding:                   enabled
TUNNEL NAME      DESTINATION     UP IF   DOWN IF     STATE/PROT
tunnel_1         10.10.10.2      -       gei-0/4     up/up
tunnel_1(hot)    10.10.10.2      -       gei-0/7     up/up

R1#sho mpls traffic-eng fast-reroute
Tunnel head end item information
Protected Tunnel   LspID    In-label Out intf/label     FRR intf/label  Status
Tunnel1              9    Tun hd   gei-0/4:147456     Tu1:3          ready
                                6

LSP midpoint frr information:
LSP identifier            In-label Out intf/label     FRR intf/label  Status

R1#sho mpls traffic-eng tunnels hot-standby
 Name: tunnel_1               (Tunnel1) Destination: 10.10.10.2
  Status:
    Admin: up  Oper: up  Path:  valid  Signalling: connected
  Fast Reroute Protection: None
  Hot-standby Protection: Ready

  InLabel: -
  OutLabel: gei-0/7, 3
  RSVP Signalling Info :
    Src 10.10.10.1, Dst 10.10.10.2, Tun_Id 1, Tun_Instance 10
    RSVP Path Info:
      Explicit Route: 57.1.1.1 57.1.1.2 10.10.10.2
      Exclude  Route: 10.10.10.3 115.1.1.2
      Record Route: NULL
      Tspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits
    RSVP Resv Info:
      Record Route: 10.10.10.2 57.1.1.2
      Fspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits
```

R1上RSVP接口BFD生效情况查看：

```
R1#show bfd neighbors rsvp lsp brief
TunnelId       LspId        LD       RD       Hold     State
te_tunnel1     16           33053    2662     150      UP

R1#show bfd neighbors rsvp lsp detail
------------------------------------------------------------------------------
--
TunnelId:te_tunnel1
LspId:16
LspRole:master
Local Discr:33053         Remote Discr:2662         State:UP
```

```
Holddown(ms):150          BFD Type:RSVP LSP[Active]
Instance Name:
--------------------------------------------------------------------------
--
Version:1                Dest UDP Port:3784        Final Bit:1
Local Diag: 0             Demand Mode:0            Poll Bit:0
MinTxInt: 50              MinRxInt:50             Multiplier:3
Received MinTxInt: 10      Received MinRxInt:10      Received Multiplier:3

Length:24                Min Echo Interval:0

Rx Count:0               Rx Interval (ms) min/max/avg:0     /0     /0
Tx Count:0               Tx Interval (ms) min/max/avg:0     /0     /0
Registered Protocols:RSVP LSP
Uptime:0 day(s),0 hour(s),0 minute(s)
Control Plane Rcv Phy Interface Name: gei-0/4
==========================================================================
==

/*R3-R2链路失效后，隧道hotstandby关系为active，rsvp lsp bfd状态为down*/
R1#sho mpls traffic-eng fast-reroute
Tunnel head end item information
Protected Tunnel   LspID    In-label Out intf/label     FRR intf/label  Status
Tunnel1              9    Tun hd   gei-0/4:147456     Tu1:3          active
                                6

LSP midpoint frr information:
LSP identifier            In-label Out intf/label     FRR intf/label  Status

R1#sho mpls traffic-eng tunnels hot-standby

Name: tunnel_1               (Tunnel1) Destination: 10.10.10.2
  Status:
    Admin: up  Oper: up  Path:  valid  Signalling: connected
  Fast Reroute Protection: None
  Hot-standby Protection: Backup lsp in use

R1(config)#show bfd neighbors rsvp lsp brief
TunnelId/PeerAddr        LD       RD       Hold     State
te_tunnel1              11       71       150      DOWN
```

6.3.2 TE-FRR

为了保证MPLS网络的可靠性，FRR借助MPLS TE的能力为LSP提供快速保护切换能力。

MPLS FRR是一种用于链路保护和节点保护的机制。当LSP链路或者节点故障时，在发现故障的节点进行保护，这样可以允许流量继续从保护链路或者保护节点的隧道中通过，使数据传输不发生中断，头节点可以在数据传输不受影响的同时继续发起主路径的重建。

MPLS FRR的基本原理是用一条预先建立的LSP来保护一条或多条LSP。预先建立的LSP称为快速重路由LSP，被保护的LSP称为主LSP。MPLS FRR的最终目的就是利用快速重路由隧道绕过故障的链路或者节点，从而达到保护主路径的功能。

6.3.2.1 配置 TE-FRR

本节介绍TE-FRR的配置步骤和命令。

1.配置隧道支持FRR功能。

步骤	命令	功能
1	inspur(config-mpls-te)#**tunnel te_tunnel** <*tunnel-number*>	进入Tunnel接口配置模式
2	inspur(config-mpls-te-tunnel-te_tunnel-tunnel-number)#**tunnel mpls traffic-eng fast-reroute** {**facility** | **one-to-one**}	配置该隧道支持fast reroute功能

2.配置备份隧道。

步骤	命令	功能
1	inspur(config-mpls-te)#**interface** <*interface-name*>	进入MPLS-TE接口配置模式
2	inspur(config-mpls-te-if-interface-name)#**backup-path te_tunnel** <*tunnel-id*>	在主隧道的出接口配置备份隧道的tunnel-id

3.配置自动备份隧道。

步骤	命令	功能
1	inspur(config-mpls-te)#**interface** <*interface-name*>	进入MPLS-TE接口配置模式
2	inspur(config-mpls-te-if-interface-name)#**auto-tunnel backup**	配置该隧道支持自动备份隧道功能
3	inspur(config-mpls-te-if-interface-name)#**auto-tunnel backup nhop-only**	自动备份隧道只支持链路保护
4	inspur(config-mpls-te)#**auto-tunnel backup tunnel-num min** <*min-value*> **max** <*max-value*>	配置自动备份隧道的最小或最大tunnel-num

<*min-value*>：自动备份隧道的最小tunnel-num，范围为32001~32999。

<*max-value*>： 自动备份隧道的最大tunnel-num，范围为32002~33000。

4.验证配置结果。

命令	功能
inspur#**show mpls traffic-eng fast-reroute**	显示全局配置的FRR映射关系
inspur#**show mpls traffic-eng auto-backup tunnels band** [**te_tunnel** <*tunnelId*>]	显示自动备份隧道和主隧道的绑定信息
inspur#**show mpls traffic-eng auto-backup tunnels summary**	显示自动备份隧道的摘要信息
inspur#**show mpls traffic-eng auto-backup parameter**	显示自动备份隧道的参数信息

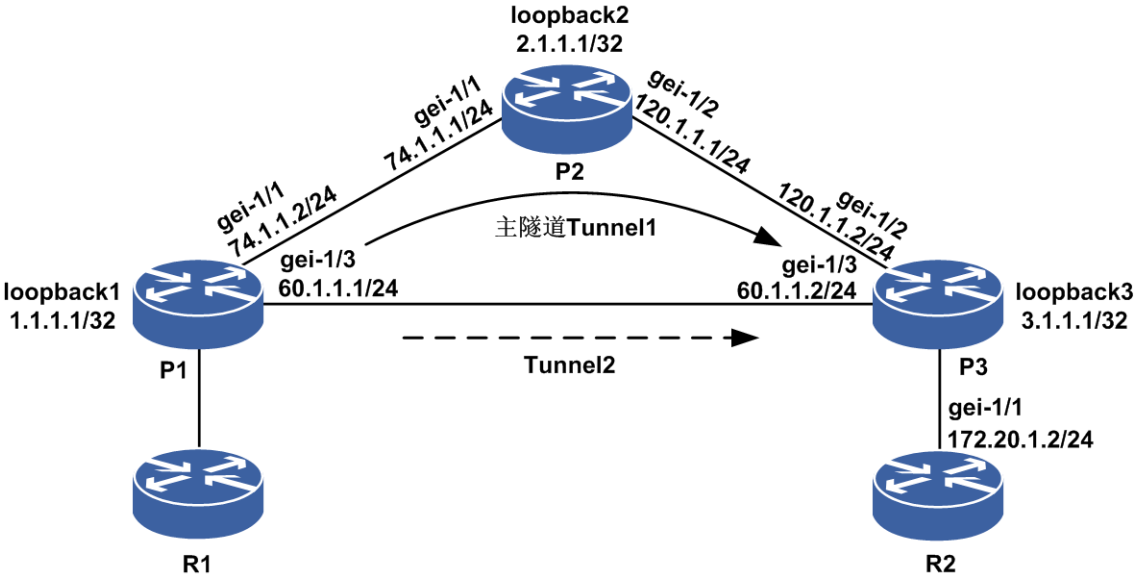
命令	功能
inspur#**debug rsvp fast-reroute**	打印手动备份隧道的debug信息

6.3.2.2 Facility 手动保护方式的配置实例

配置说明

如*图 6-134*所示，从P1到P3建立两条隧道，tunnel1通过P1、P2、P3，tunnel2通过P1、P3，其中tunnel1为主隧道，tunnel2为备份隧道，形成FRR关系。当主隧道发生故障时，备份隧道进行保护，流量切换到备份隧道上。

图 6-13 Facility 手动保护方式配置实例示意图



配置思路

1.P1、P2、P3直连接口均建立OSPF邻居，OSPF使能TE。

2.分别建立两条严格路径，主路径为P1、P2、P3，备份路径为P1、P3。

3.P1、P2、P3所用的接口均使能TE，并在P1上的gei-1/1上配置备份隧道。

4.创建主备隧道，主隧道下使能FRR facility，目的地为P3的TE的Router-ID，路径为严格路径。

5.在P1上配置一条到目的地的静态路由，下一跳为Tunnel1，这样流量通过Tunnel来转发。

配置过程

P1的配置如下：

```
P1(config)#interface gei-1/1
P1(config-if-gei-1/1)#no shutdown
P1(config-if-gei-1/1)#ip address 74.1.1.2 255.255.255.0
P1(config-if-gei-1/1)#exit
P1(config)#interface gei-1/3
P1(config-if-gei-1/3)#no shutdown
P1(config-if-gei-1/3)#ip address 60.1.1.1 255.255.255.0
P1(config-if-gei-1/3)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit
P1(config)#interface te_tunnel2
P1(config-if-te_tunnel2)#ip unnumbered loopback1
P1(config-if-te_tunnel2)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 1.1.1.1  0.0.0.0
P1(config-ospf-1-area-0)#network 74.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 60.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#explicit-path name primary
P1(config-mpls-te-expl-path-name)# next-address strict 74.1.1.1
P1(config-mpls-te-expl-path-name)#next-address strict 120.1.1.2
P1(config-mpls-te-expl-path-name)#exit
P1(config-mpls-te)#explicit-path name back
P1(config-mpls-te-expl-path-name)#next-address strict 60.1.1.2
P1(config-mpls-te-expl-path-name)#exit
P1(config-mpls-te)#interface gei-1/1
P1(config-mpls-te-if-gei-1/1)#exit
P1(config-mpls-te)#interface gei-1/3
P1(config-mpls-te-if-gei-1/3)#exit

P1(config-mpls-te)#tunnel te_tunnel1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 3.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng path-option 1
explicit-path name primary
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng record-route
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel  mpls  traffic-eng  fast-reroute
facility
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#tunnel te_tunnel2
P1(config-mpls-te-tunnel-te_tunnel2)#tunnel destination ipv4 3.1.1.1
P1(config-mpls-te- tunnel-te_tunnel2)#tunnel mpls traffic-eng path-option 1
explicit-path name back
P1(config-mpls-te-tunnel-te_tunnel2)#exit
P1(config-mpls-te)#interface gei-1/1
P1(config-mpls-te-if-gei-1/1)#backup-path te_tunnel 2
P1(config-mpls-te-if-gei-1/1)#exit
P1(config-mpls-te)#exit

P1(config)#ip route 172.20.1.2 255.255.255.255 te_tunnel1
```

P2的配置如下：

```
P2(config)#interface gei-1/1
P2(config-if-gei-1/1)#no shutdown
P2(config-if-gei-1/1)#ip address 74.1.1.1 255.255.255.0
P2(config-if-gei-1/1)#exit
P2(config)#interface gei-1/2
P2(config-if-gei-1/2)#no shutdown
P2(config-if-gei-1/2)#ip address 120.1.1.1 255.255.255.0
P2(config-if-gei-1/2)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 2.1.1.1  0.0.0.0
P2(config-ospf-1-area-0)#network 74.1.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 120.1.1.0 0.0.0.255
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-1/1
P2(config-mpls-te-if-gei-1/1)#exit
P2(config-mpls-te)#interface gei-1/2
P2(config-mpls-te-if-gei-1/2)#exit
P2(config-mpls-te)#exit
```

P3的配置如下：

```
P3(config)#interface gei-1/2
P3(config-if-gei-1/2)#no shutdown
P3(config-if-gei-1/2)#ip address 120.1.1.2 255.255.255.0
P3(config-if-gei-1/2)#exit
P3(config)#interface gei-1/3
P3(config-if-gei-1/3)#no shutdown
P3(config-if-gei-1/3)#ip address 60.1.1.2 255.255.255.0
P3(config-if-gei-1/3)#exit
P3(config)#interface loopback3
P3(config-if-loopback3)#ip address 3.1.1.1 255.255.255.255
P3(config-if-loopback3)#exit

P3(config)#router ospf 1
P3(config-ospf-1)#router-id 3.1.1.1
P3(config-ospf-1)#area 0
P3(config-ospf-1-area-0)#network 3.1.1.1  0.0.0.0
P3(config-ospf-1-area-0)#network 120.1.1.0 0.0.0.255
P3(config-ospf-1-area-0)#network 60.1.1.0 0.0.0.255
P3(config-ospf-1-area-0)#mpls traffic-eng
P3(config-ospf-1-area-0)#exit

P3(config)#mpls traffic-eng
P3(config-mpls-te)#interface loopback3
P3(config-mpls-te-if-loopback3)#exit
P3(config-mpls-te)#router-id 3.1.1.1
P3(config-mpls-te)#interface gei-1/2
P3(config-mpls-te-if-gei-1/2)#exit
P3(config-mpls-te)#interface gei-1/3
P3(config-mpls-te-if-gei-1/3)#exit
P3(config-mpls-te)#exit
```

R2的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 172.20.1.2  255.255.255.0
R2(config-if-gei-1/1)#exit
```

配置验证

当隧道up后，在P1上可以看到FRR的建立情况：

```
P1#show mpls traffic-eng tunnels brief
Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
TUNNEL NAME   DESTINATION    UP IF        DOWN IF       STATE/PROT
tunnel_1      3.1.1.1          -         gei-1/1       up/up
tunnel_2      3.1.1.1          -         gei-1/3       up/up

P1#show mpls traffic-eng fast-reroute
Tunnel head end item information
Protected Tunnel   LspID    In-label Out intf/label     FRR intf/label  Status
Tunnel1             86    Tun hd   gei-1/1:147456         Tu2:3      ready

LSP midpoint frr information:
LSP identifier            In-label Out intf/label     FRR intf/label  Status
```

当主隧道发生故障时，流量切换到备隧道上，FRR处于active状态，此时主备隧道都处于up状态。在P1上可以查看到FRR的状态，当主隧道故障消失后，FRR关系恢复到ready状态。

```
P1#show mpls traffic-eng fast-reroute
Tunnel head end item information
Protected Tunnel   LspID    In-label Out intf/label     FRR intf/label  Status
Tunnel1             86    Tun hd   gei-1/3:147456         Tu2:3      active

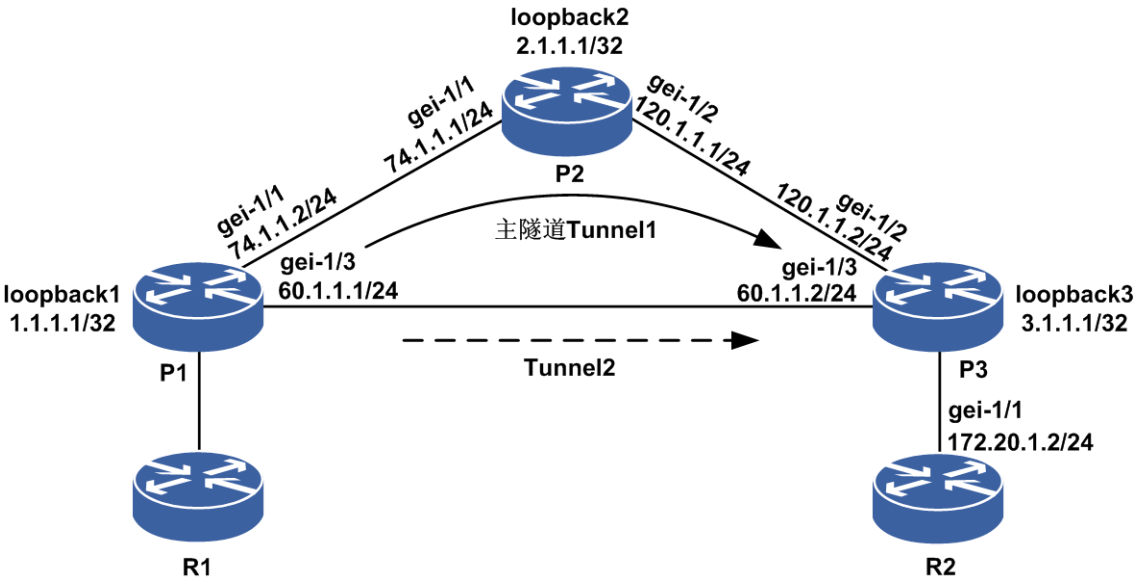
LSP midpoint frr information:
LSP identifier            In-label Out intf/label     FRR intf/label  Status
```

6.3.2.3 Facility 自动备份方式配置实例

配置说明

如*图 6-255*所示，从P1到P3建立主隧道，全局使能自动备份。tunnel1主隧道的显示路径为P1-P2-P3，主隧道上使能FRR facility保护，形成自动备份关系。当主隧道发生故障时，备份隧道进行保护，流量切换到备份隧道上。

图 6-25 Facility 自动备份方式配置实例示意图



配置思路

1.P1、P2、P3直连接口均建立OSPF邻居，OSPF使能TE。

2.TE模式下使能自动备份功能。

3.创建主隧道经过P1-P2-P3。

4.P1、P2、P3所用的接口均使能TE。

5.创建主隧道，主隧道下使能FRR facility，目的地为P3的TE的Router-ID，路径为严格路径。

6.在P1上配置一条到目的地的静态路由，下一跳为Tunnel1，这样流量通过Tunnel来转发。

配置过程

P1的配置如下：

```
P1(config)#interface gei-1/1
P1(config-if-gei-1/1)#no shutdown
P1(config-if-gei-1/1)#ip address 74.1.1.2 255.255.255.0
P1(config-if-gei-1/1)#exit
P1(config)#interface gei-1/3
P1(config-if-gei-1/3)#no shutdown
P1(config-if-gei-1/3)#ip address 60.1.1.1 255.255.255.0
P1(config-if-gei-1/3)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
```

```
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 1.1.1.1  0.0.0.0
P1(config-ospf-1-area-0)#network 74.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 60.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#explicit-path name primary
P1(config-mpls-te-expl-path-name)#next-address strict 74.1.1.1
P1(config-mpls-te-expl-path-name)#next-address strict 120.1.1.2
P1(config-mpls-te-expl-path-name)#exit

P1(config-mpls-te)#interface gei-1/1
P1(config-mpls-te-if-gei-1/1)#auto-tunnel backup
P1(config-mpls-te-if-gei-1/1)#exit
P1(config-mpls-te)#interface gei-1/3
P1(config-mpls-te-if-gei-1/3)#exit

P1(config-mpls-te)#tunnel te_tunnel 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 3.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng path-option 1
explicit-path name primary
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng record-route
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel  mpls  traffic-eng  fast-reroute
facility
P1(config-mpls-te-tunnel-te_tunnel1)#exit

P1(config)#ip route 172.20.1.2 255.255.255.255 te_tunnel1
```

P2的配置如下：

```
P2(config)#interface gei-1/1
P2(config-if-gei-1/1)#no shutdown
P2(config-if-gei-1/1)#ip address 74.1.1.1 255.255.255.0
P2(config-if-gei-1/1)#exit
P2(config)#interface gei-1/2
P2(config-if-gei-1/2)#no shutdown
P2(config-if-gei-1/2)#ip address 120.1.1.1 255.255.255.0
P2(config-if-gei-1/2)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 2.1.1.1  0.0.0.0
P2(config-ospf-1-area-0)#network 74.1.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 120.1.1.0 0.0.0.255
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-1/1
P2(config-mpls-te-if-gei-1/1)#exit
P2(config-mpls-te)#interface gei-1/2
P2(config-mpls-te-if-gei-1/2)#exit
P2(config-mpls-te)#exit
```

P3的配置如下：

```
P3(config)#interface gei-1/2
P3(config-if-gei-1/2)#no shutdown
```

```
P3(config-if-gei-1/2)#ip address 120.1.1.2 255.255.255.0
P3(config-if-gei-1/2)#exit
P3(config)#interface gei-1/3
P3(config-if-gei-1/3)#no shutdown
P3(config-if-gei-1/3)#ip address 60.1.1.2 255.255.255.0
P3(config-if-gei-1/3)#exit
P3(config)#interface loopback3
P3(config-if-loopback3)#ip address 3.1.1.1 255.255.255.255
P3(config-if-loopback3)#exit

P3(config)#router ospf 1
P3(config-ospf-1)#router-id 3.1.1.1
P3(config-ospf-1)#area 0
P3(config-ospf-1-area-0)#network 3.1.1.1  0.0.0.0
P3(config-ospf-1-area-0)#network 120.1.1.0 0.0.0.255
P3(config-ospf-1-area-0)#network 60.1.1.0 0.0.0.255
P3(config-ospf-1-area-0)#mpls traffic-eng
P3(config-ospf-1-area-0)#exit

P3(config)#mpls traffic-eng
P3(config-mpls-te)#interface loopback3
P3(config-mpls-te-if-loopback3)#exit
P3(config-mpls-te)#router-id 3.1.1.1
P3(config-mpls-te)#interface gei-1/2
P3(config-mpls-te-if-gei-1/2)#exit
P3(config-mpls-te)#interface gei-1/3
P3(config-mpls-te-if-gei-1/3)#exit
P3(config-mpls-te)#exit
```

R2的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 172.20.1.2 255.255.255.0
R2(config-if-gei-1/1)#exit
```

配置验证

在P1上可以看到主隧道和自动隧道都已经形成。

```
P1(config)##show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:          running
    RSVP Process:                 running
    Forwarding:                   enabled
TUNNEL NAME        DESTINATION    UP IF    DOWN IF       STATE/PROT
tunnel_1           3.1.1.1        -      gei-1/1       up/up
tunnel_33000       3.1.1.1         -      gei-1/3       up/up
```

在P1上查看自动备份保护关系已经形成。

```
P1(config)#show mpls traffic-eng fast-reroute
Tunnel head end item information
Protected Tunnel    LspID    In-label   Out intf/label       FRR intf/label
Status
Tunnel1             2     Tun hd    gei-1/1:147456        Tu33000:3     ready

LSP midpoint frr information:
LSP identifier            In-label Out intf/label     FRR intf/label    Status
```

当主隧道发生故障时，流量切换到备隧道上，FRR处于active状态，在P1上可以查看到FRR的状态，当主隧道故障消失后FRR关系恢复到ready状态。

```
P1(config)#show mpls traffic-eng fast-reroute
Tunnel head end item information
Protected Tunnel    LspID    In-label   Out intf/label       FRR intf/label
Status
Tunnel1             2     Tun hd    gei-1/1:147456        Tu33000:3    active
```

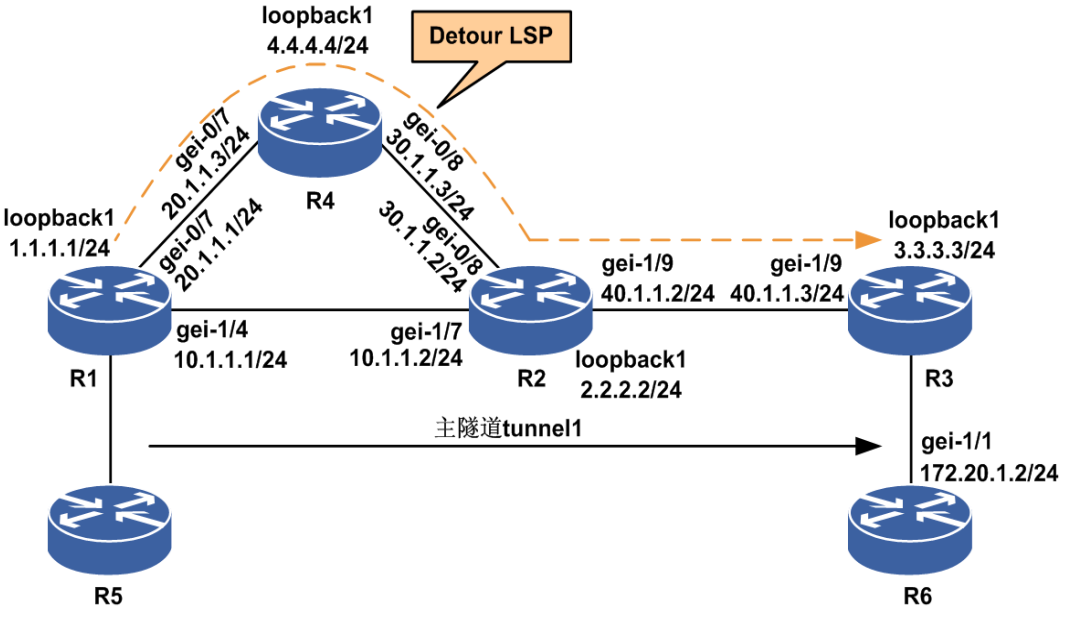
```
LSP midpoint frr information:
LSP identifier            In-label Out intf/label    FRR intf/label   Status
```

6.3.2.4 Detour 保护方式配置实例

配置说明

如*图 6-14*所示，从R1到R3建立主隧道，tunnel1通过R1、R2、R3。主隧道上使能**FRR one-to-one**保护，形成detour保护关系。当主隧道发生故障时，备份隧道进行保护，流量切换到备份隧道上。

图 6-14 Detour 保护方式配置实例示意图



配置思路

1.按*图 6-14*所示搭建环境，4台路由器R1、R2、R3和R4对接，R1、R2、R3和R4上分别配置loopback地址和接口地址。

2.在R1、R2、R3、R4上建立OSPF邻接关系，OSPF使能TE，接口使能TE。

3.在R1上的MPLS TE模式下在隧道头节点配置**FRR one-to-one**功能（指定严格路径为R1-R2-R3）。

4.在R1上配置一条到目的地的静态路由，下一跳为Tunnel1，这样流量通过Tunnel来转发。

配置过程

R1的配置如下：

```
R1(config)#interface loopback1
```

```
R1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
R1(config)#interface gei-1/4
R1(config-if-gei-1/4)#no shutdown
R1(config-if-gei-1/4)# ip address 10.1.1.1 255.255.255.0
R1(config-if-gei-1/4)#exit
R1(config)#interface gei-0/7
R1(config-if-gei-0/7)#no shutdown
R1(config-if-gei-0/7)# ip address 20.1.1.1 255.255.255.0
R1(config-if-gei-0/7)#exit
R1(config)#interface te_tunnel1
R1(config-if-te_tunnel1)#ip unnumbered loopback1
R1(config-if-te_tunnel1)#exit

R1(config)#router ospf 1
R1(config-ospf-1)#router-id 1.1.1.1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
R1(config-ospf-1-area-0)#mpls traffic-eng
R1(config-ospf-1-area-0)#network 10.1.1.0 0.0.0.255
R1(config-ospf-1-area-0)#network 20.1.1.0 0.0.0.255
R1(config-ospf-1-area-0)#exit

R1(config)#mpls traffic-eng
R1(config-mpls-te)#interface loopback1
R1(config-mpls-te-if-loopback1)#exit
R1(config-mpls-te)#router-id 1.1.1.1
R1(config-mpls-te)# interface gei-1/4
R1(config-mpls-te-if-gei-1/4)#exit
R1(config-mpls-te)# interface gei-0/7
R1(config-mpls-te-if-gei-0/7)#exit

R1(config-mpls-te)#tunnel te_tunnel1
R1(config-mpls-te-te_tunnel1)#tunnel destination ipv4 3.3.3.3
R1(config-mpls-te-te_tunnel1)#tunnel mpls traffic-eng path-option 1
explicit-path name inspur
R1(config-mpls-te-te_tunnel1)#tunnel mpls traffic-eng record-route
R1(config-mpls-te-te_tunnel1)#   tunnel   mpls   traffic-eng   fast-reroute
one-to-one
R1(config-mpls-te-)#exit
R1(config-mpls-te)#explicit-path name inspur
R1(config-mpls-te-expl-path-name)#next-address strict 10.1.1.2
R1(config-mpls-te-expl-path-name)#next-address strict 40.1.1.3
R1(config-mpls-te-expl-path-name)#exit
R1(config-mpls-te)#exit

R1(config)#ip route 172.20.1.2 255.255.255.255 te_tunnel1
```

R2的配置如下：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 2.2.2.2  255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/7
R2(config-if-gei-1/7)#no shutdown
R2(config-if-gei-1/7)#ip address 10.1.1.2 255.255.255.0
R2(config-if-gei-1/7)#exit
R2(config)#interface gei-1/9
R2(config-if-gei-1/9)#no shutdown
R2(config-if-gei-1/9)#ip address 40.1.1.2 255.255.255.0
R2(config-if-gei-1/9)#exit
R2(config)#interface gei-0/8
R2(config-if-gei-0/8)#no shutdown
R2(config-if-gei-0/8)#ip address 30.1.1.2 255.255.255.0
R2(config-if-gei-0/8)#exit

R2(config)#router ospf 1
R2(config-ospf-1)#router-id 2.2.2.2
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 2.2.2.2  0.0.0.0
R2(config-ospf-1-area-0)#mpls traffic-eng
```

```
R2(config-ospf-1-area-0)#network 10.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#network 30.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#network 40.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#exit

R2(config)#mpls traffic-eng
R2(config-mpls-te)#interface loopback1
R2(config-mpls-te-if-loopback1)#exit
R2(config-mpls-te)#router-id 2.2.2.2
R2(config-mpls-te)#interface gei-1/7
R2(config-mpls-te-if-gei-1/7)#exit
R2(config-mpls-te)# interface gei-1/9
R2(config-mpls-te-if-gei-1/9)#exit
R2(config-mpls-te)#exit
R2(config-mpls-te)#interface gei-0/8
R2(config-mpls-te-if-gei-0/8)#exit
R2(config-mpls-te)#exit
```

R3的配置如下：

```
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 3.3.3.3 255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-1/9
R3(config-if-gei-1/9)#no shutdown
R3(config-if-gei-1/9)#ip address 40.1.1.3 255.255.255.0
R3(config-if-gei-1/9)#exit

R3(config)#router ospf 1
R3(config-ospf-1)#router-id 3.3.3.3
R3(config-ospf-1)#area 0
R3(config-ospf-1-area-0)#network 3.3.3.3  0 0.0.0.0
R3(config-ospf-1-area-0)#mpls traffic-eng
R3(config-ospf-1-area-0)#network 40.1.1.0 0.0.0.255
R3(config-ospf-1-area-0)#exit

R3(config)#mpls traffic-eng
R3(config-mpls-te)#interface loopback1
R3(config-mpls-te-if-loopback1)#exit
R3(config-mpls-te)#router-id 3.3.3.3
R3(config-mpls-te)#interface gei-1/9
R3(config-mpls-te-if-gei-1/9)#exit
R3(config-mpls-te)#exit
```

R4的配置如下：

```
R4(config)#interface gei-0/7
R4(config-if-gei-0/7)#no shutdown
R4(config-if-gei-0/7)#ip address 20.1.1.3 255.255.255.0
R4(config-if-gei-0/7)#exit
R4(config)#interface gei-0/8
R4(config-if-gei-0/8)#no shutdown
R4(config-if-gei-0/8)#ip address 30.1.1.3 255.255.255.0
R4(config-if-gei-0/8)#exit
R4(config)#interface loopback1
R4(config-if-loopback1)#ip address 4.4.4.4  255.255.255.255
R4(config-if-loopback1)#exit

R4(config)#router ospf 1
R4(config-ospf-1)#router-id 4.4.4.4
R4(config-ospf-1)#area 0
R4(config-ospf-1-area-0)#network 4.4.4.4  0.0.0.0
R4(config-ospf-1-area-0)#mpls traffic-eng
R4(config-ospf-1-area-0)#network 20.1.1.0 0.0.0.255
R4(config-ospf-1-area-0)#network 30.1.1.0 0.0.0.255
R4(config-ospf-1-area-0)#exit

R4(config)#mpls traffic-eng
R4(config-mpls-te)#interface loopback1
R4(config-mpls-te-if-loopback1)#exit
```

```
R4(config-mpls-te)#router-id 4.4.4.4
R4(config-mpls-te)#interface gei-0/7
R4(config-mpls-te-if-gei-0/7)#exit
R4(config-mpls-te)#interface gei-0/8
R4(config-mpls-te-if-gei-0/8)#exit
R4(config-mpls-te)#exit
```

R6的配置如下：

```
R6(config)#interface gei-1/1
R6(config-if-gei-1/1)#no shutdown
R6(config-if-gei-1/1)#ip address 172.20.1.2  255.255.255.0
R6(config-if-gei-1/1)#exit
```

配置验证

在R1上可以看到主隧道和detour隧道都已经形成。

```
R1(config)#show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:           running
    RSVP Process:                 running
    Forwarding:                   enabled
TUNNEL NAME            DESTINATION   UP IF     DOWN IF        STATE/PROT
tunnel_1               3.3.3.3        -      gei-1/4         up/up
tunnel_1 (PLR backup)    3.3.3.3        -       gei-0/7         up/up

inspur#show mpls traffic-eng tunnels
Name: tunnel_1               (Tunnel1) Destination: 3.3.3.3
  Status:
    Admin: up  Oper: up  Path:  valid  Signalling: connected
    Path option: 1, type explicit name inspur (Basis for Setup)
    Hot-standby protection:
      no path options protected
  Config Parameters:
    Bandwidth: 0 kbps (Global) Priority: 7  7  Affinity: 0x0/0x0
    Resv-Style: SE
    Metric Type: IGP (default)   Upper Limit: 4294967295
    Facility Fast-reroute: disabled
    Detour Fast-reroute: enabled
    BFD: disabled
    Bidirect: disabled
    AutoRoute: disabled
    Forwarding-adjacency is not enabled

  InLabel:-
  OutLabel:gei-1/4,147456

  RSVP Signalling Info :
      Src 1.1.1.1, Dst 3.3.3.3, Tun_Id 1, Tun_Instance 62
    RSVP Path Info:
      Explicit Route: 10.1.1.1 10.1.1.2  40.1.1.2 40.1.1.3 3.3.3.3
      Exclude  Route: NONE
      Record   Route: NONE
Tspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits
RSVP Resv Info:
Record Route: 3.3.3.3 10.1.1.2 40.1.1.3
Fspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits

  History:
    Tunnel:
    Time since created: 0 days, 0 hours, 12 minutes
    Prior LSP: path option 1
    Current LSP: Uptime:0 days, 0 hours, 10 minutes
    Last lsp error information:
None log record.
```

```
Name: tunnel_1(PLR backup)(Tunnel) Destination: 3.3.3.3
 Status:
   Signalling: up

  RSVP Signalling Info :
InLabel:-
   OutLabel:gei-0/7,147457
     Src 1.1.1.1, Dst 13.3.3.3, Tun_Id 1, Tun_Instance 62
    RSVP Path Info:
     Explicit Route: 20.1.1.1 20.1.1.3 30.1.1.3 30.1.1.2 40.1.1.2
40.1.1.3
     Exclude  Route: NONE
Record Route: NULL
     Tspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits
    RSVP Resv Info:
     Record Route: 3.3.3.3  30.1.1.2
     Fspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits
  History:
    Tunnel:
    Time since created: 0 days, 0 hours, 10 minutes
    Current LSP: Uptime:0 days, 0 hours, 10 minutes
```

在R1上查看detour保护关系已经形成。

```
R1(config)#show mpls traffic-eng fast-reroute
Tunnel head end item information
Protected Tunnel  LspID  In-label   Out intf/label      FRR intf/label  Status
Tunnel1           1     Tun hd    gei-1/4:147456      Tu1:147457      ready

LSP midpoint frr information:
LSP identifier            In-label Out intf/label    FRR intf/label  Status
```

当主隧道发生故障时，流量切换到备隧道上，FRR处于active状态，在R1上可以查看到FRR的状态，当主隧道故障消失后FRR关系恢复到ready状态。

```
R1(config)#interface gei-1/4
R1(config-if-gei-1/4)#show mpls traffic-eng fast-reroute
Tunnel head end item information
Protected Tunnel  LspID   In-label  Out intf/label      FRR intf/label  Status
Tunnel1          1      Tun hd    gei-1/4:147456      Tu1:147457      active

R1(config-if-gei-1/4)#show mpls traffic-eng fast-reroute
Tunnel head end item information
Protected  Tunnel   LspID    In-label   Out  intf/label         FRR  intf/label
Status
Tunnel1          1      Tun hd    gei-1/4:147458      Tu1:147459      ready
```

6.3.3 MPLS TE 端到端路径保护

TE FRR和Hot_standby都属于RSVP-TE隧道保护技术，TE FRR是对局部进行保护，Hot_standby是对单条LSP进行从头结点到尾结点的全程保护和恢复（端到端保护）。

端到端的保护通过为隧道下的一条Working LSP在故障发生前预先创建一条Hot_standby LSP来提供保护，隧道下的这两条LSP的路径除首尾结点外互不相交。正常情况下流量都是经过Working LSP的，只有当Working LSP上的某段链路或结点发生故障并且头结点感知到故障后，进行切换操作，流量才会经过Hot_standby LSP。

6.3.3.1 配置 MPLS TE 端到端路径保护

本节介绍MPLS TE端到端路径保护的配置步骤和命令。

1.配置MPLS TE端到端路径保护。

步骤	命令	功能
1	inspur(config-mpls-te)#**tunnel te_tunnel** <*tunnel-number*>	进入Tunnel接口配置模式
2	inspur(config-mpls-te-tunnel-te_tunnel-tunnel-number)#**tunnel mpls traffic-engine hot-standby protect** <*path-option*>{**dynamic** | **explicit-path** {**identifier** <*id*>| **name** <*name*>}}	使能隧道下某一Path option的hot-standy功能

2.验证配置结果。

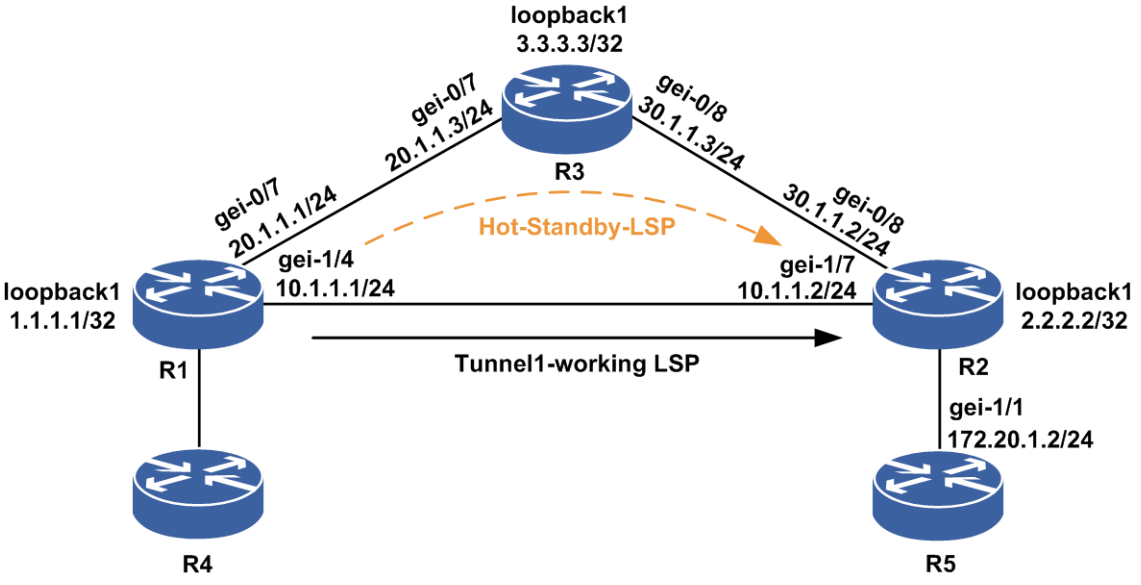
命令	功能
inspur#**show mpls traffic-eng tunnels hot-standby**	查看hot-standby LSP保护中备LSP的详细信息

6.3.3.2 MPLS TE 端到端路径保护配置实例

配置说明

如*图 6*-所示拓扑，组网中采用OSPF-TE建立MPLS TE端到端路径保护隧道，working LSP的路径为R1-R2，Hot_standby_lsp的路径为R1-R3-R2。

图 6-27 MPLS TE 端到端路径保护配置实例示意图



配置思路

1.按*图 6*-所示搭建环境，3台路由器R1、R2、R3对接，R1、R2、R3上分别配置loopback

地址和接口地址。

2.在R1、R2、R3上建立OSPF邻接关系，OSPF使能TE，接口使能TE。

3.在R1上的MPLS TE模式下在隧道头节点配置hot-standby功能（指定严格路径为R1-R2）。

4.查看hot-standby关系。

5.在R1上配置一条到目的地的静态路由，下一跳为Tunnel1，这样流量通过Tunnel来转发。

6.主隧道的链路失效后，查看hot-standby关系，流量切换到hot_standby_lsp转发。

7.主隧道的链路恢复后，查看hot-standby关系，流量恢复到working lsp转发。

配置过程

R1的配置如下。

接口相关配置：

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#interface gei-1/4
R1(config-if-gei-1/4)#no shutdown
R1(config-if-gei-1/4)#ip address 10.1.1.1 255.255.255.0
R1(config-if-gei-1/4)#exit
R1(config)#interface gei-0/7
R1(config-if-gei-0/7)#no shutdown
R1(config-if-gei-0/7)#ip address 20.1.1.1 255.255.255.0
R1(config-if-gei-0/7)#exit
R1(config)#interface te_tunnel1
R1(config-if-te_tunnel1)#ip unnumbered loopback1
R1(config-if-te_tunnel1)#exit
```

OSPF、OSPF-TE的相关配置：

```
R1(config)#router ospf 1
R1(config-ospf-1)#router-id 1.1.1.1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
R1(config-ospf-1-area-0)#mpls traffic-eng
R1(config-ospf-1-area-0)#network 10.1.1.0 0.0.0.255
R1(config-ospf-1-area-0)#network 20.1.1.0 0.0.0.255
R1(config-ospf-1-area-0)#exit
```

MPLS-TE配置：

```
R1(config)#mpls traffic-eng
R1(config-mpls-te)#interface loopback1
R1(config-mpls-te-if-loopback1)#exit
R1(config-mpls-te)#router-id 1.1.1.1
R1(config-mpls-te)#interface gei-1/4
R1(config-mpls-te-if-gei-1/4)#exit
R1(config-mpls-te)#interface gei-0/7
R1(config-mpls-te-if-gei-0/7)#exit
R1(config-mpls-te)#exit

R1(config)#mpls traffic-eng
R1(config-mpls-te)#explicit-path name inspur
R1(config-mpls-te-expl-path-name)#next-address strict 10.1.1.2
R1(config-mpls-te-expl-path-name)#exit
R1(config-mpls-te)#explicit-path name hot
R1(config-mpls-te-expl-path-name)#next-address strict 20.1.1.3
```

```
R1(config-mpls-te-expl-path-name)#next-address strict 30.1.1.2
R1(config-mpls-te-expl-path-name)#exit
R1(config-mpls-te)#tunnel te_tunnel1
R1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.2.2.2
R1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng path-option 1
explicit-path name inspur
R1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng record-route
R1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng hot-standby
protect 1 explicit-path name hot
R1(config-mpls-te-tunnel-te_tunnel1)#exit
R1(config-mpls-te)#exit

R1(config)#ip route 172.20.1.2 255.255.255.255 te_tunnel1
```

R2的配置如下。

接口相关配置：

```
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 2.2.2.2  255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#interface gei-1/7
R2(config-if-gei-1/7)#no shutdown
R2(config-if-gei-1/7)#ip address 10.1.1.2 255.255.255.0
R2(config-if-gei-1/7)#exit
R2(config)#interface gei-0/8
R2(config-if-gei-0/8)#no shutdown
R2(config-if-gei-0/8)#ip address 30.1.1.2 255.255.255.0
R2(config-if-gei-0/8)#exit
```

OSPF、OSPF-TE相关配置：

```
R2(config)#router ospf 1
R2(config-ospf-1)#router-id 2.2.2.2
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 2.2.2.2  0 0.0.0.0
R2(config-ospf-1-area-0)#mpls traffic-eng
R2(config-ospf-1-area-0)#network 10.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#network 30.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#exit
```

MPLS-TE相关配置：

```
R2(config)#mpls traffic-eng
R2(config-mpls-te)#interface loopback1
R2(config-mpls-te-if-loopback1)#exit
R2(config-mpls-te)#router-id 2.2.2.2
R2(config-mpls-te)#interface gei-1/7
R2(config-mpls-te-if-gei-1/7)#exit
R2(config-mpls-te)#interface gei-0/8
R2(config-mpls-te-if-gei-0/8)#exit
R2(config-mpls-te)#exit
```

R3的配置如下。

接口相关配置：

```
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 3.3.3.3  255.255.255.255
R3(config-if-loopback1)#exit
R3(config)#interface gei-0/7
R3(config-if-gei-0/7)#no shutdown
R3(config-if-gei-0/7)#ip address 20.1.1.3 255.255.255.0
R3(config-if-gei-0/7)#exit
R3(config)#interface gei-0/8
R3(config-if-gei-0/8)#no shutdown
R3(config-if-gei-0/8)#ip address 30.1.1.3 255.255.255.0
R3(config-if-gei-0/8)#exit
```

OSPF、OSPF-TE相关配置：

```
R3(config)#router ospf 1
```

```
R3(config-ospf-1)#router-id 3.3.3.3
R3(config-ospf-1)#area 0
R3(config-ospf-1-area-0)#network 3.3.3.3  0.0.0.0
R3(config-ospf-1-area-0)#mpls traffic-eng
R3(config-ospf-1-area-0)#network 20.1.1.0 0.0.0.255
R3(config-ospf-1-area-0)#network 30.1.1.0 0.0.0.255
R3(config-ospf-1-area-0)#exit
```

MPLS-TE配置：

```
R3(config)#mpls traffic-eng
R3(config-mpls-te)#interface loopback1
R3(config-mpls-te-if- loopback1)#exit
R3(config-mpls-te)#router-id 3.3.3.3
R3(config-mpls-te)#interface gei-0/7
R3(config-mpls-te-if-gei-0/7)#exit
R3(config-mpls-te)#interface gei-0/8
R3(config-mpls-te-if-gei-0/8)#exit
```

R5的配置如下：

```
R5(config)#interface gei-1/1
R5(config-if-gei-1/1)#no shutdown
R5(config-if-gei-1/1)#ip address 172.20.1.2  255.255.255.0
R5(config-if-gei-1/1)#exit
```

配置验证

在R1上查看隧道状态信息：

```
R1#show mpls traffic-eng tunnels brief
Signalling Summary:
           LSP Tunnels Process:          running
           RSVP Process:                running
           Forwarding:                  enabled
TUNNEL NAME  DESTINATION  UP IF   DOWN IF   STATE/PROT
tunnel_1         2.2.2.2         -       gei-1/4   up/up
tunnel_1(hot)     2.2.2.2         -       gei-0/7   up/up
```

查看hot-standby LSP与主LSP的保护关系：

```
R1(config-if)#show mpls traffic-eng tunnels hot-standby
Name: tunnel_1               (Tunnel1) Destination: 2.2.2.2
  Status:
    Admin: up  Oper: up  Path:  valid  Signaling: connected
  Fast Reroute Protection:disabled
  Hot-standby Protection: Ready
  Config Parameters:
  BFD: disabled
  InLabel: -
  OutLabel: gei-0/7, 147456
  RSVP Signaling Info :
    Src 1.1.1.1, Dst 2.2.2.2, Tun_Id 1, Tun_Instance 2
    RSVP Path Info:
      Explicit Route: 20.1.1.1 20.1.1.3 30.1.1.2  30.1.1.3 2.2.2.2
      Exclude  Route: NULL
      Record Route: 1.1.1.1  20.1.1.1
      Tspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits
    RSVP Resv Info:
      Record Route: 3.3.3.3  20.1.1.3 2.2.2.2  30.1.1.2
      Fspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits
```

主LSP的链路down后，查看hot-standby LSP与主LSP的保护关系，流量切换到hot-standby LSP上：

```
R1(config)#interface gei-1/4
R1(config-if-gei-1/4)#shutdown
R1(config-if-gei-1/4)#show mpls traffic-eng tunnels hot-standby
```

```
Name: tunnel_1              (Tunnel1) Destination: 2.2.2.2
  Status:
    Admin: up  Oper: up  Path:  valid  Signaling: connected
  Fast Reroute Protection:disabled
  Hot-standby Protection: Backup lsp in use
 Config Parameters:
 BFD: disabled
```

主LSP的链路恢复后，查看hot-standby LSP与主LSP的保护关系，流量恢复到working lsp上。

恢复后主LSP和hot-standby LSP隧道的详细显示信息：

```
R1(config-if)#show mpls traffic-eng tunnels te_tunnel 1
Name: tunnel_1              (Tunnel1) Destination: 2.2.2.2
  Status:
    Admin: up  Oper: up  Path:  valid  Signalling: connected
    Path option: 1, type explicit name inspur (Basis for Setup)
 Actual Bandwidth: N/A
    Hot-standby protection:
      protect option: 1, type explicit name: hot (Basis for Protect)
  Config Parameters:
    Bandwidth: 0 kbps (Global) Priority: 7  7  Affinity: 0x0/0x0
    Resv-Style: SE
    Metric Type: IGP (default)   Upper Limit: 4294967295
    Facility Fast-reroute: disabled
    Detour Fast-reroute: disabled
    BFD: disabled
    Bidirect: disabled
    AutoRoute: disabled
    Forwarding-adjacency: disabled
  InLabel:-
  OutLabel:gei-1/4,3
  RSVP Signalling Info :
      Src 1.1.1.1, Dst 2.2.2.2, Tun_Id 1, Tun_Instance 34
    RSVP Path Info:
      Explicit Route: 10.1.1.1 10.1.1.2 2.2.2.2
      Exclude  Route: NONE
      Record   Route: NONE
      Tspec:ave rate= 0 kbits, burst= 2000 bytes, peak rate = 0 kbits
    RSVP Resv Info:
      Record   Route: 2.2.2.2 10.1.1.2
      Fspec:ave rate= 0 kbits, burst= 2000 bytes, peak rate = 0 kbits

  History:
    Tunnel:
    Time since created: 0 days, 18 hours, 37 minutes
    Time since path change: 0 days, 0 hours, 0 minutes
    Prior LSP: path option 1 [27]
    Current LSP: Uptime:0 days, 0 hours, 11 minutes
    Last lsp error information:
    Delete mbb old inuse lsp(lspid:2,errcode:1,errvalue:1).
    Path error:rsvp sys error(lspid:3,errcode:23,errvalue:0).
    Path          error:routing          error,no          route          to
destination(lspid:1,errcode:24,errvalue:5)
```

6.3.4 MPLS TE 跨 AS 域

MPLS TE可以创建跨网络的LSP通道来传输流量，跨网络的LSP有两种：

- Inter-Area TE LSP：MPLS TE隧道的LSP穿过不在入口路由器拓扑数据库中的节点（节点在其它OSPF区域或者IS-IS level）。
- Inter-AS TE LSP：MPLS TE隧道的LSP穿过和入口路由器不在同一自治系统的节点。

6.3.4.1 配置 MPLS TE 跨 AS 域

本节介绍MPLS TE跨AS域的配置步骤和命令。

1.在全局开启TE功能。

命令	功能
inspur(config)#**mpls traffic-eng**	全局开启TE功能

2.配置TE接口的**passive-interface**属性。

步骤	命令	功能
1	inspur(config-mpls-te)#**interface** <*interface-name*>	进入TE接口配置模式
2	inspur(config-mpls-te-if-interface-name)#**passive-interface nbr-te-id** <*A.B.C.D*>[{[**nbr-if-addr** <*if-address*>],[**nbg-igp-id** {**isis** <*sysid*>| **ospf** <*sysid*>}]}]	配置TE接口的**passive-interface**属性

<*A.B.C.D*>：链路对端的邻居路由器的TE Router-ID。

<*if-address*>：远程ASBR的接口地址（不配置时，默认为邻居路由器的TE Router-ID）。

3.验证配置结果。

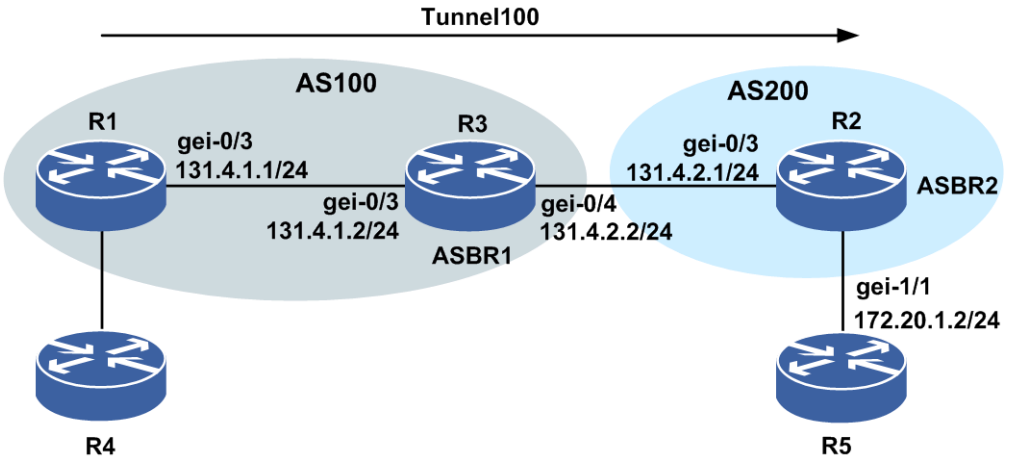
命令	功能
inspur#**show mpls traffic-eng interface detail** [<*interface-name*>]	显示TE接口下的详细配置信息
inspur#**show ip ospf database opaque-area**	查看ASBR的出接口会产生10型的Point-to-point LSA
inspur#**show isis database verbose**	查看数据库中是否有通告跨域的邻居信息

6.3.4.2 OSPF TE 跨 AS 域配置实例

配置说明

网络拓扑如*图 6-158*所示。R1和R3位于自治系统AS100，R2位于自治系统AS200， R1和R3位于同一个区域，配置全局OSPF实例，建立OSPF邻居。在ASBR1上的出接口上使能TE，并通过配置passive-interface，由ASBR1来构造一个Opaque LSA（10型点到点网络LSA），泛洪到自己所在的区域内。

图 6-158 OSPF TE 跨 AS 域配置实例示意图



配置思路

1.同一自治系统AS100的R1和R3之间建立OSPF邻居，并使能OSPF TE。

2.R1和R3上直连的2个接口使能TE。

3.在ASBR1的出接口上使能TE，并配置passive-interface。

4.ASBR2上使能OSPF TE，并将入接口gei-0/3使能TE。

5.在R1上配置一条TE隧道到R2，采用松散路径到ASBR1上。

6.在R1上配置一条到目的地的静态路由，下一跳为Tunnel1，这样流量通过Tunnel来转发。

配置过程

R1上的配置如下。

接口配置：

```
R1(config)#interface gei-0/3
R1(config-if-gei-0/3)#no shutdown
R1(config-if-gei-0/3)#ip address 131.4.1.1 255.255.255.0
R1(config-if-gei-0/3)#exit
R1(config)#interface loopback61
R1(config-if-loopback61)#ip address 61.61.61.1 255.255.255.255
R1(config-if-loopback61)#exit
```

OSPF以及OSPF TE的配置：

```
R1(config)#router ospf 777
R1(config-ospf-777)#router-id 61.61.61.1
R1(config-ospf-777)#area 0
R1(config-ospf-777-area-0)#network 61.61.61.1 0.0.0.0
R1(config-ospf-777-area-0)#network 131.4.1.0 0.0.0.255
R1(config-ospf-777-area-0)#mpls traffic-eng
R1(config-ospf-777-area-0)#exit
```

MPLS-TE配置：

```
R1(config)#mpls traffic-eng
R1(config-mpls-te)#interface loopback61
```

```
R1(config-mpls-te-if-loopback61)#exit
R1(config-mpls-te)#router-id 61.61.61.1
R1(config-mpls-te)#interface gei-0/3
R1(config-mpls-te-if-gei-0/3)#exit
R1(config-mpls-te)#exit

R1(config)#interface te_tunnel100
R1(config-if-te_tunnel100)#ip unnumbered loopback61
R1(config-if-te_tunnel100)#exit
R1(config)#mpls traffic-eng
R1(config-mpls-te)#tunnel te_tunnel 100
R1(config-mpls-te-tunnel-te_tunnel100)#tunnel destination ipv4 61.61.61.2
R1(config-mpls-te-tunnel-te_tunnel100)#tunnel mpls traffic-eng path-option 1
explicit-path identifier 100
R1(config-mpls-te-tunnel-te_tunnel100)#exit
R1(config-mpls-te)#explicit-path identifier 100
R1(config-mpls-te-expl-path-id-100)#next-address loose 61.61.61.3
R1(config-mpls-te-expl-path-id-100)#exit
R1(config-mpls-te)#exit
R1(config)#ip route 172.20.1.2 255.255.255.255 te_tunnel1
```

R2上的配置如下。

接口配置：

```
R2(config)#interface gei-0/3
R2(config-if-gei-0/3)#no shutdown
R2(config-if-gei-0/3)#ip address 131.4.2.1 255.255.255.0
R2(config-if-gei-0/3)#exit
R2(config)#interface loopback61
R2(config-if-loopback61)#ip address 61.61.61.2 255.255.255.255
R2(config-if-loopback61)#exit
```

OSPF TE的配置：

```
R2(config)#router ospf 777
R2(config-ospf-777)#router-id 61.61.61.2
R2(config-ospf-777)#area 0
R2(config-ospf-777-area-0)#mpls traffic-eng
R2(config-ospf-777-area-0)#exit
```

MPLS-TE配置：

```
R2(config)#mpls traffic-eng
R2(config-mpls-te)#interface loopback61
R2(config-mpls-te-if-loopback61)#exit
R2(config-mpls-te)#router-id 61.61.61.2
R2(config-mpls-te)#interface gei-0/3
R2(config-mpls-te-if-gei-0/3)#end
```

R3上的配置如下。

接口配置：

```
R3(config)#interface gei-0/3
R3(config-if-gei-0/3)#no shutdown
R3(config-if-gei-0/3)#ip address 131.4.1.2 255.255.255.0
R3(config-if-gei-0/3)#exit
R3(config)#interface gei-0/4
R3(config-if-gei-0/4)#no shutdown
R3(config-if-gei-0/4)#ip address 131.4.2.2 255.255.255.0
R3(config-if-gei-0/4)#exit
R3(config)#interface loopback61
R3(config-if-loopback61)#ip address 61.61.61.3 255.255.255.255
R3(config-if-loopback61)#exit
```

OSPF以及OSPF TE的配置：

```
R3(config)#router ospf 777
R3(config-ospf-777)#router-id 61.61.61.3
R3(config-ospf-777)#area 0
R3(config-ospf-777-area-0)#network 131.4.1.0 0.0.0.255
```

```
R3(config-ospf-777-area-0)#network 61.61.61.3 0.0.0.0
R3(config-ospf-777-area-0)#mpls traffic-eng
R3(config-ospf-777-area-0)#exit
```

MPLS-TE配置：

```
R3(config)#mpls traffic-eng
R3(config-mpls-te)#interface loopback61
R3(config-mpls-te-if-loopback61)#exit
R3(config-mpls-te)#router-id 61.61.61.3
R3(config-mpls-te)#interface gei-0/3
R3(config-mpls-te-if-gei-0/3)#exit
R3(config-mpls-te)#interface gei-0/4
R3(config-mpls-te-if-gei-0/4)#passive-interface nbr-te-id 61.61.61.2
 nbr-if-addr 131.4.2.1 nbr-igp-id ospf 61.61.61.2
```

R5的配置如下：

```
R5(config)#interface gei-1/1
R5(config-if-gei-1/1)#no shutdown
R5(config-if-gei-1/1)#ip address 172.20.1.2  255.255.255.0
R5(config-if-gei-1/1)#exit
```

配置验证

查看R1上的隧道建立情况：

```
R1(config)#show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:          running
    RSVP Process:                 running
    Forwarding:                   enabled
TUNNEL NAME              DESTINATION    UP IF    DOWN IF   STATE/PROT
tunnel_100               61.61.61.2     -        gei-0/3   up/up
R1(config)#show mpls traffic-eng tunnels te_tunnel 100
Name: tunnel_100              (Tunnel100) Destination: 61.61.61.2
  Status:
    Admin: up  Oper: up  Path:  valid  Signalling: connected
    Path option: 1, type explicit identifier 100 (Basis for Setup)
Hot-standby protection:
     no path options protected
  Config Parameters:

    Bandwidth: 0 kbps (Global) Priority: 7  7  Affinity: 0x0/0x0
    Resv-Style: SE
    Metric Type: IGP (default)   Upper Limit: 4294967295
    Facility Fast-reroute: disabled
    Detour Fast-reroute: disabled
    BFD: disabled
    Bidirect: disabled
    AutoRoute: disabled
    Forwarding-adjacency: disabled

  InLabel:-
  OutLabel:gei-0/3,147456

  RSVP Signalling Info :
     Src 61.61.61.1, Dst 61.61.61.2, Tun_Id 100, Tun_Instance 105
    RSVP Path Info:
      Explicit Route: 131.4.1.1 131.4.1.2 61.61.61.2
      Exclude  Route: NONE
      Record   Route: NONE
      Tspec:ave rate= 0 kbits, burst= 2000 bytes, peak rate = 0 kbits
    RSVP Resv Info:
      Record   Route: NONE
      Fspec:ave rate= 0 kbits, burst= 2000 bytes, peak rate = 0 kbits
```

查看ASBR上的数据库信息，ASBR的出接口会产生10型的Point-to-point LSA：

```
R3(config)#show ip osp database opaque-area area 0
          OSPF Router with ID (61.61.61.33) (Process ID 777)
              Type-10 Opaque Link Area Link States (Area 0.0.0.0)
  LS age: 665
  Options: (No TOS-capability, DC)
  LS Type: Opaque Area Link
  Link State ID: 1.0.0.0
  Opaque Type: 1
  Opaque ID: 0
  Advertising Router: 61.61.61.33
  LS Seq Number: 0x80000001
  Checksum: 0xabf2
  Length: 28
  Fragment number : 0

    MPLS TE router ID : 61.61.61.3

    Number of Links : 0

  LS age: 735
  Options: (No TOS-capability, DC)
  LS Type: Opaque Area Link
  Link State ID: 1.0.0.0
  Opaque Type: 1
  Opaque ID: 0
  Advertising Router: 61.61.61.2
  LS Seq Number: 0x80000001
  Checksum: 0x5c62
  Length: 28
  Fragment number : 0

    MPLS TE router ID : 61.61.61.2

    Number of Links : 0

  LS age: 752
  Options: (No TOS-capability, DC)
  LS Type: Opaque Area Link
  Link State ID: 1.0.0.0
  Opaque Type: 1
  Opaque ID: 0
  Advertising Router: 61.61.61.1
  LS Seq Number: 0x80000001
  Checksum: 0x5868
  Length: 28
  Fragment number : 0

    MPLS TE router ID : 61.61.61.1

    Number of Links : 0

  LS age: 655
  Options: (No TOS-capability, DC)
  LS Type: Opaque Area Link
  Link State ID: 1.0.0.1
  Opaque Type: 1
  Opaque ID: 1
  Advertising Router: 61.61.61.33
  LS Seq Number: 0x80000001
  Checksum: 0xd66f
  Length: 124
  Fragment number : 1


    Link connected to Broadcast network
      Link ID : 131.4.1.1
      Interface Address : 131.4.1.2
      Neighbor Interface Address : 0.0.0.0
      Admin Metric : 1
      Maximum bandwidth : 125000000
```

```
    Maximum reservable bandwidth : 0
    Number of Priority : 8
    Priority 0 : 0          Priority 1 : 0
    Priority 2 : 0          Priority 3 : 0
    Priority 4 : 0          Priority 5 : 0
    Priority 6 : 0          Priority 7 : 0
    Affinity Bit : 0x0

  Number of Links : 1

LS age: 664
Options: (No TOS-capability, DC)
LS Type: Opaque Area Link
Link State ID: 1.0.0.2
Opaque Type: 1
Opaque ID: 2
Advertising Router: 61.61.61.2
LS Seq Number: 0x80000002
Checksum: 0x99c8
Length: 124
Fragment number : 2


  Link connected to Broadcast network
    Link ID : 131.4.2.1
    Interface Address : 131.4.2.1
    Neighbor Interface Address : 0.0.0.0
    Admin Metric : 1
    Maximum bandwidth : 125000000
    Maximum reservable bandwidth : 0
    Number of Priority : 8
    Priority 0 : 0          Priority 1 : 0
    Priority 2 : 0          Priority 3 : 0
    Priority 4 : 0          Priority 5 : 0
    Priority 6 : 0          Priority 7 : 0
    Affinity Bit : 0x0

  Number of Links : 1

LS age: 659
Options: (No TOS-capability, DC)
LS Type: Opaque Area Link
Link State ID: 1.0.0.2
Opaque Type: 1
Opaque ID: 2
Advertising Router: 61.61.61.1
LS Seq Number: 0x80000003
Checksum: 0x6bf8
Length: 124
Fragment number : 2


  Link connected to Broadcast network
    Link ID : 131.4.1.1
    Interface Address : 131.4.1.1
    Neighbor Interface Address : 0.0.0.0
    Admin Metric : 1
    Maximum bandwidth : 125000000
    Maximum reservable bandwidth : 0
    Number of Priority : 8
    Priority 0 : 0          Priority 1 : 0
    Priority 2 : 0          Priority 3 : 0
    Priority 4 : 0          Priority 5 : 0
    Priority 6 : 0          Priority 7 : 0
    Affinity Bit : 0x0

  Number of Links : 1

LS age: 31
Options: (No TOS-capability, DC)
```

```
  LS Type: Opaque Area Link
  Link State ID: 1.0.0.4
  Opaque Type: 1
  Opaque ID: 4
  Advertising Router: 61.61.61.33
  LS Seq Number: 0x80000001
  Checksum: 0x3524
  Length: 124
  Fragment number : 4


    Link connected to Point-to-point network
      Link ID : 61.61.61.2
      Interface Address : 131.4.2.2
      Neighbor Interface Address : 61.61.61.2
      Admin Metric : 1
      Maximum bandwidth : 125000000
      Maximum reservable bandwidth : 0
      Number of Priority : 8
      Priority 0 : 0          Priority 1 : 0
      Priority 2 : 0          Priority 3 : 0
      Priority 4 : 0          Priority 5 : 0
      Priority 6 : 0          Priority 7 : 0
      Affinity Bit : 0x0

Number of Links : 1
```

查看ASBR上TE接口下的详细配置信息：

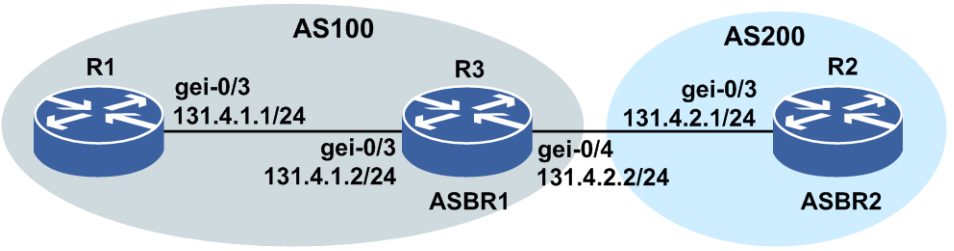
```
R3(config)#show mpls traffic-eng interface detail gei-0/4
 gei-0/4:
   State:
    ENABLE
   Traffic-eng metric:0
   Authentication: disabled
    Key:          <encrypted>
    Type:         md5
    Challenge:     disabled
    Challenge-imp:     Not implemented(simulated)
    Window size:   32
   BFD: disable
   Passive Info:
    nbr_te_id       nbr_if_addr     ospf_rid        isis_id
    61.61.61.2      131.4.2.1       61.61.61.2
   Backup path:
    None
SRLGs: None
   Intf Fast-Hello : DISABLE
    Fast-Hello interval : 10000
    Fast-Hello miss : 4
```

6.3.4.3 IS-IS TE 跨 AS 域配置实例

配置说明

网络拓扑如*图 6-169*所示。R1和R3位于自治系统AS100，R2位于自治系统AS200。 R1和R3位于同一个区域，配置全局IS-IS实例，建立IS-IS邻居。在ASBR1上的出接口上使能TE，并通过配置**passive-interface**，由ASBR1来构造一个点到点的数据库信息，泛洪到自己所在的区域内。

图 6-169 IS-IS TE 跨 AS 域配置实例示意图



配置思路

1.同一自治系统AS100的R1和R3之间建立IS-IS邻居，并使能IS-IS TE。

2.R1和R3上直连的2个接口使能TE。

3.在ASBR1的出接口上使能TE，并配置**passive-interface**。

4.ASBR2上使能IS-IS TE，并将入接口gei-0/3使能TE。

5.在R1上配置一条TE隧道到R2，采用松散路径到ASBR1上。

配置过程

R1的配置如下。

接口配置：

```
R1(config)#interface gei-0/3
R1(config-if-gei-0/3)#no shutdown
R1(config-if-gei-0/3)#ip address 131.4.1.1 255.255.255.0
R1(config-if-gei-0/3)#exit
R1(config)#interface loopback61
R1(config-if-loopback1)#ip address 61.61.61.1 255.255.255.255
R1(config-if-loopback1)#exit
```

IS-IS、IS-IS TE配置：

```
R1(config)#router isis 1
R1(config-isis-1)#area 01
R1(config-isis-1)#system-id 1236.4562.7895
R1(config-isis-1)#metric-style wide
R1(config-isis-1)#mpls traffic-eng level-1
R1(config-isis-1)#interface gei-0/3
R1(config-isis-1-if-gei-0/3)#ip router isis
R1(config-isis-1)#interface loopback61
R1(config-isis-1-if-loopback61)#ip router isis
R1(config-isis-1-if-loopback61)#exit
R1(config-isis-1)#exit
```

MPLS-TE配置：

```
R1(config)#mpls traffic-eng
R1(config-mpls-te)#interface gei-0/3
R1(config-mpls-te-if-gei-0/3)#exit
R1(config-mpls-te)#exit
R1(config)#interface te_tunnel100
R1(config-if-te_tunnel100)#ip unnumbered loopback1
R1(config-if-te_tunnel100)#exit

R1(config)#mpls traffic-eng
```

```
R1(config-mpls-te)#interface loopback61
R1(config-mpls-te-if-loopback61)#exit
R1(config-mpls-te)#router-id 61.61.61.1
R1(config-mpls-te)#tunnel te_tunnel 100
R1(config-mpls-te-tunnel-te_tunnel100)#tunnel destination ipv4 61.61.61.2
R1(config-mpls-te-tunnel-te_tunnel100)#tunnel mpls traffic-eng path-option 1
explicit-path identifier 100
R1(config-mpls-te-tunnel-te_tunnel100)#exit
R1(config-mpls-te)#explicit-path identifier 100
R1(config-mpls-te-expl-path-id-100)#next-address loose 61.61.61.3
R1(config-mpls-te-expl-path-id-100)#exit
R1(config-mpls-te)#exit
```

R2的配置如下。

接口配置：

```
R2(config)#interface gei-0/3
R2(config-if-gei-0/3)#no shutdown
R2(config-if-gei-0/3)#ip address 131.4.2.1 255.255.255.0
R2(config-if-gei-0/3)#exit
R2(config)#interface loopback61
R2(config-if-loopback61)#ip address 61.61.61.2 255.255.255.255
R2(config-if-loopback61)#exit
```

IS-IS、IS-IS TE配置：

```
R2(config)#router isis 1
R2(config-isis-1)#area 10
R2(config-isis-1)#system-id 2355.255E.3666
R2(config-isis-1)#metric-style wide
R2(config-isis-1)#mpls traffic-eng level-1
R2(config-isis-1)#interface loopback61
R2(config-isis-1-if-loopback61)#ip router isis
R2(config-isis-1-if-loopback61)#exit
R2(config-isis-1)#exit

R2(config)#mpls traffic-eng
R2(config-mpls-te)#interface loopback61
R2(config-mpls-te-if-loopback61)#exit
R2(config-mpls-te)#router-id 61.61.61.2
R2(config-mpls-te)#interface gei-0/3
R2(config-mpls-te-if-gei-0/3)#exit
R2(config-mpls-te)#exit
```

R3的配置如下。

接口配置：

```
R3(config)#interface gei-0/3
R3(config-if-gei-0/3)#no shutdown
R3(config-if-gei-0/3)# ip address 131.4.1.2 255.255.255.0
R3(config-if-gei-0/3)#exit
R3(config)#interface gei-0/4
R3(config-if-gei-0/4)#no shutdown
R3(config-if-gei-0/4)#ip address 131.4.2.2 255.255.255.0
R3(config-if-gei-0/4)#exit
R3(config)#interface loopback61
R3(config-if-loopback61)#ip address 61.61.61.3 255.255.255.255
R3(config-if-loopback61)#exit
```

IS-IS、IS-IS TE配置：

```
R3(config)#router isis 1
R3(config-isis-1)#area 01
R3(config-isis-1)#system-id 1234.5678.9101
R3(config-isis-1)#metric-style wide
R3(config-isis-1)#mpls traffic-eng level-1
R3(config-isis-1)#interface gei-0/3
R3(config-isis-1-if-gei-0/3)#ip router isis
R3(config-isis-1-if-gei-0/3)#exit
```

```
R3(config-isis-1)#interface loopback61
R3(config-isis-1-if-loopback61)#ip router isis
R3(config-isis-1-if-loopback61)#exit
R3(config-isis-1)#exit

R3(config)#mpls traffic-eng
R3(config-mpls-te)#interface loopback61
R3(config-mpls-te-if-loopback61)#exit
R3(config-mpls-te)#router-id 61.61.61.3
R3(config-mpls-te)#interface gei-0/3
R3(config-mpls-te-if-gei-0/3)#exit
R3(config-mpls-te)#interface gei-0/4
R3(config-mpls-te-if-gei-0/4)#passive-interface nbr-te-id 61.61.61.2
nbr-if-addr 131.4.2.1 nbr-igp-id isis 2355.255e.3666
R3(config-mpls-te-if-gei-0/4)#exit
R3(config-mpls-te)#exit
```

配置验证

查看R1上的隧道建立情况：

```
R1(config)#show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:          running
    RSVP Process:                 running
    Forwarding:                   enabled
TUNNEL NAME              DESTINATION    UP IF    DOWN IF   STATE/PROT
tunnel_100               61.61.61.2     -        gei-0/3   up/up

R1(config)#show mpls traffic-eng tunnels te_tunnel 100
Name: tunnel_100              (Tunnel100) Destination: 61.61.61.2
  Status:
    Admin: up  Oper: up  Path:  valid  Signalling: connected
    Path option: 1, type explicit identifier 100 (Basis for Setup)
Hot-standby protection:
     no path options protected
  Config Parameters:
    Bandwidth: 0 kbps (Global) Priority: 7  7  Affinity: 0x0/0x0
    Resv-Style: SE
    Metric Type: IGP (default)   Upper Limit: 4294967295
    Facility Fast-reroute: disabled
    Detour Fast-reroute: enabled
    BFD: disabled
    Bidirect: disabled
    AutoRoute: disabled
Forwarding-adjacency: disabled

  InLabel:-
  OutLabel:gei-0/3,147456

  RSVP Signalling Info :
     Src 61.61.61.1, Dst 61.61.61.2, Tun_Id 100, Tun_Instance 105
    RSVP Path Info:
      Explicit Route: 131.4.1.1 131.4.1.2 61.61.61.2
      Exclude  Route: NONE
      Record   Route: NONE
      Tspec:ave rate= 0 kbits, burst= 2000 bytes, peak rate = 0 kbits
    RSVP Resv Info:
      Record   Route: NONE
      Fspec:ave rate= 0 kbits, burst= 2000 bytes, peak rate = 0 kbits
```

查看R3上数据库信息：

```
R3(config)#show isis database verbose level-1
Process ID:0

Process ID:1
```

```
IS-IS level 1 link-state database:
LSPID                 LSP Seq Num    LSP Checksum    LSP Holdtime   ATT/P/OL
R3.00-00*              0x16          0x27c3          837            0/0/0
  NLPID:           0xcc
  Area Address:     01
  Ip address:       1.2.3.82
  Router ID:        61.61.61.3
  Hostname:         R3
  Metric: 16777215  IS-Extended 2355.255E.3666-00
    Affinity: 0x0
    Interface IP Address: 131.4.2.2
    Neighbor IP Address: 61.61.61.2
    Physical BW: 1000000 kbits/sec
    Reservable Global Pool BW: 0 kbits/sec
    Global Pool BW Unreserved:
      [0]:     0         kbits/sec, [1]:     0         kbits/sec
      [2]:     0         kbits/sec, [3]:     0         kbits/sec
      [4]:     0         kbits/sec, [5]:     0         kbits/sec
      [6]:     0         kbits/sec, [7]:     0         kbits/sec
  Metric: 10        IS-Extended R3.03
    Affinity: 0x0
    Interface IP Address: 131.4.1.2
    Physical BW: 1000000 kbits/sec
    Reservable Global Pool BW: 0 kbits/sec
    Global Pool BW Unreserved:
      [0]:     0         kbits/sec, [1]:     0         kbits/sec
      [2]:     0         kbits/sec, [3]:     0         kbits/sec
      [4]:     0         kbits/sec, [5]:     0         kbits/sec
      [6]:     0         kbits/sec, [7]:     0         kbits/sec
  Metric: 10        IP 131.4.1.0/24
  Metric: 10        IP 166.166.7.0/24
  Metric: 10        IP 1.2.3.82/32
  Metric: 10        IP 61.61.61.3/32
LSPID                 LSP Seq Num    LSP Checksum    LSP Holdtime   ATT/P/OL
R3.03-00*              0x8           0x7404          401            0/0/0
  Metric: 0         IS-Extended R1.00
  Metric: 0         IS-Extended R3.00
LSPID                 LSP Seq Num    LSP Checksum    LSP Holdtime   ATT/P/OL
R1.00-00               0xf           0xb98c          491            0/0/0
  NLPID:           0xcc
  Area Address:     01
  Ip address:       1.2.3.80
  Router ID:        61.61.61.1
  Hostname:         R1
  Metric: 10        IS-Extended R3.03
    Affinity: 0x0
    Interface IP Address: 131.4.1.1
    Physical BW: 1000000 kbits/sec
    Reservable Global Pool BW: 0 kbits/sec
    Global Pool BW Unreserved:
      [0]:     0         kbits/sec, [1]:     0         kbits/sec
      [2]:     0         kbits/sec, [3]:     0         kbits/sec
      [4]:     0         kbits/sec, [5]:     0         kbits/sec
      [6]:     0         kbits/sec, [7]:     0         kbits/sec
  Metric: 10        IP 131.4.1.0/24
  Metric: 10        IP 166.166.3.0/24
  Metric: 10        IP 1.2.3.80/32
  Metric: 10        IP 61.61.61.1/32
```

查看ASBR上TE接口下的详细配置信息：

```
R3(config)#show mpls traffic-eng interface detail gei-0/4
 gei-0/4:
   State:
    ENABLE
   Traffic-eng metric: 0
   Authentication: disabled
    Key:          <encrypted>
    Type:         md5
    Challenge:    disabled
```

```
 Challenge-imp:    Not implemented(simulated)
 Window size:   32
BFD: disable
LSP counter : 0
Passive Info:
 nbr_te_id       nbr_if_addr     ospf_rid        isis_id
 61.61.61.2      131.4.2.1                      2355.255e.3666
Backup path:
 None
SRLGs: None
 Intf Fast-Hello : DISABLE
 Fast-Hello interval : 10000
 Fast-Hello miss : 4
```

6.3.5 TE 认证

RSVP认证机制是指在RSVP环境下相邻的两个节点间发送消息过程中，通过在消息发送端对消息进行加密，在消息接收端对消息进行认证的一种手段。通过这种机制来保护RSVP消息不被非法的篡改伪造以及遭受重复发送攻击。

6.3.5.1 配置 TE 认证

本节介绍TE认证的配置步骤和命令。

相关信息

配置TE认证时，需要在相邻两节点的接口上都进行配置才能实现认证功能。

1.在全局和接口上开启MPLS TE功能。

步骤	命令	功能
1	inspur(config)#**mpls traffic-eng**	开启MPLS TE功能，并进入TE配置模式
2	inspur(config-mpls-te)#**interface** <*interface-name*>	在指定接口上开启MPLS TE功能

2.配置接口的认证功能。

步骤	命令	功能
1	inspur(config-mpls-te-if-interface-name)#**authentication**	使能接口的认证功能
2	inspur(config-mpls-te-if-interface-name)#**authentication challenge**	作为接收方需要跟邻居进行Challenge/Response握手
3	inspur(config-mpls-te-if-interface-name)#**authentication challenge-imp**	作为发送方实现跟邻居进行Challenge/Response握手
4	inspur(config-mpls-te-if-interface-name)#**authentication key passphrase** {**encrypted** <*encrypted-password*>|<*password*>}	设置认证密钥，<*encrypted-password*>表示已经加密的认证密钥，

步骤	命令	功能
		<*password*>表示未加密的认证密钥
5	inspur(config-mpls-te-if-interface-name)#**authentication type** {**md5** | **sha1**}	设置认证类型
6	inspur(config-mpls-te-if-interface-name)#**authentication window-size** <*window-size*>	设置接收认证消息时可容纳的窗体大小，范围：1~64

3.验证配置结果。

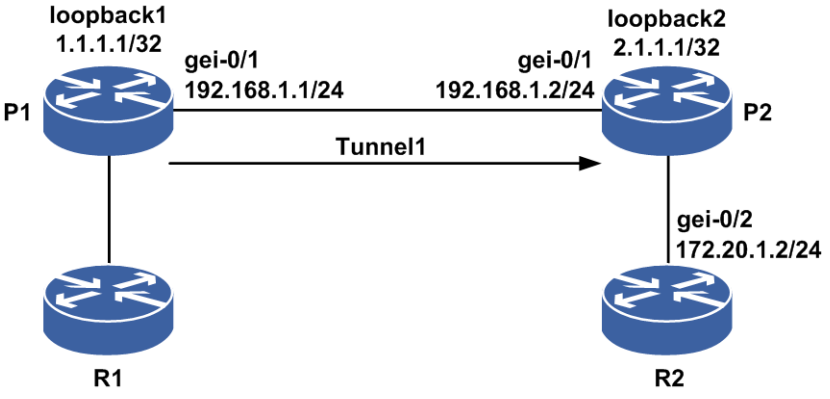
命令	功能
inspur#**show ip rsvp authentication**	查看认证关系

6.3.5.2 TE 认证配置实例

配置说明

如*图 6-30*所示，从P1到P2的RSVP普通隧道建立采用OSPF TE进行严格选路的方式，接口下采用SHA1认证方式。

图 6-30 TE 接口认证配置实例图



配置思路

1.P1、P2直连接口建立OSPF邻居，OSPF使能TE。

2.P1、P2直连接口使能TE，接口下采用认证方式，P1、P2相连接口都使能challenge和challenge-imp，采用SHA1认证方式，密码均为“12345678”。

3.P1上设置隧道的目的地和严格选路方式。

4.在P1上配置一条到目的地的静态路由，下一跳为Tunnel1，这样流量通过Tunnel来转发。

配置过程

P1上的配置如下：

```
P1(config)#interface gei-0/1
P1(config-if-gei-0/1)#no shutdown
P1(config-if-gei-0/1)#ip address 192.168.1.1 255.255.255.0
P1(config-if-gei-0/1)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#interface gei-0/1
P1(config-mpls-te-if-gei-0/1)#authentication
P1(config-mpls-te-if-gei-0/1)#authentication type sha1
/*设置TE接口认证类型为SHA1*/
P1(config-mpls-te-if-gei-0/1)#authentication key passphrase 12345678
/*设置认证密钥*/
P1(config-mpls-te-if-gei-0/1)#authentication challenge
P1(config-mpls-te-if-gei-0/1)#authentication challenge-imp
P1(config-mpls-te-if-gei-0/1)#authentication window-size 10
P1(config-mpls-te-if-gei-0/1)#exit
P1(config-mpls-te)#explicit-path identifier 1
P1(config-mpls-te-expl-path-id-1)#next-address strict 192.168.1.2
P1(config-mpls-te-expl-path-id-1)#exit
P1(config-mpls-te)#tunnel te_tunnel 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng path-option 1
explicit-path identifier 1
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#exit
P1(config)#ip route 172.20.1.2 255.255.255.255 te_tunnel1
```

P2上的配置如下：

```
P2(config)#interface gei-0/1
P2(config-if-gei-0/1)#no shutdown
P2(config-if-gei-0/1)#ip address 192.168.1.2 255.255.255.0
P2(config-if-gei-0/1)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit
```

```
P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-0/1
P2(config-mpls-te-if-gei-0/1)#authentication
P2(config-mpls-te-if-gei-0/1)#authentication challenge
P2(config-mpls-te-if-gei-0/1)#authentication challenge-imp
P2(config-mpls-te-if-gei-0/1)#authentication type sha1
/*设置TE接口认证类型为SHA1*/
P2(config-mpls-te-if-gei-0/1)#authentication key passphrase 12345678
/*设置认证密钥*/
P2(config-mpls-te-if-gei-0/1)#authentication window-size 10
P2(config-mpls-te-if-gei-0/1)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-0/2
R2(config-if-gei-0/2)#no shutdown
R2(config-if-gei-0/2)#ip address 172.20.1.2  255.255.255.0
R2(config-if-gei-0/2)#exit
```

配置验证

在P1上查看隧道情况，处于up状态，且可以查看Tunnel1的认证信息：

```
P1(config)#show mpls traffic-eng tunnels brief
Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
TUNNEL NAME DESTINATION UP IF DOWN IF STATE/PROT
tunnel_1    2.1.1.1     -  gei-0/1    up/up

P1(config)#show mpls traffic-eng interface detail gei-0/1
gei-0/1:
   State:
    ENABLE
   Traffic-eng metric: 0
   Authentication: enabled
    Key:          <encrypted>
    Type:         sha-1
    Challenge:     enabled
    Challenge-imp: Implemented
    Window size:   10
   BFD: disabled
   Backup path:
    None
   SRLGs: None
   Intf Fast-Hello: DISABLE
    Fast-Hello interval: 10000
    Fast-Hello miss: 4
```

在P1上查看TE认证信息：

```
P1#show ip rsvp authentication
Neighbor: 192.168.1.2
 Interface: gei-0/1
 Direction: Send
 Crypto Auth:Enable
 Send Key ID (hex): 0x6896a0010000
 Next valid seq:  1c9f 6bafc3
 Challenge-imp: Configured
 challenge-imp state: CHALL_IMP_WAIT
Direction: recv
 Challenge: Configured
 challenge state: CHALL_SUCC
```

```
Rcv Key ID (hex): 0x6896a0030000
Windowsize: 10
Recved Largest Sequence: 1cd3 6c6b47
```

6.3.6 TE 消息确认与重传

消息确认与重传最主要的用途是为摘要刷新功能提供保障基础，使需要确认的报文在接收到确认之前进行重传，从而保证消息的可靠性。

6.3.6.1 配置 TE 消息确认与重传

本节介绍TE消息确认与重传的配置步骤和命令。

相关信息

配置TE消息确认与重传时，需要在相邻两节点的TE配置模式下配置消息确认与重传功能。

1.开启MPLS TE功能。

命令	功能
inspur(config)#**mpls traffic-eng**	开启MPLS TE功能，并进入TE配置模式

2.配置消息确认与重传功能

步骤	命令	功能
1	inspur(config-mpls-te)#**signalling retransmit**	配置消息确认与重传功能
2	inspur(config-mpls-te)#**signalling retransmit interval** < *interval-value* >	配置消息确认与重传功能的重传间隔，范围：500~3000 (ms)
3	inspur(config-mpls-te)#**signalling retransmit limit** < *limit-count* >	配置消息确认与重传功能的重传报文次数，范围：2~10

3.验证配置结果。

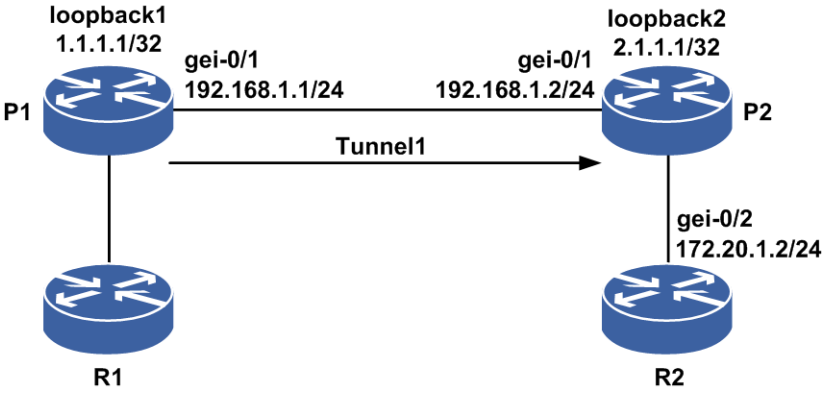
命令	功能
inspur#**show ip rsvp refresh reduction**	查看TE消息确认与重传

6.3.6.2 TE 消息确认与重传配置实例

配置说明

如*图 6-1731*所示，从P1到P2的RSVP普通隧道建立采用OSPF TE进行严格选路的方式，在隧道头尾的P1和P2 TE模式下配置消息确认和重传。

图 6-171 TE 消息确认与重传配置实例图



配置思路

1.P1、P2直连接口建立OSPF邻居，OSPF开启TE。

2.P1、P2直连接口开启TE。

3.P1上设置隧道的目的地和严格选路方式。

4.在P1和P2的TE模式下配置消息确认与重传。

配置过程

P1上的配置如下：

```
P1(config)#interface gei-0/1
P1(config-if-gei-0/1)#no shutdown
P1(config-if-gei-0/1)#ip address 192.168.1.1 255.255.255.0
P1(config-if-gei-0/1)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
```

```
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#interface gei-0/1
P1(config-mpls-te-if-gei-0/1)#exit
P1(config-mpls-te)#explicit-path identifier 1
P1(config-mpls-te-expl-path-id-1)#next-address strict 192.168.1.2
P1(config-mpls-te-expl-path-id-1)#exit
P1(config-mpls-te)#tunnel te_tunnel 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 path-option 1 explicit-path identifier 1
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#exit
```

P2上的配置如下：

```
P2(config)#interface gei-0/1
P2(config-if-gei-0/1)#no shutdown
P2(config-if-gei-0/1)#ip address 192.168.1.2 255.255.255.0
P2(config-if-gei-0/1)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-0/1
P2(config-mpls-te-if-gei-0/1)#exit
```

配置验证

在P1上查看隧道情况，处于up状态：

```
P1(config)#show mpls traffic-eng tunnels brief
Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
TUNNEL NAME DESTINATION UP IF DOWN IF  STATE/PROT
tunnel_1    2.1.1.1     -  gei-0/1    up/up
```

在P1上用**show ip rsvp refresh reduction**命令查看消息确认与重传情况：

```
P1(config)#show ip rsvp refresh reduction
/*重传未开启*/
Retransmit:disabled
Initial retransmit delay:1000ms
Retransmit limit:3
Refresh Reduction:disabled
```

在P1上配置消息确认和重传：

```
P1(config-mpls-te)#signalling retransmit
P1(config-mpls-te)#signalling retransmit interval 2000
P1(config-mpls-te)#signalling retransmit limit 5
```

P2上同P1配置。

再在P1上用**show ip rsvp refresh reduction**命令查看消息确认与重传情况：

```
P1(config-mpls-te)#sho ip rsvp refresh reduction
/*开启了重传*/
Retransmit:enabled
Initial retransmit delay:2000ms
Retransmit limit:5
Refresh Reduction:disabled
```

6.3.7 TE 摘要刷新

摘要刷新的原理是通过一个新的消息类型—摘要刷新消息替代标准的PATH和RESV消息，来减少刷新消息所产生的流量负荷，可以更有效得利用有限的系统资源。

6.3.7.1 配置 TE 摘要刷新

本节介绍TE摘要刷新的配置步骤和命令。

相关信息

配置TE摘要刷新时，需要在相邻两节点的TE配置模式下配置消息确认与重传功能，再配置摘要刷新功能。

1.开启MPLS TE功能。

命令	功能
inspur(config)#**mpls traffic-eng**	使能MPLS TE，进入TE配置模式

2.配置摘要刷新功能。

步骤	命令	功能
1	inspur(config-mpls-te)#**signalling retransmit**	配置摘要刷新功能前，需要先配置消息确认与重传功能
2	inspur(config-mpls-te)#**signalling refresh reduction**	配置摘要刷新功能

3.验证配置结果。

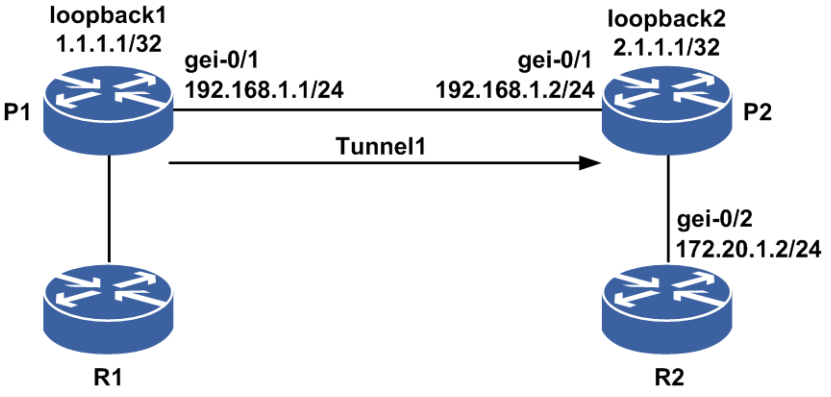
命令	功能
inspur#**show ip rsvp refresh reduction**	查看摘要刷新关系

6.3.7.2 TE 摘要刷新配置实例

配置说明

如*图 6-18*所示，从P1到P2的RSVP普通隧道建立采用OSPF TE进行严格选路的方式，在隧道头尾P1和P2的TE模式下配置摘要刷新。

图 6-182 TE 摘要刷新配置实例图



配置思路

1.P1、P2直连接口建立OSPF邻居，OSPF开启TE。

2.P1、P2直连接口开启TE。

3.P1上设置隧道的目的地和严格选路方式。

4.在隧道头尾P1和P2的TE模式下配置摘要刷新。

配置过程

P1上的配置如下：

```
P1(config)#interface gei-0/1
P1(config-if-gei-0/1)#no shutdown
P1(config-if-gei-0/1)#ip address 192.168.1.1 255.255.255.0
P1(config-if-gei-0/1)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
```

```
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#interface gei-0/1
P1(config-mpls-te-if-gei-0/1)#exit
P1(config-mpls-te)#explicit-path identifier 1
P1(config-mpls-te-expl-path-id-1)#next-address strict 192.168.1.2
P1(config-mpls-te-expl-path-id-1)#exit
P1(config-mpls-te)#tunnel te_tunnel 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 path-option 1 explicit-path identifier 1
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#exit
```

P2上的配置如下：

```
P2(config)#interface gei-0/1
P2(config-if-gei-0/1)#no shutdown
P2(config-if-gei-0/1)#ip address 192.168.1.2 255.255.255.0
P2(config-if-gei-0/1)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-0/1
P2(config-mpls-te-if-gei-0/1)#exit
```

配置TE摘要刷新：

```
P1(config-mpls-te)#signalling retransmit
P1(config-mpls-te)#signalling refresh reduction
P2(config-mpls-te)#signalling retransmit
P2(config-mpls-te)#signalling refresh reduction
```

配置验证

在P1上查看隧道情况，处于up状态：

```
P1(config)#show mpls traffic-eng tunnels brief
Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
TUNNEL NAME DESTINATION UP IF DOWN IF STATE/PROT
tunnel_1    2.1.1.1      -   gei-0/1   up/up
```

在P1上用**show ip rsvp refresh reduction**命令查看TE摘要刷新：

```
P1(config)#show ip rsvp refresh reduction
Retransmit:enabled
Initial retransmit delay:1000ms
Retransmit limit:3
Refresh Reduction:enabled
next_hop type tunnel_id lsp_id ingressegress
192.168.1.2 Path 1 2 1.1.1.12.1.1.1
```

在P2上用**show ip rsvp refresh reduction**命令查看TE摘要刷新：

```
P2(config-mpls-te)#show ip rsvp refresh reduction
Retransmit:enabled
Initial retransmit delay:1000ms
Retransmit limit:3
Refresh Reduction:enabled
next_hop type tunnel_id lsp_id ingressegress
192.168.1.1 Resv 1 2 1.1.1.12.1.1.1
```

6.3.8 RESV CONFIRM

在传统MPLS网络中，要建立双向LSP就必须分别建立两个单向的LSP，这种方式存在LSP建立的时延过长、开销过多、可靠性差和管理复杂等缺点。为了解决以上问题以及满足光通路的要求，MPLS TP动态TE要求支持双向LSP（共路径）的建立。

由于双向LSP是在RESV的信令过程中进行转发表项下发，一般情况下是从正向的尾节点开始到头结点依次下发，尾节点下发转发表项时上游结点的转发表项还没完成下发，不宜导入流量，因此需要一种机制，在头结点完成转发表项下发后回复一个确认消息给尾节点，以示全部节点完成下转发，可以导入流量。RESV CONFIRM消息机制即用于此场景。

6.3.8.1 配置 RESV CONFIRM

本节介绍RESV CONFIRM的配置步骤和命令。

相关信息

配置RESV CONFIRM功能需要注意：

- 需要在尾节点的TE配置模式下配置RESV CONFIRM功能。
- 需要使能RESV CONFIRM功能，该功能常与双向隧道联用，用于通知正向尾节点可导入流量。
- 应在配有双向隧道的尾节点配置，在尾节点的双向隧道定时器到期前使隧道UP可导入流量。

1.开启MPLS TE功能。

命令	功能
inspur(config)#**mpls traffic-eng**	使能MPLS TE，进入TE配置模式

2.配置RESV CONFIRM。

命令	功能
inspur(config-mpls-te)#**resv-confirm**	配置RESV CONFIRM

3.维护RESV CONFIRM。

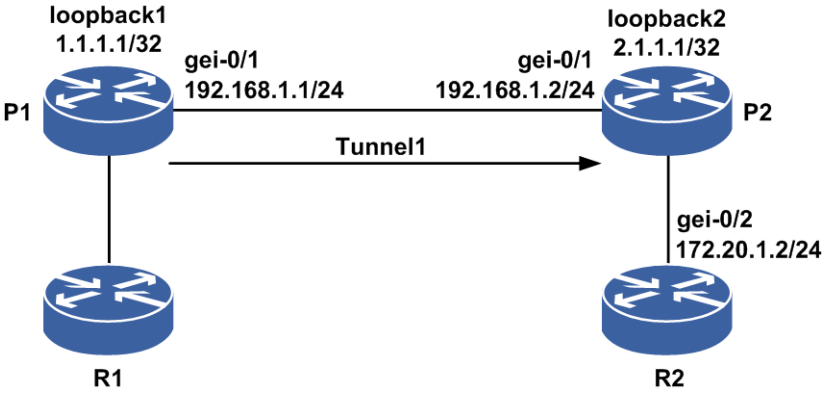
命令	功能
inspur#**debug rsvp resv-confirm**	打开RESV CONFIRM的调试函数

6.3.8.2 RESV CONFIRM 配置实例

配置说明

如*图 6-3319*所示，从P1到P2的RSVP普通隧道建立采用OSPF TE进行严格选路的方式，在隧道尾节点P2的TE模式下配置RESV CONFIRM。

图 6-3319 RESV CONFIRM 配置实例图



配置思路

1.P1、P2直连接口建立OSPF邻居，OSPF开启TE。

2.P1、P2直连接口开启TE。

3.配置双向隧道。

4.在隧道尾节点P2的TE模式下配置RESV CONFIRM。

配置过程

P1上的配置如下：

```
P1(config)#interface gei-0/1
P1(config-if-gei-0/1)#no shutdown
P1(config-if-gei-0/1)#ip address 192.168.1.1 255.255.255.0
P1(config-if-gei-0/1)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
```

```
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#interface gei-0/1
P1(config-mpls-te-if-gei-0/1)#exit
P1(config-mpls-te)#explicit-path identifier 1
P1(config-mpls-te-expl-path-id-1)#next-address strict 192.168.1.2
P1(config-mpls-te-expl-path-id-1)#exit
P1(config-mpls-te)#tunnel te_tunnel 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 path-option 1 explicit-path identifier 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 co-routed-tunnel
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#exit
```

P2上的配置如下：

```
P2(config)#interface gei-0/1
P2(config-if-gei-0/1)#no shutdown
P2(config-if-gei-0/1)#ip address 192.168.1.2 255.255.255.0
P2(config-if-gei-0/1)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-0/1
P2(config-mpls-te-if-gei-0/1)#exit

P2(config-mpls-te)#resv-confirm

P2(config)#interface te_tunnel8001
P2(config-if-te_tunnel8001)#ip unnumbered loopback2
P2(config-if-te_tunnel8001)#exit
P2(config)#mpls traffic-eng
P2(config-mpls-te)#tunnel te_tunnel8001
P2(config-mpls-te-access_tunnel-te_tunnel8001)#role       egress       type
bidirectional
P2(config-mpls-te-access_tunnel-te_tunnel8001)# ingress-tunnel-id 1
 ingress 1.1.1.1 egress 2.1.1.1
P2(config-mpls-te-access_tunnel-te_tunnel8001)#exit
```

配置验证

在P1和P2上执行**debug rsvp resv-confirm**命令，在P1上看到debug打印如下：

```
P1#P1 MPFU-8/0 2013-2-5 15:33:08 RSVP-RESVCONF: Copy
RESV_CONFIRM object to RSB(tnnlID: 1, lspID: 21, nhop :<192.168.1.2>).
P1 MPFU-8/0 2013-2-5 15:33:08 RSVP-RESVCONF: get confirm.
P1 MPFU-8/0 2013-2-5 15:33:08 RSVP-RESVCONF: Send ResvConf
```

```
(tnnlID: 1, lspID: 21, nhop :<192.168.1.2>).
P1 MPFU-8/0 2013-2-5 15:33:08 RSVP-RESVCONF: Fsb have receive resv-conf,
not get confirm again.
```

在P2上看到debug打印如下：

```
P2#P2 MPFU-8/0 2013-2-5 15:37:59 RSVP-RESVCONF: Copy
RESV_CONFIRM object to RSB(tnnlID: 1, lspID: 21, nhop :<255.255.255.255>).
P2 MPFU-8/0 2013-2-5 15:38:00 RSVP-RESVCONF: get confirm.
P2 MPFU-8/0 2013-2-5 15:38:00 RSVP-RESVCONF: accept_resv_conf:2.1.1.1.
P2 MPFU-8/0 2013-2-5 15:38:00 RSVP-RESVCONF: match fsb with filter_spec:
src_addr=1.1.1.1,lspId=21.
P2 MPFU-8/0 2013-2-5 15:38:00 RSVP-RESVCONF: Addresses are equal with
rp(tnnlID: 1, lspID: 21, nhop :<255.255.255.255>).
```

6.3.9 GR

控制平面的故障主要有两种：

•第一种故障是节点间通讯故障，控制面的通讯在两个节点间丢失，但是节点没有丢失控制面或转发平面状态。

•第二种故障是节点故障，RSVP-TE控制平面发生了故障，控制面状态丢失，但是数据平面没有发生故障，LSR仍然维持数据转发状态。

控制面要从上述两种故障中进行恢复需要基于GR技术：

1.将要进行重启的LSR通告邻居LSR，本设备是否支持GR。

2.邻居检测故障发生的时间和重启完毕时间，HELLO的重新建立。

3.邻居帮助重启LSR进行控制面状态恢复以及控制面状态与数据转发平面状态的重新同步。

6.3.9.1 配置 GR

本节介绍GR功能的配置步骤和命令。

相关信息

配置GR功能时，需要在隧道通过的每个节点上面配置GR。

注意配置时，GR功能和FRR HELLO功能是互斥的。

1.开启MPLS TE功能。

命令	功能
inspur(config)#**mpls traffic-eng**	开启MPLS TE功能，进入TE配置模式

2.配置GR功能。

步骤	命令	功能
1	inspur(config-mpls-te)#**signalling graceful-restart**	配置graceful-restart功能

步骤	命令	功能
2	inspur(config-mpls-te)#**signalling hello graceful-restart refresh interval** *<interval>*	配置graceful-restart功能的hello刷新时间，范围是1000~30000，单位：ms
	inspur(config-mpls-te)#**signalling hello graceful-restart refresh misses** *<num>*	配置graceful-restart功能的hello的丢失次数，范围是4~10
	inspur(config-mpls-te)#**signalling hello graceful-restart timers restart-time** *<restart-time>*	配置graceful-restart功能的重启时间，范围是120000~600000，单位：ms
	inspur(config-mpls-te)#**signalling hello graceful-restart timers recovery-time** *<recover-time>*	配置graceful-restart功能的恢复时间，范围是120000~600000，单位：ms

3.验证配置结果。

命令	功能
inspur#**show ip rsvp hello graceful-restart**	显示GR的配置信息
inspur#**show ip rsvp hello instance summary**	显示RSVP HELLO实例的概要信息
inspur#**show ip rsvp hello instance detail**	显示RSVP HELLO实例的详细信息

4.维护GR功能。

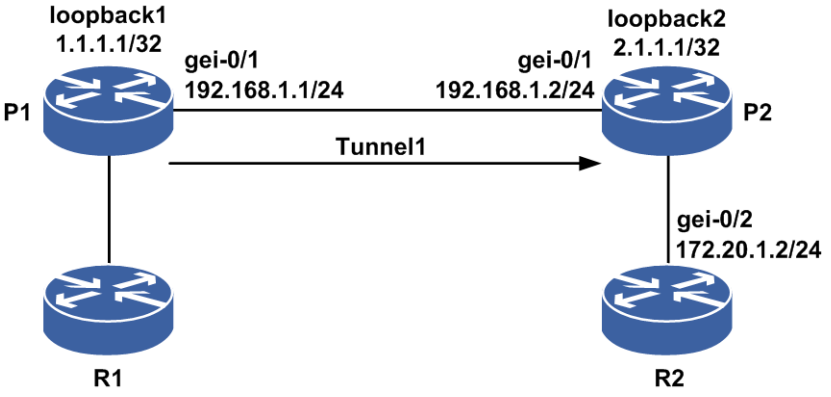
命令	功能
inspur#**debug rsvp hello**	打开GR HELLO调试函数

6.3.9.2 GR 配置实例

配置说明

如*图 6-204*所示，采用OSPF TE进行严格选路的方式从P1到P2建立RSVP普通隧道，在隧道头尾节点P1和P2的TE模式下配置GR功能。

图 6-20 TE GR 配置实例图



配置思路

1.P1、P2直连接口建立OSPF邻居，OSPF使能TE

2.P1、P2直连接口使能TE

3.P1上设置隧道的目的地和严格选路方式

4.在隧道头尾节点P1和P2的TE模式下配置GR

配置过程

P1上的配置如下：

```
P1(config)#interface gei-0/1
P1(config-if-gei-0/1)#no shutdown
P1(config-if-gei-0/1)#ip address 192.168.1.1 255.255.255.0
P1(config-if-gei-0/1)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#interface gei-0/1
P1(config-mpls-te-if-gei-0/1)#exit
P1(config-mpls-te)#explicit-path identifier 1
P1(config-mpls-te-expl-path-id-1)#next-address strict 192.168.1.2
P1(config-mpls-te-expl-path-id-1)#exit
P1(config-mpls-te)#tunnel te_tunnel 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
```

```
 path-option 1 explicit-path identifier 1
P1(config-mpls-te-tunnel-te_tunnel1)#exit

P1(config-mpls-te)#signalling graceful-restart
P1(config-mpls-te)#exit
```

P2上的配置如下：

```
P2(config)#interface gei-0/1
P2(config-if-gei-0/1)#no shutdown
P2(config-if-gei-0/1)#ip address 192.168.1.2 255.255.255.0
P2(config-if-gei-0/1)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-0/1
P2(config-mpls-te-if-gei-0/1)#exit

P2(config-mpls-te)#signalling graceful-restart
```

配置验证

在P1上查看隧道情况，处于up状态：

```
P1(config)#show mpls traffic-eng tunnels brief
Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
TUNNEL NAME DESTINATION UP IF DOWN IF STATE/PROT
tunnel_1    2.1.1.1      -    gei-0/1  up/up
```

在P1上查看GR生效情况：

```
P1(config)#show ip rsvp hello instance summary
Client I/F    Neighbor Type StateLostCnt LSPs
GR    gei-0/1 192.168.1.2  ACTIVE UP0    1

P1(config)#show ip rsvp hello graceful-restart
MPLS-TE: Enabled
Graceful Restart: Enabled
 Refresh interval: 10000 msecs
 Refresh misses: 4
 Advertised restart time: 120000 msecs
 Advertised recovery time: 120000 msecs

P1(config)#sho ip rsvp hello instance detail
Hello Graceful Restart globally enabled
Fast-Hello globally disabled
Neighbor 192.168.1.2 Source 192.168.1.1
Clients:Graceful Restart
 State:UP
 Type:ACTIVE
 I/F: gei-0/1
 LSP num:1
```

```
 Src_instance 0X15e5c62, Dst_instance 0X15e09e0
GR HELLO parameters
 Refresh Misses Configured:4
 Refresh Interval (msec)
  Configured:10000
 Current :10000
 Local restart time (msec):120000
 Local recovery time (msec):120000
 Nbr restart time (msec):120000
 Nbr recovery time (msec):0
 Lost count:0
 intf hello
FRR HELLO parameters
 Fast_hello_period (msec):10000
 Fast_hello_miss:4
 Fast_hello_protect_lsps:0
 Fast_hello_del_time (msec):0
 Fast_hello_reroute_time (msec):0
```

6.3.10 FRR HELLO

由于RSVP FRR的快速切换要求，需要为之提供快速故障检测技术，比如广泛应用的BFD检测、MPLS OAM检测等。但有些情况下这些检测手段无法提供邻居故障检测，比如用户不使用这些检测技术，或者没有及时检测到邻居故障，这就要求RSVP自己提供一种邻居故障检测技术—RSVP HELLO故障检测机制。

6.3.10.1 配置 FRR HELLO

本节介绍FRR HELLO功能的配置步骤和命令。

相关信息

配置FRR HELLO时，需要在FRR保护形成的PLR节点及其邻居的被保护隧道信令接口上配置FRR HELLO功能。

注意配置时，FRR HELLO功能和GR功能是互斥的。

1.开启MPLS TE功能。

命令	功能
inspur(config)#**mpls traffic-eng**	开启MPLS TE，进入TE配置模式

2.配置FRR HELLO功能。

步骤	命令	功能
1	inspur(config-mpls-te)#**signalling hello**	全局开启FRR HELLO功能
2	inspur(config-mpls-te)#**interface** <*interface-name*>	进入需要保护的信令接口
3	inspur(config-mpls-te-if-interface-name)#**signalling hello**	接口下开启FRR HELLO功能

步骤	命令	功能
4	inspur(config-mpls-te-if-interface-name)#**signalling hello refresh interval** *<interval>*	配置FRR HELLO功能的hello刷新时间，范围是1000~30000，单位：ms
	inspur(config-mpls-te-if-interface-name)#**signalling hello refresh misses** *<num>*	配置FRR HELLO功能的hello的丢失次数，范围是4~10

3.验证配置结果。

命令	功能
inspur#**show ip rsvp hello instance summary**	显示RSVP HELLO实例的概要信息
inspur#**show ip rsvp hello instance detail**	显示RSVP HELLO实例的详细信息

4.维护FRR HELLO功能。

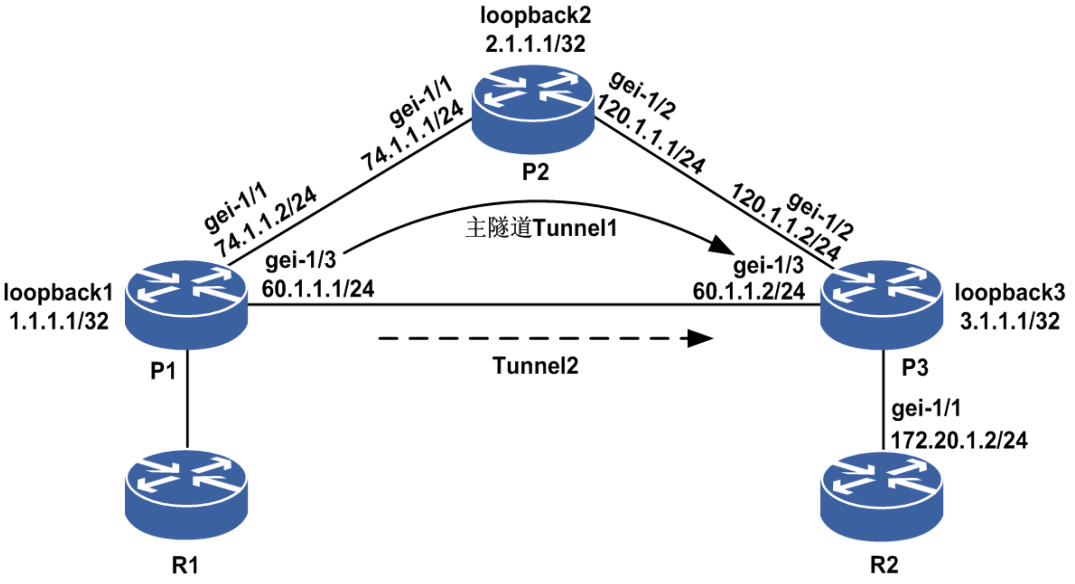
命令	功能
inspur#**debug rsvp hello**	打开FRR HELLO调试函数

6.3.10.2 FRR HELLO 配置实例

配置说明

如*图 6-2135*所示，从P1到P3建立两条隧道，Tunnel1通过P1、P2、P3，Tunnel2通过P1、P3。其中Tunnel1为主隧道，Tunnel2为备份隧道，形成FRR关系，在P1和P2上配置FRR HELLO功能。

图 6-215 FRR HELLO 配置实例图



配置思路

1.P1、P2、P3直连接口均建立OSPF邻居，OSPF开启TE。

2.分别建立两条严格路径，主路径为P1、P2、P3，备份路径为P1、P3。

3.P1、P2、P3所用的接口均开启TE，并在P1上的gei-1/1接口上配置备份隧道。

4.创建主备隧道，主隧道下开启FRR facility，目的地为P3的router-id，路径为严格路径。

5.在P1和P2上配置FRR HELLO。

配置过程

P1的配置如下：

```
P1(config)#interface gei-1/1
P1(config-if-gei-1/1)#no shutdown
P1(config-if-gei-1/1)#ip address 74.1.1.2 255.255.255.0
P1(config-if-gei-1/1)#exit
P1(config)#interface gei-1/3
P1(config-if-gei-1/3)#no shutdown
P1(config-if-gei-1/3)#ip address 60.1.1.1 255.255.255.0
P1(config-if-gei-1/3)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit
P1(config)#interface te_tunnel2
P1(config-if-te_tunnel2)#ip unnumbered loopback1
P1(config-if-te_tunnel2)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
```

```
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
P1(config-ospf-1-area-0)#network 74.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 60.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#explicit-path name primary
P1(config-mpls-te-expl-path-name)#next-address strict 74.1.1.1
P1(config-mpls-te-expl-path-name)#next-address strict 120.1.1.2
P1(config-mpls-te-expl-path-name)#exit
P1(config-mpls-te)#explicit-path name back
P1(config-mpls-te-expl-path-name)#next-address strict 60.1.1.2
P1(config-mpls-te-expl-path-name)#exit
P1(config-mpls-te)#interface gei-1/1
P1(config-mpls-te-if-gei-1/1)#exit
P1(config-mpls-te)#interface gei-1/3
P1(config-mpls-te-if-gei-1/3)#exit

P1(config-mpls-te)#tunnel te_tunnel1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 3.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 path-option 1 explicit-path name primary
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng record-route
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 fast-reroute facility
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#tunnel te_tunnel2
P1(config-mpls-te-tunnel-te_tunnel2)#tunnel destination ipv4 3.1.1.1
P1(config-mpls-te- tunnel-te_tunnel2)#tunnel mpls traffic-eng
 path-option 1 explicit-path name back
P1(config-mpls-te-tunnel-te_tunnel2)#exit
P1(config-mpls-te)#interface gei-1/1
P1(config-mpls-te-if-gei-1/1)#backup-path te_tunnel 2
P1(config-mpls-te-if-gei-1/1)#exit

P1(config-mpls-te)#signalling hello
P1(config-mpls-te)#interface gei-1/1
P1(config-mpls-te-if-gei-1/1)#signalling hello
P1(config-mpls-te-if-gei-1/1)#exit
P1(config-mpls-te)#exit
```

P2的配置如下：

```
P2(config)#interface gei-1/1
P2(config-if-gei-1/1)#no shutdown
P2(config-if-gei-1/1)#ip address 74.1.1.1 255.255.255.0
P2(config-if-gei-1/1)#exit
P2(config)#interface gei-1/2
P2(config-if-gei-1/2)#no shutdown
P2(config-if-gei-1/2)#ip address 120.1.1.1 255.255.255.0
P2(config-if-gei-1/2)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#network 74.1.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 120.1.1.0 0.0.0.255
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
```

```
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-1/1
P2(config-mpls-te-if-gei-1/1)#exit
P2(config-mpls-te)#interface gei-1/2
P2(config-mpls-te-if-gei-1/2)#exit

P2(config-mpls-te)#signalling hello
P2(config-mpls-te)#interface gei-1/1
P2(config-mpls-te-if-gei-1/1)#signalling hello
P2(config-mpls-te-if-gei-1/1)#exit
P2(config-mpls-te)#exit
```

P3的配置如下：

```
P3(config)#interface gei-1/2
P3(config-if-gei-1/2)#no shutdown
P3(config-if-gei-1/2)#ip address 120.1.1.2 255.255.255.0
P3(config-if-gei-1/2)#exit
P3(config)#interface gei-1/3
P3(config-if-gei-1/3)#no shutdown
P3(config-if-gei-1/3)#ip address 60.1.1.2 255.255.255.0
P3(config-if-gei-1/3)#exit
P3(config)#interface loopback3
P3(config-if-loopback3)#ip address 3.1.1.1 255.255.255.255
P3(config-if-loopback3)#exit

P3(config)#router ospf 1
P3(config-ospf-1)#router-id 3.1.1.1
P3(config-ospf-1)#area 0
P3(config-ospf-1-area-0)#network 3.1.1.1 0.0.0.0
P3(config-ospf-1-area-0)#network 120.1.1.0 0.0.0.255
P3(config-ospf-1-area-0)#network 60.1.1.0 0.0.0.255
P3(config-ospf-1-area-0)#mpls traffic-eng
P3(config-ospf-1-area-0)#exit

P3(config)#mpls traffic-eng
P3(config-mpls-te)#interface loopback3
P3(config-mpls-te-if-loopback3)#exit
P3(config-mpls-te)#router-id 3.1.1.1
P3(config-mpls-te)#interface gei-1/2
P3(config-mpls-te-if-gei-1/2)#exit
P3(config-mpls-te)#interface gei-1/3
P3(config-mpls-te-if-gei-1/3)#exit
P3(config-mpls-te)#exit
```

配置验证

当隧道up后，在P1上可以看到FRR的建立情况：

```
P1#show mpls traffic-eng tunnels brief
Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
TUNNEL NAME DESTINATION UP IF DOWN IF STATE/PROT
tunnel_1    3.1.1.1     -    gei-1/1   up/up
tunnel_2    3.1.1.1     -    gei-1/3   up/up

P1#show mpls traffic-eng fast-reroute
Tunnel head end item information
Protected Tunnel LspID In-label Out intf/label FRR intf/label Status
Tunnel1 86 Tun hd     gei-1/1:147456 Tu2:3 ready

LSP midpoint frr information:
LSP identifier In-label Out intf/label FRR intf/label Status
```

```
R5(config)#show ip rsvp hello ins s
Client I/F Neighbor Type State LostCnt LSPs
FRR    gei-1/1 74.1.1.1 ACTIVE UP 0 1

R5(config)#show ip rsvp hello ins detail
Hello Graceful Restart globally disabled
Fast-Hello globally enabled
Neighbor 74.1.1.1 Source 74.1.1.2
Clients:Fast Reroute
 State:UP
 Type:ACTIVE
 I/F: gei-1/1
 LSP num:1
 Src_instance 0X195998e, Dst_instance 0X1954fe4
GR HELLO parameters
 Refresh Misses Configured:4
 Refresh Interval (msec)
 Configured:10000
 Current :0
 Local restart time (msec):120000
 Local recovery time (msec):120000
 Nbr restart time (msec):0
 Nbr recovery time (msec):0
 Lost count:0
 intf hello
FRR HELLO parameters
 Fast_hello_period (msec):10000
 Fast_hello_miss:4
 Fast_hello_protect_lsps:1
 Fast_hello_lost_count:0
 Fast_hello_del_time (msec):0
 Fast_hello_reroute_time (msec):2600
```

6.3.11 FRR 提升

由于一个接口可以配置多个备份隧道，FRR的提升功能是为了适时调整主备的保护关系。比如说，一个接口原来只有一条备份隧道Tunnel1，与主隧道只能形成链路保护。在已经形成了主备保护关系的情况下，接口下又增加了一条备份隧道Tunnel2，这条备份隧道可以与主隧道形成节点保护，这个时候就需要有FRR提升功能，触发Tunnel2去保护主隧道。

6.3.11.1 配置 FRR 提升

本节介绍FRR提升功能的配置步骤和命令。

相关信息

配置FRR提升时，需要在FRR保护形成的PLR节点上面配置。

1.开启MPLS TE功能。

命令	功能
inspur(config)#**mpls traffic-eng**	开启MPLS TE，进入TE配置模式

2.配置FRR提升功能。

步骤	命令	功能
1	inspur(config-mpls-te)#**fast-reroute promote**	配置手动FRR提升功能，单次触发当前节点上的所有已经形成的FRR关系删除后重建
2	inspur(config-mpls-te)#**fast-reroute timers promotion**	开启FRR提升定时器
3	inspur(config-mpls-te)#**fast-reroute timers promotion interval** *<interval>*	配置周期性触发FRR关系删除后重建

3.验证配置结果。

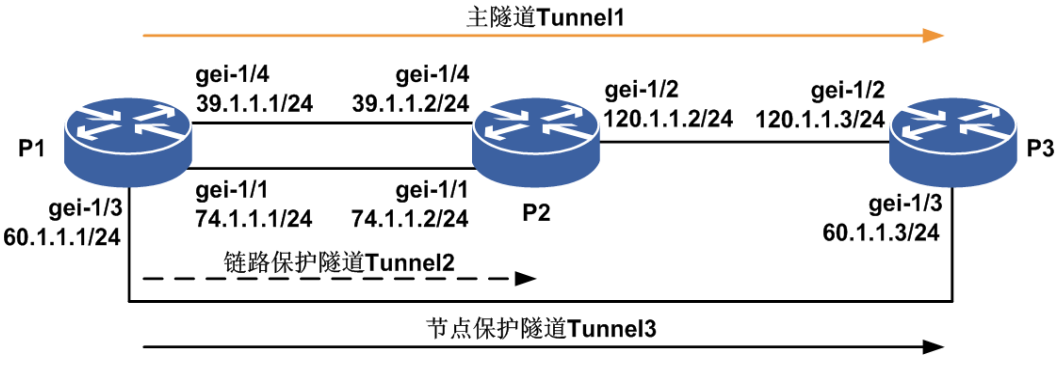
命令	功能
inspur#**show mpls traffic-eng fast-reroute promotion**	显示FRR提升的内容信息

6.3.11.2 FRR 提升节点保护优于链路保护配置实例

配置说明

如*图 6-22*所示，从P1到P3建立一条隧道，Tunnel1通过P1、P2、P3，Tunnel2通过P1、P2，Tunnel3通过P1、P3。其中Tunnel1为主隧道，Tunnel2和Tunnel3为备份隧道，Tunnel2为链路保护，Tunnel3为节点保护。

图 6-22 FRR 提升节点保护优于链路保护配置实例图



配置思路

1.P1、P2、P3直连接口均建立OSPF邻居，OSPF开启TE。

2.建立三条隧道， Tunnel1通过P1、P2、P3，Tunnel2通过P1、P2，Tunnel3通过P1、P3，其中Tunnel1为主隧道，Tunnel2和Tunnel3都为备份隧道。

3.在P1的TE模式下配置FRR提升功能。

4.在P1的gei-1/1接口上配置Tunnel2和Tunnel3为备份隧道。

配置过程

P1的配置如下：

```
P1(config)#interface gei-1/1
P1(config-if-gei-1/1)#no shutdown
P1(config-if-gei-1/1)#ip address 74.1.1.1 255.255.255.0
P1(config-if-gei-1/1)#exit
P1(config)#interface gei-1/3
P1(config-if-gei-1/3)#no shutdown
P1(config-if-gei-1/3)#ip address 60.1.1.1 255.255.255.0
P1(config-if-gei-1/3)#exit
P1(config)#interface gei-1/4
P1(config-if-gei-1/4)#no shutdown
P1(config-if-gei-1/4)#ip address 39.1.1.1 255.255.255.0
P1(config-if-gei-1/4)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit
P1(config)#interface te_tunnel2
P1(config-if-te_tunnel2)#ip unnumbered loopback1
P1(config-if-te_tunnel2)#exit
P1(config)#interface te_tunnel3
P1(config-if-te_tunnel3)#ip unnumbered loopback1
P1(config-if-te_tunnel3)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
P1(config-ospf-1-area-0)#network 74.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 60.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 39.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#explicit-path name primary
P1(config-mpls-te-expl-path-name)#next-address strict 74.1.1.2
P1(config-mpls-te-expl-path-name)#next-address strict 120.1.1.3
P1(config-mpls-te-expl-path-name)#exit
P1(config-mpls-te)#explicit-path name back1
P1(config-mpls-te-expl-path-name)#next-address strict 39.1.1.2
P1(config-mpls-te)#explicit-path name back2
P1(config-mpls-te-expl-path-name)#next-address strict 60.1.1.3
P1(config-mpls-te-expl-path-name)#exit
P1(config-mpls-te)#interface gei-1/1
P1(config-mpls-te-if-gei-1/1)#exit
P1(config-mpls-te)#interface gei-1/3
P1(config-mpls-te-if-gei-1/3)#exit
P1(config-mpls-te)#interface gei-1/4
P1(config-mpls-te-if-gei-1/4)#exit

P1(config-mpls-te)#fast-reroute promote
P1(config-mpls-te)#fast-reroute timers promotion
P1(config-mpls-te)#fast-reroute timers promotion interval 60

P1(config-mpls-te)#tunnel te_tunnel1
```

```
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 3.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 path-option 1 explicit-path name primary
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng record-route
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 fast-reroute facility
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#tunnel te_tunnel2
P1(config-mpls-te-tunnel-te_tunnel2)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te- tunnel-te_tunnel2)#tunnel mpls traffic-eng
 path-option 1 explicit-path name back1
P1(config-mpls-te-tunnel-te_tunnel2)#exit
P1(config-mpls-te)#tunnel te_tunnel3
P1(config-mpls-te-tunnel-te_tunnel3)#tunnel destination ipv4 3.1.1.1
P1(config-mpls-te-tunnel-te_tunnel3)#tunnel mpls traffic-eng
 path-option 1 explicit-path name back2
P1(config-mpls-te-tunnel-te_tunnel2)#exit
P1(config-mpls-te)#interface gei-1/1
P1(config-mpls-te-if-gei-1/1)#backup-path te_tunnel 2
P1(config-mpls-te-if-gei-1/1)#backup-path te_tunnel 3
P1(config-mpls-te-if-gei-1/1)#exit
P1(config-mpls-te)#exit
```

P2的配置如下：

```
P2(config)#interface gei-1/1
P2(config-if-gei-1/1)#no shutdown
P2(config-if-gei-1/1)#ip address 74.1.1.2 255.255.255.0
P2(config-if-gei-1/1)#exit
P2(config)#interface gei-1/2
P2(config-if-gei-1/2)#no shutdown
P2(config-if-gei-1/2)#ip address 120.1.1.2 255.255.255.0
P2(config-if-gei-1/2)#exit
P2(config)#interface gei-1/4
P2(config-if-gei-1/4)#no shutdown
P2(config-if-gei-1/4)#ip address 39.1.1.2 255.255.255.0
P2(config-if-gei-1/4)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#network 74.1.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 120.1.1.0 0.0.0.255
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-1/1
P2(config-mpls-te-if-gei-1/1)#exit
P2(config-mpls-te)#interface gei-1/2
P2(config-mpls-te-if-gei-1/2)#exit
P2(config-mpls-te)#interface gei-1/4
P2(config-mpls-te-if-gei-1/4)#exit
P2(config-mpls-te)#exit
```

P3的配置如下：

```
P3(config)#interface gei-1/2
P3(config-if-gei-1/2)#no shutdown
P3(config-if-gei-1/2)#ip address 120.1.1.3 255.255.255.0
P3(config-if-gei-1/2)#exit
P3(config)#interface gei-1/3
P3(config-if-gei-1/3)#no shutdown
```

```
P3(config-if-gei-1/3)#ip address 60.1.1.3 255.255.255.0
P3(config-if-gei-1/3)#exit
P3(config)#interface loopback3
P3(config-if-loopback3)#ip address 3.1.1.1 255.255.255.255
P3(config-if-loopback3)#exit

P3(config)#router ospf 1
P3(config-ospf-1)#router-id 3.1.1.1
P3(config-ospf-1)#area 0
P3(config-ospf-1-area-0)#network 3.1.1.1 0.0.0.0
P3(config-ospf-1-area-0)#network 120.1.1.0 0.0.0.255
P3(config-ospf-1-area-0)#network 60.1.1.0 0.0.0.255
P3(config-ospf-1-area-0)#mpls traffic-eng
P3(config-ospf-1-area-0)#exit

P3(config)#mpls traffic-eng
P3(config-mpls-te)#interface loopback3
P3(config-mpls-te-if-loopback3)#exit
P3(config-mpls-te)#router-id 3.1.1.1
P3(config-mpls-te)#interface gei-1/2
P3(config-mpls-te-if-gei-1/2)#exit
P3(config-mpls-te)#interface gei-1/3
P3(config-mpls-te-if-gei-1/3)#exit
P3(config-mpls-te)#exit
```

配置验证

当隧道up后，在P1上可以看到FRR的建立情况：

```
P1#show mpls traffic-eng tunnels brief
Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
TUNNEL NAME DESTINATION UP IF DOWN IF STATE/PROT
tunnel_1    3.1.1.1     -     gei-1/1 up/up
tunnel_2    2.1.1.1     -     gei-1/4 up/up
tunnel_3    3.1.1.1     -     gei-1/3 up/up

P1#show mpls traffic-eng fast-reroute
Tunnel head end item information
Protected Tunnel LspIDIn-label Out intf/label FRR intf/label Status
Tunnel186 Tun hd gei-1/1:147456    Tu3:3     ready

LSP midpoint frr information:
LSP identifierIn-label Out intf/label FRR intf/label Status

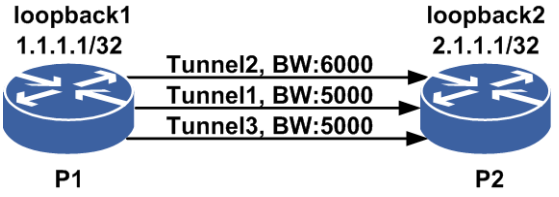
P1(config)#show mpls traffic-eng fast-reroute promotion
MPLS-TE: Enabled
 Periodic FRR Promotion: every 60 seconds, next in 4 second
```

6.3.11.3 FRR 提升备份带宽满足时的配置实例

配置说明

如*图 6-23*所示，从P1到P2建立一条主隧道Tunnel1，配置带宽5000，建立Tunnel2和Tunnel3分别通过另两条链路作为备份隧道，隧道带宽分别为6000和5000。配置FRR提升功能，形成FRR。

图 6-237 FRR 提升备份带宽满足时的配置实例图



配置思路

1.P1、P2直连接口均建立OSPF邻居，OSPF使能TE，并配置带宽。

2.分别建立三条严格路径，主路径配置在P1、P2的gei-0/2接口之间，备份路径配置在P1、P2的gei-0/3接口之间和gei-0/4接口之间。

3.建立Tunnel1为主隧道，配置带宽5000，Tunnel2和Tunnel3为备份隧道，带宽分别为6000和5000。

4.配置FRR提升功能，在P1主隧道的出接口gei-0/2上配置Tunnel2和Tunnel3为备份隧道。

配置过程

P1上的配置如下：

```
P1(config)#interface gei-0/2
P1(config-if-gei-0/2)#no shutdown
P1(config-if-gei-0/2)#ip address 192.168.1.1 255.255.255.0
P1(config-if-gei-0/2)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface gei-0/3
P1(config-if-gei-0/3)#no shutdown
P1(config-if-gei-0/3)#ip address 31.1.1.1 255.255.255.0
P1(config-if-gei-0/3)#exit
P1(config)#interface gei-0/4
P1(config-if-gei-0/4)#no shutdown
P1(config-if-gei-0/4)#ip address 32.1.1.1 255.255.255.0
P1(config-if-gei-0/4)#exit

P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit
P1(config)#interface te_tunnel2
P1(config-if-te_tunnel2)#ip unnumbered loopback1
P1(config-if-te_tunnel2)#exit
P1(config)#interface te_tunnel3
P1(config-if-te_tunnel3)#ip unnumbered loopback1
P1(config-if-te_tunnel3)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 31.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 32.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
P1(config-ospf-1-area-0)#mpls traffic-eng
```

```
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1

P1(config-mpls-te)#fast-reroute timers promotion
P1(config-mpls-te)#fast-reroute timers promotion interval 60

P1(config-mpls-te)#interface gei-0/2
P1(config-mpls-te-if-gei-0/2)#bandwidth 20000
P1(config-mpls-te-if-gei-0/2)#exit
P1(config-mpls-te)#interface gei-0/3
P1(config-mpls-te-if-gei-0/3)#bandwidth 20000
P1(config-mpls-te-if-gei-0/3)#exit
P1(config-mpls-te)#interface gei-0/4
P1(config-mpls-te-if-gei-0/4)#bandwidth 20000
P1(config-mpls-te-if-gei-0/4)#exit
P1(config-mpls-te)#explicit-path identifier 1
P1(config-mpls-te-expl-path-id-1)#next-address strict 192.168.1.2
P1(config-mpls-te-expl-path-id-1)#exit
P1(config-mpls-te)#explicit-path identifier 2
P1(config-mpls-te-expl-path-id-2)#next-address strict 31.1.1.2
P1(config-mpls-te-expl-path-id-2)#exit
P1(config-mpls-te)#explicit-path identifier 3
P1(config-mpls-te-expl-path-id-3)#next-address strict 32.1.1.2
P1(config-mpls-te-expl-path-id-3)#exit
P1(config-mpls-te)#tunnel te_tunnel 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 path-option 1 explicit-path identifier 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng record-route
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 fast-reroute facility
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 bandwidth 5000
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#tunnel te_tunnel 2
P1(config-mpls-te-tunnel-te_tunnel2)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel2)#tunnel mpls traffic-eng
 path-option 1 explicit-path identifier 2
P1(config-mpls-te-tunnel-te_tunnel2)#tunnel mpls traffic-eng
 backup-bw 6000
P1(config-mpls-te)#tunnel te_tunnel 3
P1(config-mpls-te-tunnel-te_tunnel3)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel3)#tunnel mpls traffic-eng
 path-option 1 explicit-path identifier 3
P1(config-mpls-te-tunnel-te_tunnel3)#tunnel mpls traffic-eng
 backup-bw 5000
P1(config-mpls-te-tunnel-te_tunnel3)#exit

P1(config-mpls-te)#interface gei-0/2
P1(config-mpls-te-if-gei-0/2)#backup-path te_tunnel 2
P1(config-mpls-te-if-gei-0/2)#backup-path te_tunnel 3
P1(config-mpls-te)#exit
```

P2上的配置如下：

```
P2(config)#interface gei-0/2
P2(config-if-gei-0/2)#no shutdown
P2(config-if-gei-0/2)#ip address 192.168.1.2 255.255.255.0
P2(config-if-gei-0/2)#exit
P2(config)#interface gei-0/3
P2(config-if-gei-0/3)#no shutdown
P2(config-if-gei-0/3)#ip address 31.1.1.2 255.255.255.0
P2(config-if-gei-0/3)#exit
P2(config)#interface gei-0/4
P2(config-if-gei-0/4)#no shutdown
P2(config-if-gei-0/4)#ip address 32.1.1.2 255.255.255.0
```

```
P2(config-if-gei-0/4)#exit

P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 31.1.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 32.1.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-0/2
P2(config-mpls-te-if-gei-0/2)#exit
P2(config-mpls-te)#interface gei-0/3
P2(config-mpls-te-if-gei-0/3)#exit
P2(config-mpls-te)#interface gei-0/4
P2(config-mpls-te-if-gei-0/4)#exit
```

配置验证

当隧道up后，在P1上可以看到FRR的建立情况：

```
P1#show mpls traffic-eng tunnels brief
Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
TUNNEL NAME DESTINATION UP IF  DOWN IF STATE/PROT
tunnel_1    2.1.1.1     -    gei-0/2 up/up
tunnel_2    2.1.1.1     -    gei-0/3 up/up
tunnel_3    2.1.1.1     -    gei-0/4 up/up

P1#show mpls traffic-eng fast-reroute
Tunnel head end item information
Tunnel head end item information
Protected Tunnel LspID In-label Out intf/label FRR intf/label Status
Tunnel176    Tun hd gei-0/2:3 Tu3:3   ready

LSP midpoint frr information:
LSP identifierIn-label Out intf/label FRR intf/label Status

P1(config)#show mpls traffic-eng fast-reroute promotion
MPLS-TE: Enabled
 Periodic FRR Promotion: every 60 seconds, next in 4 second
```

6.3.12 TE 的共路径双向隧道

在传统MPLS网络中，要建立双向LSP就必须分别建立两个单向的LSP，这种方式存在LSP建立的时延过长、开销过多、可靠性差和管理复杂等缺点。为了解决以上问题以及满足光通路的要求，MPLS TP动态TE要求支持双向LSP（共路径）的建立。

MPLS TP动态TE特别定义了建立双向LSP（共路径）的方法：双向LSP规定两个方向的LSP都应具有相同的流量工程参数，包括LSP生存期、保护和恢复等级、资源要求

（如时延、抖动等）。由于在GMPLS的双向LSP中，上行和下行的数据通路均采用同一条信令消息，两个LSP同时建立，可以有效地降低LSP的建立时延，同时也可减少建立LSP所需的控制开销。

6.3.12.1 配置 TE 共路径双向隧道

本节介绍TE共路径双向隧道功能的配置步骤和命令。

1.配置TE共路径双向隧道功能。

步骤	命令	功能
1	inspur(config-mpls-te)#**tunnel te_tunnel** <*tunnel-number*>	进入Tunnel接口配置模式，<*tunnel-number*>：隧道头节点的隧道号，范围是1~8000
2	inspur(config-mpls-te-tunnel-te_tunnel-tunnel-number)#**tunnel mpls traffic-eng co-routed-tunnel**	开启隧道下的双向隧道功能
3	inspur(config-mpls-te)#**tunnel te_tunnel** <*tunnel-number*>	在隧道的尾节点配置接入型隧道，<*tunnel-number*>：尾节点接入型隧道的隧道号，范围是8001~16000
4	inspur(config-mpls-te-access_tunnel-te_tunne-tunnel-number)#**role egress type bidirectional**	配置接入型隧道的role为尾节点，type为双向
5	inspur(config-mpls-te-access_tunnel-te_tunnel-tunnel-number)#**ingress-tunnel-id**<*access-tunnel-id*>**ingress**<*A.B.C.D*>**egress**<*A.B.C.D*>	配置三元组绑定到此接入型隧道上

<*access-tunnel-id*>：尾节点接入型隧道需要绑定的远端隧道的ID号。

ingress<*A.B.C.D*>：远端隧道源设备的router-id。

egress<*A.B.C.D*>：远端隧道目的设备的router-id，即当前节点的router-id。

2.验证配置结果。

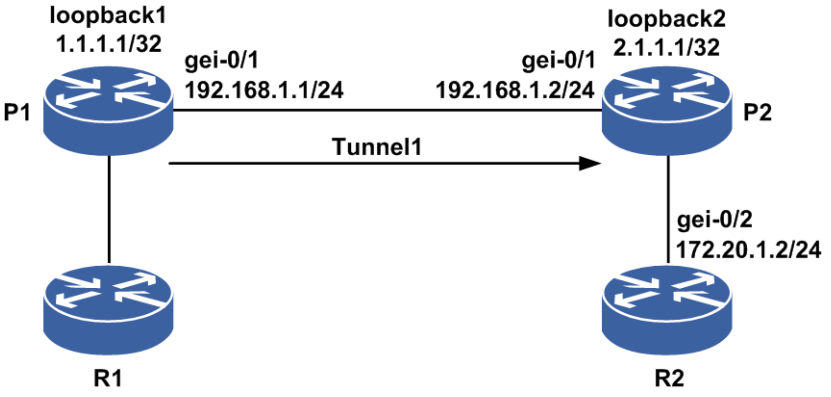
命令	功能
inspur#**show mpls traffic-eng tunnels**	查看隧道详细信息

6.3.12.2 TE 的共路径双向隧道配置实例

配置说明

如图 6-24所示，采用OSPF TE进行严格选路的方式从P1到P2建立一条RSVP普通隧道，在P2上配置一条接入隧道。

图 6-24 TE 的共路径双向隧道配置实例图



配置思路

1.P1、P2直连接口建立OSPF邻居，OSPF开启TE。

2.P1、P2直连接口开启TE。

3.在P1上建立一条隧道Tunnel1。

4.在P2上配置一条接入隧道。

配置过程

P1上的配置如下：

```
P1(config)#interface gei-0/1
P1(config-if-gei-0/1)#no shutdown
P1(config-if-gei-0/1)#ip address 192.168.1.1 255.255.255.0
P1(config-if-gei-0/1)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#interface gei-0/1
P1(config-mpls-te-if-gei-0/1)#exit
P1(config-mpls-te)#explicit-path identifier 1
P1(config-mpls-te-expl-path-id-1)#next-address strict 192.168.1.2
P1(config-mpls-te-expl-path-id-1)#exit
P1(config-mpls-te)#tunnel te_tunnel 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
```

```
 path-option 1 explicit-path identifier 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 co-routed-tunnel
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#exit
```

P2上的配置如下：

```
P2(config)#interface gei-0/1
P2(config-if-gei-0/1)#no shutdown
P2(config-if-gei-0/1)#ip address 192.168.1.2 255.255.255.0
P2(config-if-gei-0/1)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-0/1
P2(config-mpls-te-if-gei-0/1)#exit

P2(config)#interface te_tunnel8001
P2(config-if-te_tunnel8001)#ip unnumbered loopback2
P2(config-if-te_tunnel8001)#exit
P2(config)#mpls traffic-eng
P2(config-mpls-te)#tunnel te_tunnel8001
P2(config-mpls-te-access_tunnel-te_tunnel8001)#role egress
 type bidirectional
P2(config-mpls-te-access_tunnel-te_tunnel8001)# ingress-tunnel-id 1
 ingress 1.1.1.1 egress 2.1.1.1
P2(config-mpls-te-access_tunnel-te_tunnel8001)#exit
```

配置验证

在P1上查看隧道情况：

```
P1(config)#show mpls traffic-eng tunnels te_tunnel 1
Name: tunnel_1 (Tunnel1) Destination: 2.1.1.1
 Status:
 Admin: up Oper: up Path: valid Signalling: connected
 Path option: 1, type explicit identifier: 1 (Basis for Setup)
 Actual Bandwidth: N/A
 Hot-standby protection:
 no path options protected
Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0x0
  Resv-Style: SE
 Metric Type: IGP (default) Upper Limit: 4294967295
 Record-Route: disabled
 Facility Fast-reroute: disabled
 Detour Fast-reroute: disabled
 BFD: disabled
 Auto-bw: disabled
 Bidirect: enabled
  AutoRoute: disabled
  Forwarding-adjacency: disabled
```

```
InLabel: -
OutLabel: gei-0/1, 147456
Rvs-InLabel: gei-0/1, 147456
Rvs-OutLabel: -
RSVP Signalling Info :
Src 1.1.1.1, Dst 2.1.1.1, Tun_Id 1, Tun_Instance 7
RSVP Path Info:
Explicit Route: 192.168.1.1 192.168.1.2 2.1.1.1
Exclude Route: NULL
Record Route: NULL
Tspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits
RSVP Resv Info:
Record Route: NULL
Fspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits

History:
Tunnel:
Time since created: 0 days, 0 hours, 41 minutes, 48 seconds
Prior LSP: path option 1
Current LSP: Uptime:0 days, 0 hours, 0 minutes, 14 seconds
Last lsp error information:
Path error: admission fail(lspid:6,errcode:1,errvalue:4).
Path error: admission fail(lspid:5,errcode:1,errvalue:4).
Path error: admission fail(lspid:4,errcode:1,errvalue:4).
```

6.3.13 2.3.13TE 隧道 FA

路由协议通过建立一个相当庞大的数据库来保存报文转发的路径信息。当网络非常复杂的时候，对于需要转发的报文，通过查找数据库来实现转发很消耗系统资源。如果充分使用TE隧道的功能，将一条TE隧道当作路由的一个转发条目，将大大降低报文转发所消耗的系统资源，实现高速转发，TE隧道FA技术用于实现该功能。

6.3.13.1 2.3.13.1 配置 TE 隧道 FA

本节介绍TE隧道FA功能的配置步骤和命令。

1.配置TE隧道FA功能。

步骤	命令	功能
1	inspur(config-mpls-te)#**tunnel te_tunnel** <*tunnel-number*>	进入Tunnel接口配置模式
2	inspur(config-mpls-te-tunnel-te_tunnel-tunnel-number)#**tunnel mpls traffic-eng forwarding-adjacency**[<*holdtime*>]	开启隧道的FA功能或者开启FA功能并配置holdtime值

<*holdtime*>：在隧道由于链路down后，需要holdtime时间来通知路由此隧道真正down了，让路由感知不到隧道的震荡，配置范围是1~4294967295，单位：m。

2.验证配置结果。

命令	功能
inspur#**show mpls traffic-eng tunnels**	查看隧道详细信息
inspur#**show mpls traffic-eng**	查看FA的详细信息

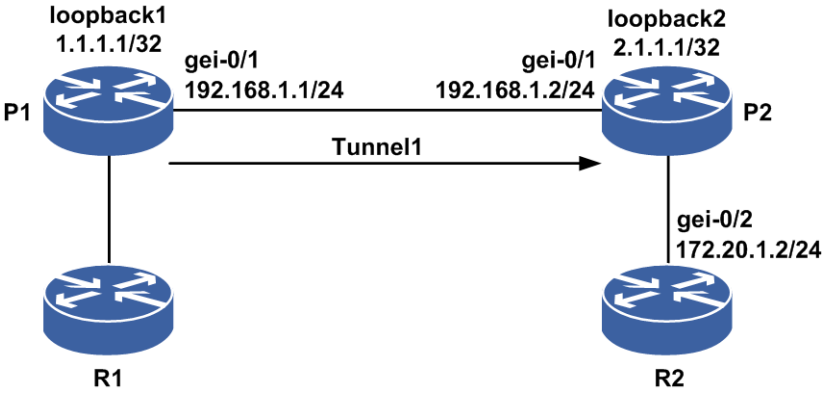
命令	功能
forwarding-adjacency	

6.3.13.2 TE 隧道 FA 配置实例

配置说明

如*图 6-259*所示，采用OSPF TE进行严格选路的方式从P1到P2建立一条RSVP普通隧道，在隧道下配置FA功能。

图 6-259 TE 隧道的 FA 配置实例图



配置思路

1.P1、P2直连接口建立OSPF邻居，OSPF开启TE。

2.P1、P2直连接口开启TE。

3.在P1上建立一条隧道Tunnel1，P2上建立反方向隧道Tunnel2。

4.在两条隧道下配置FA功能。

配置过程

P1上的配置如下：

```
P1(config)#interface gei-0/1
P1(config-if-gei-0/1)#no shutdown
P1(config-if-gei-0/1)#ip address 192.168.1.1 255.255.255.0
P1(config-if-gei-0/1)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit
```

```
P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#interface gei-0/1
P1(config-mpls-te-if-gei-0/1)#exit
P1(config-mpls-te)#explicit-path identifier 1
P1(config-mpls-te-expl-path-id-1)#next-address strict 192.168.1.2
P1(config-mpls-te-expl-path-id-1)#exit
P1(config-mpls-te)#tunnel te_tunnel 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 path-option 1 explicit-path identifier 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 forwarding-adjacency
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 forwarding-adjacency holdtime 1000
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#exit
```

P2上的配置如下：

```
P2(config)#interface gei-0/1
P2(config-if-gei-0/1)#no shutdown
P2(config-if-gei-0/1)#ip address 192.168.1.2 255.255.255.0
P2(config-if-gei-0/1)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit
P2(config)#interface te_tunnel2
P2(config-if-te_tunnel2)#ip unnumbered loopback2
P2(config-if-te_tunnel2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-0/1
P2(config-mpls-te-if-gei-0/1)#exit
P2(config-mpls-te)#explicit-path identifier 2
P2(config-mpls-te-expl-path-id-2)#next-address strict 192.168.1.1
P2(config-mpls-te-expl-path-id-2)#exit
P2(config-mpls-te)#tunnel te_tunnel 2
P2(config-mpls-te-tunnel-te_tunnel2)#tunnel destination ipv4 1.1.1.1
P2(config-mpls-te-tunnel-te_tunnel2)#tunnel mpls traffic-eng
 path-option 1 explicit-path identifier 2
P2(config-mpls-te-tunnel-te_tunnel2)#tunnel mpls traffic-eng
 forwarding-adjacency
P2(config-mpls-te-tunnel-te_tunnel2)#tunnel mpls traffic-eng
 forwarding-adjacency holdtime 1000
P2(config-mpls-te-tunnel-te_tunnel2)#exit
P2(config-mpls-te)#exit
```

配置验证

在P1上查看隧道情况：

```
P1(config)#show mpls traffic-eng tunnels te_tunnel 1
Name: tunnel_1 (Tunnel1) Destination: 2.1.1.1
 Status:
 Admin: up Oper: up Path: valid Signalling: connected
 Path option: 1, type explicit identifier: 2 (Basis for Setup)
 Actual Bandwidth: N/A
 Hot-standby protection:
 no path options protected
 Config Parameters:
 Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0x0
 Resv-Style: SE
 Metric Type: IGP (default) Upper Limit: 4294967295
 Record-Route: disabled
 Facility Fast-reroute: disabled
 Detour Fast-reroute: disabled
 BFD: disabled
 Auto-bw: disabled
 Bidirect: disabled
 AutoRoute: disabled
 Forwarding adjacency: holdtime 1000s

 InLabel: -
 OutLabel: gei-0/1, 3
 RSVP Signalling Info :
 Src 1.1.1.1, Dst 2.1.1.1, Tun_Id 1, Tun_Instance 9
 RSVP Path Info:
 Explicit Route: 192.168.1.1 192.168.1.2 2.1.1.1
 Exclude Route: NULL
 Record Route: NULL
 Tspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits
 RSVP Resv Info:
 Record Route: NULL
 Fspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits

 History:
 Tunnel:
 Time since created: 0 days, 0 hours, 56 minutes, 22 seconds
 Prior LSP: path option 1
 Current LSP: Uptime:0 days, 0 hours, 5 minutes, 39 seconds
 Last lsp error information:
 Path error: admission fail(lspid:8,errcode:1,errvalue:4).
 Tunnel config changed(lspid:7,errcode:1,errvalue:3).
    Path error: admission fail(lspid:6,errcode:1,errvalue:4)

P1(config)#show mpls traffic-eng forwarding-adjacency
    MPLS TE forwarding-adjacency enabled
     Destination 2.1.1.1 has 1 tunnels
     TunnelName Destination State Nexthop Holdtime
     tunnel_1 2.1.1.1 Up 2.1.1.1 1000s
```

6.3.14 TE 隧道 AR

TE隧道的自动路由发布，有Auto Route（AR）和Forwarding Adjacency（FA）两个特性，这两个特性的原理都是使TE隧道接口参与IGP的SPF计算。

- 启用AR特性的路由设备使用CR-LSP作为出接口，但不将链路发布给上游邻居路由设备。因此，其它路由设备的链路数据库中没有这条路径信息存在。
- 启用FA特性的路由设备在使用CR-LSP作为出接口的同时，也将这条CR-LSP作为一条普通的LSA/LSP发布给上游邻居路由设备。因此，其它路由设备收到后将CR-LSP

存放在链路数据库中，且能够使用。

6.3.14.1 配置 TE 隧道 AR

本节介绍TE隧道AR功能的配置步骤和命令。

1.配置TE隧道AR功能。

步骤	命令	功能
1	inspur(config-mpls-te)#**tunnel te_tunnel** <*tunnel-number*>	进入Tunnel接口配置模式
2	inspur(config-mpls-te-tunnel-te_tunnel-tunnel-number)#**tunnel mpls traffic-eng autoroute announce**	使能隧道下的AR功能
3	inspur(config-mpls-te-tunnel-te_tunnel-tunnel-number)#**tunnel mpls traffic-eng autoroute metric** {<*value0*>| **absolute** <*value1*>| **relative** <*value2*>}	配置AR的metric值

<*value0*>：配置AR的默认metric类型值，默认的metric类型为absolute，其范围是1~4294967295。

absolute <*value1*>：显式配置absolute类型的AR metric值，其范围是1~4294967295。

relative <*value2*>：显式配置relative类型的AR metric值，其范围是-10~+10。

2.验证配置结果。

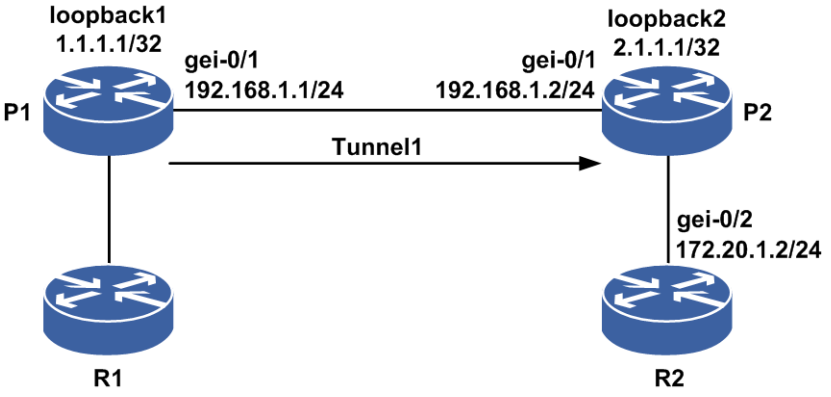
命令	功能
inspur#**show mpls traffic-eng tunnels**	查看隧道详细信息
inspur#**show mpls traffic-eng autoroute**	查看AR的详细信息

6.3.14.2 TE 隧道的 AR 配置实例

配置说明

如*图 6-40*所示，采用OSPF TE进行严格选路的方式从P1到P2建立一条RSVP普通隧道，在隧道下配置AR功能。

图 6-40 TE 隧道的 AR 配置实例图



配置思路

1.P1、P2直连接口建立OSPF邻居，OSPF开启TE。

2.P1、P2直连接口开启TE。

3.在P1上建立一条隧道Tunnel1。

4.在隧道下配置AR功能。

配置过程

P1上的配置如下：

```
P1(config)#interface gei-0/1
P1(config-if-gei-0/1)#no shutdown
P1(config-if-gei-0/1)#ip address 192.168.1.1 255.255.255.0
P1(config-if-gei-0/1)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#interface gei-0/1
P1(config-mpls-te-if-gei-0/1)#exit
P1(config-mpls-te)#explicit-path identifier 1
P1(config-mpls-te-expl-path-id-1)#next-address strict 192.168.1.2
P1(config-mpls-te-expl-path-id-1)#exit
P1(config-mpls-te)#tunnel te_tunnel 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
```

```
 path-option 1 explicit-path identifier 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 autoroute announce
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 autoroute metric absolute 12
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#exit
```

P2上的配置如下：

```
P2(config)#interface gei-0/1
P2(config-if-gei-0/1)#no shutdown
P2(config-if-gei-0/1)#ip address 192.168.1.2 255.255.255.0
P2(config-if-gei-0/1)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-0/1
P2(config-mpls-te-if-gei-0/1)#exit
```

配置验证

在P1上查看隧道情况：

```
P1(config)#show mpls traffic-eng tunnels te_tunnel 1
   Name: tunnel_1 (Tunnel1) Destination: 2.1.1.1
    Status:
    Admin: up Oper: up Path: valid Signalling: connected
    Path option: 1, type explicit identifier: 1 (Basis for Setup)
    Actual Bandwidth: N/A
    Hot-standby protection:
    no path options protected
    Config Parameters:
    Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0x0
     Resv-Style: SE
    Metric Type: IGP (default) Upper Limit: 4294967295
    Record-Route: disabled
    Facility Fast-reroute: disabled
    Detour Fast-reroute: disabled
    BFD: disabled
    Auto-bw: disabled
    Bidirect: disabled
    AutoRoute: enabledAutoRouteMetricType: absoluteAutoRouteMetric: 12
    Forwarding-adjacency: disabled

    InLabel: -
    OutLabel: gei-0/1, 3
    RSVP Signalling Info :
     Src 1.1.1.1, Dst 2.1.1.1, Tun_Id 1, Tun_Instance 30
    RSVP Path Info:
    Explicit Route: 192.168.1.1 192.168.1.2 2.1.1.1
    Exclude Route: NULL
    Record Route: NULL
    Tspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits
```

```
    RSVP Resv Info:
    Record Route: NULL
    Fspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits

    History:
    Tunnel:
    Time since created: 0 days, 0 hours, 19 minutes, 4 seconds
     Prior LSP: path option 1
    Current LSP: Uptime:0 days, 0 hours, 9 minutes, 56 seconds
    Last lsp error information:
    None log record.

P1(config)#show mpls traffic-eng autoroute
  MPLS TE autorouting enabled
    Destination 2.1.1.1 has 1 tunnels
    TunnelName Destination State NexthopMetricType MetricValue
    tunnel_1 2.1.1.1 Up 2.1.1.1Absolute 12
```

6.3.15 TE Metric

通过对MPLS-TE隧道使能TE Metric功能以及配置接口TE Metric值，使MPLS-TE隧道在进行CSPF选路的过程中，优先选择经过沿路所有出接口TE Metric总和最小的路径。这样通过修改接口Metric值可以间接指定TE隧道选择的路径，实现选路的可管理性。

6.3.15.1 配置 TE metric

本节介绍TE metric的配置步骤和命令。

1.配置TE metric值。

步骤	命令	功能
1	inspur(config-mpls-te)#**tunnel te_tunnel** <*tunnel-number*>	进入Tunnel接口配置模式
2	inspur(config-mpls-te-tunnel-te_tunnel-tunnel-number)#**tunnel mpls traffic-eng administrative-weight**<*value*>	配置隧道下的metric值，其范围是1~4294967295
3	inspur(config-mpls-te)#**interface** <*interface-name*>	进入TE接口配置模式
4	inspur(config-mpls-te-if-interface-name)#**administrative-weight**<*value*>	配置TE接口下的metric值，其范围是1~65535

2.验证配置结果。

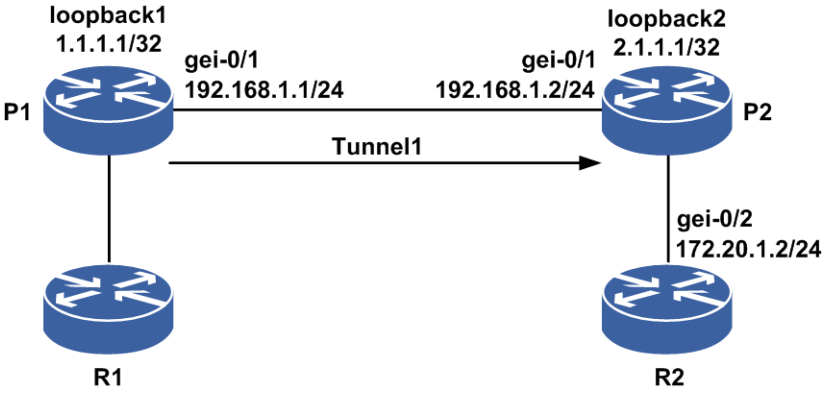
命令	功能
inspur#**show mpls traffic-eng tunnels**	查看隧道详细信息
inspur#**show mpls traffic-eng interface detail**	查看MPLS TE接口的详细信息

6.3.15.2 TE metric 配置实例

配置说明

如*图 6-*所示，采用OSPF TE进行严格选路的方式从P1到P2建立一条RSVP普通隧道，在隧道和相应的接口下配置TE metric。

图 6-41 TE 的 metric 配置实例图



配置思路

1.P1、P2直连接口建立OSPF邻居，OSPF开启TE。

2.P1、P2直连接口开启TE。

3.在P1上建立一条隧道Tunnel1。

4.在隧道和相应接口下配置TE metric。

配置过程

P1上的配置如下：

```
P1(config)#interface gei-0/1
P1(config-if-gei-0/1)#no shutdown
P1(config-if-gei-0/1)#ip address 192.168.1.1 255.255.255.0
P1(config-if-gei-0/1)#exit
P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit
P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
```

```
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#interface gei-0/1
P1(config-mpls-te-if-gei-0/1)#administrative-weight 7
P1(config-mpls-te-if-gei-0/1)#exit
P1(config-mpls-te)#explicit-path identifier 1
P1(config-mpls-te-expl-path-id-1)#next-address strict 192.168.1.2
P1(config-mpls-te-expl-path-id-1)#exit
P1(config-mpls-te)#tunnel te_tunnel 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 path-option 1 explicit-path identifier 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 administrative-weight 12
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#exit
```

P2上的配置如下：

```
P2(config)#interface gei-0/1
P2(config-if-gei-0/1)#no shutdown
P2(config-if-gei-0/1)#ip address 192.168.1.2 255.255.255.0
P2(config-if-gei-0/1)#exit
P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-0/1
P2(config-mpls-te-if-gei-0/1)#exit
```

配置验证

在P1上查看隧道情况：

```
P1(config)#show mpls traffic-eng tunnels te_tunnel 1
    Name: tunnel_1 (Tunnel1) Destination: 2.1.1.1
     Status:
     Admin: up Oper: up Path: valid Signalling: connected
     Path option: 1, type explicit identifier: 1 (Basis for Setup)
     Actual Bandwidth: N/A
     Hot-standby protection:
     no path options protected
     Config Parameters:
     Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0x0
     Resv-Style: SE
      Metric Type: TE Upper Limit: 12
     Record-Route: disabled
     Facility Fast-reroute: disabled
     Detour Fast-reroute: disabled
     BFD: disabled
     Auto-bw: disabled
     Bidirect: disabled
     AutoRoute:disabled
     Forwarding-adjacency: disabled
```

```
    InLabel: -
    OutLabel: gei-0/1, 3
    RSVP Signalling Info :
    Src 1.1.1.1, Dst 2.1.1.1, Tun_Id 1, Tun_Instance 30
    RSVP Path Info:
    Explicit Route: 192.168.1.1 192.168.1.2 2.1.1.1
    Exclude Route: NULL
    Record Route: NULL
    Tspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits
    RSVP Resv Info:
    Record Route: NULL
    Fspec: ave rate= 0 kbits, burst= 1000 bytes, peak rate= 0 kbits

    History:
    Tunnel:
    Time since created: 0 days, 0 hours, 19 minutes, 4 seconds
    Prior LSP: path option 1
    Current LSP: Uptime:0 days, 0 hours, 9 minutes, 56 seconds
    Last lsp error information:
    None log record.

P1(config)#show mpls traffic-eng interface detail
gei-0/1:
 State:
 ENABLE
 Traffic-eng metric: 7
 Authentication: disabled
 Key: <encrypted>
 Type: md5
 Challenge: disabled
 Challenge-imp: Not implemented(simulated)
 Window size: 32
 BFD: disabled
 Backup path:
 None
 SRLGs: None
 Intf Fast-Hello: DISABLE
 Fast-Hello interval: 10000
 Fast-Hello miss: 4
```

6.3.16 TE SRLG

SRLG是指一组共享相同风险的链路，如果其中一条链路故障，其它链路可能都会失效。

SRLG在MPLS TE部署中被广泛考虑。在MPLS TE中引入SRLG，可以使备份路径在选路时，避免和被保护的链路选在同一个SRLG，提供更好的保护有效性。

TE SRLG通常是针对MPLS TE-FRR业务，可以利用SRLG来优化备份路径的选择。SRLG信息可被用于CSPF计算，因此如果备份路径是动态生成的，可以计算并生成和被保护链路不在同一个SRLG的路径；如果备份路径是手工生成，只能手工避免。

6.3.16.1 配置 TE SRLG

本节介绍TE SRLG功能的配置步骤和命令。

1.配置MPLS TE SRLG值。

步骤	命令	功能

步骤	命令	功能
1	inspur(config-mpls-te)#**auto-tunnel backup srlg exclude**{**force**|**preferred**}	在全局模式下配置SRLG的排除方式，强制或者优选
2	inspur(config-mpls-te)#**interface** <*interface-name*>	进入TE接口配置模式
3	inspur(config-mpls-te-if-interface-name)#**srlg**<*value*>	配置TE接口下的SRLG的值，范围：0~4294967295，一个接口下最多允许配置3个SRLG的值

2.验证配置结果。

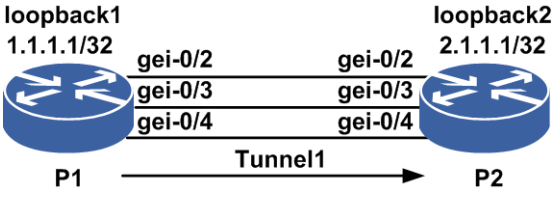
命令	功能
inspur#**show mpls traffic-eng auto-backup parameter**	查看自动备份隧道的配置信息
inspur#**show mpls traffic-eng interface detail**	查看接口下的SRLG的配置信息

6.3.16.2 TE 的 SRLG 配置实例

配置说明

如*图 6-262*所示，采用OSPF TE进行严格选路的方式从P1到P2建立一条RSVP普通隧道为主隧道，配置自动备份方式，并在主隧道出接口配置SRLG值，其它链路的出接口也配置SRLG值（该配置实例以force强制为例）。

图 6-262 TE 的 SRLG 配置实例图



配置思路

1.P1、P2直连接口建立OSPF邻居，OSPF开启TE。

2.P1、P2直连接口开启TE。

3.在P1上建立一条隧道Tunnel1，配置自动备份。

4.在主隧道的的出接口上配置SRLG。

5.在其他链路的出接口上配置SRLG。

配置过程

P1上的配置如下：

```
P1(config)#interface gei-0/2
P1(config-if-gei-0/2)#no shutdown
P1(config-if-gei-0/2)#ip address 192.168.1.1 255.255.255.0
P1(config-if-gei-0/2)#exit
P1(config)#interface gei-0/3
P1(config-if-gei-0/3)#no shutdown
P1(config-if-gei-0/3)#ip address 31.1.1.1 255.255.255.0
P1(config-if-gei-0/3)#exit
P1(config)#interface gei-0/4
P1(config-if-gei-0/4)#no shutdown
P1(config-if-gei-0/4)#ip address 32.1.1.1 255.255.255.0
P1(config-if-gei-0/4)#exit

P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit

P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 31.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 32.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1
P1(config-mpls-te)#auto-tunnel backup srlg exclude force
P1(config-mpls-te)#interface gei-0/2
P1(config-mpls-te-if-gei-0/2)#auto-tunnel backup
P1(config-mpls-te-if-gei-0/2)#srlg 1
P1(config-mpls-te-if-gei-0/2)#srlg 2
P1(config-mpls-te-if-gei-0/2)#srlg 3 /*一个接口下最多配3个SRLG值*/
P1(config-mpls-te-if-gei-0/2)#exit
P1(config-mpls-te)#interface gei-0/3
P1(config-mpls-te-if-gei-0/3)#srlg 1
P1(config-mpls-te-if-gei-0/3)#exit
P1(config-mpls-te)#interface gei-0/4
P1(config-mpls-te-if-gei-0/4)#srlg 4
P1(config-mpls-te-if-gei-0/4)#exit
P1(config-mpls-te)#explicit-path identifier 1
P1(config-mpls-te-expl-path-id-1)#next-address strict 192.168.1.2
P1(config-mpls-te-expl-path-id-1)#exit
P1(config-mpls-te)#tunnel te_tunnel 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 path-option 1 explicit-path identifier 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng record-route
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 fast-reroute facility
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#exit
```

P2上的配置如下：

```
P2(config)#interface gei-0/2
P2(config-if-gei-0/2)#no shutdown
```

```
P2(config-if-gei-0/2)#ip address 192.168.1.2 255.255.255.0
P2(config-if-gei-0/2)#exit
P2(config)#interface gei-0/3
P2(config-if-gei-0/3)#no shutdown
P2(config-if-gei-0/3)#ip address 31.1.1.2 255.255.255.0
P2(config-if-gei-0/3)#exit
P2(config)#interface gei-0/4
P2(config-if-gei-0/4)#no shutdown
P2(config-if-gei-0/4)#ip address 32.1.1.2 255.255.255.0
P2(config-if-gei-0/4)#exit

P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 31.1.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 32.1.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-0/2
P2(config-mpls-te-if-gei-0/2)#exit
P2(config-mpls-te)#interface gei-0/3
P2(config-mpls-te-if-gei-0/3)#exit
P2(config-mpls-te)#interface gei-0/4
P2(config-mpls-te-if-gei-0/4)#exit
```

配置验证

在P1上查看隧道情况：

```
P1(config)#show mpls traffic-eng auto-backup parameter
MPLS-TE: Enabled
The setting of auto-tunnel minID is: 32001
The setting of auto-tunnel maxID is:  33000
Auto-tunnel minID in used is:  33000
Auto-tunnel maxID in used is:  33000
Auto-tunnel backup srlg exclude: Force

P1(config)#show mpls traffic-eng interface detail
gei-0/2:
 State:
 ENABLE
 Traffic-eng metric: 0
 Authentication: disabled
 Key: <encrypted>
 Type: md5
 Challenge: disabled
 Challenge-imp: Not implemented(simulated)
 Window size: 32
 BFD: disabled
 Backup path:
 auto-tunnel backup
 SRLGs: 1 2 3
 Intf Fast-Hello: DISABLE
 Fast-Hello interval: 10000
 Fast-Hello miss: 4
gei-0/3:
```

```
 State:
 ENABLE
 Traffic-eng metric: 0
 Authentication: disabled
 Key: <encrypted>
 Type: md5
 Challenge: disabled
 Challenge-imp: Not implemented(simulated)
 Window size: 32
 BFD: disabled
 Backup path:
 None
 SRLGs: 1
 Intf Fast-Hello: DISABLE
 Fast-Hello interval: 10000
 Fast-Hello miss: 4
gei-0/4:
 State:
 ENABLE
 Traffic-eng metric: 0
 Authentication: disabled
 Key: <encrypted>
 Type: md5
 Challenge: disabled
 Challenge-imp: Not implemented(simulated)
 Window size: 32
 BFD: disabled
 Backup path:
 None
 SRLGs: 4
 Intf Fast-Hello: DISABLE
 Fast-Hello interval: 10000
 Fast-Hello miss: 4

P1(config)#show mpls traffic-eng tunnels brief
Signalling Summary:
 LSP Tunnels Process: running
 RSVP Process: running
 Forwarding: enabled
TUNNEL NAMEDESTINATION UP IFDOWN IFSTATE/PROT
tunnel_12.1.1.1 -gei-0/2 up/up
tunnel_33000 2.1.1.1 -    gei-0/4  up/up
P1(config)#show mpls traffic-eng fast-reroute
Tunnel head end item information
Protected Tunnel LspIDIn-label Out intf/labelFRR intf/label Status
Tunnel1545  Tun hd  gei-0/2:3 Tu33000:3 ready

LSP midpoint frr information:
LSP identifierIn-label Out intf/label FRR intf/label Status
```

6.3.17 TE 隧道重优化

重优化技术可以帮助TE隧道选择最优的路径，也可以在发生保护切换之后，帮助切换后的隧道恢复到合理的主路径上。重优化利用MBB技术实现选路过程的流量不丢失。

6.3.17.1 配置 TE 隧道重优化

本节介绍TE隧道重优化功能的配置步骤和命令。

1.配置TE隧道的重优化。

步骤	命令	功能
1	inspur(config-mpls-te)#**reoptimize events link-up**	全局模式下，配置在链路up事件发生时进行重优化
2	inspur(config-mpls-te)#**reoptimize timers frequency**<*timer*>	全局模式下，配置定时重优化时间，范围是30~604800，单位是秒
3	inspur(config-mpls-te)#**reoptimize tunnel**{<*tunnel-id*>|**all**}	全局模式下，配置手动重优化一条隧道或者全部隧道 此命令是一次触发式命令

<*tunnel-id*>：手动对某一条隧道进行一次重优化。

all：手动对所有隧道进行一次重优化。

2.验证配置结果。

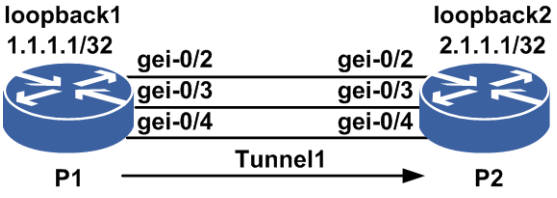
命令	功能
inspur#**show mpls traffic-eng tunnels summary**	查看用户配置的重优化定时器

6.3.17.2 TE 隧道的重优化配置实例

配置说明

如*图 6-27*所示，从P1到P2建立一条隧道，配置3个path-option 1、2、3，分别对应3条链路，在隧道两条链路断开时，进行手动重优化。

图 6-273 TE 隧道的重优化配置实例图



配置思路

1.P1、P2三条链路都建立OSPF邻居并开启TE。

2.隧道下配置3个path-option 1、2、3，分别对应3条链路。

3.先将path-option 1、2对应链路**shutdown**，**shutdown**、**no shutdown**隧道接口后触发隧道建立。

4.将path-option 1、2对应的链路**no shutdown**，进行手动重优化。

配置过程

P1上的配置如下：

```
P1(config)#interface gei-0/2
P1(config-if-gei-0/2)#no shutdown
P1(config-if-gei-0/2)#ip address 192.168.1.1 255.255.255.0
P1(config-if-gei-0/2)#exit
P1(config)#interface gei-0/3
P1(config-if-gei-0/3)#no shutdown
P1(config-if-gei-0/3)#ip address 31.1.1.1 255.255.255.0
P1(config-if-gei-0/3)#exit
P1(config)#interface gei-0/4
P1(config-if-gei-0/4)#no shutdown
P1(config-if-gei-0/4)#ip address 32.1.1.1 255.255.255.0
P1(config-if-gei-0/4)#exit

P1(config)#interface loopback1
P1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
P1(config-if-loopback1)#exit

P1(config)#interface te_tunnel1
P1(config-if-te_tunnel1)#ip unnumbered loopback1
P1(config-if-te_tunnel1)#exit

P1(config)#router ospf 1
P1(config-ospf-1)#router-id 1.1.1.1
P1(config-ospf-1)#area 0
P1(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 31.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 32.1.1.0 0.0.0.255
P1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
P1(config-ospf-1-area-0)#mpls traffic-eng
P1(config-ospf-1-area-0)#exit

P1(config)#mpls traffic-eng
P1(config-mpls-te)#interface loopback1
P1(config-mpls-te-if-loopback1)#exit
P1(config-mpls-te)#router-id 1.1.1.1

P1(config-mpls-te)#reoptimize events link-up

P1(config-mpls-te)#interface gei-0/2
P1(config-mpls-te-if-gei-0/2)#exit
P1(config-mpls-te)#interface gei-0/3
P1(config-mpls-te-if-gei-0/3)#exit
P1(config-mpls-te)#interface gei-0/4
P1(config-mpls-te-if-gei-0/4)#exit
P1(config-mpls-te)#explicit-path identifier 1
P1(config-mpls-te-expl-path-id-1)#next-address strict 192.168.1.2
P1(config-mpls-te-expl-path-id-1)#exit
P1(config-mpls-te)#explicit-path identifier 2
P1(config-mpls-te-expl-path-id-2)#next-address strict 31.1.1.2
P1(config-mpls-te-expl-path-id-2)#exit
P1(config-mpls-te)#explicit-path identifier 3
P1(config-mpls-te-expl-path-id-3)#next-address strict 32.1.1.2
P1(config-mpls-te-expl-path-id-3)#exit
P1(config-mpls-te)#tunnel te_tunnel 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel destination ipv4 2.1.1.1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 path-option 1 explicit-path identifier 2
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 path-option 2 explicit-path identifier 1
P1(config-mpls-te-tunnel-te_tunnel1)#tunnel mpls traffic-eng
 path-option 3 explicit-path identifier 3
P1(config-mpls-te-tunnel-te_tunnel1)#exit
P1(config-mpls-te)#exit
```

P2上的配置如下：

```
P2(config)#interface gei-0/2
P2(config-if-gei-0/2)#no shutdown
P2(config-if-gei-0/2)#ip address 192.168.1.2 255.255.255.0
P2(config-if-gei-0/2)#exit
P2(config)#interface gei-0/3
P2(config-if-gei-0/3)#no shutdown
P2(config-if-gei-0/3)#ip address 31.1.1.2 255.255.255.0
P2(config-if-gei-0/3)#exit
P2(config)#interface gei-0/4
P2(config-if-gei-0/4)#no shutdown
P2(config-if-gei-0/4)#ip address 32.1.1.2 255.255.255.0
P2(config-if-gei-0/4)#exit

P2(config)#interface loopback2
P2(config-if-loopback2)#ip address 2.1.1.1 255.255.255.255
P2(config-if-loopback2)#exit

P2(config)#router ospf 1
P2(config-ospf-1)#router-id 2.1.1.1
P2(config-ospf-1)#area 0
P2(config-ospf-1-area-0)#network 192.168.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 31.1.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 32.1.1.0 0.0.0.255
P2(config-ospf-1-area-0)#network 2.1.1.1 0.0.0.0
P2(config-ospf-1-area-0)#mpls traffic-eng
P2(config-ospf-1-area-0)#exit

P2(config)#mpls traffic-eng
P2(config-mpls-te)#interface loopback2
P2(config-mpls-te-if-loopback2)#exit
P2(config-mpls-te)#router-id 2.1.1.1
P2(config-mpls-te)#interface gei-0/2
P2(config-mpls-te-if-gei-0/2)#exit
P2(config-mpls-te)#interface gei-0/3
P2(config-mpls-te-if-gei-0/3)#exit
P2(config-mpls-te)#interface gei-0/4
P2(config-mpls-te-if-gei-0/4)#exit
```

配置验证

先将P1的gei-0/2和gei-0/3接口**shutdown**，使用**show mpls traffic-eng tunnels brief**命令查看，可以看到隧道选择的是gei-0/4接口下的链路。

```
P1(config)#show mpls traffic-eng tunnels brief
Signalling Summary:
 LSP Tunnels Process: running
  RSVP Process: running
 Forwarding: enabled
TUNNEL NAME  DESTINATION UP IF  DOWN IF  STATE/PROT
tunnel_1     2.1.1.1      -     gei-0/4  up/up
```

将P1的gei-0/2和gei-0/3接口**no shutdown**，在P1的TE模式下进行手动重优化。

```
P1(config-mpls-te)#reoptimize tunnel 1
```

使用**show mpls traffic-eng tunnels brief**命令查看，可以看到隧道选择的是gei-0/2接口下的链路。

```
P1(config)#show mpls traffic-eng tunnels brief
Signalling Summary:
 LSP Tunnels Process: running
 RSVP Process: running
 Forwarding: enabled
TUNNEL NAME  DESTINATION UP IF  DOWN IF  STATE/PROT
tunnel_1     2.1.1.1      -     gei-0/2  up/up
```

7 VPN

7.1 VPN 简介

网络经济的发展

随着社会的发展，IT技术越来越多地影响现代企业的业务流程，如企业资源规划、基于IP的语音、基于网络的会议和教学活动等IT技术，为企业的自动化办公和信息的获取提供了构架。随着网络经济的发展，越来越多的企业的分布范围日益扩大，合作伙伴日益增多，公司员工的移动性也不断增加。这使得企业迫切需要借助电信运营商网络连接企业总部和分支机构，组成自己的企业网，同时移动办公人员能在企业以外的地方方便地访问企业内部网络。

传统专网的缺陷

最初，电信运营商是以租赁专线（Leased Line）的方式为企业提供二层链路，这种方式的主要缺点是：

- 建设时间长
- 价格昂贵
- 难于管理

此后，随着ATM（Asynchronous Transfer Mode，异步传输模式）和FR（Frame Relay，帧中继）技术的兴起，电信运营商转而使用虚电路方式为客户提供点到点的二层连接，客户再在其上建立自己的三层网络以承载IP等数据流。虚电路方式与租赁专线相比，运营商提供服务的时间短、价格低，能在不同专网之间共享运营商的网络结构。虚电路这种传统专网的不足之处在于：

- 依赖于专用的介质（如ATM或FR）：为提供基于ATM的VPN（Virtual Private Network，虚拟专用网）服务，运营商需要建立覆盖全部服务范围的ATM网络；为提供基于FR的VPN服务，又需要建立覆盖全部服务范围的FR网络。在网络建设上造成浪费。
- 速率较慢，达不到当前Internet中已实现的速率。
- 部署复杂，尤其是向已有的私有网络加入新的站点时，需要同时修改所有接入此站点的边缘节点的配置。

VPN的引入

传统专网的应用，促使了企业的效益日益增长，但传统专网难以满足企业对网络的灵活性、安全性、经济性和扩展性等方面的要求。这导致了新的替代方案的产生，即在现有IP网络上模拟传统专网。这种新的解决方案就是VPN（Virtual Private Network，

虚拟专用网）。

VPN是依靠ISP（Internet Service Provider，因特网业务提供者）和NSP（Network Service Provider，网络服务提供商），在公共网络中建立的虚拟专用通信网络。

7.2 MPLS L2VPN

MPLS技术已经被普遍认为是下一代核心网络的发展方向，其最主要的优势之一就是可以很好地支持VPN业务。网络提供商采用基于MPLS技术的网络提供二层VPN服务，可以仅维护和管理单一的网络基础设施，同时提供二层VPN业务、三层VPN业务以及其它各种灵活的“尽力而为”或担保服务质量的IP业务，且VPN业务的配置实施将更加自动化。

二层MPLS VPN主要支持以下几种业务功能。

- VPWS：虚拟专线服务，使用点到点连接方式实现VPN内每个站点之间的通信。
- VPLS：虚拟LAN服务，将运营商网络仿真成LAN交换机或桥接器，连接用户所有的LAN，提供二层交换服务。
- MSPW：又称多跳伪线（MH-PW），是指一条伪线是由多条分段伪线构成，实现伪线的跨域功能。
- VLSS：虚拟本地交换业务，支持2个本地CE之间的互通。

7.2.1 VPLS

VPLS在MPLS网络中提供以太网的仿真业务，将多个LAN/VLAN网络连在一起，属于多点到多点的L2VPN业务。

VPLS MAC过滤功能是为了响应用户对VPLS网络访问安全和可控的需求而设置的。根据用户设置的过滤规则对VPLS报文的MAC进行过滤，从而达到限制VPLS MAC的学习和限制VPLS转发的目的。

7.2.2 配置 VPLS

VPLS在MPLS网络中提供以太网的仿真业务，是多点到多点的L2VPN业务。

本节介绍VPLS的配置命令和步骤。

1.全局开启L2VPN功能。

命令	功能
`inspur(config)#`**mpls l2vpn enable**	全局开启L2VPN功能

2.创建PW虚接口以及隧道策略名称。

步骤	命令	功能
1	inspur(config)#**pw pw**<*1-115968*>	全局配置模式下创建PW
2	inspur(config)#**tunnel-policy** <*tunnel-policy-name*>	配置隧道策略名称 PW外层走隧道时才需要此配置

3. 配置VPLS实例并绑定AC和PW实体。

步骤	命令	功能
1	inspur(config)#**vpls** <*vpls-name*>[**multi-mac-spaces**]	创建VPLS实例名称
2	inspur(config-vpls-vpls-name)#**access-point** <*ac-interface*>[**split-horizon**]	指定绑定为接入链路（AC）的接口，并进入AC配置模式 不带**split-horizon**参数表示AC为server模式；带**split-horizon**参数表示AC为client模式
3	inspur(config-vpls-vpls-name-ac-ac-interface)#**access-params ethernet**	配置AC为ethernet类型
4	inspur(config-vpls-vpls-name)#**pseudo-wire pw**<*1-115968*>[**spoke**]	配置PW与业务绑定
5	inspur(config-vpls-vpls-name-pw-pw-number)#**neighbour** <*A.B.C.D*>[**vcid** <*1-4294967295*>]	配置PW实体

[**multi-mac-spaces**]：表示配置的是qualified类型的VPLS。

步骤4命令中，如果不带**spoke**选项表示工作在hub转发模式，并进入pw配置模式；带**spoke**选项表示工作在spoke转发模式，并进入spoke-pw配置模式。

<*vcid*>：指定该PW所使用的VCID，范围为1~4294967295，如果缺省配置该参数，需要先在config-vpls模式下配置好default-vcid。

<*A.B.C.D*>：远端LSRID。

4.（可选）配置VPLS实例相关属性。

步骤	命令	功能
1	inspur(config-vpls-vpls-name)#**default-vcid** <*vcid*>	VPLS服务的缺省VCID
2	inspur(config-vpls-vpls-name)#**mac**	进入MAC-VFI模式
3	inspur(config-vpls-vpls-name)#**mac-withdraw**	使能mac-withdraw功能

步骤	命令	功能
4	inspur(config-vpls-vpls-name)#**description** <*string*>	配置VPLS实例描述功能
5	inspur(config-vpls-vpls-name)#**mtu** <*mtu*>	设置和修改实例的MTU值

5.（可选）配置VPLS实例下AC接口相关属性。

步骤	命令	功能
1	inspur(config-vpls-vpls-name-ac-ac-interface-eth)#**ingress-adjust rewrite** <*1-4094*>	配置VLAN翻译（修改VLAN值）
2	inspur(config-vpls-vpls-name-ac-ac-interface-eth)#**ingress-adjust push** {<*1-4094*>}	配置VLAN翻译（加一层VLAN）

6.（可选）配置VPLS实例下PW实体的相关属性。

步骤	命令	功能
1	inspur(config-vpls-vpls-name-pw-pw-number-neighbour)#**control-word preferred**	修改PW是否使用控制字
2	inspur(config-vpls-vpls-name-pw-pw-number-neighbour)#**vccv bfd capability** {**basic** | **status**} **encapsulation** {**ip** | **raw**}	配置PW支持VCCV能力
3	inspur(config-vpls-vpls-name-pw-pw-number-neighbour)#**tunnel-policy** <*tunnel-policy-name*>	修改PW的外层隧道策略
4	inspur(config-vpls-vpls-name-pw-pw-number-neighbour)#**signal** {**dynamic** | **static local-label** <*16-1048575*> **remote-label** <*16-1048575*>}	修改PW的建立方式为信令触发
5	inspur(config-vpls-vpls-name-pw-pw-number-neighbour)#**encapsulation** {**tagged** | **raw**}	修改PW的封装模式
6	inspur(config-vpls-vpls-name-pw-pw-number-neighbour)#**track** <*track-name*>	配置PW track功能 Track中可以绑定BFD、CFM和EFM，PW绑定track后，可以和samgr进行联动检测

bfd：配置CV类型为PW-BFD。

dynamic：配置PW类型为动态。

static：配置PW类型为静态。

<*16-1048575*>：PW标签可配置的范围。

tagged：配置PW使用Tagged模式。

raw：配置PW使用Raw模式。

7.验证配置结果。

命令	功能
inspur#**show l2vpn brief**	显示L2VPN服务实例的列表和每个实例AC和PW的绑定数量
inspur#**show l2vpn summary**	显示VPN实例的个数
inspur#**show l2vpn forwardinfo** [**vpnname** <*vpn-name*>| **peer** <*A.B.C.D*>][**detail**]	根据实例名称或peer-id等特征，显示生效的PW列表
inspur#**show pwe3 signal fec128**[[**peer** <*ip-address*>][**vcid** <*vcid*>][**pw-type** <*pw-type*>]|**local-label** <*value*>|**remote-label** <*value*>|**service-type** {**vpls**|**vpws**|**mspw**}[**id** <*value*>|**name** <*instance-name*>]|**used-only**|**unuse-only** [**no-remote**|**no-config**]]	用于查看PW的信息摘要
inspur#**show pwe3 signal fec128**[[**peer** <*ip-address*>][**vcid** <*vcid*>][**pw-type** <*pw-type*>]|**local-label** <*value*>|**remote-label** <*value*>|**service-type** {**vpls**|**vpws**|**mspw**}[**id** <*value*>|**name** <*instance-name*>]|**used-only**|**unuse-only** [**no-remote**|**no-config**]] **detail**	用于查看PW的详细信息，且对状态为down的PW给出原因提示
inspur#**show pwe3 signal statistic**	查看各种类型的PW的信令状态的统计信息
inspur#**show l2vpn protectgroup** [<*pw-name*>]	显示所有PW保护组的信息

7.2.2.1 配置 VPLS-MAC 过滤

本节介绍VPLS-MAC过滤的配置步骤和命令。

1.创建L2VPN的VPLS服务实例。

命令	功能
inspur(config)#**vpls** <*vpls-name*>[**multi-mac-spaces**]	建立L2VPN的VPLS服务实例[**multi-mac-spaces**]缺省时，表示**unqualified**

[**multi-mac-spaces**]：MAC学习的策略，在指定的VLAN 中学习MAC。

2.配置VPLS实例下根据MAC地址过滤数据帧。

步骤	命令	功能
1	inspur(config-vpls-vpls-name)#**mac**	进入MAC-VFI模式
2	inspur(config-vpls-vpls-name-mac)#**filter**	配置VPLS实例下根据MAC

步骤	命令	功能
	{**source** | **both** | **destination**}<*mac-address*>[**vlan** <*vlan-id*>]	地址过滤数据帧

source：根据源MAC地址进行数据帧的过滤。

both：根据源或目的MAC地址进行数据帧的过滤。

destination：根据目的MAC地址进行数据帧的过滤。

<*vlan-id*>：VLAN ID，范围1~4094，在**qualified**模式下，用此参数指定MAC地址仅在此VLAN中进行学习。

3.验证配置结果。

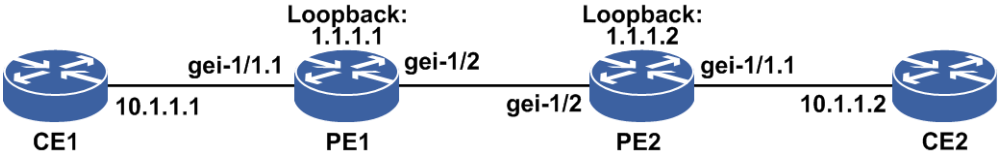
命令	功能
`inspur(config)#`**show mac vpls instance**<*vpls-name*>	显示VPLS实例下配置的MAC地址表项

7.2.2.2 VPLSunqualified 配置实例

配置说明

L2VPN VPLS unqualified实例配置组网如*图 7-1*所示。

图 7-1 L2VPN VPLS unqualified 实例基本组网图



配置思路

1.配置CE1、CE2上和PE相连的接口，按照这两个接口是在同一个以太网当中的情况进行必要配置。

2.配置PE1、PE2上和CE相连的接口。选择子接口作为AC，则必须对子接口配置vlan/qinq封装。

3.配置PE1和PE2之间直连接口，使得PE1与PE2能互联； 配置PE1、PE2上loopback接口，作为LDP的Router-ID。

4.配置路由协议，相互通告loopback接口地址，注意保证路由的下一跳/出接口是下面一个步骤的LDP公网接口。

5.配置LDP实例，将PE1和PE2之间直连的接口使能mpls ldp能力，作为LDP的公网接口。PE1和PE2直连，无需建立target-session。

6.配置VPLS实例，注意VPLS的neighbor要和ldp的neighbor一致。

配置过程

CE1上配置如下：

```
CE1(config)#interface gei-1/1.1
CE1(config-gei-1/1.1)#exit
CE1(config)#vlan-configuration
CE1(config-vlan)#interface gei-1/1.1
CE1(config-vlan-if-gei-1/1.1)#encapsulation-dot1q 100
CE1(config-vlan-if-gei-1/1.1)#exit
CE1(config-vlan)#exit
CE1(config)#interface gei-1/1.1
CE1(config-gei-1/1.1)#ip address 10.1.1.1 255.255.255.0
CE1(config-gei-1/1.1)#exit
```

配置PE之间直连接口和Loopback接口以及ac侧子接口：

```
PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#no shutdown
PE1(config-if-gei-1/2)#ip address 100.10.1.1 255.255.255.0
PE1(config-if-gei-1/2)#no shutdown
PE1(config-if-gei-1/2)#exit
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255

PE1(config-if-loopback1)#exit
PE1(config)#interface gei-1/1.1
PE1(config-gei-1/1.1)#exit
PE1(config)#vlan-configuration
PE1(config-vlan)#interface gei-1/1.1
PE1(config-vlan-if-gei-1/1.1)#encapsulation-dot1q 100
PE1(config-vlan-if-gei-1/1.1)#exit
PE1(config-vlan)#exit
```

配置路由协议：

```
PE1(config)#router ospf 1
PE1(config-ospf-1)#router-id 1.1.1.1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
PE1(config-ospf-1-area-0)#network 100.10.1.0 0.0.0.255
PE1(config-ospf-1-area-0)#exit
PE1(config-ospf-1)#exit
```

配置LDP：

```
PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#interface gei-1/2
PE1(config-ldp-1-if-gei-1/2)#exit
PE1(config-ldp-1)#exit
```

配置L2VPN VPLS：

```
PE1(config)#mpls l2vpn enable
PE1(config)#pw pw1
PE1(config)#vpls inspur1
PE1(config-vpls-inspur1)#pseudo-wire pw1
PE1(config-vpls-inspur1-pw-pw1)#neighbour 1.1.1.2 vcid 10
/*配置peerip以及vcid，默认raw模式*/
```

```
PE1(config-vpls-inspur1-pw-pw1-neighbour)#exit
PE1(config-vpls-inspur1-pw-pw1)#exit
PE1(config-vpls-inspur1)#access-point gei-1/1.1     /*配置AC侧接口*/
PE1(config-vpls-inspur1-ac-gei-1/1.1)#access-params ethernet
/*这句必须要配，否则AC成员不生效*/
PE1(config-vpls-inspur1-ac-gei-1/1.1-eth)#end
```

PE2上的配置如下：

配置PE之间直连接口和Loopback接口地址以及ac侧子接口：

```
PE2(config)#interface gei-1/2
PE2(config-if-gei-1/2)#ip address 100.10.1.2 255.255.255.0
PE2(config-if-gei-1/2)#no shutdown
PE2(config-if-gei-1/2)#exit
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255

PE2(config-if-loopback1)#exit
PE2(config)#interface gei-1/1.1
PE2(config-gei-1/1.1)#exit
PE2(config)#vlan-configuration
PE2(config-vlan)#interface gei-1/1.1
PE2(config-vlan-if-gei-1/1.1)#encapsulation-dot1q 100
PE2(config-vlan-if-gei-1/1.1)#exit
PE2(config-vlan)#exit
```

配置路由协议：

```
PE2(config)#router ospf 1
PE2(config-ospf-1)#router-id 1.1.1.2
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 1.1.1.2 0.0.0.0
PE2(config-ospf-1-area-0)#network 100.10.1.0 0.0.0.255
PE2(config-ospf-1-area-0)#exit
PE2(config-ospf-1)#exit
```

配置LDP：

```
PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#interface gei-1/2
PE2(config-ldp-1-if-gei-1/2)#exit
PE2(config-ldp-1)#exit
```

配置L2VPN VPLS：

```
PE2(config)#mpls l2vpn enable
PE2(config)#pw pw1
PE2(config)#vpls inspur1
PE2(config-vpls-inspur1)#pseudo-wire pw1
PE2(config-vpls-inspur1-pw-pw1)#neighbour 1.1.1.1 vcid 10
PE2(config-vpls-inspur1-pw-pw1-neighbour)#exit
PE2(config-vpls-inspur1-pw-pw1)#exit
PE2(config-vpls-inspur1)#access-point gei-1/1.1
PE2(config-vpls-inspur1-ac-gei-1/1.1)#access-params ethernet
PE2(config-vpls-inspur1-ac-gei-1/1.1-eth)#end
```

CE2上配置如下：

```
CE2(config)#interface gei-1/1.1
CE2(config-gei-1/1.1)#exit
CE2(config)#vlan-configuration
CE2(config-vlan)#interface gei-1/1.1
CE2(config-vlan-if-gei-1/1.1)#encapsulation-dot1q 100
CE2(config-vlan-if-gei-1/1.1)#exit
CE2(config-vlan)#exit
CE2(config)#interface gei-1/1.1
CE2(config-gei-1/1.1)#ip address  10.1.1.2  255.255.255.0
CE2(config-gei-1/1.1)#exit
```

配置验证

配置结果验证，以PE1为例，PE2上验证过程相同。

1.用**show running-config ospfv2**命令查看路由配置是否正确，用**show ip forwarding route**命令检查路由配置结果：

```
PE1#show running-config ospfv2
!<ospf>
router ospf 1
  area 0
    network 1.1.1.1 0.0.0.0
/*通告将在VPLS中作为pw neighbor的地址。在下一个步骤配置LDP时注意必须将这个地址作为
LDP router-id，用这个地址建立LDP会话。*/
    network 100.10.1.0 0.0.0.255
 $
/*通告和对端PE直连接口的地址作为OSPF邻居建链地址*/
  router-id 1.1.1.1
$
!/<ospfv2>

PE1#show ip forwarding route 1.1.1.2
IPv4 Routing Table:
status codes: *valid, >best
   Dest           Gw          Interface     Owner   Pri Metric
*> 1.1.1.2/32      100.10.1.2    gei-1/2       o       110 1
```

经过路由配置，到VPLS的pw neighbor同时也是LDP对等体的Rrouter-ID的路由生成，本地出接口是gei-1/2，下一跳地址是100.10.1.2。

2.用**show running-config ldp**命令检查LDP配置是否正确，用**show mpls ldp neighbor instance**命令查看LDP邻居建链结果：

```
PE1#show running-config ldp
!<ldp>
mpls ldp instance 1
  router-id loopback1
  interface gei-1/2
/*步骤1中查看到的gei-1/2，即是到LDP邻居的路由出接口*/
$
!</ldp>

PE1#show mpls ldp neighbor instance 1
Peer LDP Ident: 100.10.1.2:0; Local LDP Ident: 100.10.1.1:0
 /*Peer LDP Ident<—->Local LDP Ident,发现潜在的LDP对等体100.10.1.2:0，
尝试为这个对等体建立LDP会话（LDP session）*/
       TCP connection: 100.10.1.2.2278 - 100.10.1.1.646
/*到潜在对等体的TCP连接建立成功，本示例中未配置建链传输地址，
所以这里是默认的router-id地址*/
       State: Oper; Msgs sent/rcvd: 80/72; Downstream
/*到潜在对等体的TCP连接建立成功，在TCP连接上LDP邻居协商成功，成功建立到对等体的会话
（LDP session UP）。ldp state:Oper表示ldp session（LDP会话）建立成功*/
       Up Time: 00:54:04
       LDP discovery sources:
         gei-1/2; Src IP addr: 100.10.1.2
/*通过gei-1/2接口发送ldp邻居发现消息，由这个接口维护
100.10.1.2:0<—> 100.10.1.1:0 之间的会话，这个接口down，则会话关闭*/
       Addresses bound to peer LDP Ident:
         100.10.1.2  100.10.1.2    /*LDP邻居对等体上可以作为LSP公网接口的地址*/
```

提示：

当要建立vpls pw时会先检查是否有到指定neighbor的LDP会话，如没有这个会话，则不会发送pw建链信令，pw无法建立。

3.在对端PE2上用**show mpls ldp bindings**命令检查LDP是否为pw neighbor分配了公网的local标签，在PE1上看这个标签mapping到本地后，作为remote标签是否打上了inuse标记。

```
PE2#show mpls ldp bindings 1.1.1.2 32 detail instance 1
 1.1.1.2/32
    local binding:  label: imp-null
     advertised to:
     1.1.1.1:0
    remote binding: lsr: 1.1.1.1:0, label: 16484

PE1#show mpls ldp bindings 1.1.1.2 32 detail instance 1
 1.1.1.2/32
    local binding:  label: 16484
      advertised to:
      1.1.1.2:0
    remote binding: lsr: 1.1.1.2:0, label: imp-null(inuse)
```

PE2上为本地loopback1地址100.10.10.2分配隐式空标签3，PE1上学到PE2为100.10.10.2分配的3标签，并且打上了**inuse**标记。

4.用**show mpls forwarding**命令检查是否将分配给pw neighbor的标签写入了标签转发表，用**ping mpls ipv4**命令验证到指定的pw neighbor的公网隧道是否建立成功：

```
PE1#show mpls forwarding-table
Local    Outgoing  Prefix or         Outgoing         Next Hop     M/S

label    label     Tunnel Id         interface
16484    Poptag    1.1.1.2/32        gei-0/8          100.10.1.2    M


PE1#ping mpls ipv4 1.1.1.2 32
sending 5,120-byte MPLS echos to 1.1.1.2,timeout is 2 seconds.
Codes: '!' - success,   'Q' - request not transmitted,
      '.' - timeout,   'U' - unreachable,
      'R' - downstream router but not target
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/1 ms.
```

5.用**show pwe3 signal**命令查看本地是否能发送pw建链的信令，一般来说，只要上面步骤2的检查结果中有到达指定的pw neighbor的LDP会话，pwe3信令就可以发送了。

```
PE1(config)#show pwe3 signal fec128 detail
The detailed signal information of dynamic fec128 PWs or PW-segments:

Some signal information are referred to as follows :
   NON  - the LDP session is absent,
   UP   - the LDP session is OPERATIONAL,
   GR1  - the LDP session is reconnecting,
   GR2  - the LDP session's remote mappings are recovering,
   DOWN - not UP(or NON,or GR1,or GR2).


PW entity    : < 1.1.1.2 , 10 , Ethernet >
LSPs formed  : YES
C-bits       : local       : NO        , remote     : NO
               negotiated   : NO
```

```
MTU          : local       : 1500      , remote     : 1500
               negotiated  : 1500
labels       : local       : 81920     , remote     : 81920
signal       : Configured  : YES       , Received   : YES
               Negotiated  : YES       , Sent       : YES
               AC ready    : YES
oam status   : local       : PSN rcv(?),snd(?); AC rcv(?),snd(?); Error(?)
               remote      : PSN rcv(?),snd(?); AC rcv(?),snd(?); Error(?)
redundancy   : local       : ??        , remote     : ??
               negotiated  : ??
application  : service-type : VPLS      , instance-id: 4
MAC-withdraw : received    : 0         , sent       : 0
local-VCCV   : CC-type     : AL|TTL    , CV-type    : LSP
remote-VCCV  : CC-type     : AL|TTL    , CV-type    : LSP
actual-VCCV  : CC-type     : AL        , CV-type    : LSP
LDP session  : The LDP session's state is UP.
attachment-circuit : ??
local-description  : inspur1
remote-description : inspur1
```

6.用**show l2vpn forwardinfo**命令查看pw是否建立成功，用detail选项可以看到这条pw的内外层标签等具体信息。

```
PE1#show l2vpn forwardinfo vpnname inspur1
Hearders: PWType - Pseudowire type and Pseudowire connection mode
        Llabel - Local label, Rlabel - Remote label
        VPNowner - owner type and instance name
Codes:   H - HUB mode, S - SPOKE mode, L - VPLS, W - VPWS, M - MSPW

PWName   PeerIP         FEC PWType     State Llabel  Rlabel  VPNowner
pw1      1.1.1.2        128 Ethernet  H UP    81920   81920   L:inspur1

PE1#show l2vpn forwardinfo vpnname inspur1 detail
Headers: ALLOK - Pseudo Wire Forwarding
        PWNF  - Pseudo Wire Not Forwarding
        AR    - Local AC (ingress) Receive Fault
        AT    - Local AC (egress) Transmit Fault
        PSNR  - Local PSN-facing PW (ingress) Receive Fault
        PSNT  - Local PSN-facing PW (egress) Transmit Fault
        PWFS  - Pseudo Wire Forwarding Standby
        RS    - Request Switchover to this PW
        PWSA  - Pseudo Wire Status All Fault
Codes  : -unknown, *yes, .no
-------------------------------------------------------------------------
-------

Service type and instance name:[VPLS  inspur1]
  Peer IP address        : 1.1.1.2                VCID        : 10
  Connection mode        : HUB                    VCID Extend  : 0
  Signaling protocol     : LDP                    VC type      : Ethernet
  Last status change time : 00:03:31               Create time  : 00:10:59
  MPLS VC local label    : 81920                  Remote label : 81920
  PW name                : pw1                   Control Word : -
  Related PW name        : -                      PW FRR type  : NULL
  Activation status      : ENABLE                 Band Width   : 0
  VC status              : UP
  Remote status          : ALLOK
  VCCV CC type           : ALERT_LABEL
  VCCV CV type           : LSP
  Tunnel label           : { 3 }
  Output interface       : gei-1/2
  Imposed label stack    : { 81920 3 }
```

7.用**ping mpls pseudowire**命令验证pw是否正确建立。

```
PE1#ping mpls pseudowire pw1
sending 5,120-byte MPLS echo(es) to ,timeout is 2 second(s).
```

```
Codes: '!' - success,   'Q' - request not transmitted,
       '.' - timeout,   'U' - unreachable,
       'R' - downstream router but not target

!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 2/4/6
```

经过VPLS的应用，两台CE设备应当能够互相ping通。

```
CE1#ping 10.1.1.2
sending 5,100-byte ICMP echoes to 10.1.1.2,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.

CE2#ping 10.1.1.1
sending 5,100-byte ICMP echoes to 10.1.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.
```

7.2.2.3 VPLS qualified 配置实例

VPLS qualified配置思路和配置过程与VPLS unqualified实例类似，只是实例配置略有不同。

PE1上配置如下：

```
PE1(config)#mpls l2vpn enable
PE1(config)#pw pw1
PE1(config)#vpls inspur1 multi-mac-spaces
PE1(config-vpls-inspur1)#pseudo-wire pw1
PE1(config-vpls-inspur1-pw-pw1)#neighbour 1.1.1.2 vcid 10
/*配置peerip以及vcid，pw-type默认tagged模式*/
PE1(config-vpls-inspur1-pw-pw1-neighbour-1.1.1.2)#exit
PE1(config-vpls-inspur1-pw-pw1)#exit
PE1(config-vpls-inspur1)#access-point gei-1/1.1     /*配置AC侧接口*/
PE1(config-vpls-inspur1-ac-gei-1/1.1)#access-params ethernet
/*这句必须要配，否则AC成员不生效*/
```

PE2上配置如下：

```
PE2(config)#mpls l2vpn enable
PE2(config)#pw pw1
PE2(config)#vpls inspur1 multi-mac-spaces
PE2(config-vpls-inspur1)#pseudo-wire pw1
PE2(config-vpls-inspur1-pw-pw1)#neighbour 1.1.1.1 vcid 10
PE2(config-vpls-inspur1-pw-pw1-neighbour-1.1.1.1)#exit
PE2(config-vpls-inspur1-pw-pw1)#exit
PE2(config-vpls-inspur1)#access-point gei-1/1.1
PE2(config-vpls-inspur1-ac-gei-1/1.1)#access-params ethernet
```

配置验证过程与VPLS unqualified相同。

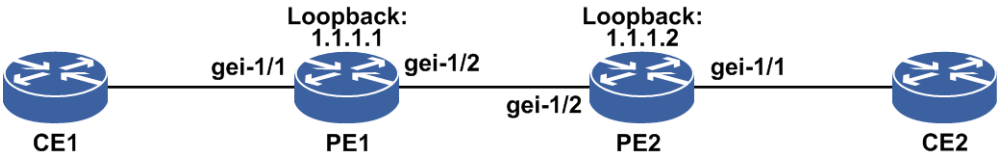
7.2.2.4 VPLS-MAC 过滤配置实例

配置说明

VPLS MAC过滤功能是为了响应用户对VPLS网络访问安全和可控的需求而设置的。主要应用于根据用户设置的过滤规则对VPLS报文的源MAC、目的MAC或者源和目的

MAC进行过滤，以达到限制VPLS MAC学习和限制VPLS MAC的转发功能。典型组网如*图 7-2*所示。

图 7-2 VPLS-MAC 过滤配置实例拓扑图



配置思路

1.在PE1和PE2之间建立VPLS连接。

2.在PE上进入VPLS MAC配置模式，配置MAC过滤规则。

配置过程

PE1上的配置如下：

```
PE1(config)#mpls l2vpn enable
PE1(config)#pw pw1
PE1(config)#vpls vpls_a
PE1(config-vpls-vpls_a)#pseudo-wire pw1
PE1(config-vpls-vpls_a-pw-pw1)#neighbour 1.1.1.2 vcid 100
PE1(config-vpls-vpls_a-pw-pw1-neighbour)#exit
PE1(config-vpls-vpls_a-pw-pw1)#exit

PE1(config-vpls-vpls_a)#access-point gei-1/1
PE1(config-vpls-vpls_a-ac-gei-1/1)#access-params ethernet
PE1(config-vpls-vpls_a-ac-gei-1/1-eth)#exit
PE1(config-vpls-vpls_a-ac-gei-1/1)#exit
PE1(config-vpls-vpls_a)#exit

PE1(config)#interface loopback10
PE1(config-if-loopback10)#ip address 1.1.1.1 255.255.255.255
PE1(config-if-loopback10)#exit
PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#no shutdown
PE1(config-if-gei-1/2)#ip address 2.2.2.1 255.255.255.0
PE1(config-if-gei-1/2)#exit

PE1(config)#router ospf 1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
PE1(config-ospf-1-area-0)#network 2.2.2.0 0.0.0.255
PE1(config-ospf-1-area-0)#router-id 1.1.1.1
PE1(config-ospf-1-area-0)#exit
PE1(config-ospf-1)#exit

PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback10
PE1(config-ldp-1)#interface gei-1/2
PE1(config-ldp-1-if-gei-1/2)#exit
PE1(config-ldp-1)#exit
```

PE2上的配置如下：

```
PE2(config)#mpls l2vpn enable
PE2(config)#pw pw1
PE2(config)#vpls vpls_a
PE2(config-vpls-vpls_a)#pseudo-wire pw1
PE2(config-vpls-vpls_a-pw-pw1)#neighbour 1.1.1.1 vcid 100
PE2(config-vpls-vpls_a-pw-pw1-neighbour)#exit
PE2(config-vpls-vpls_a-pw-pw1)#exit

PE2(config-vpls-vpls_a)#access-point gei-1/1
PE2(config-vpls-vpls_a-ac-gei-1/1)#access-params ethernet
PE2(config-vpls-vpls_a-ac-gei-1/1-eth)#exit
PE2(config-vpls-vpls_a-ac-gei-1/1)#exit
PE2(config-vpls-vpls_a)#exit

PE2(config)#interface loopback10
PE2(config-if-loopback10)#ip address 1.1.1.2 255.255.255.255
PE2(config-if-loopback10)#exit
PE2(config)#interface gei-1/2
PE2(config-if-gei-1/2)#no shutdown
PE2(config-if-gei-1/2)#ip address 2.2.2.2 255.255.255.0
PE2(config-if-gei-1/2)#exit

PE2(config)#router ospf 1
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 1.1.1.2 0.0.0.0
PE2(config-ospf-1-area-0)#network 2.2.2.0 0.0.0.255
PE2(config-ospf-1-area-0)#router-id 1.1.1.2
PE2(config-ospf-1-area-0)#exit
PE2(config-ospf-1)#exit

PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback10
PE2(config-ldp-1)#interface gei-1/2
PE2(config-ldp-1-if-gei-1/2)#exit
PE2(config-ldp-1)#exit
```

配置验证

在PE1上验证配置结果：

```
/*查看PW建链情况*/
PE1(config)#show l2vpn forwardinfo vpnname vpls_a
Headers: PWType - Pseudo Wire type and Pseudo Wire connection mode
        Llabel - Local label, Rlabel - Remote label
        VPNowner - Owner type and instance name
Codes  : H - HUB mode, S - SPOKE mode, L - VPLS, W - VPWS, M - MSPW, MO - MONITO
R
        $pw - auto_pw

PWName   PeerIP      FEC PWType     State Llabel  Rlabel  VPNowner
pw1      1.1.1.2     128 Ethernet   H UP  81920   81920   L:vpls_a

/*查看MAC过滤的配置*/
/*此时没有配置MAC过滤策略，L2VPN中MAC过滤部分无MAC显示*/
PE1(config)#show running-config l2vpn
!<l2vpn>
mpls l2vpn enable
vpls vpls_a
  pseudo-wire pw1
    neighbour 1.1.1.2 vcid 100
    $
  $
$
!</l2vpn>
```

CE1和CE2分别发源MAC为0000.0000.1111和0000.0000.2222的流，查看MAC学习情况：

```
PE1(config)#show mac vpls instance vpls_a
/*type字段为dynamic表示动态学习到*/
MAC           vlan  peer-address  outInterface   type
------------------------------------------------------------
0000.0000.1111  0     0.0.0.0      gei-1/1       dynamic
/*本地源MAC没有配置过滤，不过滤，学习*/
0000.0000.2222  0     1.1.1.2      pw1           dynamic
/*远端源MAC没有配置过滤，不过滤，学习*/
```

在上述配置的基础上，在PE1上添加MAC过滤配置，配置如下：

```
PE1(config)#vpls vpls_a
PE1(config-vpls-vpls_a)#mac
PE1(config-vpls-vpls_a-mac)#filter source 0000.0000.1111
PE1(config-vpls-vpls_a-mac)#filter source 0000.0000.2222
PE1(config-vpls-vpls_a-mac)#exit
PE1(config-vpls-vpls_a)#exit
```

PE1上配置过滤后的验证：

```
查看MAC过滤的配置：
PE1(config)#show running-config l2vpn
!<l2vpn>
mpls l2vpn enable
vpls vpls_a
  pseudo-wire pw1
    neighbour 1.1.1.2 vcid 100
    $
  $
  mac
    filter source 0000.0000.1111
    filter source 0000.0000.2222
  $
$
!</l2vpn>
```

CE1和CE2分别发源MAC为0000.0000.1111和0000.0000.2222的流，查看MAC学习情况：

```
PE1(config-vpls-mac-vpls_a)#show mac vpls instance vpls_a
/*type字段为src filter表示为源过滤，不学习对应源MAC*/
MAC             VLAN  peer-address    outInterface    type
------------------------------------------------------------------
0000.0000.2222  0       NULL            NULL        src filter
/*远端源MAC配置了过滤，不学习*/
0000.0000.1111  0       NULL            NULL        src filter
/*本地源MAC配置了过滤，不学习*/
```

7.2.3 VPWS

VPWS建立在MPLS网络的基础设施之上，使用点到点连接方式实现VPN内每个站点之间的通信。这种方式多用于正在使用PPP、HDLC、ATM、FR连接的用户，用户和网络提供商之间的连接保持不变，但业务经封装后在网络提供商的IP骨干网上传输。

为了适应移动网络IP化和宽带化的发展需求，移动Backhual向IP RAN转型已成为必然趋势。移动Backhual的IP化改造过程就是将旧的原有的SDH和ATM升级为IP RAN的过程。在这个升级过程中，VPWS异构提供了一种低成本解决方案。

7.2.3.1 配置 VPWS

VPWS以MPLS网络为基础，使用点到点连接方式实现VPN内每个站点之间的通信。本节介绍VPWS的配置步骤和命令。

1.全局开启L2VPN功能。

命令	功能
inspur(config)#**mpls l2vpn enable**	全局开启L2VPN功能

2.创建PW虚接口以及隧道名称。

步骤	命令	功能
1	inspur(config)#**pw pw** <*1-115968*>	创建PW接口
2	inspur(config)#**tunnel-policy** <*tunnel-policy-name*>	配置隧道策略名称 PW外层走隧道时才需要此配置

须先在全局配置模式下创建PW，才能在VPWS实例中将PW绑定到VPWS。

3.配置VPWS实例并绑定AC和PW实体。

步骤	命令	功能
1	inspur(config)#**vpws** <*vpws-name*>	创建vpws实例名称
2	inspur(config-vpws-vpws-name)#**access-point** <*ac-interface*>	指定绑定为接入链路（AC）的接口，并进入AC配置模式
3	inspur(config-vpws-vpws-name-ac-ac-interface)#**access-params** {**ethernet** | **fr** | **hdlc** | **ppp** | **tdm**}	配置AC的封装类型
4	inspur(config-vpws-vpws-name)#**pseudo-wire pw**<*1-115968*>	配置PW与业务绑定
5	inspur(config-vpws-vpws-name-pw-pw-number)#**neighbour** <*A.B.C.D*>[**vcid** <*1-4294967295*>]	配置PW实体

<*vcid*>：指定该PW所使用的VCID，范围为1~4294967295，如果缺省配置该参数，需要先在config-vpws模式下配置好default-vcid。

<*A.B.C.D*>：远端LSRID。

4.（可选）配置VPWS实例相关属性。

命令	功能

命令	功能
inspur(config-vpws-vpws-name)#**mtu** <*mtu*>	设置和修改实例的MTU值
inspur(config-vpws-vpws-name)#**description** <*string*>	配置对VPWS实例的描述

5.（可选）配置VPWS实例下AC接口相关属性。

步骤	命令	功能
1	inspur(config-vpws-vpws-name-ac-ac-interface-eth)#**ingress-adjust rewrite** <*1-4094*>	配置VLAN翻译（修改VLAN值）
2	inspur(config-vpws-vpws-name-ac-ac-interface-eth)#**ingress-adjust push** {<*1-4094*>}	配置VLAN翻译（加一层VLAN）

6.（可选）配置VPWS实例下PW实体的相关属性。

步骤	命令	功能
1	inspur(config-vpws-vpws-name-pw-pw-number-neighbour)#**control-word preferred**	修改PW是否使用控制字
2	inspur(config-vpws-vpws-name-pw-pw-number-neighbour)#**encapsulation** {**tagged** | **raw**}	修改PW的封装模式
3	inspur(config-vpws-vpws-name-pw-pw-number-neighbour)#**vccv bfd capability** {**basic** | **status**} **encapsulation** {**ip** | **raw**}	配置PW支持VCCV能力
4	inspur(config-vpws-vpws-name-pw-pw-number-neighbour)#**tunnel-policy** <*tunnel-policy-name*>	修改PW的外层隧道策略
5	inspur(config-vpws-vpws-name-pw-pw-number-neighbour)#**signal** {**dynamic** | **static local-label** <*16-1048575*> **remote-label** <*16-1048575*>}	修改PW的建立方式为信令触发

bfd：配置CV类型为PW-BFD。

dynamic：配置PW类型为动态。

static：配置PW类型为静态。

<*16-1048575*>：PW标签可配置的范围。

tagged：配置PW使用Tagged模式。

raw：配置PW使用Raw模式。

7.验证配置结果。

命令	功能

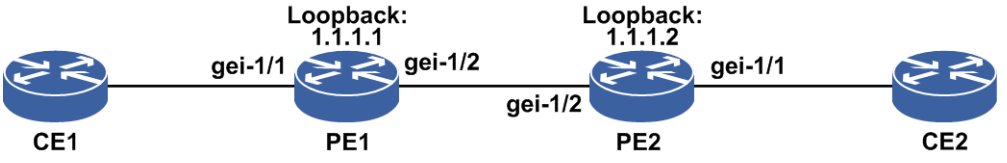
命令	功能
inspur#**show l2vpn brief**	显示L2VPN服务实例的列表和每个实例AC和PW的绑定数量
inspur#**show l2vpn summary**	显示VPN实例的个数
inspur#**show l2vpn forwordinfo vpnname** <*vpn-name*>[**detail**]	根据实例名称，显示生效的PW列表
inspur#**show pwe3 signal fec128** [[**peer** <*A.B.C.D*>][**vcid** <*value*>][**pw-type** <*pw-type*>]| **used-only** |**unused-only** [**no-remote** | **no-config**]| **service-type vpws** [**id** <*value*>| **name** <*name*>]}|**local-label** <*value*>}|**remote-label** <*value*>]	用于查看PW的信息摘要
inspur#**show pwe3 signal fec128** [[**peer** <*A.B.C.D*>][**vcid** <*value*>][**pw-type** <*pw-type*>]}| **used-only** |**unused-only** [**no-remote** | **no-config**]| **service-type vpws** [**id** <*value*>| **name** <*name*>]|**local-label** <*value*>}|**remote-label** <*value*>] **detail**	用于查看PW的详细信息，且对状态为down的PW给出原因提示
inspur#**show pwe3 signal statistic**	查看各种类型的PW的信令状态的统计信息
inspur#**show l2vpn protectgroup** [<*pw-name*>]	显示所有PW保护组的信息

7.2.3.2 VPWS ethernet PW 配置实例

配置说明

L2VPN VPWS ethernet PW实例配置组网如*图 7-3*所示。

图 7-3 L2VPN VPWS ethernet PW 实例配置拓扑图



配置思路

1.配置路由器接口地址，使得PE1与PE2能互联。

2.配置Loopback接口，作为LDP的Router-ID。

3.配置OSPF路由协议，相互通告Loopback接口地址。

4.配置LDP实例，直连的无需建立target-session。

5.配置L2VPN实例。

配置过程

PE1上的配置：

```
PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#ip address 10.1.1.1 255.255.255.0
PE1(config-if-gei-1/2)#no shutdown
PE1(config-if-gei-1/2)#exit
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
PE1(config-if-loopback1)#exit

PE1(config)#router ospf 200
PE1(config-ospf-200)#router-id 1.1.1.1
PE1(config-ospf-200)#area 0
PE1(config-ospf-200-area-0)#network 10.1.1.0 0.0.0.255
PE1(config-ospf-200-area-0)#network 1.1.1.1 0.0.0.0
PE1(config-ospf-200-area-0)#exit
PE1(config-ospf-200)#exit

PE1(config)#mpls ldp instance 100
PE1(config-ldp-100)#router-id loopback1
PE1(config-ldp-100)#interface gei-1/2
PE1(config-ldp-100-if-gei-1/2)#exit
PE1(config-ldp-100)#exit

PE1(config)#pw pw1
PE1(config)#vpws vpws_inspur1
PE1(config-vpws-vpws_inspur1)#pseudo-wire pw1
PE1(config-vpws-vpws_inspur1-pw-pw1)#neighbour 1.1.1.2 vcid 20
PE1(config-vpws-vpws_inspur1-pw-pw1-neighbour)#control-word preferred
PE1(config-vpws-vpws_inspur1-pw-pw1-neighbour)#signal dynamic
PE1(config-vpws-vpws_inspur1-pw-pw1-neighbour)#encapsulation raw
PE1(config-vpws-vpws_inspur1-pw-pw1-neighbour)#exit
PE1(config-vpws-vpws_inspur1-pw-pw1)#exit
PE1(config-vpws-vpws_inspur1)#access-point gei-1/1
PE1(config-vpws-vpws_inspur1-ac-gei-1/1)#access-params ethernet
PE1(config-vpws-vpws_inspur1-ac-gei-1/1-eth)#exit
PE1(config-vpws-vpws_inspur1-ac)#exit
PE1(config-vpws)#exit
```

PE2上的配置：

```
PE2(config)#interface gei-1/2
PE2(config-if-gei-1/2)#ip address 10.1.1.2 255.255.255.0
PE2(config-if-gei-1/2)#no shutdown
PE2(config-if-gei-1/2)#exit
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
PE2(config-if-loopback1)#exit

PE2(config)#router ospf 200
PE2(config-ospf-200)#router-id 1.1.1.2
PE2(config-ospf-200)#area 0
PE2(config-ospf-200-area-0)#network 1.1.1.2 0.0.0.0
PE2(config-ospf-200-area-0)#network 10.1.1.0 0.0.0.255
PE2(config-ospf-200-area-0)#exit
PE2(config-ospf-200)#exit

PE2(config)#mpls ldp instance 100
PE2(config-ldp-100)#router-id loopback1
PE2(config-ldp-100)#interface gei-1/2
PE2(config-ldp-100-if-gei-1/2)#exit
PE2(config-ldp-100)#exit

PE2(config)#pw pw1
PE2(config)#mpls l2vpn enable
```

```
PE2(config)#vpws vpws_inspur1
PE2(config-vpws-vpws_inspur1)#pseudo-wire pw1
PE2(config-vpws-vpws_inspur1-pw-pw1)#neighbour 1.1.1.1 vcid 20
PE2(config-vpws-vpws_inspur1-pw-pw1-neighbour)#control-word preferred
PE2(config-vpws-vpws_inspur1-pw-pw1-neighbour)#signal dynamic
PE2(config-vpws-vpws_inspur1-pw-pw1-neighbour)#encapsulation raw
PE2(config-vpws-vpws_inspur1-pw-pw1-neighbour)#exit
PE2(config-vpws-vpws_inspur1-pw-pw1)#exit
PE2(config-vpws-vpws_inspur1)#access-point gei-1/1
PE2(config-vpws-vpws_inspur1-ac-gei-1/1)#access-params ethernet
PE2(config-vpws-vpws_inspur1-ac-gei-1/1-eth)#exit
PE2(config-vpws-vpws_inspur1-ac-gei-1/1)#exit
PE2(config-vpws-vpws_inspur1)#exit
```

配置验证

正确配置后，VPWS PW应该能够成功建立，下面是路由器上成功配置后的验证。

```
PE1#show l2vpn for vpn vpws_inspur1
Headers: PWType - Pseudo Wire type and Pseudo Wire connection mode
        Llabel - Local label, Rlabel - Remote label
        VPNowner - Owner type and instance name
Codes  : H - HUB mode, S - SPOKE mode, L - VPLS, W - VPWS, M - MSPW, MO - MONITOR
        $pw - auto_pw

PWName   PeerIP         FEC PWType     State Llabel  Rlabel  VPNowner
pw1      1.1.1.2     128 Ethernet    up    81921   81921   W:vpws_inspur1

PE1#show l2vpn for vpn vpws_inspur1 detail
Hearders : ALLOK - Pseudowire Forwarding
          PWNF  - Pseudowire Not Forwarding
          AR    - Local AC (ingress) Receive Fault
          AT    - Local AC (egress) Transmit Fault
          PSNR  - Local PSN-facing PW (ingress) Receive Fault
          PSNT  - Local PSN-facing PW (egress) Transmit Fault
          PWFS  - Pseudowire forwarding standby
          RS    - Request switchover to this PW
          PWSA  - Pseudowire Status All Fault
Codes    : -unknown, *yes, .no
------------------------------------------------------------------------------
-----

Service type and instance name:[VPWS  vpws1]
  Peer IP address        : 1.1.1.2             VCID       : 20
  Connection mode        :                       VCID Extend  : 0
  Signaling protocol     : LDP                     VC type      : Ethernet
  Last status change time : 00:01:09                 Create time  : 00:02:27
  MPLS VC local label    : 81921                   Remote label : 81921
  PW name               : pw2                    Control Word : ENABLE
  Related PW name        : -                       PW FRR type  : NULL
  Activation status      : ENABLE                  Band Width   : 0
  VC status             : UP
  Remote status          : ALLOK
  VCCV CC type           : CWORD
  VCCV CV type           : LSP
  Tunnel label           : { 3 }
  Output interface       : gei-1/2
  Imposed label stack    : { 81921 3 }
```

7.2.3.3 VPWS BFD 配置实例

配置说明

如图 7-4所示，R1、R2配置VPWS，在VPWS下配置BFD。

图 7-4 VPWS BFD 配置实例



配置思路

1.R1、R2配置VPWS实例。

2.R1、R2在VPWS下配置BFD。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-0/3
R1(config-if-gei-0/3)#ip address 201.2.3.2 255.255.255.0
R1(config-if-gei-0/3)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 100.1.1.2 255.255.255.255
R1(config-if-loopback1)#exit

R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 201.2.3.0 0.0.0.255
R1(config-ospf-1-area-0)#network 100.1.1.2 0.0.0.0
R1(config-ospf-1-area-0)#exit
R1(config-ospf-1)#exit

R1(config)#mpls ldp instance 1
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-0/3
R1(config-ldp-1-gei-0/3)#exit
R1(config-ldp-1)#exit

R1(config)#pw pw1
R1(config)#vpws vpws-bfd
R1(config-vpws-vpws-bfd)#access-point gei-0/4
R1(config-vpws-vpws-bfd-ac-gei-0/4)#access-params ethernet
R1(config-vpws-vpws-bfd-ac-gei-0/4-eth)#exit
R1(config-vpws-vpws-bfd-ac-gei-0/4)#exit
R1(config-vpws-vpws-bfd)#pseudo-wire pw1
R1(config-vpws-vpws-bfd-pw-pw1)#neighbour 100.1.1.3 vcid 1
R1(config-vpws-vpws-bfd-pw-pw1-neighbour)#vccv bfd capability basic
encapsulation ip
R1(config-vpws-vpws-bfd-pw-pw1-neighbour)#exit
R1(config-vpws-vpws-bfd-pw-pw1)#exit
R1(config-vpws-vpws-bfd)#exit
```

```
R1(config)#bfd
R1(config-bfd)#session pw-bfd pw-bfd pw-name pw1
R1(config-bfd-pw-pw-bfd)#exit
R1(config-bfd)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-0/3
R2(config-if-gei-0/3)#ip address 201.2.3.3 255.255.255.0
R2(config-if-gei-0/3)#exit
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 100.1.1.3 255.255.255.255
R2(config-if-loopback1)#exit

R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 201.2.3.0 0.0.0.255
R2(config-ospf-1-area-0)#network 100.1.1.3 0.0.0.0
R2(config-ospf-1-area-0)#exit
R2(config-ospf-1)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#interface gei-0/3
R2(config-ldp-1)#exit

R2(config)#pw pw1
R2(config)#vpws vpws-bfd
R2(config-vpws-vpws-bfd)#access-point gei-0/4
R2(config-vpws-vpws-bfd-ac-gei-0/4)#access-params ethernet
R2(config-vpws-vpws-bfd-ac-gei-0/4-eth)#exit
R2(config-vpws-vpws-bfd-ac-gei-0/4)#exit
R2(config-vpws-vpws-bfd)#pseudo-wire pw1
R2(config-vpws-vpws-bfd-pw-pw1)#neighbour 100.1.1.2 vcid 1
R2(config-vpws-vpws-bfd-pw-pw1-neighbour)#vccv bfd capability basic
encapsulation ip
R2(config-vpws-vpws-bfd-pw-pw1-neighbour)#exit
R2(config-vpws-vpws-bfd-pw-pw1)#exit
R2(config-vpws-vpws-bfd)#exit

R2(config)#bfd
R2(config-bfd)#session pw-bfd pw-bfd pw-name pw1
R2(config-bfd-pw-pw-bfd)#exit
R2(config-bfd)#exit
```

配置验证

正确配置后，**show l2vpn forwardinfo vpnname**查看VPWS实例，**show bfd neighbors pw brief**查看VPWS BFD情况。

R1上查看：

```
R1(config)#show l2vpn forwardinfo vpnname vpws-bfd
Headers: PWType - Pseudowire type and Pseudowire connection mode
         Llabel - Local label, Rlabel - Remote label
         VPNowner - owner type and instance name
Codes  : H - HUB mode, S - SPOKE mode, L - VPLS, W - VPWS, M - MSPW
        $pw - auto_pw

PWName   PeerIP     FEC PWType      State Llabel  Rlabel  VPNowner
pw1      100.1.1.3  128 Ethernet    UP    81922   81921   W:vpws-bfd

R1(config)#show bfd neighbors pw brief

Pwname    LD       RD       Hold       State
```

```
pw1      33233     2981      150         UP
```

R2上查看：

```
R2(config)#show l2vpn forwardinfo vpnname vpws-bfd
Headers: PWType - Pseudowire type and Pseudowire connection mode
         Llabel - Local label, Rlabel - Remote label
         VPNowner - owner type and instance name
Codes  : H - HUB mode, S - SPOKE mode, L - VPLS, W - VPWS, M - MSPW
         $pw - auto_pw

PWName   PeerIP     FEC PWType      State Llabel  Rlabel  VPNowner
pw1      100.1.1.2  128 Ethernet    UP    81921   81922   W:vpws-bfd
R2(config)#show bfd neighbors pw brief

Pwname    LD        RD        Hold       State
pw1       2981      33233     150        UP
```

7.2.4 MSPW

MSPW是指一条伪线由多条单段伪线构成，通常是为了实现伪线的跨域。

7.2.4.1 配置 MSPW

本节介绍MSPW的配置步骤和命令。

1.创建MSPW实例。

步骤	命令	功能
1	inspur(config)#**mpls l2vpn enable**	全局开启L2VPN功能
2	inspur(config)#**pw pw**<*1-2147483647*>	全局模式下创建PW接口
3	inspur(config)#**mspw** <*instance-name*>[**for {ethernet {tagged | raw}| fr {port | dlci | dlci-old}| tdm {aal1 | aal2 | satop e1| cesopsn {basic | cas}| sonet-sdh {cesom | ceop}}|atm {port | vpc | vcc | vpc-group | vcc-group | sdu | pdu}| ip | hdlc | ppp}**]	创建MSPW实例
4（可选）	inspur(config-mspw-mspw-name)#**status-signaling terminal**	配置MSPW的状态通告终结属性

2.配置PW并绑定MSPW实例。

步骤	命令	功能
1	inspur(config-mspw-mspw-name)#**seudo-wire pw**<*1-2147483647*>	配置PW并绑定MSPW实例
2	inspur(config-mspw-mspw-name-seg-pw-number)#**neighbour** <*peer-ip*>[**vcid** <*vcid*>]	配置PW实体

步骤	命令	功能
3	inspur(config-mspw-mspw-name-seg-pw-number-neighbour)#**signal** {**dynamic** | **static local-label** *<16~1048575>* **remote-label** *<16~1048575>*}	修改PW的建立方式为信令触发
4	inspur(config-mspw-mspw-name-seg-pw-number-neighbour)#**tunnel-policy** *<tunnel-policy-name>*	修改PW的外层隧道策略 需先在全局配置模式下用命令**tunnel-policy** *<tunnel-policy-name>*定义隧道策略，才可在PW下绑定隧道策略

<peer-ip>：远端LSR ID。

tunnel-policy *<tunnel-policy-name>*：优选的RSVP隧道信息。

<16~1048575>：静态标签值。

3.配置MSPW的动静PW远端接口参数。

步骤	命令	功能
1	inspur(config-mspw-mspw-name)#**interface-params**	进入MSPW远端接口参数模式
2	inspur(config-mspw-mspw-name-if-params)# **description** *<text>*	配置接口描述符
3	inspur(config-mspw-mspw-name-if-params)# **mtu***<60-9216>*	配置服务实例的最大传输单元
4	inspur(config-mspw-mspw-name-if-params)# **fragmentation**	分包指示
5	inspur(config-mspw-mspw-name-if-params)# **fcs-retention header-length** {2|4}	配置Frame Check Sequence保持，并指定FCS的长度
6	inspur(config-mspw-mspw-name-if-params)# **atm cell-concatenate** *<1-64>*	配置ATM cells最大可连接的个数
7	inspur(config-mspw-mspw-name-if-params)# **distribute-period** *<2-64>*	配置TDM仿真的打包周期
8	inspur(config-mspw-mspw-name-if-params)# **ethernet request-vlan-id** *<1-4094>*	配置以太请求VLAN
9	inspur(config-mspw-mspw-name-if-params)# **fr dlci-header-length** *<2-4>*	配置FR DLCI头的长度
10	inspur(config-mspw-mspw-name-if-params)# **ts-count** *<1-400>*	配置TDM仿真的时隙个数
11	inspur(config-mspw-mspw-name-if-params)# **tdm aal1 mode** {**unstructured** | **structured** | **structured-with-cas**}	配置AAL1的模式

步骤	命令	功能
12	inspur(config-mspw-mspw-name-if-params)# **tdm aal1 cells-per-packet** *<1-100>*	配置单个PW封装报文中包含的AAL1 cells的个数
13	inspur(config-mspw-mspw-name-if-params)# **tdm aal2 vad-mode** {**signal-indicated** | **by-dectection** | **always-active**}	配置AAL2的VAD（Voice Activity Detection）能力
14	inspur(config-mspw-mspw-name-if-params)# **tdm aal2 max-duration** *<1-64>*	配置AAL2的最大打包周期
15	inspur(config-mspw-mspw-name-if-params)# **tdm cas-trunk** { **e1** | **t1-esf** | **t1-sf** }	配置CAS trunk类型
16	inspur(config-mspw-mspw-name-if-params)# **tdm rtp frequency** *<1-65535>*	配置时间戳时钟的频率
17	inspur(config-mspw-mspw-name-if-params)# **tdm rtp header**	配置RTP头
18	inspur(config-mspw-mspw-name-if-params)# **tdm rtp payload-type** *<1-127>*	配置RTP头中的载荷类型
19	inspur(config-mspw-mspw-name-if-params)# **tdm rtp timestamp differential ssrc-id** *<1-4294967295>*	配置RTP差分时间戳模式，并指定同步源ID（Synchronization source ID）
20	inspur(config-mspw-mspw-name-if-params)# **tdm signaling-packets** {**non-transmitted**|**together-with-data**|**apart-from-data** {**just-here**|**over-there**}}	配置CESoPSN信令报文的传输方式
21	inspur(config-mspw-mspw-name-if-params)# **tdm sonet-sdh dba-trigger-event** {**ais** [**une**]|**une** [**ais**]}	配置PE发送DBA报文的触发事件
22	inspur(config-mspw-mspw-name-if-params)# **tdm sonet-sdh ebm-extension**	配置EMB扩展头
23	inspur(config-mspw-mspw-name-if-params)# **tdm sonet-sdh async-type** { **e3** | **t3** }	配置异步衰减类型
24	inspur(config-mspw-mspw-name-if-params)# **tdm sonet-sdh connection-type** { **spe** | **vt** | **fractional-spe** }	配置CEP连接类型。**no**命令删除该配置

对于MSPW远端接口参数配置模式下的所有命令，需要检查和对应的MSPW类型是否匹配，具体的匹配检查如下：

- **mtu***<60-9216>*：MSPW类型为除atm和tdm类型外都允许配置。
- **ethernet request-vlan-id** *<1-4094>*：MSPW类型为ethernet tagged类型才允许配置。
- **description** *<text>*：MSPW业务的各种类型都可以配置。
- **fragmentation**：MSPW业务的各种类型都可以配置。
- **fr dlci-header-length** *<2-4>*：MSPW类型为fr dlci和fr dlci-old类型才允许配置。

- **fcs-retention header-length** {**2**|**4**}：MSPW类型为HDLC、PPP和FR才允许配置，ethernet tagged和ethernet raw不允许配置。
- **atm cell-concatenate** *<1-64>*：MSPW类型为atm {port|vpc|vcc|vpc-group|vcc-group}五种才可配置。
- **ts-count** *<1-400>*：MSPW类型为tdm的均可配置：**tdm** {**aal1** | **aal2** | **satop** { **e1** | **t1** | **e3** |**t3** }| **cesopsn** { **basic** | **cas** }| **sonet-sdh** {**cesom** | **ceop**}}。
- **distribute-period** *<2-64>*：MSPW类型为tdm的均可配置：tdm { aal1 | aal2 | satop { e1 | t1 | e3 | t3 } | cesopsn { basic | cas } | sonet-sdh {cesom | ceop} }。PWE3在封信令包时，对于aal1和all2类型忽略该参数，其他tdm类型tdm { satop { e1 | t1 | e3 | t3 } | cesopsn { basic | cas } | sonet-sdh {cesom | ceop} }需要提取该参数。
- **tdm rtp header**：MSPW类型为tdm的均可配置。
- **tdm rtp timestamp differential ssrc-id** *<1-4294967295>*：MSPW类型为tdm的均可配置。PWE3在封信令包时，如果tdm rtp header没有配置，忽略该参数。
- **tdm rtp frequency** *<1-65535>*：MSPW类型为tdm的均可配置。PWE3在封信令包时，如果tdm rtp header没有配置，忽略该参数。
- **tdm rtp payload-type** *<1-127>*：MSPW类型为tdm的均可配置。PWE3在封信令包时，如果tdm rtp header没有配置，忽略该参数。
- **tdm cas-trunk** { **e1** | **t1-esf** | **t1-sf** }：MSPW类型为tdm的均可配置。PWE3在封信令包时，根据具体的类型，有选择的提取该参数。
- **tdm signaling-packets** {**non-transmitted**|**together-with-data**|**apart-from-data** {**just-here**|**over-there**}}：MSPW类型为tdm的均可配置。PWE3在封信令包时，对于CES类型的PW: **tdm** {**satop** {**e1** | **t1** | **e3** |**t3**}| **cesopsn** {**basic** | **cas**}}，选择提取该参数。
- **tdm sonet-sdh dba-trigger-event** {[**ais**],[**une**]}：MSPW类型为tdm cep的均可配置：**tdm sonet-sdh** {**cesom** | **ceop**}。
- **tdm sonet-sdh ebm-extension**：MSPW类型为tdm cep的均可配置：**tdm sonet-sdh** {**cesom** |**ceop**}。
- **tdm sonet-sdh async-type** { **e3** | **t3** }：MSPW类型为tdm cep的均可配置：**tdm sonet-sdh** {**cesom** |**ceop**}。
- **tdm sonet-sdh connection-type** { **spe** | **vt** | **fractional-spe** }：MSPW类型为tdm cep的均可配置：**tdm sonet-sdh** {**cesom** | **ceop**}。
- **tdm aal1 cells-per-packet** *<1-100>*：MSPW类型为tdm all1的可配置。
- **tdm aal1 mode** {**unstructured** | **structured** | **structured-with-cas**}：MSPW类型为tdm all1的可配置。
- **tdm aal2 max-duration** *<1-64>*：MSPW类型为tdm all2的可配置。
- **tdm aal2 vad-mode** {**signal-indicated** | **by-dectection** | **always-active**}：MSPW类型为tdm all2的可配置。

对于上述的接口参数配置和MSPW类型冲突的情况，统一用一个错误码提示："This parameter conflicts with the PW type of the MSPW instance! "。至于该参数配置支持在哪些类型的MSPW下配置，可以参考CLI中配置命令的说明描述。

4.验证配置结果。

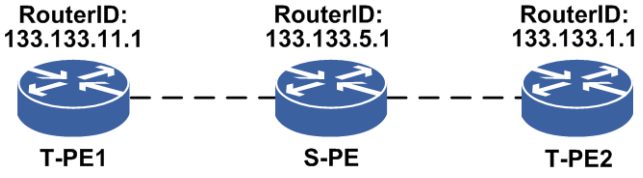
MSPW的配置结果验证与VPLS基本功能的配置结果验证相同，参见配置VPLS。

7.2.4.2 MSPW 配置实例

配置说明

如*图 7-5*所示，T-PE1、T-PE2和S-PE的LDP Route-ID分别为133.133.11.1、133.133.1.1、133.133.5.1。

图 7-5 MSPW 配置实例示意图



配置思路

1.在T-PE1与S-PE、T-PE2与S-PE之间建立LDP session，具体配置可以参见"MPLS"中的内容。

2.在S-PE上配置MSPW，在T-PE上配置普通的VPLS实例。

配置过程

T-PE1上的配置如下：

```
T-PE1(config)#pw pw1
T-PE1(config)#vpls inspur
T-PE1(config-vpls-inspur)#pseudo-wire pw1
T-PE1(config-vpls-inspur-pw-pw1)#neighbour 133.133.5.1 vcid 1
T-PE1(config-vpls-inspur-pw-pw1-neighbour)#exit
T-PE1(config-vpls-inspur)#exit
```

S-PE上的配置如下：

```
S-PE(config)#pw pw1
S-PE(config)#pw pw2
S-PE(config)#mspw inspur for ethernet raw
S-PE(config-mspw-inspur)#pseudo-wire pw1
S-PE(config-mspw-inspur-seg-pw1)#neighbour 133.133.1.1 vcid 1
S-PE(config-mspw-inspur-seg-pw1-neighbour)#signal dynamic
S-PE(config-mspw-inspur-seg-pw1-neighbour)#exit
S-PE(config-mspw-inspur-seg-pw1)#exit
```

```
S-PE(config-mspw-inspur)#pseudo-wire pw2
S-PE(config-mspw-inspur-seg-pw2)#neighbour 133.133.11.1 vcid 1
S-PE(config-mspw-inspur-seg-pw2-neighbour)#signal dynamic
S-PE(config-mspw-inspur-seg-pw2-neighbour)#exit
S-PE(config-mspw-inspur-seg-pw2)#exit
```

T-PE2上的配置如下：

```
T-PE2(config)#pw pw1
T-PE2(config)#vpls inspur
T-PE2(config-vpls-inspur)#pseudo-wire pw1
T-PE2(config-vpls-inspur-pw-pw1)#neighbour 133.133.5.1 vcid 1
T-PE2(config-vpls-inspur-pw-pw1-neighbour)#exit
T-PE2(config-vpls-inspur-pw-pw1)#exit
T-PE2(config-vpls-inspur)#exit
```

配置验证

在S-PE上使用**show pwe3 signal fec128 detail**命令查看PWE3的相关信息。

```
S-PE#show pwe3 signal fec128 detail
The detailed signal information of dynamic PWs or PW-segments:

Some signal information are referred to as follows :
   NON  - the LDP session is absent,
   UP   - the LDP session is OPERATIONAL,
   GR1  - the LDP session is reconnecting,
   GR2  - the LDP session's remote mappings are recovering,
   DOWN - not UP(or NON,or GR1,or GR2).
PW entity    : < 133.133.11.1 , 1 , ethernet >
LSPs formed  : YES
C-bits       : local       : NO        , remote     : NO
            negotiated   : NO
MTU        : local       : 1500      , remote     : 1500
            negotiated   : 1500
labels       : local       : 81923     , remote     : 83420
signal       : Configured   : YES       , Received   : YES
            Negotiated   : YES       , Sent       : YES
            AC ready     : YES
oam status   : local       : PSN rcv(0|0),snd(0|0); AC rcv(0),snd(0); Error(0)
             remote      : PSN rcv(0),snd(0); AC rcv(0),snd(0); Error(0)
redundancy   : local       : ACTIVE    , remote     : ACTIVE
             negotiated   : --
application  : service-type : MSPW      , instance-id: 2
MAC-withdraw : received    : 0         , sent       : 0
local-VCCV   : CC-type     : CW|TTL    , CV-type    : LSP
remote-VCCV  : CC-type     : CW|AL|TTL  , CV-type    : LSP
actual-VCCV  : CC-type     : TTL       , CV-type    : LSP
LDP session  : The LDP session's state is UP.
attachment-circuit : ??
local-description  : ??
remote-description : inspur

PW entity    : < 133.133.1.1 , 1 , ethernet >
LSPs formed  : YES
C-bits       : local       : NO        , remote     : NO
            negotiated   : NO
MTU        : local       : 1500      , remote     : 1500
             negotiated   : 1500
labels       : local       : 81922     , remote     : 81929
signal       : Configured   : YES       , Received   : YES
            Negotiated   : YES       , Sent       : YES
            AC ready     : YES
```

```
oam status   : local       : PSN rcv(0|0),snd(0|0); AC rcv(0),snd(0); Error(0)
               remote      : PSN rcv(0),snd(0); AC rcv(0),snd(0); Error(0)
redundancy   : local       : ??        , remote     : ??
           negotiated   : ??
application  : service-type : MSPW      , instance-id: 2
MAC-withdraw : received     : 0         , sent       : 0
local-VCCV   : CC-type      : CW|TTL    , CV-type    : LSP
remote-VCCV  : CC-type      : CW|AL|TTL , CV-type    : LSP
actual-VCCV  : CC-type      : TTL       , CV-type    : LSP
LDP session  : The LDP session's state is UP.
attachment-circuit : ??
local-description  : ??
remote-description : inspur
received-SPE-TLV   : ?
```

在S-PE上使用**show l2vpn forwardinfo vpnname**命令查看PW是否建立成功，用detail选项可以看到这条PW的内外层标签等具体信息。

```
S-PE#show l2vpn forwardinfo vpnname inspur
Headers: PWType - Pseudo Wire type and Pseudo Wire connection mode
       Llabel - Local label, Rlabel - Remote label
       VPNowner - Owner type and instance name
Codes  : H - HUB mode, S - SPOKE mode, L - VPLS, W - VPWS, M - MSPW
       MO - MONITOR, AL - Admin-VPLS, $pw - auto_pw

PWName   PeerIP      FEC  PWType  State  Llabel   Rlabel  VPNowner
pw2      133.133.11.1   128   Ethernet   UP    81923   83420   M:inspur
pw1      133.133.1.1    128   Ethernet   UP    81922   81929   M:inspur

inspur#show l2vpn forwardinfo vpnname inspur  detail
Hearders : ALLOK - Pseudowire Forwarding
         PWNF  - Pseudowire Not Forwarding
         AR    - Local AC (ingress) Receive Fault
         AT    - Local AC (egress) Transmit Fault
         PSNR  - Local PSN-facing PW (ingress) Receive Fault
         PSNT  - Local PSN-facing PW (egress) Transmit Fault
         PWFS  - Pseudowire forwarding standby
         RS    - Request switchover to this PW
         PWSA  - Pseudowire Status All Fault
Codes    : -unknown, *yes, .no
------------------------------------------------------------------------
-----

Service type and instance name:[MSPW  inspur]
  Peer IP address        : 133.133.11.1          VCID        : 1
  Connection mode        :                      VCID Extend  : 0
  Signaling protocol     : LDP                   VC type      : Ethernet
  Last status change time : 00:07:09              Create time  : 00:07:54
  MPLS VC local label    : 81922                 Remote label : 81921
  PW name              : pw2                   Control Word : -
  Related PW name        : -                     PW FRR type  : NULL
  Activation status      : ENABLE                Band Width   : 0
  VC status            : UP
  Remote status         : ALLOK
  VCCV CC type          : TTL
  VCCV CV type          : LSP
  Tunnel label          : { 3 }
  Output interface      : gei-4/1
  Imposed label stack   : { 81921 3 }

Service type and instance name:[MSPW  inspur]
  Peer IP address        : 133.133.1.1           VCID        : 1
  Connection mode        :                      VCID Extend  : 0
  Signaling protocol     : LDP                   VC type      : Ethernet
  Last status change time : 00:07:09              Create time  : 00:07:54
  MPLS VC local label    : 81921                 Remote label : 81920
  PW name              : pw1                   Control Word : -
```

```
Related PW name        : -                          PW FRR type  : NULL
Activation status      : ENABLE                      Band Width   : 0
VC status             : UP
Remote status         : ALLOK
VCCV CC type          : TTL
VCCV CV type          : LSP
Tunnel label          : { 3 }
Output interface       : smartgroup22
Imposed label stack    : { 81920 3 }
```

7.2.5 VLSS

VLSS是一种本地虚拟专线业务，主要实现L2VPN的本地交换功能，使本地成员之间互通。

在一个VLSS实例中绑定两个AC，使流量在两个AC间进行交换，即从一个AC上来的流量可以从另外一个AC转发出去。

7.2.5.1 配置 VLSS

VLSS实现本地交换功能，支持本地2个AC成员之间互通。

1.配置VLSS。

步骤	命令	功能
1	inspur(config)#**mpls l2vpn enable**	全局开启L2VPN功能
2	inspur(config)#**vlss**<*vlss-name*>	创建VLSS实例名称
3	inspur(config-vlss-name)#**description** <*string*>	配置对VLSS实例的描述
4	inspur(config-vlss-name)#**traffic-statistics** {**enable**|**disable**}	配置实例的流量统计启用
5	inspur(config-vlss)#**access-point**<*ac-interface*>	绑定接口AC的接口名 <*ac-interface*>：增加一种VLAN接入
6	inspur(config-vlss-vlss-name-ac-ac-interface)#**access-params** {**ethernet** | **fr** | **hdlc** | **ppp** | **tdm**}	配置AC的封装类型
7	inspur(config-vlss-vlss-name-ac-ac-interface-eth)#**ingress-adjust** {**push** <*1-4094*>| **rewrite** <*1-4094*>| **tag-as-payload** {**all**|**from-sublayer**}}	配置入向预处理 **push**：添加一层tag **rewrite**：改写ptag **tag-as-payload**：AC上行业务流的tag全部或部分视为载荷
8	inspur(config-vlss-vlss-name-ac-ac-interface-eth)#**traffic-statistics**{**enable**|**disable**}	配置AC流量统计启用

步骤	命令	功能
9	inspur(config-vlss-vlss-name-ac-ac-interface-eth)#**traffic-statistics threshold** [**broadcast** | **drop** | **unknown-unicast**] **input-rate** [**bps** <*1-18446744073709551615*>][**pps** <*1-4294967295*>]	配置广播流量/丢弃报文流量/未知单播流量速率告警阈值设置
10	inspur(config-vlss-vlss-name-ac-ac-interface-eth)#**monitor-ip** <*ipv4-address*>[**mac** <*mac-address*>][**echo-balance**]	配置NNI-ping功能

ethernet | fr | hdlc | ppp | tdm：VLSS实例中AC的封装类型。

2.验证配置结果。

命令	功能
inspur#**show l2vpn brief**	显示L2VPN服务实例的列表和每个实例AC和PW的绑定数量
inspur#**show l2vpn summary**	显示VPN实例的个数

7.2.5.2 VLSS 配置实例

配置说明

VLSS功能只需在单台设备本地配置即可。

以下实例描述了在一个路由器上配置一个VLSS实例的过程。在VLSS实例中绑定两个本地连接，使之互通。

配置思路

1.全局开启L2VPN功能。

2.配置VLSS实例并绑定本地连接。

配置过程

在IR12000智能路由器上的配置如下：

```
inspur(config)#mpls l2vpn enable
inspur(config)#vlss inspur
inspur(config-vlss-inspur)#description l2vpn-inspur
inspur(config-vlss-inspur)#access-point gei-1/3
inspur(config-vlss-inspur-ac-gei-1/3)#access-params ethernet
inspur(config-vlss-inspur-ac-gei-1/3-eth)#exit
```

```
inspur(config-vlss-inspur-ac-gei-1/3)#exit
inspur(config-vlss-inspur)#access-point gei-1/4
inspur(config-vlss-inspur-ac-gei-1/4)#access-params ethernet
inspur(config-vlss-inspur-ac-gei-1/4-eth)#exit
inspur(config-vlss-inspur-ac-gei-1/4)#exit
```

配置验证

用**show l2vpn brief**命令查看VLSS实例的配置情况：

```
inspur(config)#show l2vpn brief
VPLS count:0  VPWS count:0  VLSS count:1  MSPW count:0  MONITOR count:0
name              type          Default-VCID PW   AC   description
inspur              VLSS          -          0    2    l2vpn-inspur

inspur(config)#show l2vpn instance-name inspur
Name:inspur
Type:VLSS  Default-VCID:-  PW count:0  AC count:2
Kompella PW count:0
Activation Status:ENABLE
Default Cword:-
Description:l2vpn-inspur

Attachment Circuit(AC):
  InterfaceName                Client/Server
  gei-1/3                    -
  gei-1/4                    -
```

7.2.6 MC-ELAM

为了满足运营商对MPLS L2VPN的可靠性及端到端业务实时性的要求，在CE接入、PW接入、PW间链路保护三个方面均需要引入相应的保护机制。

针对CE接入方面，可以采用CE双归接入主备PE，MC-ELAM技术正是用于PE间协调主备及状态感知。

根据应用场景的不同，CE双归PE又可以分为两种，一种是在VPLS应用中的CE双归PE，另一种是在PWE3应用中的CE双归PE。

7.2.6.1 配置 MC-ELAM

本节介绍MC-ELAM的配置步骤和命令。

1.创建MC-ELAM实例。

步骤	命令	功能
1	inspur(config)#**mc-elam-configuration**	全局模式下进入MC-ELAM配置模式
2	inspur(config-mc-elam-configuration)#**mc-elam** *<id>*	创建指定的MC-ELAM实例，进入MC-ELAM实例配置模式，实例号范围为1~64

2.配置MC-ELAM实例地址。

步骤	命令	功能
1	inspur(config-mc-elam-configuration-mc-elam-instance)#**source** <*source-ip*>	配置MC-ELAM实例的源IP地址
2	inspur(config-mc-elam-configuration-mc-elam-instance)#**destination** <*destination-ip*>	配置MC-ELAM实例的目的IP地址

3.配置MC-ELAM实例属性。

步骤	命令	功能
1	inspur(config-mc-elam-configuration-mc-elam-instance)#**system-priority** <*priority-value*>	配置MC-ELAM实例的系统优先级，缺省为32768，范围1~65535
2	inspur(config-mc-elam-configuration-mc-elam-instance)#**system-mac** <*value*>	配置MC-ELAM实例的系统MAC，缺省值为系统基MAC，范围0~FFFFFFFFFFFF
3	inspur(config-mc-elam-configuration-mc-elam-instance)#**timeradvertise** <*advertise-interval*>	配置MC-ELAM实例的协议报文发送周期，时间间隔为5~100，缺省值为10，单位：100毫秒
4	inspur(config-mc-elam-configuration-mc-elam-instance)#**detect-multiplier** <*multiplier*>	配置MC-ELAM实例的协议报文超时时间倍数，范围3~180，缺省值为5
5	inspur(config-mc-elam-configuration-mc-elam-instance)#**restore** { **revertive** <*holdoff-time*>| **immediately** | **non-revertive**}	配置MC-ELAM实例的回切模式及回切时间 **immediately**为立即回切（缺省值） **non-revertive**为不回切模式
6	inspur(config-mc-elam-configuration-mc-elam-instance)#**track** <*track-name*>{ **link-type** | **peer-type** | **pw-type**}	配置MC-ELAM实例与SAMGR的联动关系 **link-type**：按Link类型处理 **peer-type**：按Peer类型处理 **pw-type**：按公网PW类型处理
7	inspur(config-mc-elam-configuration-mc-elam-instance)#**bind smartgroup** <*id*>[**mode** { **auto** | **master** | **slave** }]	配置SmartGroup关联MC-ELAM实例及其协商模式 **auto**：主备自动协商模式 **master**：主用模式 **slave**：备用模式

4.验证配置结果。

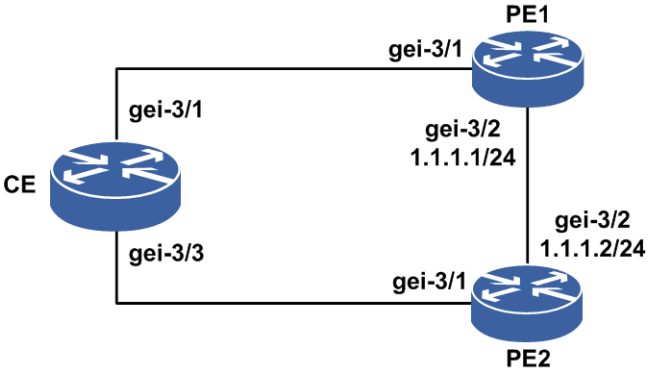
命令	功能
inspur(config)#**show mc-elam** {**all** | **brief**| **id** }	显示设备MC-ELAM实例的信息

7.2.6.2 MC-ELAM 配置实例

配置说明

如*图 7-6*所示，将CE设备上的接口gei-3/1、gei-3/3加入smartgroup1。PE1和PE2通过gei-3/2直连。

图 7-6 MC-ELAM 配置实例



配置思路

1.配置MC-ELAM实例。

2.配置MC-ELAM实例的源IP地址和目的IP地址。

3.配置MC-ELAM实例以auto模式绑定SmartGroup接口。

4.配置MC-ELAM实例的回切模式。

配置过程

CE的配置如下：

```
CE(config)#interface smartgroup1
CE(config-if-smartgroup1)#exit
CE(config)#lacp
CE(config-lacp)#interface smartgroup1
CE(config-lacp-sg-if-smartgroup1)#lacp mode 802.3ad
CE(config-lacp-sg-if-smartgroup1)#exit
CE(config-lacp)#interface gei-3/1
CE(config-lacp-member-if-gei-3/1)#smartgroup 1 mode active
CE(config-lacp-member-if-gei-3/1)#exit
CE(config-lacp)#interface gei-3/3
```

```
CE(config-lacp-member-if-gei-3/3)#smartgroup 1 mode active
CE(config-lacp-member-if-gei-3/3)#exit
CE(config-lacp)#exit
```

PE1配置如下：

```
PE1(config)#interface smartgroup1
PE1(config-if-smartgroup1)#exit
PE1(config)#lacp
PE1(config-lacp)#interface smartgroup1
PE1(config-lacp-sg-if-smartgroup1)#lacp mode 802.3ad
PE1(config-lacp-sg-if-smartgroup1)#exit
PE1(config-lacp)#interface gei-3/1
PE1(config-lacp-member-if-gei-3/1)#smartgroup 1 mode active
PE1(config-lacp-member-if-gei-3/1)#exit
PE1(config-lacp)#exit
PE1(config)#interface gei-3/2
PE1(config-if-gei-3/2)#no shutdown
PE1(config-if-gei-3/2)#ip address 1.1.1.1 255.255.255.0
PE1(config-if-gei-3/2)#exit

PE1(config)#mc-elam-configuration
PE1(config-mc-elam-configuration)#mc-elam 1
PE1(config-mc-elam-configuration-mc-elam-instance)#bind smartgroup 1 mode
auto
PE1(config-mc-elam-configuration-mc-elam-instance)#source 1.1.1.1
PE1(config-mc-elam-configuration-mc-elam-instance)#destination 1.1.1.2
PE1(config-mc-elam-configuration-mc-elam-instance)#restore immediately
PE1(config-mc-elam-configuration-mc-elam-instance)#system-priority 30000
PE1(config-mc-elam-configuration-mc-elam-instance)#end
```

PE2配置如下：

```
PE2(config)#interface smartgroup1
PE2(config-if-smartgroup1)#exit
PE2(config)#lacp
PE2(config-lacp)#interface smartgroup1
PE2(config-lacp-sg-if-smartgroup1)#lacp mode 802.3ad
PE2(config-lacp-sg-if-smartgroup1)#exit
PE2(config-lacp)#interface gei-3/1
PE2(config-lacp-member-if-gei-3/1)#smartgroup 1 mode active
PE2(config-lacp-member-if-gei-3/1)#exit
PE2(config-lacp)#exit
PE2(config)#interface gei-3/2
PE2(config-if-gei-3/2)#no shutdown
PE2(config-if-gei-3/2)#ip address 1.1.1.2 255.255.255.0
PE2(config-if-gei-3/2)#exit

PE2(config)#mc-elam-configuration
PE2(config-mc-elam-configuration)#mc-elam 1
PE2(config-mc-elam-configuration-mc-elam-instance)#bind smartgroup 1 mode
auto
PE2(config-mc-elam-configuration-mc-elam-instance)#source 1.1.1.2
PE2(config-mc-elam-configuration-mc-elam-instance)#destination 1.1.1.1
PE2(config-mc-elam-configuration-mc-elam-instance)#restore immediately
PE2(config-mc-elam-configuration-mc-elam-instance)#system-priority 40000
PE2(config-mc-elam-configuration-mc-elam-instance)#end
```

配置验证

切换之前。

用命令**show mc-elam 1**来查看PE1的配置结果：

```
PE1#show mc-elam 1
------------------------------------------------------
```

```
mcelam-instance-id      :1

destination_ip          :1.1.1.2
source_ip              :1.1.1.1
system_priority         :30000
system_mac             :0022.4432.edac
virtual_mcelam_priority  :30000
virtual_mcelam_smac     :0022.4432.edac
sm_state               :MCELAM_LINK_MS
smartgroup_id           :1
bind_mode              :MCELAM_AUTO_MODE

actor_mcelam_role       :MASTER
actor_lacp_role         :MASTER
actor_sg_admin_state     :UP
actor_sg_protocol_state  :UP
actor_revertive_mode     :MCELAM_IMMEDIATELY_MODE
revertive_time          :0
actor_adver_int         :10
actor_detect_multiplier  :5
actor_pwfault           :0

partner_mcelam_role     :SLAVE
partner_lacp_role       :SLAVE
partner_sg_protocol_state:DOWN
partner_adver_int       :10
partner_detect_multiplier:5
partner_pwfault         :0
/*查看smartgroup接口状态（没有切换之前，主上的应该是up）*/
PE1(config)#show ip int brief smartgroup1
Interface              IP-Address     Mask          Admin Phy  Prot
Smartgroup1            unassigned     unassigned     up    up   up
```

用命令**show mc-elam 1**来查看PE2的配置结果：

```
PE2#show mc 1
-------------------------------------------------------
mcelam-instance-id      :1

destination_ip          :1.1.1.1
source_ip              :1.1.1.2
system_priority         :40000
system_mac             :001e.739a.b21f
virtual_mcelam_priority  :30000
virtual_mcelam_smac     :0022.4432.edac
sm_state               :MCELAM_LINK_MS
smartgroup_id           :1
bind_mode              :MCELAM_AUTO_MODE

actor_mcelam_role       :SLAVE
actor_lacp_role         :SLAVE
actor_sg_admin_state     :UP
actor_sg_protocol_state  :DOWN
actor_revertive_mode     :MCELAM_IMMEDIATELY_MODE
revertive_time          :0
actor_adver_int         :10
actor_detect_multiplier  :5
actor_pwfault           :0

partner_mcelam_role     :MASTER
partner_lacp_role       :MASTER
partner_sg_protocol_state:UP
partner_adver_int       :10
partner_detect_multiplier:5
partner_pwfault         :0

/*查看smartgroup接口状态（没有切换之前，备上的应该是down）*/
PE2(config)#show ip int brief smartgroup1
```

```
Interface              IP-Address      Mask          Admin Phy  Prot
Smartgroup1            unassigned      unassigned      up    up   down
```

CE上查看：

```
CE(config)#show lacp 1 internal
Smartgroup:1
Flags:          * - Port is Active member Port
               S - Port is requested in Slow LACPDUs
               F - Port is requested in Fast LACPDUs
               A - Port is in Active mode
               P - Port is in Passive mode
Actor           Agg      LACPDUs  Port  Oper   Port  RX          Mux
Port[Flags]      State    Interval Pri   Key    State Machine      Machine
-------------------------------------------------------------------------
-----
gei-3/1[SA*]     ACTIVE    30      32768 0x4011 0x3d  CURRENT      COLL&DIST
gei-3/3[SA ]     INACTIVE  30      32768 0x4011 0xd   CURRENT      ATTACHED

/*PE1上与CE相接的链路发生故障断链，发生切换*/
PE1(config-if-gei-3/1)#shutdown
```

切换之后。

用命令**show mc-elam 1**来查看PE1的配置结果：

```
PE1#show mc-elam 1
------------------------------------------------------
mcelam-instance-id      :1
destination_ip          :1.1.1.2
source_ip               :1.1.1.1
system_priority         :30000
system_mac              :00d0.1234.561f
virtual_mcelam_priority  :30000
virtual_mcelam_smac     :00d0.1234.561f
sm_state                :MCELAM_LINK_MS
smartgroup_id           :1
bind_mode               :MCELAM_AUTO_MODE

actor_mcelam_role       :MASTER
actor_lacp_role         :SLAVE
actor_sg_admin_state    :UP
actor_sg_protocol_state  :DOWN
actor_revertive_mode    :MCELAM_IMMEDIATELY_MODE
revertive_time          :0
actor_adver_int         :10
actor_detect_multiplier  :5
actor_pwfault           :0

partner_mcelam_role     :SLAVE
partner_lacp_role       :MASTER
partner_sg_protocol_state:UP
partner_adver_int       :10
partner_detect_multiplier:5
partner_pwfault         :0

/*查看smartgroup接口状态：*/
PE1(config)#show ip int brief smartgroup1
Interface              IP-Address      Mask          Admin Phy  Prot
Smartgroup1            unassigned      unassigned      up    up   down
```

用命令**show mc-elam 1**来查看PE2的配置结果：

```
PE2#show mc-elam 1
------------------------------------------------------
mcelam-instance-id      :1
destination_ip          :1.1.1.1
source_ip               :1.1.1.2
system_priority         :40000
```

```
system_mac             :0023.e422.1134
virtual_mcelam_priority  :30000
virtual_mcelam_smac     :00d0.1234.561f
sm_state               :MCELAM_LINK_MS
smartgroup_id           :1
bind_mode              :MCELAM_AUTO_MODE

actor_mcelam_role       :SLAVE
actor_lacp_role         :MASTER
actor_sg_admin_state     :UP
actor_sg_protocol_state  :UP
actor_revertive_mode     :MCELAM_IMMEDIATELY_MODE
revertive_time          :0
actor_adver_int         :10
actor_detect_multiplier  :5
actor_pwfault           :0

partner_mcelam_role     :MASTER
partner_lacp_role       :SLAVE
partner_sg_protocol_state:DOWN
partner_adver_int       :10
partner_detect_multiplier:5
partner_pwfault         :0

/*查看smartgroup接口状态*/
PE2(config)#show ip int brief smartgroup1
Interface              IP-Address     Mask          Admin Phy  Prot
Smartgroup1            unassigned     unassigned     up    up   up
```

CE上查看：

```
CE(config)#show lacp 1 internal
Smartgroup:1
Flags:          * - Port is Active member Port
               S - Port is requested in Slow LACPDUs
               F - Port is requested in Fast LACPDUs
               A - Port is in Active mode
               P - Port is in Passive mode
Actor           Agg      LACPDUs  Port  Oper   Port  RX          Mux
Port[Flags]      State    Interval Pri   Key    State Machine      Machine
-------------------------------------------------------------------------------
-----
gei-3/1[ A ]    INACTIVE  30      32768 0x4011 0x45  PORT_DISABLED DETACHED
gei-3/3[SA*]    ACTIVE    30      32768 0x4011 0x3d  CURRENT       COLL&DIST
```

7.2.7 L2VPN 与 L3VPN 桥接

当在L2VPN业务需要跨过L3VPN网络时，需要在中间PE设备上终结L2VPN业务，将L2VPN业务转换为L3VPN接入。同理，L3VPN业务需要跨过L2VPN网络时，也需要在中间PE设备上终结L3VPN业务，将L3VPN业务转换为L2VPN接入。

L2VPN与L3VPN桥接原理是通过配置L2VPN与L3VPN桥接接口，完成L2VPN报文与L3VPN报文的转换与转发。

7.2.7.1 配置 L2VPN 与 L3VPN 桥接

本节介绍L2VPN与L3VPN桥接功能的配置步骤和命令。

相关信息

在IR12000智能路由器上配置L2VPN与L3VPN桥接包括以下几个步骤：

1.在PE上创建L2VPN和L3VPN实例，具体参见VPLS配置和MPLS VPN配置部分。

2.创建L2、L3桥接接口，即ulei口。

3.将L2、L3桥接接口加入到L2VPN和L3VPN实例。

1.创建L2、L3桥接接口，即ulei口。

命令	功能
inspur(config)#**request interface ulei**<*ulei-number*>	创建L2、L3桥接接口

2.配置桥接业务。

步骤	命令	功能
1	inspur(config)#**service-bridging virtual-links**	进入桥接配置模式
2	inspur(config-bridge)#**virtual-link** <*interface-name*><*interface-name*>	配置接口桥接

3.将L3桥接接口加入到L3VPN实例。

步骤	命令	功能
1	inspur(config)#**interface ulei** <*ulei-number*>	进入L3桥接接口
2	inspur(config-if-ulei-number)#**ip vrf forwarding** <*vrf-name*>	将L3桥接接口加入到L3VPN实例

4.将L2桥接接口加入到L2VPN实例。

步骤	命令	功能
1	inspur(config)#**vpls** <*instance-name*>[**multi-mac-spaces**]	配置VPLS实例
2	inspur(config-vpls-vpls-name)#**access-point ulei** <*ulei-number*>	配置接口与业务实例的绑定关系，并使其成为AC
3	inspur(config-vpls-vpls-name-ac-ulei-number)#**access-params ethernet**	配置AC的Ethernet仿真参数

5.验证配置结果。

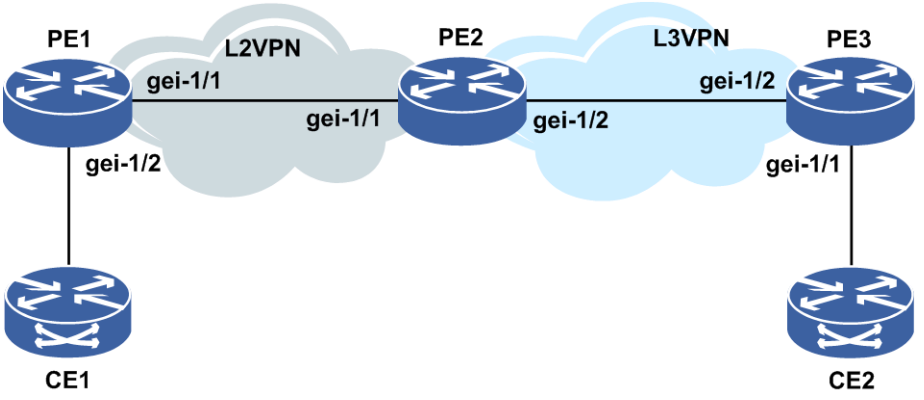
命令	功能
inspur(config)#**show arp interface** <*ulei-number*>	查看三层ulei接口是否学到ARP

7.2.7.2 L2VPN 与 L3VPN 桥接配置实例

配置说明

L2VPN与L3VPN桥接主要功能是通过配置L2、L3桥接口，实现L2VPN接入公网或L3VPN业务的功能，减少了传统接入方式的设备需求，并简化了网络结构。典型L2VPN与L3VPN桥接的组网如*图 7-7*所示。

图 7-7 L2VPN 与 L3VPN 桥接典型组网



配置思路

1.在PE1和PE2、PE2和PE3之间配置IGP路由使之互通。

2.在PE1和PE2、PE2和PE3的loopback口之间建立LDP邻居。

3.在PE1和PE2之间建立VPLS实例inspur1，同时CE1作为AC接入PE1。

4.在PE2和PE3上建立L3VPN，vrf实例名为inspur2。

5.在PE2上按如下顺序创建、配置L2、L3桥接口：封装VLAN，接入vrf inspur2，接入VPLS实例inspur1，配置IP地址。

配置过程

PE1上配置如下：

```
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
PE1(config-if-loopback1)#no shutdown
PE1(config-if-loopback1)#exit
PE1(config)#interface gei-1/1
PE1(config-if-gei-1/1)#ip address 104.110.111.1 255.255.255.0
PE1(config-if-gei-1/1)#no shutdown
PE1(config-if-gei-1/1)#exit

PE1(config)#router ospf 1
```

```
PE1(config-ospf-1)#router-id 1.1.1.1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
PE1(config-ospf-1-area-0)#network 104.110.111.0 0.0.0.255
PE1(config-ospf-1-area-0)#exit
PE1(config-ospf-1)#exit

PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#interface gei-1/1
PE1(config-ldp-1-if-gei-1/1)#exit
PE1(config-ldp-1)#exit

PE1(config)#mpls l2vpn enable
PE1(config)#pw pw1
PE1(config)#vpls inspur1
PE1(config-vpls-inspur1)#pseudo-wire pw1
PE1(config-vpls-inspur1-pw-pw1)#neighbour 1.1.1.2 vcid 100
PE1(config-vpls-inspur1-pw-pw1-neighbour)#exit
PE1(config-vpls-inspur1-pw-pw1)#exit
PE1(config-vpls-inspur1)#access-point gei-1/2
PE1(config-vpls-inspur1-ac-gei-1/2)#access-params ethernet
PE1(config-vpls-inspur1-ac-gei-1/2-eth)#end
```

PE2上配置如下：

```
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
PE2(config-if-loopback1)#no shutdown
PE2(config-if-loopback1)#exit
PE2(config)#interface gei-1/1
PE2(config-if-gei-1/1)#ip address 104.110.111.2 255.255.255.0
PE2(config-if-gei-1/1)#no shutdown
PE2(config-if-gei-1/1)#exit
PE2(config)#interface gei-1/2
PE2(config-if-gei-1/2)#ip address 104.130.131.2 255.255.255.0
PE2(config-if-gei-1/2)#no shutdown
PE2(config-if-gei-1/2)#exit

PE2(config)#router ospf 1
PE2(config-ospf-1)#router-id 1.1.1.2
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 1.1.1.2 0.0.0.0
PE2(config-ospf-1-area-0)#network 104.110.111.0 0.0.0.255
PE2(config-ospf-1-area-0)#network 104.130.131.0 0.0.0.255
PE2(config-ospf-1-area-0)#exit
PE2(config-ospf-1)#exit

PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#interface gei-1/1
PE2(config-ldp-1-if-gei-1/1)#exit
PE2(config-ldp-1)#interface gei-1/2
PE2(config-ldp-1-if-gei-1/2)#exit
PE2(config-ldp-1)#exit

PE2(config)#mpls l2vpn enable
PE2(config)#pw pw1
PE2(config)#vpls inspur1
PE2(config-vpls-inspur1)#pseudo-wire pw1
PE2(config-vpls-inspur1-pw-pw1)#neighbour 1.1.1.1 vcid 100
PE2(config-vpls-inspur1-pw-pw1-neighbour)#exit
PE2(config-vpls-inspur1-pw-pw1)#exit
PE2(config-vpls-inspur1)#exit

PE2(config)#ip vrf inspur2
PE2(config-vrf-inspur2)#rd 100:100
PE2(config-vrf-inspur2)#route-target 100:100
```

```
PE2(config-vrf-inspur2)#address-family ipv4
PE2(config-vrf-inspur2-af-ipv4)#exit
PE2(config-vrf-inspur2)#exit
```

L2、L3桥接配置在PE2上完成，配置如下：

```
PE2(config)#request interface ulei-1/1
PE2(config)#request interface ulei-1/2
PE2(config)#service-bridging virtual-links
PE2(config-bridge)#virtual-link ulei-1/1 ulei-1/2
PE2(config-bridge)#exit
PE2(config)#interface ulei-1/1
PE2(config-if-ulei-1/1)#no shutdown
PE2(config-if-ulei-1/1)#exit
PE2(config)#interface ulei-1/2
PE2(config-if-ulei-1/2)#no shutdown
PE2(config-if-ulei-1/2)#ip vrf forwarding inspur2
PE2(config-if-ulei-1/2)#exit

PE2(config)#vpls inspur1
PE2(config-vpls-inspur1)#access-point ulei-1/1
PE2(config-vpls-inspur1-ac-ulei-1/1)#access-params ethernet
PE2(config-vpls-inspur1-ac-ulei-1/1-eth)#exit
PE2(config-vpls-inspur1-ac-ulei-1/1)#exit
PE2(config-vpls-inspur1)#exit
PE2(config)#interface ulei-1/2
PE2(config-if-ulei-1/2)#ip address 10.10.10.1 255.255.255.0
PE2(config-if-ulei-1/2)#exit

PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.3 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.3 update-source loopback1
PE2(config-bgp)#address-family ipv4 vrf inspur2
PE2(config-bgp-af-ipv4-vrf)#redistribute connected
PE2(config-bgp-af-ipv4-vrf)#exit
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 1.1.1.3 activate
PE2(config-bgp-af-vpnv4)#exit
```

PE3上配置如下：

```
PE3(config)#interface loopback1
PE3(config-if-loopback1)#ip address 1.1.1.3 255.255.255.255
PE3(config-if-loopback1)#exit
PE3(config)#interface gei-1/2
PE3(config-if-gei-1/2)#ip address 104.130.131.3  255.255.255.0
PE3(config-if-gei-1/2)#exit

PE3(config)#router ospf 1
PE3(config-ospf-1)#router-id 1.1.1.3
PE3(config-ospf-1)#area 0.0.0.0
PE3(config-ospf-1-area-0)#network 1.1.1.3 0.0.0.0
PE3(config-ospf-1-area-0)#network 104.130.131.0 0.0.0.255
PE3(config-ospf-1-area-0)#exit
PE3(config-ospf-1)#exit

PE3(config)#mpls ldp instance 1
PE3(config-ldp-1)#router-id loopback1
PE3(config-ldp-1)#interface gei-1/2
PE3(config-ldp-1-if-gei-1/2)#exit
PE3(config-ldp-1)#exit

PE3(config)#ip vrf inspur2
PE3(config-vrf-inspur2)#rd 100:100
PE3(config-vrf-inspur2)#route-target 100:100
PE3(config-vrf-inspur2)#address-family ipv4
PE3(config-vrf-inspur2-af-ipv4)#exit
PE3(config-vrf-inspur2)#exit
```

```
PE3(config)#interface gei-1/1
PE3(config-if-gei-1/1)#ip vrf forwarding inspur2
PE3(config-if-gei-1/1)#ip address 20.20.20.1 255.255.255.0
PE3(config-if-gei-1/1)#exit

PE3(config)#router bgp 100
PE3(config-bgp)#neighbor 1.1.1.2 remote-as 100
PE3(config-bgp)#neighbor 1.1.1.2 update-source loopback1
PE3(config-bgp)#address-family ipv4 vrf inspur2
PE3(config-bgp-af-ipv4-vrf)#redistribute connected
PE3(config-bgp-af-ipv4-vrf)#exit
PE3(config-bgp)#address-family vpnv4
PE3(config-bgp-af-vpnv4)#neighbor 1.1.1.2 activate
PE3(config-bgp-af-vpnv4)#exit
```

配置验证

在PE2上验证配置结果：

```
inspur(config)#show running-config-interface ulei-1/2
!<pm_rm>
request interface ulei-1/2
!</pm_rm>
!<if-intf>
interface ulei-1/2
  ip vrf forwarding inspur2
  ip address 10.10.10.1    255.255.255.0
  no shutdown
$
!</if-intf>
!<bridge>
service-bridging virtual-links
  virtual-link ulei-1/1 ulei-1/2
$
!</bridge>

inspur(config)#show running-config-interface ulei-1/1
!<pm_rm>
request interface ulei-1/1
!</pm_rm>
!<if-intf>
interface ulei-1/1
  no shutdown
$
!</if-intf>
!<bridge>
service-bridging virtual-links
  virtual-link ulei-1/1 ulei-1/2
$
!</bridge>
!<l2vpn >
vpls inspur1
  access-point ulei-1/1
    access-params ethernet
    $
  $
$
!</l2vpn>

inspur(config)#show arp interface ulei-1/2

Arp protect interface is disabled
The count is 2
Address     Age     Hardware  Address Interface    Exter   Inter   Sub
                                                    VlanID  VlanID  Interface
```

```
------------------------------------------------------------------------------
--
10.10.10.1 -       1010.1111.1135    ulei-1/1      0        N/A   N/A
10.10.10.2 01:31:09 00e0.e1d0.5533    ulei-1/1      0        N/A   N/A
```

7.2.8 L2VPN FRR

VPN FRR功能主要是通过建立主备链路确保VPN流量在主链路故障时快速切换到备链路，保障VPN通信的可靠性。对于L2VPN FRR而言，其主要应用在两个网络侧PE之间的PW保护。通过PW的BFD或者VCCV检测确保二层VPN FRR的快速切换，同时通过**mac-withdraw**信令完成全网VPLS的MAC的更新。

7.2.8.1 配置 L2VPN FRR

本节介绍L2VPN FRR的配置步骤和命令。

1.全局开启L2VPN功能。

命令	功能
inspur(config)#**mpls l2vpn enable**	使能MPLS L2VPN

2.创建主、备PW。

命令	功能
inspur(config)#**pw pw**<*1-115968*>	创建PW，并配置PW的接口名，可配置的PW接口范围为1~115968

3.创建VPLS实例并进入VPLS配置模式。

命令	功能
inspur(config)#**vpls** <*name*>[**multi-mac-spaces**]	建立L2VPN的VPLS服务实例并进入VPLS配置模式

4.将当前实例绑定先前创建的PW，并指定工作在spoke模式同时进入VPLS的Spoke PW配置模式，配置主PW的邻居。

步骤	命令	功能
1	inspur(config-vpls-vpls-name)#**pseudo-wire pw**<*number*> **spoke**	将指定的PW绑定到VPLS实例中，并让其工作在spoke转发模式
2	inspur(config-vpls-name-spoke-pw-pw-number)#**neighbour** <*A.B.C.D*>[**vcid** <*VC-ID*>]	在spoke-pw下建立主用PW

<*A.B.C.D*>：远端LSRID。

5.在VPLS的Spoke PW配置模式下，绑定PW冗余管理模式，并进行冗余组类型的相关配置。

步骤	命令	功能
1	inspur(config-vpls-name-spoke-pw-pw-number)#**redundancy-manager**	Spoke-pw下绑定PW冗余组，同时进入PW冗余管理模式
2	inspur(config-vpls-name-spoke-pw-pw-number-rm)#**protect-type** {**1+1** | **1:1**}{**bidirectional** | **unidirectional**}[**receiving** {**selective** | **both**}] **protect-strategy** {**aps**}	配置PW保护类型
3	inspur(config-vpls-name-spoke-pw-pw-number-rm)#**exit**	退出PW冗余管理模式
	inspur(config-vpls-name-spoke-pw-pw-number)#**exit**	

1+1 | **1:1**：配置PW保护类型。

bidirectional | **unidirectional**：置APS协商类型，**bidirectional**为双边类型，**unidirectional**为单边类型。

selective | **both**：配置APS为选收还是双收。

6.配置备用PW，并配置备用PW的邻居。

步骤	命令	功能
1	inspur(config-vpws-vpws-name)#**backup-pw** <*pw-name*> **protect** <*pw-name*>	配置备PW绑定实例
2	inspur(config-vpws-vpws-name-protect-pw-number)#**neighbour** <*A.B.C.D*>[**vcid** <*1-4294967295*>]	配置备PW实体

<*A.B.C.D*>：远端LSRID。

7.进行APS的相关配置。

步骤	命令	功能
1	inspur(config)#**aps**	进入APS配置模式
2	inspur(config-aps)#**linear-protect**	配置线性APS实例
3	inspur(config-aps-linear-protect)#**pw-protector pw**<*1-115968*>	创建伪线保护组APS实例或者进入APS伪线保护模式
4	inspur(config-aps-linear-protect-pw-number)#**revertive-mode revertive wtr 0**	设置线性保护的保护模式
5	inspur(config-vpws-vpws-name)#**backup-pw**	配置备PW绑定实例

步骤	命令	功能
	<pw-name> **protect** *<pw-name>*	

8.在VPLS实例中配置mac-withdraw。

命令	功能
`inspur(config-vpls)#`**mac-withdraw**	配置mac-withdraw，当PW down的时候会发送mac-withdraw消息，完成全网VPLS的MAC更新

9.验证配置结果。

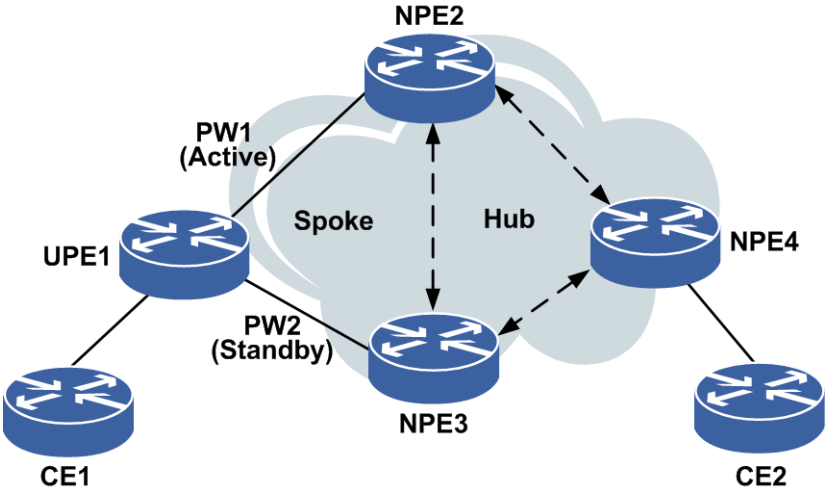
L2VPN FRR的配置结果验证与VPLS和VPWS相同，具体参见配置VPLS或配置VPWS小节。

7.2.8.2 L2VPN FRR 配置实例

配置说明

L2VPN FRR主要功能是通过建立主备PW链路确保L2VPN流量在主链路故障时快速切换到备链路，保证L2VPN通信的可靠性。其主要应用在用户侧UPE和网络侧NPE之间的Spoke-pw的保护，通过pw的检测功能确保L2VPN FRR的快速切换，同时通过Mac-withdraw信令完成全网VPLS的Mac的更新。典型VPLS FRR的组网如*图 7-8*所示。

图 7-8 VPLS FRR 典型组网



配置思路

1.在UPE1、NPE2、NPE3和NPE4之间配置IGP路由使之互通，各设备Route-ID参见下表。

设备名称	Route-ID
UPE1	1.1.1.1
NPE2	2.2.2.2
NPE3	3.3.3.3
NPE4	4.4.4.4

2.在UPE1、NPE2、NPE3和NPE4之间两两建立LDP邻居。

3.在NPE2、NPE3、NPE4之间建立VPLS实例inspur，VCID：100，PW-TYPE：ethernet-vlan，两两之间以Hub方式接入；同时CE2作为AC接入NPE4。

4.关联VPLS FRR功能，在UPE1上进入VPLS 实例配置模式，配置VPLS实例inspur相关信息和主备PW地址，即UPE1和NPE2之间的链路为主PW，UPE1和NPE3之间的链路为备PW；CE1作为AC接入UPE1。

配置过程

各路由器上IGP和LDP配置省略。

UPE1上的关联VPLS FRR配置如下：

```
UPE1(config)#mpls l2vpn enable
UPE1(config)#pw pw1
UPE1(config)#pw pw2
UPE1(config)#vpls inspur
UPE1(config-vpls-inspur)#pseudo-wire pw1 spoke
UPE1(config-vpls-inspur-spoke-pw-pw1)#neighbour 2.2.2.2 vcid 100
UPE1(config-vpls-inspur-spoke-pw-pw1-neighbour)#exit
UPE1(config-vpls-inspur-spoke-pw-pw1)#redundancy-manager
UPE1(config-vpls-inspur-spoke-pw-pw1-rm)#protect-type 1:1 unidirectional
 protect-strategy aps
UPE1(config-vpls-inspur-spoke-pw-pw1-rm)#exit
UPE1(config-vpls-inspur-spoke-pw-pw1)#exit

UPE1(config-vpls-inspur)#backup-pw pw2 protect pw1
UPE1(config-vpls-inspur-protect-pw2)#neighbour 3.3.3.3 vcid 100
UPE1(config-vpls-inspur-protect-pw2-neighbour)#control-word preferred
UPE1(config-vpls-inspur-protect-pw2-neighbour)#signal dynamic
UPE1(config-vpls-inspur-protect-pw2-neighbour)#exit
UPE1(config-vpls-inspur-protect-pw2)#exit
UPE1(config-vpls-inspur)#mac-withdraw
UPE1(config-vpls-inspur)#access-point gei-0/9
UPE1(config-vpls-inspur-ac-gei-0/9)#access-params ethernet
UPE1(config-vpls-inspur)#exit
```

NPE2上的关联VPLS FRR配置如下：

```
NPE2(config)#mpls l2vpn enable
NPE2(config)#pw pw1
NPE2(config)#vpls inspur
```

```
NPE2(config-vpls-inspur)#pseudo-wire pw1 spoke
NPE2(config-vpls-inspur-spoke-pw-pw1)#neighbour 1.1.1.1 vcid 100
NPE2(config-vpls-inspur-spoke-pw-pw1-neighbour)#exit
NPE2(config-vpls-inspur-spoke-pw-pw1)#exit
NPE2(config-vpls-inspur)#exit
```

NPE3上的关联VPLS FRR配置如下：

```
NPE3(config)#mpls l2vpn enable
NPE3(config)#pw pw1
NPE3(config)#vpls inspur
NPE3(config-vpls-inspur)#pseudo-wire pw1 spoke
NPE3(config-vpls-inspur-spoke-pw-pw1)#neighbour 1.1.1.1 vcid 100
NPE3(config-vpls-inspur-spoke-pw-pw1-neighbour)#exit
NPE3(config-vpls-inspur-spoke-pw-pw1)#exit
NPE3(config-vpls-inspur)#exit
```

配置验证

在UPE1上验证配置结果：

```
UPE1#show running-config l2vpn
!<l2vpn>
mpls l2vpn enable
vpls inspur
  access-point gei-0/9
    access-params ethernet
    $
  $
  pseudo-wire pw1 spoke
    neighbour 2.2.2.2 vcid 100
      control-word preferred
    $
    redundancy-manager
      protect-type 1:1 unidirectional protect-strategy aps
    $
  $
  backup-pw pw2 protect pw1
    neighbour 3.3.3.3 vcid 100
      control-word preferred
    $
  $
$
!</l2vpn>
```

在UPE1上查看PW建链情况：

```
UPE1#show l2vpn forwardinfo vpnname inspur
Headers: PWType - Pseudo Wire type and Pseudo Wire connection mode
        Llabel - Local label, Rlabel - Remote label
        VPNowner - Owner type and instance name
Codes  : H - HUB mode, S - SPOKE mode, L - VPLS, W - VPWS, M - MSPW, MO - MONITOR
        $pw - auto_pw

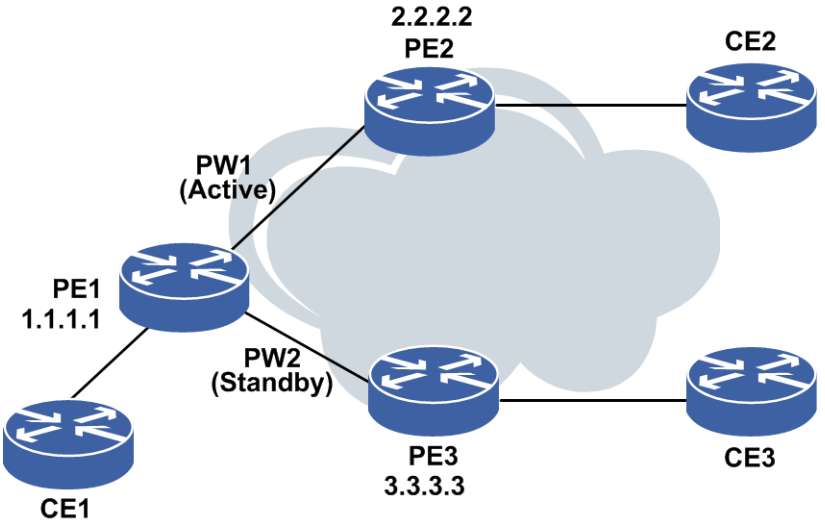
PWName   PeerIP   FEC  PWType     State  Llabel   Rlabel  VPNowner
Pw1      2.2.2.2  128  Ethernet   S UP   81921    81921   L:inspur
Pw2      3.3.3.3  128  Ethernet   S UP   81921    81921   L:inspur
```

7.2.8.3 VPWS FRR 配置实例

配置说明

VPWS FRR主要功能是通过建立主备PW链路确保L2VPN流量在主链路故障时快速切换到备链路，保证L2VPN通信的可靠性。其主要应用在PE之间的PW的保护，通过PW的检测功能确保L2VPN FRR的快速切换。典型VPWS FRR的组网如*图 7-9*所示。

图 7-9 VPWS FRR 典型组网图



配置思路

1.在PE1、PE2和PE3之间配置IGP路由使之互通，各设备Route-ID如下：

设备名称	Route-ID
PE1	1.1.1.1
PE2	2.2.2.2
PE3	3.3.3.3

2.在PE1、PE2和PE3之间两两建立LDP邻居

3.在PE1和PE2、PE1和PE3之间建立VPWS实例inspur，同时CE2作为AC接入PE2，CE3作为AC接入PE3

4.关联VPWS FRR功能，在PE1上进入VPWS实例配置模式，配置VPWS实例inspur相关信息和主备PW地址，即PE1和PE2之间的链路为主PW，PE1和PE3之间的链路为备PW；CE1作为AC接入PE1

配置过程

各设备上IGP和LDP配置省略。

PE1上的关联VPWS FRR配置如下：

```
PE1(config)#mpls l2vpn enable
PE1(config)#pw pw1
PE1(config)#pw pw2
PE1(config)#vpws inspur
PE1(config-vpws-inspur)#pseudo-wire pw1
PE1(config-vpws-inspur-pw-pw1)#neighbour 2.2.2.2 vcid 100
PE1(config-vpws-inspur-pw-pw1-neighbour)#track 1
PE1(config-vpws-inspur-pw-pw1-neighbour)#exit
PE1(config-vpws-inspur-pw-pw1)#redundancy-manager
PE1(config-vpws-inspur-pw-pw1-rm)#pfs-bits negotiate independent
PE1(config-vpws-inspur-pw-pw1-rm)#protect-type      1:1      unidirectional
protect-strategy aps
PE1(config-vpws-inspur-pw-pw1-rm)#exit
PE1(config-vpws-inspur-pw-pw1)#exit
PE1(config-vpws-inspur)#backup-pw pw2 protect pw1
PE1(config-vpws-inspur-protect-pw2)#neighbour 3.3.3.3 vcid 100
PE1(config-vpws-inspur-protect-pw2-neighbour)#control-word preferred
PE1(config-vpws-inspur-protect-pw2-neighbour)#signal dynamic
PE1(config-vpws-inspur-protect-pw2-neighbour)#exit
PE1(config-vpws-inspur-protect-pw2)#exit
PE1(config-vpws-inspur)#access-point smartgroup1
PE1(config-vpws-inspur-ac-smartgroup1)#access-params ethernet
PE1(config-vpws-inspur-ac-smartgroup1-eth)#exit
PE1(config-vpws-inspur-ac-smartgroup1)#exit
PE1(config-vpws-inspur)#exit
```

PE2上的关联VPWS FRR配置如下：

```
PE2(config)#mpls l2vpn enable
PE2(config)#pw pw1
PE2(config)#vpws inspur
PE2(config-vpws-inspur)#pseudo-wire pw1
PE2(config-vpws-inspur-spoke-pw-pw1)#neighbour 1.1.1.1 vcid 100
PE2(config-vpws-inspur-pw-pw1-neighbour)#exit
PE2(config-vpws-inspur-spoke-pw-pw1)#exit
PE2(config-vpws-inspur)#access-point smartgroup1
PE2(config-vpws-inspur-ac-smartgroup1)#access-params ethernet
PE1(config-vpws-inspur-ac-smartgroup1-eth)#exit
PE1(config-vpws-inspur-ac-smartgroup1)#exit
PE2(config-vpws-inspur)#exit
```

PE3上的关联VPWS FRR配置如下：

```
PE3(config)#mpls l2vpn enable
PE3(config)#pw pw1
PE3(config)#vpws inspur
PE3(config-vpws-inspur)#pseudo-wire pw1
PE3(config-vpws-inspur-pw-pw1)#neighbour 1.1.1.1 vcid 100
PE3(config-vpws-inspur-pw-pw1-neighbour)#control-word preferred
PE3(config-vpws-inspur-pw-pw1-neighbour)#signal dynamic
PE3(config-vpws-inspur-pw-pw1-neighbour)#exit
PE3(config-vpws-inspur-pw-pw1)#exit
PE3(config-vpws-inspur)#access-point smartgroup1
PE3(config-vpws-inspur-ac-smartgroup1)#access-params ethernet
PE3(config-vpws-inspur-ac-smartgroup1-eth)#exit
PE3(config-vpws-inspur-ac-smartgroup1)#exit
PE3(config-vpws-inspur)#exit
```

配置验证

PE1上验证配置结果：

```
PE1#show running-config l2vpn
!<l2vpn>
mpls l2vpn enable
vpws inspur
  access-point smartgroup1
    access-params ethernet
    $
  $
  pseudo-wire pw1
    neighbour 2.2.2.2 vcid 100
      track 1
    $
    redundancy-manager
      pfs-bits negotiate independent
      protect-type 1:1 unidirectional protect-strategy aps
    $
  $
  backup-pw pw2 protect pw1
    neighbour 3.3.3.3 vcid 100
      control-word preferred
    $
  $
$
!</l2vpn>
```

在PE1上查看PW建链情况：

```
PE1#show l2vpn forwardinfo vpnname inspur
Headers: PWType - Pseudo Wire type and Pseudo Wire connection mode
         Llabel - Local label, Rlabel - Remote label
         VPNowner - Owner type and instance name
Codes  : H - HUB mode, S - SPOKE mode, L - VPLS, W - VPWS, M - MSPW, MO - MONITOR
         $pw - auto_pw

PWName   PeerIP      FEC PWType     State Llabel  Rlabel  VPNowner
pw1      2.2.2.2     128 Ethernet   UP    82021   82520   W:inspur
pw2      3.3.3.3     128 Ethernet   UP    82020   81920   W:inspur
```

7.2.9 VPLS 跨域 Option C

Option C方式的跨域，是一种称作“第三种跨域”的隧道技术，其功能是使两个AS域的PE路由器之间MPLS转发可达。Option C是独立于MPLS L2VPN/MPLS L3VPN的隧道技术，但灵活组建的MPLS L2VPN/MPLS L3VPN网络可实现Option C方式的跨域。

7.2.9.1 配置 VPLS 跨域 Option C

本节介绍VPLS跨域Option C的配置步骤和命令。

1.配置VPLS跨域Option C。

VPLS跨域Option C的具体配置参见"配置VPLS"小节。

2.验证配置结果。

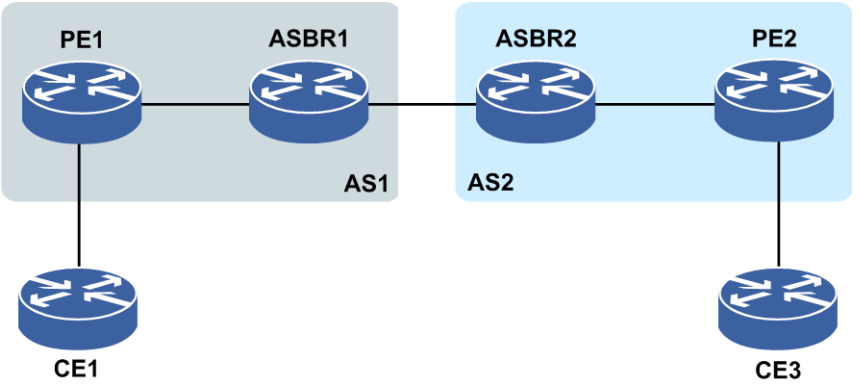
VPLS跨域Option C的配置结果验证参见"配置VPLS"小节。

7.2.9.2 VPLS 跨域 Option C 配置实例

配置说明

如*图 7-10*所示，客户的两个站点之间需要有VPN连接。但是，站点1（CE1）连接到AS1，而站点2（CE3）连接到AS2，两个站点都提供MPLS VPN。为了建立两个站点间的MPLS VPN的连接性，运用跨域OptionC的方法。

图 7-10 VPLS 跨域 Option C 配置实例示意图



配置思路

1.按*图 7-10*所示搭建环境，配置接口地址：

PE1的左接口：gei-0/2，PE1的右接口：gei-0/1 100.1.12.1/24。

ASBR1的左接口：gei-0/2 100.1.12.2/24，ASBR1的右接口：gei-0/3 100.1.23.2/24。

ASBR2的左接口：gei-0/4 100.1.23.3/24，ASBR2的右接口：gei-0/5 100.1.34.3/24。

PE2的左接口：gei-0/6 100.1.34.4/24，PE2的右接口：gei-0/2。

CE1：gei-0/2 191.1.1.1/24，CE3：gei-0/2 191.1.1.2/24。

2.每个路由器上配置一个Loopback地址，自左向右依次为100.1.5.1/32，100.1.5.2/32，100.1.5.3/32，100.1.5.4/32。

3.PE1和PE2在同一个VPN中，PE1和ASBR1处于AS100中，PE2和ASBR2处于AS200中。

4.PE与ASBR间建立IBGP邻居并且互相配置send-lable能力，PE与ASBR间建立IGP+LDP标签分发隧道。

5.ASBR间使用直连接口建立普通的EBGP邻居，并使用**network**通告PE的Loopback

地址到对端ASBR，BGP下配置到邻居的send-lable能力，并配置**route-map**，route-map配置**set mpls lable**并配置匹配前缀过滤路由，PE1与PE2间建立**ldp target-session**。

6.PE1、PE2上分别配置vpls inspur实例。

7.在CE1上ping CE3。

配置过程

PE1的配置如下：

```
PE1(config)#router ospf 10
PE1(config-ospf-10)#router-id 100.1.5.1
PE1(config-ospf-10)#area 0
PE1(config-ospf-10-area-0)#network 100.1.0.0 0.0.255.255
PE1(config-ospf-10-area-0)#exit
PE1(config-ospf-10)#exit

PE1(config)#router bgp 100
PE1(config-bgp)#no synchronization
PE1(config-bgp)#neighbor 100.1.5.2 remote-as 100
PE1(config-bgp)#neighbor 100.1.5.2 update-source loopback10
PE1(config-bgp)#neighbor 100.1.5.2 send-label
PE1(config-bgp)#exit

PE1(config)#mpls ldp  instance 1
PE1(config-ldp-1)#router-id loopback10
PE1(config-ldp-1)#target-session 100.1.5.4
PE1(config-ldp-1)#interface gei-0/1
PE1(config-ldp-1-if-gei-0/1)#exit
PE1(config-ldp-1)#exit

PE1(config)#mpls l2vpn enable
PE1(config)#pw pw1
PE1(config)#vpls inspur
PE1(config-vpls-inspur)#access-point gei-0/2
PE1(config-vpls-inspur-ac-gei-0/2)#access-params ethernet
PE1(config-vpls-inspur-ac-gei-0/2-eth)#exit
PE1(config-vpls-inspur-ac-gei-0/2)#exit
PE1(config-vpls-inspur)#pseudo-wire pw1
PE1(config-vpls-inspur-pw-pw1)#neighbour 100.1.5.4 vcid 10000
PE1(config-vpls-inspur-pw-pw1-neighbour)#exit
```

ASBR1的配置如下：

```
ASBR1(config)#router ospf 10
ASBR1(config-ospf-10)#router-id 100.1.5.2
ASBR1(config-ospf-10)#area 0
ASBR1(config-ospf-10-area-0)#network 100.1.0.0 0.0.255.255
ASBR1(config-ospf-10-area-0)#exit
ASBR1(config-ospf-10)#exit

ASBR1(config)#mpls ldp  instance 1
ASBR1(config-ldp-1)#router-id loopback10
ASBR1(config-ldp-1)#interface gei-0/2
ASBR1(config-ldp-1-if-gei-0/2)#exit
ASBR1(config-ldp-1)#access-fec bgp
ASBR1(config-ldp-1)#exit

ASBR1(config)#ipv4-access-list inspur
ASBR1(config-ipv4-acl)#rule 1 permit 100.1.5.1 0.0.0.0
ASBR1(config-ipv4-acl)#exit
ASBR1(config)#route-map inspur
```

```
ASBR1(config-route-map)#match ip address inspur
ASBR1(config-route-map)#set mpls-label
ASBR1(config-route-map)#exit

ASBR1(config)#router bgp100
ASBR1(config-bgp)#no synchronization
ASBR1(config-bgp)#neighbor 100.1.23.3 remote-as 200
ASBR1(config-bgp)#neighbor 100.1.23.3 route-map inspur out
ASBR1(config-bgp)#neighbor 100.1.23.3 send-label
ASBR1(config-bgp)#neighbor 100.1.5.1 remote-as 100
ASBR1(config-bgp)#neighbor 100.1.5.1 update-source loopback10
ASBR1(config-bgp)#neighbor 100.1.5.1 next-hop-self
ASBR1(config-bgp)#neighbor 100.1.5.1 send-label
ASBR1(config-bgp)#network 100.1.5.1 255.255.255.255
ASBR1(config-bgp)#exit
```

ASBR2的配置如下：

```
ASBR2(config)#router ospf 10
ASBR2(config-ospf-10)#router-id 100.1.5.3
ASBR2(config-ospf-10)#area 0
ASBR2(config-ospf-10-area-0)#network 100.1.0.0 0.0.255.255
ASBR2(config-ospf-10-area-0)#exit
ASBR2(config-ospf-10)#exit

ASBR2(config)#mpls ldp instance 1
ASBR2(config-ldp-1)#router-id loopback10
ASBR2(config-ldp-1)#interface gei-0/5
ASBR2(config-ldp-1-if-gei-0/5)#exit
ASBR2(config-ldp-1)#access-fec bgp
ASBR2(config-ldp-1)#exit

ASBR2(config)#ipv4-access-list inspur
ASBR2(config-ipv4-acl)#rule 1 permit 100.1.5.4 0.0.0.0
ASBR2(config-ipv4-acl)#exit
ASBR2(config)#route-map inspur
ASBR2(config-route-map)#match ip address inspur
ASBR2(config-route-map)#set mpls-label
ASBR2(config-route-map)#exit

ASBR2(config)#router bgp 200
ASBR2(config-bgp)#no synchronization
ASBR2(config-bgp)#neighbor 100.1.23.2 remote-as 100
ASBR2(config-bgp)#neighbor 100.1.23.2 route-map inspur out
ASBR2(config-bgp)#neighbor 100.1.23.2 send-label
ASBR2(config-bgp)#neighbor 100.1.5.4 remote-as 200
ASBR2(config-bgp)#neighbor 100.1.5.4 update-source loopback10
ASBR2(config-bgp)#neighbor 100.1.5.4 next-hop-self
ASBR2(config-bgp)#neighbor 100.1.5.4 send-label
ASBR2(config-bgp)#network 100.1.5.4 255.255.255.255
ASBR2(config-bgp)#exit
```

PE2的配置如下：

```
PE2(config)#router ospf 10
PE2(config-ospf-10)#router-id 100.1.5.4
PE2(config-ospf-10)#area 0
PE2(config-ospf-10-area-0)#network 100.1.0.0 0.0.255.255
PE2(config-ospf-10-area-0)#exit
PE2(config-ospf-10)#exit

PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback10
PE2(config-ldp-1)#target-session 100.1.5.1
PE2(config-ldp-1)#interface gei-0/6
PE2(config-ldp-1-if-gei-0/6)#exit
PE2(config-ldp-1)#exit

PE2(config)#router bgp 200
```

```
PE2(config-bgp)#no synchronization
PE2(config-bgp)#neighbor 100.1.5.3 remote-as 200
PE2(config-bgp)#neighbor 100.1.5.3 update-source loopback10
PE2(config-bgp)#neighbor 100.1.5.3 send-label
PE2(config-bgp)#exit

PE2(config)#mpls l2vpn enable
PE2(config)#pw pw1
PE2(config)#vpls inspur
PE2(config-vpls-inspur)#access-point gei-0/2
PE2(config-vpls-inspur-ac-gei-0/2)#access-params ethernet
PE2(config-vpls-inspur-ac-gei-0/2-eth)#exit
PE2(config-vpls-inspur-ac-gei-0/2)#exit
PE2(config-vpls-inspur)#pseudo-wire pw1
PE2(config-vpls-inspur-pw-pw1)#neighbour 100.1.5.1 vcid 10000
PE2(config-vpls-inspur-pw-pw1-neighbour)#exit
PE2(config-vpls-inspur-pw-pw1)#exit
PE2(config-vpls-inspur)#exit
```

配置验证

在PE1或PE2上使用**show l2vpn forwardinfo vpnname**命令查看PW是否建立成功，用detail选项可以看到该PW的内外层标签等具体信息。

```
PE1(config)#show l2vpn forwardinfo vpnname inspur
Headers: PWType - Pseudo Wire type and Pseudo Wire connection mode
        Llabel - Local label, Rlabel - Remote label
        VPNowner - Owner type and instance name
Codes  : H - HUB mode, S - SPOKE mode, L - VPLS, W - VPWS, M - MSPW, MO - MONITOR
        $pw - auto_pw

PWName   PeerIP    FEC  PWType   State  Llabel  Rlabel  VPNowner
pw1      100.1.5.4 128  Ethernet  H UP  81920   81920   L:inspur
PE1(config)#show l2vpn forwardinfo detail
Headers : ALLOK - Pseudowire Forwarding
          PWNF  - Pseudowire Not Forwarding
          AR    - Local AC (ingress) Receive Fault
          AT    - Local AC (egress) Transmit Fault
          PSNR  - Local PSN-facing PW (ingress) Receive Fault
          PSNT  - Local PSN-facing PW (egress) Transmit Fault
          PWFS  - Pseudowire forwarding standby
          RS    - Request switchover to this PW
          PWSA  - Pseudowire Status All Fault
Codes    : -unknown, *yes, .no
-------------------------------------------------------------------------
-----

Service type and instance name:[VPLS  inspur]
  Peer IP address        : 100.1.5.4              VCID        : 10000
  Connection mode        : HUB                   VCID Extend  : 0
  Signaling protocol     : LDP                    VC type     : Ethernet
  Last status change time : 00:00:13               Create time  : 00:00:13
  MPLS VC local label    : 81920                  Remote label : 81921
  PW name               : pw1                   Control Word : -
  Related PW name        : -                      PW FRR type  : NULL
  Activation status      : ENABLE                 Band Width   : 0
  VC status             : UP
  Remote status          : ALLOK
  VCCV CC type           : TTL
  VCCV CV type           : LSP
  Tunnel label           : { 3 }
  Output interface       : gei-0/1
  Imposed label stack    : { 81921 3 }
```

在PE1上查看到ASBR1的LDP标签信息：

```
PE1(config)#show mpls forwarding-table 100.1.5.2
Local     Outgoing  Prefix or         Outgoing          Next Hop     M/S
label      label    Tunnel Id         interface
16389      Poptag   100.1.5.2/32      gei-0/1       100.1.12.2   M
```

在PE1上查看到其他设备的BGP标签信息：

```
PE1(config)#show ip bgp labels
  Network          Next Hop        In Label/Out Label
 100.1.5.1/32       100.1.5.2       notag/nolabel
 100.1.5.2/32       100.1.5.2       213006/213024
 100.1.5.3/32       100.1.5.2       213007/213025
 100.1.5.4/32       100.1.5.2       212999/212996
```

7.3 MPLS L3VPN

MPLS L3VPN是一种基于MPLS技术的IP VPN，也就是三层VPN，是在网络路由和交换设备上应用MPLS技术，简化核心路由设备的路由选择方式，结合传统路由技术的标记交换实现的IP虚拟专用网络。

在基于IP的网络中，MPLS具有很多优点：

·降低成本

·提高资源利用率

·提高网络速度

·提高灵活性和可扩展性

·方便用户

·提高安全性

·增强业务综合能力

·MPLS的QoS保证

7.3.1 MPLS L3VPN 基本功能

MPLS L3VPN基本功能配置的主要步骤如下：

1.在PE路由器上创建VRF。

2.配置CE与PE之间运行静态路由或动态路由。

3.配置MPBGP。

4.（可选）配置MPLS L3VPN其他功能。

7.3.1.1 配置 VRF

本节介绍在PE路由器上创建VRF的步骤和命令。

相关信息

在PE上为每组VPN设定一个VRF，此VRF中仅保存本VPN相关的路由信息。每个VRF

都是互相独立的，拥有各自的接口表、路由表、标签表、路由协议等。

1.创建一个VPN实例。

命令	功能
inspur(config)#**ip vrf** < *vrf-name*>	创建一个VPN实例

2.配置VPN实例。

步骤	命令	功能
1	inspur(config-vrf-vrf-name)#**rd** <*route-distinguisher*>	定义VRF的路由标识符
2	inspur(config-vrf-vrf-name)#**address-family** {**ipv4**|**ipv6**}	激活IPv4或者IPv6地址族
3	inspur(config-vrf-vrf-name-af-ipv4)#**route-target** [**import** | **export** | **both**]<*extended-community*>	创建与VRF关联的route-target扩展团体属性

<*route-distinguisher*>：VRF的路由标识符，有三种格式如下。

- <0~65535>:<0~4294967295>
- A.B.C.D:<0~65535>
- <1-65535>.<0-65535>:<0-65535>

ipv4|**ipv6**：激活IPv4地址族或者IPv6地址族。

import：根据route-target扩展团体属性导入路由到VRF。

export：导出VRF路由携带route-target扩展团体属性。

both：等同于同时配置**import**和**export**。

<*extended-community*>：Route-target扩展团体属性，有三种格式如下。

- <0~65535>:<0~4294967295>
- A.B.C.D:<0~65535>
- <1-65535>.<0-65535>:<0-65535>

3.配置接口与VRF关联。

步骤	命令	功能
1	inspur(config)#**interface** < *interface-name*>	进入接口配置模式
2	inspur(config-if-interface-name)#**ip vrf forwarding** < *vrf-name*>	将接口与VRF关联，如果该接口预先配置了IP地址，必须删除已经配置的IP地址，再重新配置该命令
3	inspur(config-if-interface-name)#**ip**	配置接口地址

步骤	命令	功能
	address < *ip-address*>< *netmask*>	

4.验证配置结果。

命令	功能
inspur#**show ip vrf** [**brief** [<*vrf-name*>]|**detail** [<*vrf-name*>]|**summary**]	查看VRF的信息

7.3.1.2 配置 CE 与 PE 之间运行静态路由协议

本节介绍在CE与PE之间运行静态路由协议的步骤和命令。

相关信息

在CE与PE之间运行静态路由协议时，需要在PE上配置一条到CE的静态路由，并将该静态路由分发到BGP中。

1.在PE上配置一条到CE的静态路由。

命令	功能
inspur(config)#**ip route vrf** {**mng** |<*vrf-name*>}<*prefix*><*net-mask*>{<*forwarding-router's-addres*>[**global**]|<*interface-name*>[<*forwarding-router's-address*>]}[<*distance-metric*>][**metric** <*metric-value*>][**tag** <*tag-value*>][**bfd enable**][**track** <*track-name*>][**name** <*description-name*>]	在PE上配置一条到CE的静态路由，在配置时，需要指定该静态路由所属的VRF

2.在BGP VRF的地址族配置模式下重分发静态路由。

步骤	命令	功能
1	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**address-family ipv4 vrf** < *vrf-name*>	进入相应VRF的地址族配置模式
3	inspur(config-bgp-af-ipv4-vrf)#**redistribute static**	重分发静态路由

3.验证配置结果。

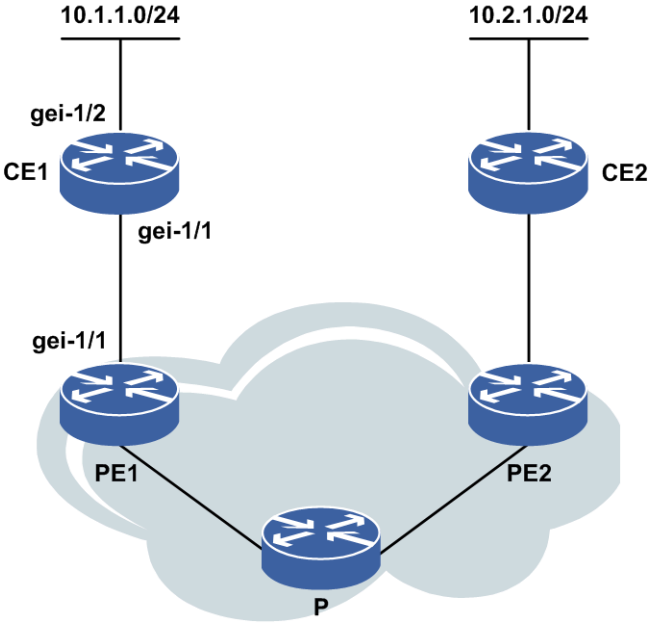
命令	功能
inspur#**show ip vrf** [**brief** [<*vrf-name*>]|**detail** [<*vrf-name*>]|**summary**]	查看VRF的信息

命令	功能
inspur#**show ip protocol routing vrf** <*vrf-name*>[**migp**]{[**network** <*ipv4-address*>|[**mask** <*ipv4-address-mask*>]]|[**all**]|[<*protocol*>]}	查看VRF协议路由表

举例

如*图 7-11*所示，要在CE1和PE1之间运行静态路由协议。

图 7-11 配置 CE 与 PE 之间运行静态路由协议



在CE1和PE1的直连接口配置同网段地址，在PE1上配置静态路由。

CE1上的配置：

```
CE1(config)#interface gei-1/1
CE1(config-if-gei-1/1)#ip address 10.1.0.1 255.255.255.252
CE1(config-if-gei-1/1)#exit
CE1(config)#interface gei-1/2
CE1(config-if-gei-1/2)#ip address 10.1.1.254 255.255.255.0
CE1(config-if-gei-1/2)#exit
CE1(config)#ip route 10.2.0.0 255.255.0.0 10.1.0.2
```

PE1上的配置：

```
PE1(config)#ip route vrf vpn_a 10.1.0.0 255.255.0.0 10.1.0.1
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf vpn_a
PE1(config-bgp-af-ipv4-vrf)#redistribute static
PE1(config-bgp-af-ipv4-vrf)#end
```

7.3.1.3 配置 CE 与 PE 之间运行 RIP 协议

本节介绍在CE与PE之间运行RIP协议的配置步骤和命令。

1.启动RIP协议。

步骤	命令	功能
1	inspur(config)#**router rip**	启动并进入RIP配置模式
2	inspur(config-rip)#**version 2**	配置RIP版本2

2.在RIP的VRF的地址族配置模式下配置RIP协议。

步骤	命令	功能
1	inspur(config-rip)#**address-family ipv4 vrf** < *vrf-name*>	进入相应VRF的地址族配置模式
2	inspur(config-rip-af)#**no auto-summary**	取消自动聚合功能
3	inspur(config-rip-af)#**version 2**	配置RIP版本2
4	inspur(config-rip-af)#**network** <*network-number*><*wild-card*>	为路由信息协议（RIP）选择路由 指定网络表
5	inspur(config-rip-af)#**redistribute connected**	重分发直连路由到RIP中
6	inspur(config-rip-af)#**redistribute bgp-int**	重分发bgp-int到RIP中

3.在BGP的VRF的地址族配置模式下重分发RIP路由。

步骤	命令	功能
1	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**address-family ipv4 vrf** < *vrf- name*>	进入相应VRF的地址族配置模式
3	inspur(config-bgp-af-ipv4-vrf)#**redistribute rip**	重分发RIP路由

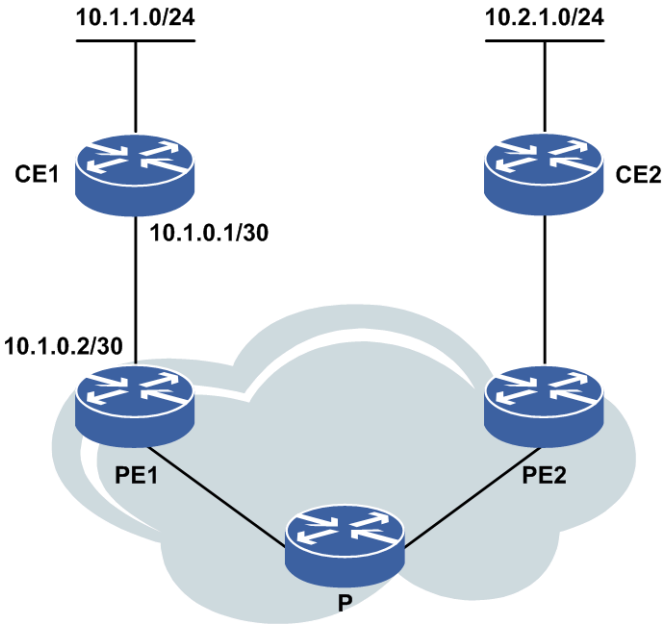
4.验证配置结果。

命令	功能
inspur#**show ip vrf** [**brief** [<*vrf-name*>]|**detail** [<*vrf-name*>]|**summary**]	查看VRF的信息
inspur#**show ip protocol routing vrf** <*vrf-name*>[**migp**]{[**network** <*ipv4-address*>|[**mask** <*ipv4-address-mask*>]]|[**all**]|[<*protocol*>]}	查看VRF协议路由表

举例

如*图 7-12*所示，要在CE1和PE1之间运行RIP协议。

图 7-12 配置 CE 和 PE 之间运行 RIP 协议



在CE1和PE1上分别启用RIP协议，在PE1上的rip vrf和bgp vrf中互相分发路由信息。

CE1上的配置如下：

```
CE1(config)#router rip
CE1(config-rip)#no auto-summary
CE1(config-rip)#version 2
CE1(config-rip)#network 10.1.0.0 0.0.0.3
CE1(config-rip)#redistribute connected
CE1(config-rip)#exit
```

PE1上的配置如下：

```
PE1(config)#router rip
PE1(config-rip)#version 2
PE1(config-rip)#address-family ipv4 vrf vpn_a
PE1(config-rip-af)#no auto-summary
PE1(config-rip-af)#version 2
PE1(config-rip-af)#network 10.1.0.0 0.0.0.3
PE1(config-rip-af)#redistribute bgp-int
PE1(config-rip-af)#exit
PE1(config-rip)#exit

PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf vpn_a
PE1(config-bgp-af-ipv4-vrf)#redistribute rip
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#exit
```

7.3.1.4 配置 CE 与 PE 之间运行 OSPF 协议

本节描述了CE与PE之间运行OSPF协议的配置步骤和命令。

1.启动并配置OSPF。

步骤	命令	功能

步骤	命令	功能
1	inspur(config)#**router ospf** < *process-id*>[**vrf** < *vrf-name*>]	启动并进入OSPF VRF配置模式
2	inspur(config-ospf-process-id)#**area** < *area-id*>	定义OSPF协议运行的接口以及对这些接口定义区域ID
	inspur(config-ospf-process-id-area-id)#**network**<*network-number*>< *wild-card*>	
3	inspur(config-ospf-process-id)#**redistribute bgp-int**	重分发bgp-int路由

2.在BGP的VRF的地址族配置模式下重分发OSPF路由。

步骤	命令	功能
1	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**address-family ipv4 vrf** < *vrf-name*>	进入相应VRF的地址族配置模式
3	inspur(config-bgp-af-ipv4-vrf)#**redistribute** {**ospf-int** | **ospf-ext**}<*process-id*>	重分发ospf-int或者ospf-ext路由

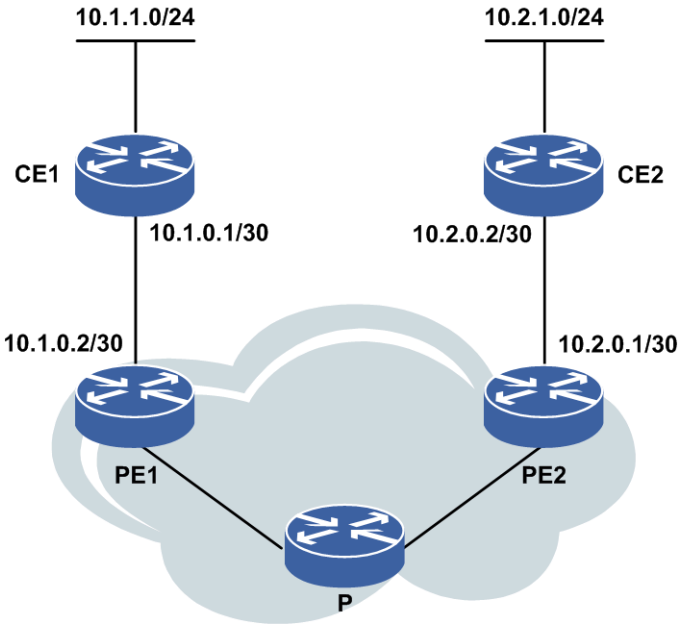
3.验证配置结果。

命令	功能
inspur#**show ip vrf** [**brief** [<*vrf-name*>]|**detail** [<*vrf-name*>]|**summary**]	查看VRF的信息
inspur#**show ip protocol routing vrf** <*vrf-name*>[**migp**]{[**network** <*ipv4-address*>|[**mask** <*ipv4-address-mask*>]]|[**all**]|[<*protocol*>]}	查看VRF协议路由表

举例

如*图 7-13*所示，要在CE1和PE1上分别启用OSPF协议，互相分发路由信息。

图 7-13 *配置 CE 与 PE 之间运行 OSPF 协议*



CE1上的配置如下：

```
CE1(config)#router ospf 1
CE1(config-ospf-1)#area 0
CE1(config-ospf-1-area-0)#network 10.1.0.0 0.0.0.3
CE1(config-ospf-1-area-0)#network 10.1.1.0 0.0.0.255
CE1(config-ospf-1-area-0)#exit
```

PE1上的配置如下：

```
PE1(config)#router ospf 2 vrf vpn_a
PE1(config-ospf-2)#area 0
PE1(config-ospf-2-area-0)#network 10.1.0.0 0.0.0.3
PE1(config-ospf-2-area-0)#exit
PE1(config-ospf-2)#redistribute bgp-int
PE1(config-ospf-2)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf vpn_a
PE1(config-bgp-af-ipv4-vrf)#redistribute ospf-int 2
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#exit
```

7.3.1.5 配置 CE 与 PE 之间运行 IS-IS 协议

本节描述了CE与PE之间运行IS-IS协议的配置步骤和命令。

1.启动并配置IS-IS。

步骤	命令	功能
1	inspur(config)#**router isis**< *process-id*>[**vrf** < *vrf-name*>]	启动并进入IS-IS vrf配置模式
2	inspur(config-isis-process-id)#**area** <*area-address*>	定义IS-IS协议区域地址

步骤	命令	功能
3	inspur(config-isis-process-id)#**system-id** <*system-id*>	定义IS-IS协议系统ID
4	inspur(config-isis-process-id)#**interface** <*interface-name*>	定义运行IS-IS协议的接口
5	inspur(config-isis-process-id)#**redistribute bgp**	重分发IS-IS路由

2.在BGP的VRF的地址族配置模式下重分发IS-IS路由。

步骤	命令	功能
1	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**address-family ipv4 vrf** < *vrf-name*>	进入相应VRF的地址族配置模式
3	inspur(config-bgp-af-ipv4-vrf)#**redistribute** {**isis-1** |**isis-1-2**|**isis-2**}<*process-id*>	重分发IS-IS路由

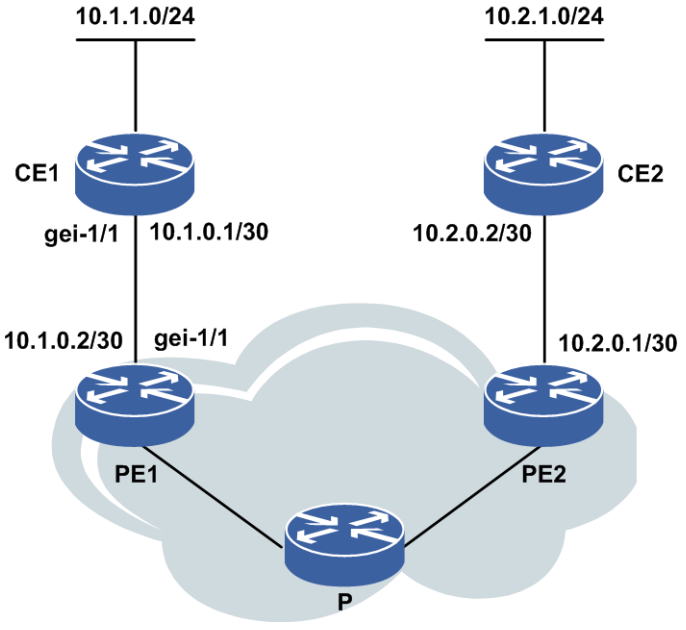
3.验证配置结果。

命令	功能
inspur#**show ip vrf** [**brief** [<*vrf-name*>]|**detail** [<*vrf-name*>]|**summary**]	查看VRF的信息
inspur#**show ip protocol routing vrf** <*vrf-name*>[**network** <*ip-address*>[**mask** <*net-mask*>]]	查看VRF协议路由表

举例

如*图 7-14*所示，要在CE1和PE1上分别启用IS-IS协议，互相分发路由信息。

图 7-14 配置 CE 与 PE 之间运行 IS-IS 协议



CE1上的配置如下：

```
CE1(config)#router isis 1
CE1(config-isis-1)#area 01
CE1(config-isis-1)#system-id 0121.4567.8956
CE1(config-isis-1)#exit
CE1(config)#interface gei-1/1
CE1(config-if-gei-1/1)#no shutdown
CE1(config-if-gei-1/1)#ip address 10.1.0.1/30
CE1(config-if-gei-1/1)#exit
CE1(config)#router isis 1
CE1(config-isis-1)#interface gei-1/1
CE1(config-isis-1-if-gei-1/1)ip router isis
CE1(config-isis-1-if-gei-1/1)#end
```

PE1上的配置如下：

```
PE1(config)#router isis 2 vrf vpn_a
PE1(config-isis-2)#area 02
PE1(config-isis-2)#system-id0181.4857.8969
PE1(config-isis-2)#redistribute bgp
PE1(config-isis-2)#exit
PE1(config)#interface gei-1/1
PE1(config-if-gei-1/1)#no shutdown
PE1(config-if-gei-1/1)#ip address 10.1.0.2/30
PE1(config-if-gei-1/1)#exit
PE1(config)#router isis 2
PE1(config-isis-2)#interface gei-1/1
PE1(config-isis-2-if-gei-1/1)ip router isis
PE1(config-isis-2-if-gei-1/1)#end
PE1#configure terminal
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf vpn_b
PE1(config-bgp-af-ipv4-vrf)#redistribute isis-2 2
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#exit
```

7.3.1.6 配置 CE 与 PE 之间运行 EBGP 协议

本节介绍CE与PE之间运行EBGP协议的配置步骤和命令。

1.配置在CE与PE之间运行EBGP协议。

步骤	命令	功能
1	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**address-family ipv4 vrf** < *vrf-name*>	进入相应VRF的地址族配置模式
3	inspur(config-bgp-af-ipv4-vrf)#**neighbor** < *ip-address*> **remote-as** <*as-number*>	配置一个EBGP邻居或配置一个邻居对等体组的自治系统号

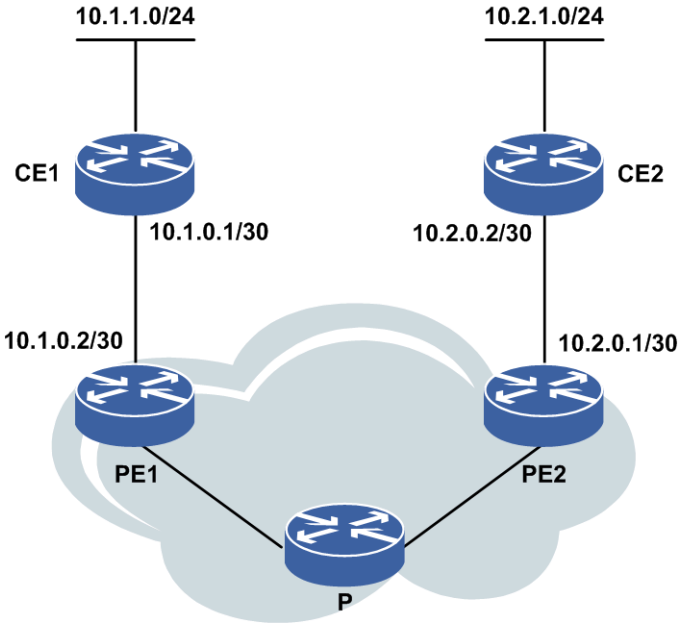
2.验证配置结果。

命令	功能
inspur#**show ip vrf** [**brief** [<*vrf-name*>]|**detail** [<*vrf-name*>]|**summary**]	查看VRF的信息
inspur#**show ip protocol routing vrf** <*vrf-name*>[**migp**]{[**network** <*ipv4-address*>|[**mask** <*ipv4-address-mask*>]]|[**all**]|[<*protocol*>]}	查看VRF协议路由表
inspur#**show ip forwarding route vrf** <*vrf-name*>{[{<*Network to display information*>}[<*Network mask*>{**weak-match**|**exact-match**}]]|[<*Protocol name*>]}	查看VRF转发路由表

举例

如*图 7-15*所示，要在CE1和PE1之间运行EBGP协议。

图 7-15 配置 CE 和 PE 之间运行 EBGP 协议



分别在CE1和PE1上配置BGP协议，互相分发路由信息。

CE1上的配置：

```
CE1(config)#router bgp 65001
CE1(config-bgp)#neighbor 10.1.0.2 remote-as 100
CE1(config-bgp)#neighbor 10.1.0.2 activate
CE1(config-bgp)#redistribute connected
CE1(config-bgp)#exit
```

PE1上的配置：

```
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf vpn_a
PE1(config-bgp-af-ipv4-vrf)#neighbor 10.1.0.1 remote-as 65001
PE1(config-bgp-af-ipv4-vrf)#neighbor 10.1.0.1 activate
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#end
```

7.3.1.7 配置 MPBGP 协议

本节介绍了MPBGP协议的配置步骤和命令。

1.配置BGP邻居。

步骤	命令	功能
1	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**neighbor** <*ip-address*> **remote-as** <*as-number*>	配置BGP邻居
3	inspur(config-bgp)#**neighbor** <*ip-address*> **update-source** <*interface-name*>	指定路由更新的源地址为自己的MPBGP建链使用的loopback地址

2.激活邻居的VPNv4能力。

步骤	命令	功能
1	inspur(config-bgp)#**address-family vpnv4**	进入VPNv4地址族配置模式
2	inspur(config-bgp-af-vpnv4)#**neighbor** <*ip-address*> **activate**	激活邻居的VPNv4能力

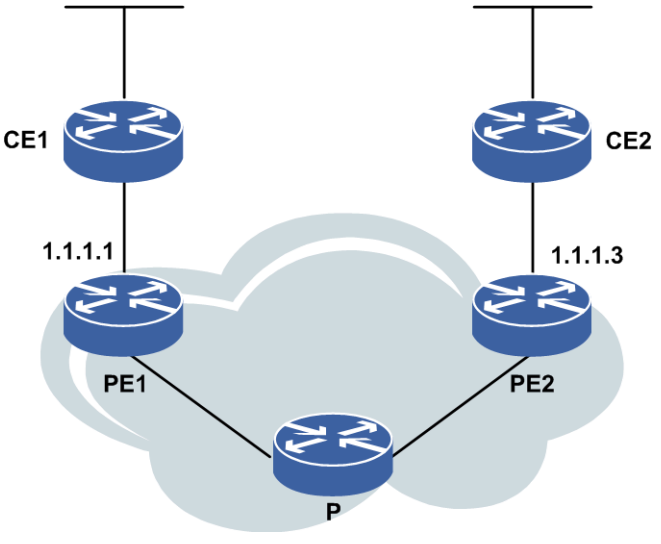
3.验证配置结果。

命令	功能
inspur#**ping vrf** <*vrf-name*><*ip-address*>	检查网络连通性
inspur#**show ip vrf** [**brief** [<*vrf-name*>]|**detail** [<*vrf-name*>]|**summary**]	查看VRF的信息
inspur#**show ip protocol routing vrf** <*vrf-name*>[**migp**]{[**network** <*ipv4-address*>|[**mask** <*ipv4-address-mask*>]]|[**all**]|[<*protocol*>]	查看VRF协议路由表
inspur#**show ip forwarding route vrf** <*vrf-name*>{[{<*Network to display informatio*>}[<*Network mask*>{**weak-match**|**exact-match**}]]|[<*Protocol name*>]}	查看VRF转发路由表
inspur#**show bgp vpnv4 unicast summary**	查看MPBGP邻居概要信息

举例

如*图 7-16*所示，要在PE1和PE2之间运行MPBGP协议。

图 7-16 配置 MPBGP 协议



PE1上的配置如下：

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 1.1.1.3 remote-as 100
PE1(config-bgp)#neighbor 1.1.1.3 activate
PE1(config-bgp)#neighbor 1.1.1.3 update-source loopback1
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 1.1.1.3 activate
PE1(config-bgp-af-vpnv4)#end
```

PE2上的配置如下：

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.1 activate
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback1
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 1.1.1.1 activate
PE2(config-bgp-af-vpnv4)#end
```

注意：

这里需要事先确保PE1和PE2上loopback地址能够相互ping通。

7.3.1.8 配置 MPLS L3VPN 其他功能

配置AS覆盖

当PE和CE之间运行BGP时，客户可能希望在不同的站点内重用AS号。为了提供CE1和CE2之间的连通性，可以实施一种叫AS覆盖的新方法。当在PE上配置了AS覆盖后，在向CE发送路由更新之前，PE就把整个AS_PATH中每一个直连的CE设备AS号替换成自己的AS号。使用AS覆盖时还保留了AS_PATH的长度。

配置AS覆盖的命令如下。

步骤	命令	功能
1	inspur(config)#**router bgp** <*as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**address-family ipv4 vrf** < *vrf-name*>	进入IPv4 vrf地址族配置模式
3	inspur(config-bgp-af-ipv4-vrf)#**neighbor** <*neighbor-address*> **as-override**	把整个AS_PATH中每一个直连的CE设备AS号替换成自己的AS号

配置Export Map和Import Map

Export Map和import Map的含义如下：

·Import Map

通过对导入VRF的路由进行过滤（import map），VRF中可以只存储自己关心的路由前缀。

·Export Map

使用export map 给路由前缀设置不同的RT ，不同的VRF可以选择接受不同RT的前缀。

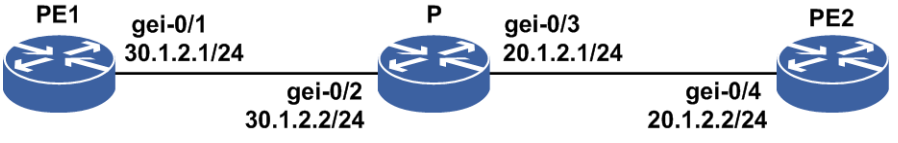
Export Map和import Map的配置命令如下：

步骤	命令	功能
1	inspur(config)#**ip vrf** <*vrf-name*>	配置一个VPN实例，并进入VPN实例配置模式
2	inspur(config-vrf-vrf-name)#**address-family** {**ipv4**|**ipv6**}	激活IPv4或者IPv6地址族
3	inspur(config-vrf-vrf-name-af-ipv4)#**export map** < *route-map-name*>	配置与VRF关联的导出路由映射，路由映射名称长度为1~31个字符
	inspur(config-vrf-vrf-name-af-ipv4)#**import map** < *route-map-name*>	配置与VRF关联的导入路由映射，路由映射名称长度为1~31个字符

举例

下面介绍一下RR反射器的配置实例。如*图 7-17*所示，P作为路由反射器RR，PE1的loopback1 地 址 为 61.139.36.34/32 ， PE2 的 loopback1 地 址 为 61.139.36.35/32 ， P 的loopback1地址为61.139.36.31/32。

图 7-17 RR 反射器的配置实例拓扑图



配置要求：

•通过OSPF协议使得各自能学到对端的loopback地址，PE1、PE2和RR之间建立LDP邻居。

•RR反射器分别和PE1、PE2建立MP-IBGP邻居，PE1、PE2为RR的客户端，Loopback地址作为BGP的建链地址。

•PE1、PE2上都配置vrf ok，两边配置一样的RD和RT。

RR反射器分别与PE1和PE2建立MP-IBGP，PE1和PE2都是RR的客户端，在PE1和PE2上分别在私网内通告一个loopback接口形成的直连路由。配置结果是PE能学到对端PE的私网loopback路由，此路由的下一跳是对端PE和RR建立igp邻居的直连地址。

RR（P）的配置如下：

```
P(config)#router bgp 65190
P(config-bgp)#no bgp default route-target filter
P(config-bgp)#neighbor 61.139.36.34 remote-as 65190
P(config-bgp)#neighbor 61.139.36.34 update-source loopback1
P(config-bgp)#neighbor 61.139.36.35 remote-as 65190
P(config-bgp)#neighbor 61.139.36.35 update-source loopback1
P(config-bgp)#address-family vpnv4
P(config-bgp-af-vpnv4)#neighbor 61.139.36.34 active
```

```
P(config-bgp-af-vpnv4)#neighbor 61.139.36.35 active
P(config-bgp-af-vpnv4)#neighbor 61.139.36.34 route-reflector-client
P(config-bgp-af-vpnv4)#neighbor 61.139.36.35 route-reflector-client
P(config-bgp-af-vpnv4)#end
```

PE1上的配置如下：

```
PE1(config)#ip vrf ok
PE1(config-vrf-ok)#rd 1:1
PE1(config-vrf-ok)#address-family ipv4
PE1(config-vrf-ok-af-ipv4)#route-target 1:1
PE1(config-vrf-ok-af-ipv4)#exit
PE1(config-vrf-ok)#exit

PE1(config)#router bgp 65190
PE1(config-bgp)#neighbor 61.139.36.31  remote-as 65190
PE1(config-bgp)#neighbor 61.139.36.31 update-source loopback1
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 61.139.36.31 active
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#exit

PE1(config)#interface loopback10
PE1(config-if-loopback10)#ip vrf forwarding ok
PE1(config-if-loopback10)#ip address 10.10.10.10 255.255.0.0
PE1(config-if)#exit

PE1(config)#router bgp 65190
PE1(config-bgp)#address-family ipv4 vrf ok
PE1(config-bgp-af-vpnv4)#redistribute connected
PE1(config-bgp-af-vpnv4)#end
```

PE2上的配置如下：

```
PE2(config)#ip vrf ok
PE2(config-vrf-ok)#rd 1:1
PE2(config-vrf-ok)#address-family ipv4
PE2(config-vrf-ok-af-ipv4)#route-target 1:1
PE2(config-vrf-ok-af-ipv4)#exit
PE2(config-vrf-ok)#exit

PE2(config)#router bgp 65190
PE2(config-bgp)#neighbor 61.139.36.31  remote-as 65190
PE2(config-bgp)#neighbor 61.139.36.31 update-source loopback1
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 61.139.36.31 active
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#exit

PE2(config)#interface loopback20
PE2(config-if-loopback20)#ip vrf forwarding ok
PE2(config-if-loopback20)#ip address 20.20.20.20 255.255.0.0
PE2(config-if-loopback20)#exit

PE2(config)#router bgp 65190
PE2(config-bgp)#address-family ipv4 vrf ok
PE2(config-bgp-af-vpnv4)#redistribute connected
PE2(config-bgp-af-vpnv4)#end
```

在PE1上查看PE2传来的路由：

```
PE1#show ip protocol routing vrf ok
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
```

```
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale
Dest              NextHop     Intag    Outtag   RtPrf    Protocol
*>20.20.0.0/16     20.1.2.2    163898   34       200      BGP-INT
```

在PE2上查看PE1传来的路由：

```
PE2#show ip protocol routing vrf ok
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale
Dest              NextHop     Intag    Outtag   RtPrf    Protocol
*>10.10.0.0/16     30.1.2.1    164963   163863   200      BGP-INT
```

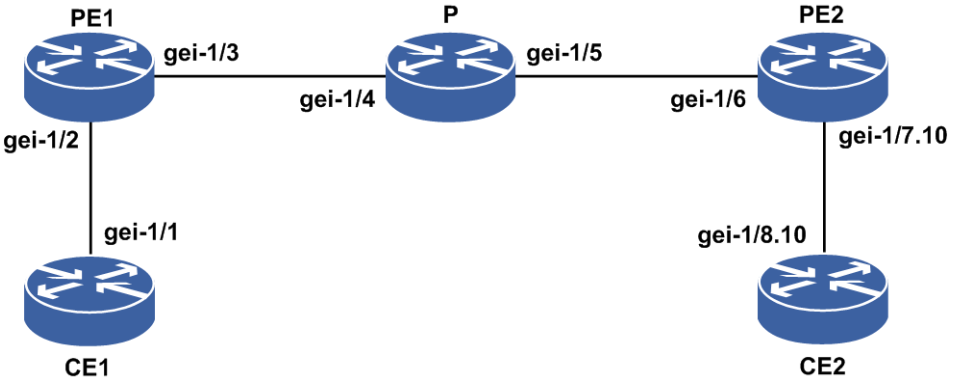
7.3.1.9 MPLS L3VPN 的基本配置实例

配置说明

如*图 7-18*所示，CE1和CE2在同一个VPN中，CE1的loopback地址为100.1.1.1/24，CE2的loopback地址为200.1.1.1/24。

要求进行适当的VPN配置，通过路由协议OSPF，使得CE1和CE2能够互相学习到对端的loopback路由。CE1与PE1之间运行BGP协议，CE2与PE2之间运行OSPF协议，使得CE1与CE2能够互相学到对方的路由，可以ping通。

图 7-18 MPLS L3VPN 基本配置拓扑图



图中各个接口的地址规划如*表 7-1*所示。

表 7-1 MPLS L3VPN 基本配置地址规划表

设备	接口名	地址
CE1	gei-1/1	10.1.1.2/24
PE1	gei-1/2	10.1.1.1/24
	gei-1/3	10.10.12.1/24

设备	接口名	地址
P	gei-1/4	10.10.12.2/24
	gei-1/5	10.10.23.2/24
PE2	gei-1/6	10.10.23.3/24
	gei-1/7.10	10.10.10.1/24
CE2	gei-1/8.10	10.10.10.2/24

配置思路

1.在CE1上配置loopback1和接口的地址，与PE1建立EBGP邻居，并将loopback在BGP中通告。

2.在PE1上配置loopback1、gei-1/3的地址，配置vrf test1，将gei-1/2绑定在vrf test1中并配置地址；配置OSPF，通告10.0.0.0/8这个网段；与PE2起MPBGP邻居，并使能VPNv4的能力，与CE1建立EBGP邻居；接口gei-1/3起LDP，指定loopback1为LDP的router-id。

3.在P上配置gei-1/4和gei-1/5的地址；配置OSPF，通告10.0.0.0/8这个网段；接口gei-1/4和gei-1/5起LDP，配置loopback1，并指定loopback1为LDP的router-id。

4.在PE2上配置loopback1、gei-1/6的地址，配置vrf test1，将子接口gei-1/7.10绑定在vrf test1中并配置地址；配置OSPF，通告10.0.0.0/8这个网段；与PE1起MPBGP邻居，并使能VPNv4的能力，与CE2建立OSPF邻居；接口gei-1/6起LDP。

5.在CE2上配置loopback1和子接口gei-1/8.10的地址，配置OSPF，通告10.10.10.2和loopback200.1.1.1。

配置过程

CE1上的配置如下：

```
CE1(config)#interface loopback1
CE1(config-if-loopback1)#ip address 100.1.1.1 255.255.255.0
CE1(config-if-loopback1)#exit
CE1(config)#interface gei-1/1
CE1(config-if-gei-1/1)#no shutdown
CE1(config-if-gei-1/1)#ip address 10.1.1.2 255.255.255.0
CE1(config-if-gei-1/1)#exit

CE1(config)#router bgp 200
CE1(config-bgp)#network 100.1.1.0 255.255.255.0
CE1(config-bgp)#neighbor 10.1.1.1 remote-as 100
CE1(config-bgp)#exit
```

PE1上的配置如下：

```
PE1(config)#ip vrf test1
PE1(config-vrf-test1)#rd 100:1
PE1(config-vrf-test1)#address-family ipv4
PE1(config-vrf-test1-af-ipv4)#route-target import 100:1
PE1(config-vrf-test1-af-ipv4)#route-target export 100:1
PE1(config-vrf-test1-af-ipv4)#exit
PE1(config-vrf-test1)#exit
```

```
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 10.10.1.1 255.255.255.255
PE1(config-if-loopback1)#exit
PE1(config)#interface gei-1/3
PE1(config-if-gei-1/3)#no shutdown
PE1(config-if-gei-1/3)#ip address 10.10.12.1 255.255.255.0
PE1(config-if-gei-1/3)#exit

PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#route-id loopback1
PE1(config-ldp-1)#interface gei-1/3
PE1(config-ldp-1-if-gei-1/3)#exit
PE1(config-ldp-1)#exit

PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#ip vrf forwarding test1
PE1(config-if-gei-1/2)#ip address 10.1.1.1 255.255.255.0
PE1(config-if-gei-1/2)#exit

PE1(config)#router ospf 1
PE1(config-ospf-1)#router-id 10.10.1.1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 10.0.0.0 0.255.255.255
PE1(config-ospf-1-area-0)#exit
PE1(config-ospf-1)#exit

PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 10.10.3.3 remote-as 200
PE1(config-bgp)#neighbor 10.10.3.3 update-source loopback1
PE1(config-bgp)#address-family ipv4 vrf test1
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#neighbor 10.1.1.2 remote-as 200
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 10.10.3.3 activate
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#exit
```

P上的配置如下：

```
P(config)#interface gei-1/4
P(config-if-gei-1/4)#no shutdown
P(config-if-gei-1/4)#ip address 10.10.12.2 255.255.255.0
P(config-if-gei-1/4)#exit

P(config)#interface gei-1/5
P(config-if-gei-1/5)#no shutdown
P(config-if-gei-1/5)#ip address 10.10.23.2 255.255.255.0
P(config-if-gei-1/5)#exit

P(config)#interface loopback1
P(config-if-loopback1)#ip address 10.10.2.2 255.255.255.255
P(config-if-loopback1)#exit

P(config)#mpls ldp instance 1
P(config-ldp-1)#router-id loopback1
P(config-ldp-1)#interface gei-1/4
P(config-ldp-1-if-gei-1/4)#exit
P(config-ldp-1)#interface gei-1/5
P(config-ldp-1-if-gei-1/5)#exit
P(config-ldp-1)#exit

P(config)#router ospf 1
P(config-ospf-1)#router-id 10.10.2.2
P(config-ospf-1)#area 0
P(config-ospf-1-area-0)#network 10.0.0.0 0.255.255.255
P(config-ospf-1-area-0)#exit
```

```
P(config-ospf-1)#exit
```

PE2上的配置（这里使用了以太网子接口与CE2连接）：

```
PE2(config)#ip vrf test1
PE2(config-vrf-test1)#rd 100:1
PE2(config-vrf-test1)#address-family ipv4
PE2(config-vrf-test1-af-ipv4)#route-target import 100:1
PE2(config-vrf-test1-af-ipv4)#route-target export 100:1
PE2(config-vrf-test1-af-ipv4)#exit
PE2(config-vrf-test1)#exit

PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 10.10.3.3 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#interface gei-1/6
PE2(config-if-gei-1/6)#no shutdown
PE2(config-if-gei-1/6)#ip address 10.10.23.3 255.255.255.0
PE2(config-if-gei-1/6)#exit

PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#interface gei-1/6
PE2(config-ldp-1-if-gei-1/6)#exit
PE2(config-ldp-1)#exit

PE2(config)#interface gei-1/7.10
PE2(config-if-gei-1/7.10)#exit

PE2(config)#vlan-configuration
PE2(config-vlan)#interface gei-1/7.10
PE2(config-vlan-if-gei-1/7.10)#encapsulation-dot1q 10
PE2(config-vlan-if-gei-1/7.10)#exit
PE2(config-vlan)#exit

PE2(config)#interface gei-1/7.10
PE2(config-if-gei-1/7.10)#ip vrf forwarding test1
PE2(config-if-gei-1/7.10)#ip address 10.10.10.1 255.255.255.0
PE2(config-if-gei-1/7.10)#exit

PE2(config)#router ospf 1
PE2(config-ospf-1)#router-id 10.10.3.3
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 10.0.0.0 0.255.255.255
PE2(config-ospf-1-area-0)#exit
PE2(config-ospf-1)#exit

PE2(config)#router ospf 2 vrf test1
PE2(config-ospf-2)#area 0
PE2(config-ospf-2-area-0)#network 10.10.10.1 0.0.0.0
PE2(config-ospf-2-area-0)#exit
PE2(config-ospf-2)#redistribute bgp-int
PE2(config-ospf-2)#exit

PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 10.10.1.1 remote-as 100
PE2(config-bgp)#neighbor 10.10.1.1 update-source loopback1
PE2(config-bgp)#address-family ipv4 vrf test1
PE2(config-bgp-af-ipv4-vrf)#redistribute ospf-int 2
PE2(config-bgp-af-ipv4-vrf)#redistribute connected
PE2(config-bgp-af-ipv4-vrf)#exit
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 10.10.1.1 activate
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#exit
```

CE2上的配置如下：

```
CE2(config)#interface loopback1
```

```
CE2(config-if-loopback1)#ip address 200.1.1.1 255.255.255.0
CE2(config-if-loopback1)#exit
CE2(config)#interface gei-1/8.10
CE2(config-if-gei-1/8.10)#exit

CE2(config)#vlan-configuration
CE2(config-vlan)#interface gei-1/8.10
CE2(config-vlan-if-gei-1/8.10)#encapsulation-dot1q 10
CE2(config-vlan-if-gei-1/8.10)#exit
CE2(config-vlan)#exit

CE2(config)#interface gei-1/8.10
CE2(config-if-gei-1/8.10)#ip address 10.10.10.2 255.255.255.0
CE2(config-if-gei-1/8.10)#exit

CE2(config)#router ospf 1
CE2(config-ospf-1)#area 0
CE2(config-ospf-1-area-0)#network 10.10.10.2 0.0.0.255
CE2(config-ospf-1-area-0)#network 200.1.1.1 0.0.0.255
CE2(config-ospf-1-area-0)#exit
CE2(config-ospf-1)#exit
```

配置验证

查看CE1与PE1建立了EBGP连接：

```
PE1#show bgp vpnv4 unicast vrf-summary test1

Neighbor  Ver  As  MsgRcvd   MsgSend   Up/Down   State/PfxRcd
10.1.1.1  4    100 0         12        00:00:09  0
```

查看CE1的路由表如下，其中的BGP路由就是CE1学习到的VPN路由：

```
CE1#show ip forwarding route
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest          Gw          Interface      Owner     Pri  Metric
10.1.1.0/24    10.1.1.2     gei-1/1        Direct      0   0
10.1.1.2/32    10.1.1.2     gei-1/1        Address     0   0
100.1.1.0/24   100.1.1.1    loopback1       Direct      0   0
100.1.1.1/32   100.1.1.1    loopback1       Address     0   0
200.1.1.1/32   10.1.1.1     gei-1/1        BGP        20   0
```

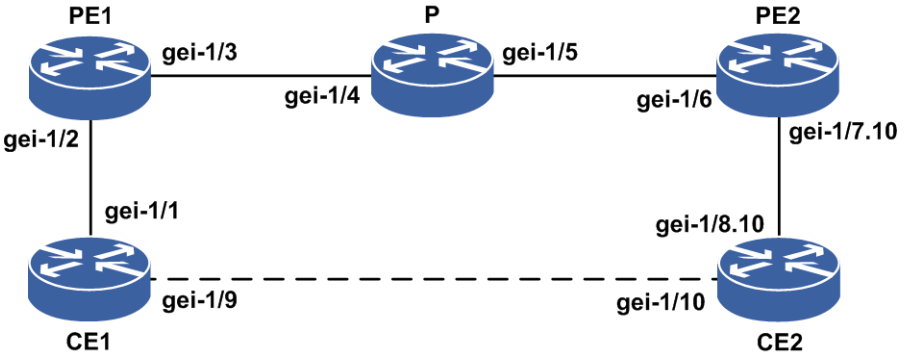
7.3.1.10 MPLS L3VPN OSPF SHAM-LINK 配置实例

配置说明

如*图 7-19*所示，CE1和CE2在同一个VPN中，CE1的loopback地址为100.1.1.1 /24，CE2的loopback地址为200.1.1.1/24。

要求进行适当的VPN配置，使得CE1和CE2能够通过PE1、PE2间sham-link互相学习到对端的loopback路由。CE1与PE1之间运行OSPF VRF协议，CE2与PE2之间运行OSPF VRF协议。

图 7-19 MPLS L3VPN OSPF SHAM-LINK 配置拓扑图



图中各个接口的地址规划如*表 3-2*所示。

表 7-2 MPLS L3VPN OSPF SHAM-LINK 配置地址规划表

设备	接口名	地址
CE1	gei-1/1	10.1.1.2/24
	gei-1/9	20.1.1.2/24
PE1	gei-1/2	10.1.1.1/24
	gei-1/3	10.10.12.1/24
P	gei-1/4	10.10.12.2/24
	gei-1/5	10.10.23.2/24
PE2	gei-1/6	10.10.23.3/24
	gei-1/7.10	10.10.10.1/24
CE2	gei-1/8.10	10.10.10.2/24
	gei-1/10	20.1.1.1/24

配置思路

1.在CE1上配置loopback地址和接口的地址，配置基本的OSPF路由。

2.将loopback和直连的网段通告进OSPF。

3.建立SHAM-LINK。

配置过程

CE1的配置如下：

```
CE1(config)#interface loopback1
CE1(config-if-loopback1)#ip address 100.1.1.1 255.255.255.0
CE1(config-if-loopback1)#exit
CE1(config)#interface gei-1/1
```

```
CE1(config-if-gei-1/1)#no shutdown
CE1(config-if-gei-1/1)#ip address 10.1.1.2 255.255.255.0
CE1(config-if-gei-1/1)#exit
CE1(config)#interface gei-1/9
CE1(config-if-gei-1/9)#no shutdown
CE1(config-if-gei-1/9)#ip address 20.1.1.2 255.255.255.0
CE1(config-if-gei-1/9)#exit

CE1(config)#router ospf 1
CE1(config-ospf-1)#area 0
CE1(config-ospf-1-area-0)#network 10.1.1.0 0.0.0.255
CE1(config-ospf-1-area-0)#network 20.1.1.0 0.0.0.255
CE1(config-ospf-1-area-0)#network 100.1.1.1 0.0.0.0
CE1(config-ospf-1-area-0)#exit
```

PE1的配置如下：

```
PE1(config)#ip vrf test1
PE1(config-vrf-test1)#rd 100:1
PE1(config-vrf-test1)#address-family ipv4
PE1(config-vrf-test1-af-ipv4)#route-target import 100:1
PE1(config-vrf-test1-af-ipv4)#route-target export 100:1
PE1(config-vrf-test1-af-ipv4)#exit
PE1(config-vrf-test1)#exit

PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 10.10.1.1 255.255.255.255
PE1(config-if-loopback1)#exit
PE1(config)#interface gei-1/3
PE1(config-if-gei-1/3)#no shutdown
PE1(config-if-gei-1/3)#ip address 10.10.12.1 255.255.255.0
PE1(config-if-gei-1/3)#exit
PE1(config)#interface loopback64
PE1(config-if-loopback64)#ip vrf forwarding test1
PE1(config-if-loopback64)#ip address 64.64.64.1 255.255.255.255
PE1(config-if-loopback64)#exit

PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#interface gei-1/3
PE1(config-ldp-1-if-gei-1/3)#exit
PE1(config-ldp-1)#exit

PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#no shutdown
PE1(config-if-gei-1/2)#ip vrf forwarding test1
PE1(config-if-gei-1/2)#ip address 10.1.1.1 255.255.255.0
PE1(config-if-gei-1/2)#exit

PE1(config)#router ospf 1
PE1(config-ospf-1)#router-id 10.10.1.1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 10.0.0.0 0.255.255.255
PE1(config-ospf-1-area-0)#exit

PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 10.10.3.3 remote-as 100
PE1(config-bgp)#neighbor 10.10.3.3 update-source loopback1
PE1(config-bgp)#address-family ipv4 vrf test1
PE1(config-bgp-af-ipv4-vrf))#redistribute connected
PE1(config-bgp-af-ipv4-vrf))#redistribute ospf-int 100
PE1(config-bgp-af-ipv4-vrf))#exit
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 10.10.3.3 activate
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#exit

PE1(config)#router ospf 100 vrf test1
```

```
PE1(config-ospf-100)#redistribute bgp-int
PE1(config-ospf-100)#area 0
PE1(config-ospf-100-area-0)#network 10.1.1.0 0.0.0.255
PE1(config-ospf-100-area-0)#redistribute bgp-int
PE1(config-ospf-100-area-0)#sham-link 64.64.64.1 64.64.64.2
PE1(config-ospf-100-area-0)#exit
```

P上的配置如下：

```
P(config)#interface gei-1/4
P(config-if-gei-1/4)#no shutdown
P(config-if-gei-1/4)#ip address 10.10.12.2 255.255.255.0
P(config-if-gei-1/4)#exit

P(config)#interface gei-1/5
P(config-if-gei-1/5)#no shutdown
P(config-if-gei-1/5)#ip address 10.10.23.2 255.255.255.0
P(config-if-gei-1/5)#exit

P(config)#interface loopback1
P(config-if-loopback1)#ip address 10.10.2.2 255.255.255.255
P(config-if-loopback1)#exit

P(config)#router ospf 1
P(config-ospf-1)#router-id 10.10.2.2
P(config-ospf-1)#area 0
P(config-ospf-1-area-0)#network 10.0.0.0 0.255.255.255
P(config-ospf-1-area-0)#exit

P(config)#mpls ldp instance 1
P(config-ldp-1)#router-id loopback1
P(config-ldp-1)#interface gei-1/4
P(config-ldp-1-if-gei-1/4)#exit
P(config-ldp-1)#interface gei-1/5
P(config-ldp-1-if-gei-1/5)#exit
P(config-ldp-1)#exit
```

PE2的配置（这里使用了以太网子接口与CE2连接）：

```
PE2(config)#ip vrf test1
PE2(config-vr-test1)#rd 100:1
PE2(config-vrf-test1)#address-family ipv4
PE2(config-vrf-test1-af-ipv4)#route-target import 100:1
PE2(config-vrf-test1-af-ipv4)#route-target export 100:1
PE2(config-vrf-test1-af-ipv4)#exit
PE2(config-vrf-test1)#exit

PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 10.10.3.3 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#interface gei-1/6
PE2(config-if-gei-1/6)#no shutdown
PE2(config-if-gei-1/6)#ip address 10.10.23.3 255.255.255.0
PE2(config-if-gei-1/6)#exit
PE2(config)#interface loopback64
PE2(config-if-loopback64)#ip vrf forwarding test1
PE2(config-if-loopback64)#ip address 64.64.64.2 255.255.255.255
PE2(config-if-loopback64)#exit

PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#interface gei-1/6
PE2(config-ldp-1-if-gei-1/6)#exit
PE2(config-ldp-1)#exit

PE2(config)#interface gei-1/7.10
PE2(config-if-gei-1/7.10)#exit

PE2(config)#vlan-configuration
```

```
PE2(config-vlan)#interface gei-1/7.10
PE2(config-vlan-if-gei-1/7.10)#encapsulation-dot1q 10
PE2(config-vlan-if-gei-1/7.10)#exit
PE2(config-vlan)#exit

PE2(config)#interface gei-1/7.10
PE2(config-if-gei-1/7.10)#ip vrf forwarding test1
PE2(config-if-gei-1/7.10)#ip address 10.10.10.1 255.255.255.0
PE2(config-if-gei-1/7.10)#exit

PE2(config)#router ospf 1
PE2(config-ospf-1)#router-id 10.10.3.3
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 10.0.0.0 0.255.255.255
PE2(config-ospf-1-area-0)#exit

PE2(config)#router ospf 100 vrf test1
PE2(config-ospf-100)#redistribute bgp-int
PE2(config-ospf-100)#area 0
PE2(config-ospf-100-area-0)#network 10.10.10.1 0.0.0.0
PE2(config-ospf-100-area-0)#sham-link 64.64.64.2 64.64.64.1
PE2(config-ospf-100-area-0)#exit

PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 10.10.1.1 remote-as 100
PE2(config-bgp)#neighbor 10.10.1.1 update-source loopback1
PE2(config-bgp)#address-family ipv4 vrf test1
PE2(config-bgp-af-ipv4-vrf)#redistribute connected
PE2(config-bgp-af-ipv4-vrf)#redistribute ospf-int 100
PE2(config-bgp-af-ipv4-vrf)#exit
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 10.10.1.1 activate
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#exit
```

CE2的配置如下：

```
CE2(config)#interface loopback1
CE2(config-if-loopback1)#ip address 200.1.1.1 255.255.255.0
CE2(config-if-loopback1)#exit
CE2(config)#interface gei-1/8.10
CE2(config-if-gei-1/8.10)#exit

CE2(config)#vlan-configuration
CE2(config-vlan)#interface gei-1/8.10
CE2(config-vlan-if-gei-1/8.10)#encapsulation-dot1q 10
CE2(config-vlan-if-gei-1/8.10)#exit
CE2(config-vlan)#exit

CE2(config)#interface gei-1/8.10
CE2(config-if-gei-1/8.10)#ip address 10.10.10.2 255.255.255.0
CE2(config-if-gei-1/8.10)#exit
CE2(config)#interface gei-1/10
CE2(config-if-gei-1/10)#ip address 20.1.1.1 255.255.255.0
CE2(config-if-gei-1/10)#exit

CE2(config)#router ospf 1
CE2(config-ospf-1)#area 0
CE2(config-ospf-1-area-0)#network 10.10.10.0 0.0.0.255
CE2(config-ospf-1-area-0)#network 200.1.1.0 0.0.0.255
CE2(config-ospf-1-area-0)#network 20.1.1.0 0.0.0.255
CE2(config-ospf-1-area-0)#exit
```

配置验证

PE1上查看shamlink邻居的建立：

```
inspur(config)#sho ip ospf neighbor detail process 100
 OSPF Router with ID (64.64.64.1) (Process ID 100)
Neighbor 0.0.0.0
 In the area 0.0.0.0
 Via interface sl(To 64.64.64.2) 64.64.64.2
 State DOWN, Priority 0, Cost 1
 Queue count : Retransmit 0, DD 0, LS Req 0
 Dead time : 00:00:40 Options : 0x0
    In Full State for 00:00:09
```

在CE1查看到CE2上的路由：

```
inspur#show ip forwarding route 200.1.1.1
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
   Dest Gw Interface Owner Pri Metric
*> 200.1.1.1/32 20.1.1.1 gei-1/9  OSPF 110 2
```

在CE1上断开gei-1/9接口：

```
CE1(config)#interface gei-1/9
CE1(config-if-gei-1/9)#shutdown
CE1(config-if-gei-1/9)#exit
```

在CE1上重新查看到CE2的路由，此时经过PE1的BGP路由：

```
inspur#show ip forwarding route 200.1.1.1
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
  ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
 Dest Gw Interface Owner Pri Metric
*> 200.1.1.1/32 104.1.1.1 gei-1/1 OSPF 110 4
```

7.3.2 MPLS L3VPN 路由聚合

在大规模的三层网络中，BGP路由表十分庞大，存储路由表会占用大量的路由器内存资源，路由器传送与处理路由信息所需要的带宽也需要大量的资源。使用路由聚合（Routes Aggregation）可以大大减小路由表的规模。

7.3.2.1 配置 MPLS L3VPN 路由聚合

本节介绍MPLS L3VPN路由聚合的配置步骤和命令。

1.配置MPLS L3VPN路由聚合。

步骤	命令	功能
1	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**address-family ipv4 vrf** < *vrf-name*>	进入IPv4 VRF地址族配置模式
3	inspur(config-bgp-af-ipv4-vrf)#**aggregate-address** <*ip-address*><*net-mask*>{[**as-set**],[**summary-only**],[**strict**],[**attribute-map**<*map-tag*>],[**suppress-map**<*map-tag*>]}	在VRF路由表中创建一条聚合策略

as-set：产生自治系统设置路径信息。

summary-only：配置该参数后，向MPBGP邻居只通告聚合路由而不包含被聚合的子网路由。

strict：只有对MED和NEXT_HOP属性相同的路由才能聚合，否则聚合条件放宽，不考虑MED和NEXT_HOP属性。

2.验证配置结果。

命令	功能
inspur#**show ip route vpn**	显示VPN实例的路由信息

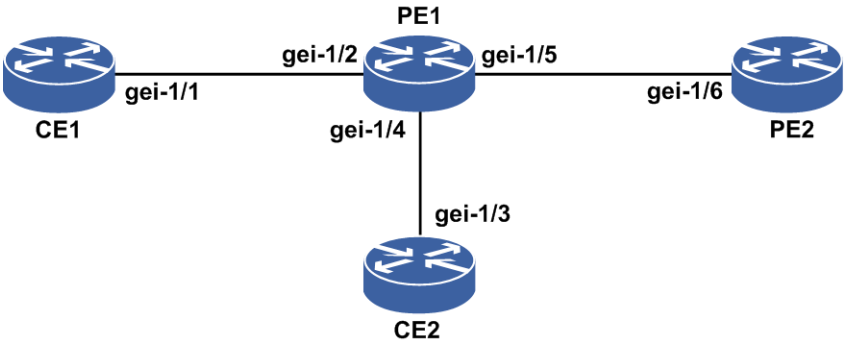
7.3.2.2 MPLS L3VPN 路由聚合配置实例

配置说明

如*图 7-20*所示，CE1属于AS200，PE1和PE2属于AS100，CE2属于AS300。PE1和PE2之间通过loopback地址建立MPBGP邻居。CE1与PE1之间建立EBGP邻居，CE2与PE1之间建立EBGP邻居。

路由器CE1和CE2同在一个VPN中，分别通告路由150.1.0.0/16和150.2.0.0/16给PE1。PE1将该两条路由信息聚合成150.0.0.0/8通告给PE2。配置聚合后，PE2的路由表中将仅能学习到聚合路由150.0.0.0/8。

图 7-20 MPLS VPN 路由聚合配置实例拓扑图



图中各个接口的地址规划如*表 7-3*所示。

表 7-3 MPLS VPN 基本配置地址规划表

设备	接口名	地址
CE1	gei-1/1	20.0.0.2/24
PE1	gei-1/2	20.0.0.1/24
	gei-1/4	30.0.0.1/24
	gei-1/5	10.0.0.1/24
PE2	gei-1/6	10.0.0.2/24
CE2	gei-1/3	30.0.0.2/24

配置思路

1.PE1与PE2之间建立MP-IBGP邻居，PE1的loopback地址为1.1.1.1/32，PE2的loopback地址为1.1.1.2/32。

2.PE1和PE2上配置相同的vpn1，gei-1/2和gei-1/4都绑定到vpn1中。

3.CE2和PE1、CE1和PE1分别建立EBGP邻居。

配置过程

CE1上的配置如下：

```
CE1(config)#interface gei-1/1
CE1(config-if-gei-1/1)#no shutdown
CE1(config-if-gei-1/1)#ip address 20.0.0.2 255.255.255.0
CE1(config-if-gei-1/1)#exit

CE1(config)#router bgp 200
CE1(config-bgp)#network 150.1.0.0 255.255.0.0
CE1(config-bgp)#neighbor 20.0.0.1 remote-as 100
CE1(config-bgp)#exit
```

CE2上的配置如下：

```
CE2(config)#interface gei-1/3
CE2(config-if-gei-1/3)#no shutdown
CE2(config-if-gei-1/3)#ip address 30.0.0.2 255.255.255.0
CE2(config-if-gei-1/3)#exit

CE2(config)#router bgp 300
CE2(config-bgp)#network 150.2.0.0 255.255.0.0
CE2(config-bgp)#neighbor 30.0.0.1 remote-as 100
CE2(config-bgp)#exit
```

PE1上的配置如下：

```
PE1(config)#ip vrf test1
PE1(config-vrf-test1)#rd 100:1
PE1(config-vrf-test1)#address-family ipv4
PE1(config-vrf-test1-af-ipv4)#route-target import 100:1
PE1(config-vrf-test1-af-ipv4)#route-target export 100:1
PE1(config-vrf-test1-af-ipv4)#exit
PE1(config-vrf-test1)#exit

PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
PE1(config-if-loopback1)#exit
PE1(config)#interface gei-1/5
PE1(config-if-gei-1/5)#no shutdown
PE1(config-if-gei-1/5)#ip address 10.0.0.1 255.255.255.0
PE1(config-if-gei-1/5)#exit

PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#interface gei-1/5
PE1(config-ldp-1-if-gei-1/5)#exit
PE1(config-ldp-1)#exit

PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#no shutdown
PE1(config-if-gei-1/2)#ip vrf forwarding test1
PE1(config-if-gei-1/2)#ip address 20.0.0.1 255.255.255.0
PE1(config-if-gei-1/2)#exit
PE1(config)#interface gei-1/4
PE1(config-if-gei-1/4)#no shutdown
PE1(config-if-gei-1/4)#ip vrf forwarding test1
PE1(config-if-gei-1/4)#ip address 30.0.0.1 255.255.255.0
PE1(config-if-gei-1/4)#exit

PE1(config)#router ospf 1
PE1(config-ospf-1)#router-id 1.1.1.1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
PE1(config-ospf-1-area-0)#network 10.0.0.0 0.0.0.255
PE1(config-ospf-1-area-0)#exit

PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 1.1.1.2 remote-as 100
PE1(config-bgp)#neighbor 1.1.1.2 update-source loopback1
PE1(config-bgp)#address-family ipv4 vrf test1
PE1(config-bgp-af-ipv4-vrf)#aggregate-address      150.0.0.0      255.0.0.0
summary-only
PE1(config-bgp-af-ipv4-vrf)#neighbor 20.0.0.2 remote-as 200
PE1(config-bgp-af-ipv4-vrf)#neighbor 30.0.0.2 remote-as 300
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 1.1.1.2 activate
PE1(config-bgp-af-vpnv4)#exit
```

PE2上的配置如下：

```
PE2(config)#ip vrf test1
PE2(config-vrf-test1)#rd 100:1
```

```
PE2(config-vrf-test1)#address-family ipv4
PE2(config-vrf-test1-af-ipv4)#route-target import 100:1
PE2(config-vrf-test1-af-ipv4)#route-target export 100:1
PE2(config-vrf-test1-af-ipv4)#exit
PE2(config-vrf-test1)#exit

PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#interface gei-1/6
PE2(config-if-gei-1/6)#no shutdown
PE2(config-if-gei-1/6)#ip address 10.0.0.2 255.255.255.0
PE2(config-if-gei-1/6)#exit

PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#interface gei-1/6
PE2(config-ldp-1-if-gei-1/6)#exit
PE2(config-ldp-1)#exit

PE2(config)#router ospf 1
PE2(config-ospf-1)#router-id 1.1.1.2
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 1.1.1.2 0.0.0.0
PE2(config-ospf-1-area-0)#network 10.0.0.0 0.0.0.255
PE2(config-ospf-1-area-0)#exit

PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback1
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 1.1.1.1 activate
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#exit
```

配置验证

查看PE1的VRF路由表，既可以看到子路由，又看到聚合路由：

```
PE1(config)#show ip protocol routing  vrf test1
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale

    Dest          NextHop    Intag    Outtag    RtPrf   Protocol
*>  150.0.0.0/8    0.0.0.0     87      notag     254     BGP-AD
*>  150.1.0.0/16   20.0.0.2    86       notag     20      BGP-EXT
*>  150.2.0.0/16   30.0.0.2    85       notag     20      BGP-EXT
```

查看PE2的VRF路由表，只能看到聚合路由：

```
PE2(config)#show ip protocol routing  vrf test1
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
```

```
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale

   Dest          NextHop     Intag    Outtag    RtPrf   Protocol
*> 150.0.0.0/8    1.1.1.1     165366    87       200     BGP-INT
```

7.3.3 L3VPN 路由限制和告警

在MPLS L3VPN网络中，可能会出现这样的现象：PE上因为从CE和其他PE接收了过多的路由，导致PE内存耗尽以及路由设备崩溃。因此有必要对从CE和PE邻居注入PE路由器的VRF路由进行控制，这个功能称之为L3VPN 路由限制（Route Limit）。

L3VPN Route Limit功能能够对以各种方式从CE接入PE的路由进行控制。

7.3.3.1 配置 L3VPN 路由限制和告警

本节介绍了L3VPN路由限制和告警的配置步骤和命令。

1.控制进入VRF的路由数目，并给出相关告警。

步骤	命令	功能
1	inspur(config)#**ip vrf** < *vrfi-name*>	进入已配置的VRF的配置模式
2	inspur(config-vrf-vrf-name)#**address-family** {**ipv4**|**ipv6**}	激活VRF IPv4或者IPv6能力
3	inspur(config-vrf-vrf-name-af-ipv4)#**maximum routes** <*number*>{< *thresholdvalue*>| **warning-only**}	控制进入VRF的路由数目和给出相关告警
	inspur(config-vrf-vrf-name-af-ipv6)#**maximum routes** <*number*>{< *thresholdvalue*>| **warning-only**}	

<*number*>：允许该VRF的各CE通过某种可行的接入方式通告的路由以及远端PE通告给该vrf的有效路由的总和上限，范围：1~4294967295。

< *thresholdvalue*>：达到该VRF路由上限的某个百分比时进行路由告警的阈值，路由告警限 （以百分比表示），范围：1~100。

warning-only：当某VRF的路由总数超过路由总和上限值时，只进行告警，不限制路由。

2.验证配置结果。

命令	功能
inspur#**show ip vrf detail**	显示VRF的详细配置信息

通过显示VRF的详细配置信息可以看到路由限制和告警的相关信息。

7.3.3.2 L3VPN 路由限制和告警配置实例

配置说明

如*图 7-21*所示，搭建L3VPN的环境，在PE1上存在VRF，命名为inspur，RD为1：1，RT为1：1，接口int1绑定到VRF inspur中。

接口地址分别设置为int1：10.1.1.1/24；port1：10.1.1.2/24。

CE1以EBGP方式接入PE1。

图 7-21 L3VPN 路由告警配置实例拓扑图



配置过程

1.PE1和CE1之间建立EBGP邻居，PE1的配置如下：

```
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf inspur
PE1(config-bgp-af-ipv4-vrf)#neighbor 10.1.1.2 remote-as 200
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#exit
```

CE1上进行相应配置和PE1建立EBGP邻居。

在PE1上使用命令**show bgp vpnv4 unicast vrf-summary inspur**可以看到PE1和Tester之间邻居关系已经建立。

2.在PE1上配置vrf inspur的路由上限为100条，并且告警限为60%：

```
PE1(config)#ip vrf inspur
PE1(config-vrf-inspur)#address-family ipv4
PE1(config-vrf-inspur-af-ipv4)#maximum routes 100 60
PE1(config-vrf-inspur-af-ipv4)#exit
PE1(config-vrf-inspur)#exit
```

用**show ip vrf detail inspur**命令可以看到上述**maximum routes**命令的配置。

将PE1上的告警功能和终端监视功能打开，以观察路由超过阈值后的告警：

```
PE1#terminal monitor
PE1#configure terminal
PE1#(config)#logging on
```

3.CE1向PE1通告50条EBGP路由（不超过60%的告警限），在PE1上使用命令**show ip protocol routing vrf inspur**可以看到50条vrf EBGP路由，PE1上不给出任何

告警提示。

4.CE1继续向PE1通告20条路由，总共达到70条EBGP路由（超过60%的告警限），在PE1上使用命令**show ip protocol routing vrf-summary inspur**可以看到70条路由：

```
PE1(config)#show ip protocol routing vrf-summary inspur
  VRF   Source   Count
 connected:      2
 static:         0
 ospf:           0
 rip:            0
 bgp:            70
 isis:           0
 icmp:           0
 snmp:           0
 nat:            0
 natpt:          0
 vrrp:           0
 ppp:            0
 asbr_vpn:       0
 rsvpte:         0
 usr-ipaddr:     0
 usr-net:        0
 ipsec:          0
 ps-user:        0
 ps-busi:        0
 ves:            0
 ldp:            0
 user-special:   0
 dhcp-dft:       0
 dhcp-static:    0
 sl_nat64_v4:    0
Total:          72
```

PE1上有相应的告警信息打出：

```
An alarm 200311 ID 125 level 5 occurred at 14:07:55 02-16-2012
sent by PE1 MPU-13/0 %COURIER% Routes warning limit is exceeded!
warning data:The routes warning limit of inspur is exceeded
An alarm 200311 ID 3442 level 5 occurred at 10:16:59 05-06-2013 sent by
PE1 MPU-13/0 %L3VPN% Routes warning limit is exceeded.
Warning data:The routes warning limit of inspur is exceeded
```

5.CE1继续向PE1通告40条路由，总共达到110条EBGP路由（超过100的最大路由限制），在PE1上使用命令**show ip protocol routing vrf-summary inspur**可以看到100条vrf路由：

```
PE1(config)#show ip protocol routing vrf-summary inspur
VRF Source Count
connected: 2
static: 0
ospf: 0
rip: 0
bgp: 100
isis: 0
icmp: 0
snmp: 0
nat: 0
natpt: 0
vrrp: 0
ppp: 0
asbr_vpn: 0
rsvpte: 0
usr-ipaddr: 0
usr-net: 0
ipsec: 0
```

```
ps-user: 0
ps-busi: 0
ves: 0
ldp: 0
user-special: 0
dhcp-dft: 0
dhcp-static: 0
sl_nat64_v4: 0
Total: 103
```

PE1上打出vrf路由超过最大限的告警：

```
An alarm 200310 ID 3441 level 3 occurred at 10:16:59 05-06-2013
sent by PE1 MPU-13/0 %L3VPN% Routes limit is exceeded.
Error data:The routes limit of inspur is exceeded
```

6.CE1撤销前面向PE1通告的路由，重新向PE1通告50条EBGP路由，在PE1上使用命令**show ip protocol routing vrf-summary inspur**可以看到50条vrf路由，PE1上不给出任何告警提示。

7.在PE1上将vrf inspur的路由告警限改为40%，路由上限仍为100条不变：

```
PE1(config)#ip vrf inspur
PE1(config-vrf-inspur)#address-family ipv4
PE1(config-vrf-inspur-af-ipv4)#maximum routes 100 40
PE1(config-vrf-inspur-af-ipv4)#exit
PE1(config-vrf-inspur)#exit
```

用**show ip vrf detail inspur**命令可以看到上述**maximum routes**命令的配置，显示当前路由为50条，PE1上不给出任何告警提示。

8.CE1撤消之前通告的50条EBGP路由，并重新通告，PE1上给出超过路由告警限的告警语句：

```
An alarm 200311 ID 3442 level 5 occurred at 10:16:59 05-06-2013
sent by PE1 MPU-13/0 %L3VPN% Routes warning limit is exceeded.
Warning data:The routes warning limit of inspur is exceeded
```

9.在PE1的vrf inspur下配置L3VPN的路由限制告警功能中的warning-only功能：

```
PE1(config)#ip vrf inspur
PE1(config-vrf-inspur)#address-family ipv4
PE1(config-vrf-inspur-af-ipv4)#maximum routes 100 warning-only
PE1(config-vrf-inspur-af-ipv4)#exit
PE1(config-vrf-inspur)#exit
```

10.查看PE1的vrf inspur当前的路由数以及路由限制值和告警阈值，路由总数为50条，没有超过路由上限，没有告警产生：

```
PE1(config)#show ip vrf detail inspur
VRF inspur (VRF Id = 1); default RD 1:1
  Default VPNID: <not set>

  Ttl-mode: pipe
  Ds-mode: pipe

Address family ipv4:
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
  Route warning limit 100
priority:  2
No import multicast-route
 No static outlabel configed
 No static tunnel configed
```

```
Address family ipv6:
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
Mpls label mode:
   ipv4 VRF label allocation mode: per-prefix
ipv6 VRF label allocation mode: per-prefix
per-vrf inlabel: 213009
Interfaces:
   gei-0/1.1
   gei-0/5
```

11.从CE1再通告60条路由过来，路由总数超过路由上限，PE1上有相应的告警信息打出，并且可以查看到PE1上的vrf inspur对超过100条的路由并没有进行限制，在PE1上使用命令**show ip protocol routing vrf-summary inspur**可以看到110条路由：

```
An alarm 200310 ID 143  level 3 occurred at 14:17:21 02-16-2012
sent by PE1 MPU-13/0 %COURIER% Routes warning limit is exceeded!
warning data:The routes warning limit of inspur is exceeded

PE1(config)#show ip vrf detail inspur
VRF inspur (VRF Id = 1); default RD 1:1
  Default VPNID: <not set>
  Ttl-mode: pipe
  Ds-mode: pipe

Address family ipv4:
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
  Route warning limit 100
priority:  2
No import multicast-route
 No static outlabel configed
 No static tunnel configed
Address family ipv6:
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
Mpls label mode:
 ipv4 VRF label allocation mode: per-prefix
ipv6 VRF label allocation mode: per-prefix
per-vrf inlabel: 213009
Interfaces:
   gei-0/1.1
   gei-0/5

PE1(config)#show ip protocol routing vrf-summary inspur
VRF Source Count
connected: 2
static: 0
ospf: 0
rip: 0
bgp: 110
isis: 0
icmp: 0
snmp: 0
nat: 0
natpt: 0
vrrp: 0
ppp: 0
asbr_vpn: 0
```

```
rsvpte: 0
usr-ipaddr: 0
usr-net: 0
ipsec: 0
ps-user: 0
ps-busi: 0
ves: 0
ldp: 0
user-special: 0
dhcp-dft: 0
dhcp-static: 0
sl_nat64_v4: 0
Total: 113
```

7.3.4 Global 静态路由

Global静态路由是指网络管理员通过配置命令指定到私网路由表中下一跳为公网的路由信息，不像动态路由那样根据路由算法建立路由表。Global静态路由作为私网访问Internet的可选方案之一，具有配置简单、稳定高效的特点。

7.3.4.1 配置 global 静态路由

本节介绍了global静态路由的配置步骤和命令。

1.配置global静态路由。

步骤	命令	功能
1	inspur(config)#**ip route vrf** < *vrf-name*>< *prefix*>< *net-mask*>{<*forwarding-router's-address*> **global** }[< *distance-metric*>][**metric** <*metric*>]	配置私网global下一跳静态路由
2	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
3	inspur(config-bgp)#**address-family ipv4 vrf** < *vrf-name*>	进入相应VRF的地址族配置模式
4	inspur(config-bgp-af)#**redistribute static**	重分发静态路由

<*vrf-name*>：用于配置指定VRF中的静态路由，VRF名称，长度为1~32字符。

<*prefix*>：网络IP前缀，为十进制点分形式。

<*net-mask*>：网络掩码，为十进制点分形式。

<*forwarding-router's-address*>：下一跳IP地址，为十进制点分形式。

global：私网路由配置公网下一跳，只在仅配置下一跳的私网路由时才允许配置。

<*distance-metric*>：管辖距离，范围1~255。

<*metric*>：路由的度量值，范围1~255，默认为0。

<*as-number*>：本路由器所在的自治系统号，范围为1~65535。其中AS范围1~64511是全球公用AS号，64512~65535是私网用户AS号。

2.验证配置结果。

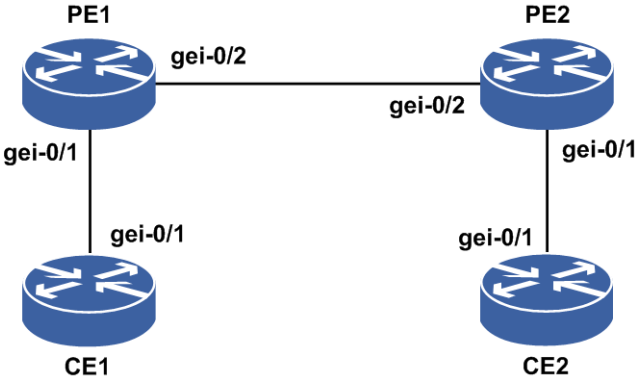
命令	功能
inspur#**show ip protocol routing vrf** < *vrf-name*>	显示路由器的全局路由表
inspur#**show ip forwarding route vrf** < *vrf-name*>	显示路由器的转发表

7.3.4.2 Global 静态路由配置实例

配置说明

如*图 7-22*所示，在PE1和PE2上分别配置到CE2 20.1.1.0/24和CE1 33.24.1.0/24的global静态路由，并重分发静态路由，在CE和PE之间建立BGP邻居。

图 7-22 Global 静态路由配置实例图



配置思路

1.配置私网global下一跳静态路由

2.配置重分发静态路由

3.CE和PE之间建立BGP邻居

配置过程

CE1上配置：

```
CE1(config)#interface gei-0/1
CE1(config-if-gei-0/1)#no shutdown
CE1(config-if-gei-0/1)#ip address 33.24.1.5 255.255.255.0
CE1(config-if-gei-0/1)#exit

CE1(config)#router bgp 1
CE1(config-bgp)#neighbor 33.24.1.6 remote-as 2
CE1(config-bgp)#exit
```

PE1上配置：

```
PE1(config)#tunnel-policy 11
PE1(config-tunnel-policy-11)#tunnel select-seq ldp-lsp te-lsp
PE1(config-tunnel-policy-11)#exit

PE1(config)#ip vrf wy
PE1(config-vrf-wy)#rd 1:100
PE1(config-vrf-wy)#route-target both 1:100
PE1(config-vrf-wy)#address-family ipv4
PE1(config-vrf-wy-af-ipv4)#peer 64.1.1.4 tunnel-policy 11
PE1(config-vrf-wy-af-ipv4)#static-outlabel 64.1.1.4 31
PE1(config-vrf-wy-af-ipv4)#exit
PE1(config-vrf-wy)#static-inlabel 21
PE1(config-vrf-wy)#exit

PE1(config)#interface gei-0/1
PE1(config-if-gei-0/1)#no shutdown
PE1(config-if-gei-0/1)#ip vrf forwarding wy
PE1(config-if-gei-0/1)#ip address 33.24.1.6 255.255.255.0
PE1(config-if-gei-0/1)#exit
PE1(config)#interface gei-0/2
PE1(config-if-gei-0/2)#no shutdown
PE1(config-if-gei-0/2)#ip address 21.33.1.6 255.255.255.0
PE1(config-if-gei-0/2)#exit
PE1(config)#interface loopback64
PE1(config-if-loopback64)#ip address 64.1.1.6 255.255.255.0
PE1(config-if-loopback64)#exit

PE1(config)#router ospf 1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 21.33.1.0 0.0.0.255
PE1(config-ospf-1-area-0)#network 64.1.1.6 0.0.0.0
PE1(config-ospf-1)#exit

PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback64
PE1(config-ldp-1)#interface gei-0/2
PE1(config-ldp-1-if-gei-0/2)#end

PE1(config)#router bgp 2
PE1(config-bgp)#address-family ipv4 vrf wy
PE1(config-bgp-af-ipv4-vrf)#neighbor 33.24.1.5 remote-as 1
PE1(config-bgp-af-ipv4-vrf)#redistribute static
PE1(config-bgp-af-ipv4-vrf)#end

PE1(config)#ip route vrf wy 20.1.1.0 255.255.255.0 64.1.1.4 global
```

PE2上配置：

```
PE2(config)#tunnel-policy 11
PE2(config-tunnel-policy-11)#tunnel select-seq ldp-lsp te-lsp
PE2(config-tunnel-policy-11)#exit

PE2(config)#ip vrf wy
PE2(config-vrf-wy)#rd 1:100
PE2(config-vrf-wy)#route-target both 1:100
PE2(config-vrf-wy)#address-family ipv4
PE2(config-vrf-wy-af-ipv4)#peer 64.1.1.6 tunnel-policy 11
PE2(config-vrf-wy-af-ipv4)#static-outlabel 64.1.1.6 21
PE2(config-vrf-wy-af-ipv4)#exit
PE2(config-vrf-wy)#static-inlabel 31
PE2(config-vrf-wy)#exit

PE2(config)#interface gei-0/1
PE2(config-if-gei-0/1)#no shutdown
```

```
PE2(config-if-gei-0/1)#ip vrf forwarding wy
PE2(config-if-gei-0/1)#ip address 20.1.1.4 255.255.255.0
PE2(config-if-gei-0/1)#exit
PE2(config)#interface gei-0/2
PE2(config-if-gei-0/2)#no shutdown
PE2(config-if-gei-0/2)#ip address 21.33.1.4 255.255.255.0
PE2(config-if-gei-0/2)#exit
PE2(config)#interface loopback64
PE2(config-if-loopback64)#ip address 64.1.1.4 255.255.255.0
PE2(config-if-loopback64)#exit

PE2(config)#router ospf 1
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 20.1.1.0 0.0.0.255
PE2(config-ospf-1-area-0)#network 64.1.1.4 0.0.0.0
PE2(config-ospf-1-area-0)#exit
PE2(config-ospf-1)#exit

PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback64
PE2(config-ldp-1)#interface gei-0/2
PE2(config-ldp-1-if-gei-0/2)#end

PE2(config)#router bgp 2
PE2(config-bgp)#address-family ipv4 vrf wy
PE2(config-bgp-af-ipv4-vrf)#neighbor 20.1.1.3 remote-as 1
PE2(config-bgp-af-ipv4-vrf)#redistribute static
PE2(config-bgp-af-ipv4-vrf)#end

PE2(config)#ip route vrf wy 33.24.1.0 255.255.255.0 64.1.1.6 global
```

CE2上配置：

```
CE2(config)#interface gei-0/1
CE2(config-if-gei-0/1)#no shutdown
CE2(config-if-gei-0/1)#ip address 20.1.1.3 255.255.255.0
CE2(config-if-gei-0/1)#exit

CE2(config)#router bgp 1
CE2(config-bgp)#neighbor 20.1.1.4 remote-as 2
CE2(config-bgp)#exit
```

配置验证

在PE1上查看：

```
PE1(config)#show ip protocol routing vrf wy
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, USER-I = user-ipaddr, RIP-D = rip-discard,
 OSPF-E = ospf-ext, ASBR-V = asbr-vpn, GW-FWD = ps-busi, GW-UE = ps-user,
 BGP-AD = bgp-aggr-discard, BGP-CE = bgp-confed-ext, NAT64 = sl-nat64-v4,
 USER-N = user-network, USER-S = user-special, DHCP-S = dhcp-static,
 DHCP-D = dhcp-dft
Marks: *valid, >best, s-stale

 Dest          NextHop    Intag   Outtag    RtPrf    Protocol
*> 20.1.1.0/24  64.1.1.4   notag   31            Static
*> 33.24.1.0/24  33.24.1.6  notag   notag     0       Direct
*> 33.24.1.6/32  33.24.1.6  notag   notag     0       Address
PE1(config)#show ip forwarding route vrf wy
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
```

```
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
   Dest         Gw        Interface    Owner   Pri Metric
*> 20.1.1.0/24   64.1.1.4   gei-0/2     STAT-V  1    0
*> 33.24.1.0/24  33.24.1.6  gei-0/1     Direct  0    0
*> 33.24.1.6/32  33.24.1.6  gei-0/1     Address 0    0
```

在PE2上查看：

```
PE2(config)#show ip protocol routing vrf wy
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, USER-I = user-ipaddr, RIP-D = rip-discard,
 OSPF-E = ospf-ext, ASBR-V = asbr-vpn, GW-FWD = ps-busi, GW-UE = ps-user,
 BGP-AD = bgp-aggr-discard, BGP-CE = bgp-confed-ext, NAT64 = sl-nat64-v4,
 USER-N = user-network, USER-S = user-special, DHCP-S = dhcp-static,
 DHCP-D = dhcp-dft
Marks: *valid, >best, s-stale
   DestNextHop   Intag   Outtag  RtPrf  Protocol
*> 20.1.1.4/32  20.1.1.4   notag   notag   0     Address
*  20.1.1.4/32  20.1.1.4   notag   notag   0     Direct
*> 33.24.1.0/24 64.1.1.6   notag   21      1     Static

PE2(config)#show ip forwarding route vrf wy
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
   Dest         Gw       Interface     Owner    Pri  Metric
*> 20.1.1.4/32   20.1.1.4 loopback63    Address  0    0
*> 33.24.1.0/24  64.1.1.6 gei-0/2       STAT-V   1    0
```

在CE1上查看：

```
CE1(config)#sho ip forwarding route 20.1.1.0
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
   Dest      Gw        Interface     Owner  Pri  Metric
*> 20.1.1.0  33.24.1.6  gei-0/1       bgp    200
```

7.3.5 L3VPN FRR

VPN FRR利用基于VPN的私网路由快速切换技术，通过预先在远端PE中设置指向主用PE和备用PE的主备用转发项，并结合PE故障快速检测，在VPN路由收敛完成之前，先将VPN流量切换到备份路径上。

L3VPN FRR支持WTR功能。

7.3.5.1 配置 L3VPN FRR

本节介绍L3VPN FRR的配置步骤和命令。

1.配置L3VPN FRR。

步骤	命令	功能
1	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**address-family ipv4 vrf** < *vpn-name*>	进入IPv4 VRF地址族配置模式
3	inspur(config-bgp-af-ipv4-vrf)#**bgp frr**	使能BGP的FRR功能

2.验证配置结果。

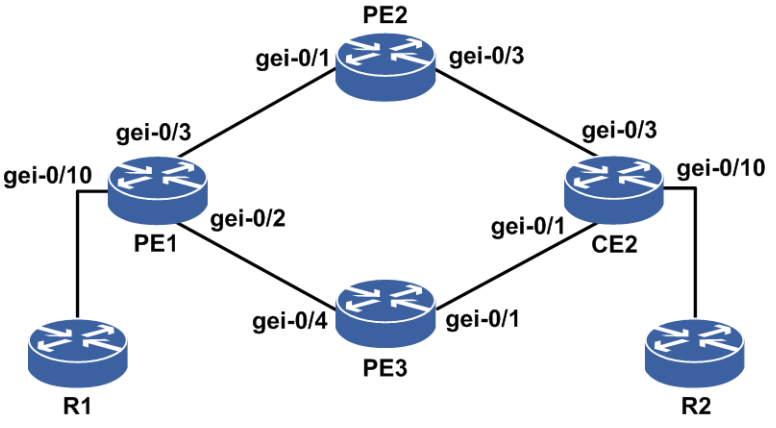
命令	功能
inspur#**show ip forwarding backup route vrf** < *vpn-name*>	查看备份私网路由

7.3.5.2 L3VPN FRR 配置实例

配置说明

如*图7-23*所示，在基本的L3VPN的环境中，CE1通过直连的方式接入到PE1上的VRF 1，CE2分别与PE2、PE3的vrf 接入接口创建OSPF邻居，CE2与R1创建OSPF邻居，分别在PE2、PE3上的VRF地址族下重分发OSPF，此时PE1上同时拥有从对端PE2和PE3上学习到的关于VRF 1的路由。PE1跟PE2、PE3同时建立LDP/MPBGP的邻居。

图 7-23 VPN 路由 FRR 配置实例



配置思路

1.按图示搭建环境，PE1分别与PE2、PE3搭建MP-IBGP环境。

2.CE2分别与PE2、PE3的VRF接入接口创建OSPF邻居，CE2与R1创建OSPF邻居。

3.分别在PE2、PE3上的VRF地址族下重分发OSPF。

4.在PE1的VRF下配置FRR。

配置过程

PE1的配置：

```
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
PE1(config-if-loopback1)#exit
PE1(config)#interface gei-0/3
PE1(config-if-gei-0/3)#no shutdown
PE1(config-if-gei-0/3)#ip address 12.1.1.1 255.255.255.0
PE1(config-if-gei-0/3)#exit
PE1(config)#interface gei-0/2
PE1(config-if-gei-0/2)#no shutdown
PE1(config-if-gei-0/2)#ip address 13.1.1.1 255.255.255.0
PE1(config-if-gei-0/2)#exit

PE1(config)#router ospf 1
PE1(config-ospf-1)#router-id 1.1.1.1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 12.1.1.0 0.0.0.255
PE1(config-ospf-1-area-0)#network 13.1.1.0 0.0.0.255
PE1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
PE1(config-ospf-1-area-0)#exit

PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#interface gei-0/3
PE1(config-ldp-1-if-gei-0/3)#exit
PE1(config-ldp-1)#interface gei-0/2
PE1(config-ldp-1-if-gei-0/2)#exit
PE1(config-ldp-1)#exit

PE1(config)#ip vrf inspur
PE1(config-vrf-inspur)#rd 1:50
PE1(config-vrf-inspur)#route-target both 1:50
PE1(config-vrf-inspur)#address-family ipv4
PE1(config-vrf-inspur-af-ipv4)#exit
PE1(config-vrf-inspur)#exit

PE1(config)#router bgp 18004
PE1(config-bgp)#neighbor 2.2.2.2 remote-as 18004
PE1(config-bgp)#neighbor 2.2.2.2 update-source loopback1
PE1(config-bgp)#neighbor 3.3.3.3 remote-as 18004
PE1(config-bgp)#neighbor 3.3.3.3 update-source loopback1
PE1(config-bgp)#neighbor 2.2.2.2 fall-over bfd
PE1(config-bgp)#neighbor 3.3.3.3 fall-over bfd
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 2.2.2.2 activate
PE1(config-bgp-af-vpnv4)#neighbor 3.3.3.3 activate
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#address-family ipv4 vrf inspur
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#bgp frr
```

```
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#exit

PE1(config)#interface gei-0/10
PE1(config-if-gei-0/10)#no shutdown
PE1(config-if-gei-0/10)#ip vrf forwarding inspur
PE1(config-if-gei-0/10)#ip address 202.10.10.61 255.255.255.0
PE1(config-if-gei-0/10)#exit
```

PE2上的配置：

```
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 2.2.2.2 255.255.255.255
PE2(config-if-loopback1)#exit

PE2(config)#ip vrf inspur
PE2(config-vrf-inspur)#rd 1:50
PE2(config-vrf-inspur)#route-target both 1:50
PE2(config-vrf-inspur)#address-family ipv4
PE2(config-vrf-inspur-af-ipv4)#exit
PE2(config-vrf-inspur)#exit

PE2(config)#interface gei-0/1
PE2(config-if-gei-0/1)#no shutdown
PE2(config-if-gei-0/1)#ip address 12.1.1.2 255.255.255.0
PE2(config-if-gei-0/1)#exit
PE2(config)#interface gei-0/3
PE2(config-if-gei-0/3)#no shutdown
PE2(config-if-gei-0/3)#ip vrf for inspur
PE2(config-if-gei-0/3)#ip address 200.1.1.60 255.255.255.0
PE2(config-if-gei-0/3)#exit

PE2(config)#router ospf 1
PE2(config-ospf-1)#router-id 2.2.2.2
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 12.1.1.0 0.0.0.255
PE2(config-ospf-1-area-0)#network 2.2.2.2 0.0.0.0
PE2(config-ospf-1-area-0)#exit

PE2(config)#router ospf 100 vrf inspur
PE2(config-ospf-100)#redistribute bgp-int
PE2(config-ospf-100)#area 0
PE2(config-ospf-100-area-0)#network 200.1.1.0 0.0.0.255
PE2(config-ospf-100-area-0)#exit

PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#interface gei-0/1
PE2(config-ldp-1-if-gei-0/1)#exit
PE2(config-ldp)#exit

PE2(config)#router bgp 18004
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 18004
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback1
PE2(config-bgp)#neighbor 1.1.1.1 fall-over bfd
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 1.1.1.1 activate
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#address-family ipv4 vrf inspur
PE2(config-bgp-af-ipv4-vrf)#redistribute ospf-int 100
PE2(config-bgp-af-ipv4-vrf)#exit
PE2(config-bgp)#exit
```

PE3上的配置：

```
PE3(config)#interface loopback1
PE3(config-if-loopback1)#ip address 3.3.3.3 255.255.255.255
PE3(config-if-loopback1)#exit
```

```
PE3(config)#ip vrf inspur
PE3(config-vrf-inspur)#rd 1:50
PE3(config-vrf-inspur)#route-target both 1:50
PE3(config-vrf-inspur)#address-family ipv4
PE3(config-vrf-inspur-af-ipv4)#exit
PE3(config-vrf-inspur)#exit

PE3(config)#interface gei-0/4
PE3(config-if-gei-0/4)#no shutdown
PE3(config-if-gei-0/4)#ip address 13.1.1.2 255.255.255.0
PE3(config-if-gei-0/4)#exit
PE3(config)#interface gei-0/1
PE3(config-if-gei-0/1)#no shutdown
PE3(config-if-gei-0/1)#ip vrf for inspur
PE3(config-if-gei-0/1)#ip address 100.1.1.63 255.255.255.0
PE3(config-if-gei-0/1)#exit

PE3(config)#router ospf 1
PE3(config-ospf-1)#router-id 3.3.3.3
PE3(config-ospf-1)#area 0
PE3(config-ospf-1-area-0)#network 13.1.1.0 0.0.0.255
PE3(config-ospf-1-area-0)#network 3.3.3.3 0.0.0.0
PE3(config-ospf-1-area-0)#exit

PE3(config)#router ospf 100 vrf inspur
PE3(config-ospf-100)#redistribute bgp-int
PE3(config-ospf-100)#area 0
PE3(config-ospf-100-area-0)#network 100.1.1.0 0.0.0.255
PE3(config-ospf-100-area-0)#exit

PE3(config)#mpls ldp instance 1
PE3(config-ldp-1)#router-id loopback1
PE3(config-ldp-1)#interface gei-0/4
PE3(config-ldp-1-if-gei-0/4)#exit
PE3(config-ldp-1)#exit

PE3(config)#router bgp 18004
PE3(config-bgp)#neighbor 1.1.1.1 remote-as 18004
PE3(config-bgp)#neighbor 1.1.1.1 update-source loopback1
PE3(config-bgp)#neighbor 1.1.1.1 fall-over bfd
PE3(config-bgp)#address-family vpnv4
PE3(config-bgp-af-vpnv4)#neighbor 1.1.1.1 activate
PE3(config-bgp-af-vpnv4)#exit
PE3(config-bgp)#address-family ipv4 vrf inspur
PE3(config-bgp-af-ipv4-vrf)#redistribute ospf-int 100
PE3(config-bgp-af-ipv4-vrf)#exit
PE3(config-bgp)#exit
```

CE2上的配置：

```
CE2(config)#interface gei-0/10
CE2(config-if-gei-0/10)#no shutdown
CE2(config-if-gei-0/10)#ip address 192.1.1.64 255.255.255.0
CE2(config-if-gei-0/10)#exit
CE2(config)#interface gei-0/3
CE2(config-if-gei-0/3)#no shutdown
CE2(config-if-gei-0/3)#ip address 200.1.1.2 255.255.255.0
CE2(config-if-gei-0/3)#exit
CE2(config)#interface gei-0/1
CE2(config-if-gei-0/1)#no shutdown
CE2(config-if-gei-0/1)#ip address 100.1.1.2 255.255.255.0
CE2(config-if-gei-0/1)#exit

CE2(config)#router ospf 1
CE2(config-ospf-1)#area 0
CE2(config-ospf-1-area-0)#network 100.1.1.0 0.0.0.255
CE2(config-ospf-1-area-0)#network 200.1.1.0 0.0.0.255
CE2(config-ospf-1-area-0)#network 192.1.1.0 0.0.0.255
```

```
CE2(config-ospf-1-area-0)#exit
```

配置验证

PE1上验证情况：

```
PE1#show ip protocol routing vrf inspur
network 192.1.1.0 mask 255.255.255.0
Heads: Dest = Destination, Prf\RoutePrf = Router preference,
      Metric\RouteMetric = Router metric
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
      OSPF-7D = ospf-type7-discard, USER-I = user-ipaddr, RIP-D = rip-discard,
      OSPF-E = ospf-ext, ASBR-V = asbr-vpn, GW-FWD = ps-busi, GW-UE = ps-user,
      BGP-AD = bgp-aggr-discard, BGP-CE = bgp-confed-ext, NAT64 = sl-nat64-v4,
      USER-N = user-network, USER-S = user-special, DHCP-S = dhcp-static,
      DHCP-D = dhcp-dft, VES = video-enhanced-service
Marks: *valid, >best, s-stale

   Dest             NextHop        InTag   OutTag  Prf Metric     Protocol
*>  192.1.1.0/24      2.2.2.2        notag   212994  200 3          BGP-INT
*>  192.1.1.0/24      3.3.3.3        notag   212994  200 3          BGP-INT
PE1(config)#show ip forwarding route vrf inspur 192.1.1.0
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest          Gw          Interface          Owner      Pri Metric
*> 192.1.1.0/24  3.3.3.3     gei-0/2            BGP        200 3
PE1(config)#show ip forwarding backup route vrf inspur 192.1.1.0
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority, M/S: Master/Slave,
 Sta: Status;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best, M: Master, S: Slave, I: Inuse, U: Unuse;
 Dest           Gw      Interface Owner Pri Metric M/S Sta
*> 192.1.1.0/24 3.3.3.3 gei-0/2   bgp   200 3      M   I
*> 192.1.1.0/24 2.2.2.2 gei-0/3   bgp   200 3      S   U

PE1(config)#show bgp vpnv4 unicast detail 1:50 192.1.1.0 255.255.255.0
BGP routing table entry for 1:50 192.1.1.0/24
3d4h received from 2.2.2.2 (2.2.2.2), path-id 0
   Origin ?, nexthop 2.2.2.2, metric 3, localpref 100,weight 0, rtpref 200, best,
   As path
   As4 path
   Extended Community:RT:1:50 ,OSPF domain id :0x0005:000000640100 ,OSPF router
id :200.1.1.60,OSPF route type :0:1:0
   Received label  212994

3d4h received from 3.3.3.3 (3.3.3.3), path-id 0
   Origin ?, nexthop 3.3.3.3, metric 3, localpref 100,weight 0, rtpref 200, best,
   As path
   As4 path
   Extended Community:RT:1:50 ,OSPF domain id :0x0005:000000640100 ,OSPF router
id :100.1.1.63,OSPF route type :0:1:0
   Received label  212994
```

由上可知，在PE1上形成了VPN的FRR关系，当PE1跟PE2之间的主链路down的时候，

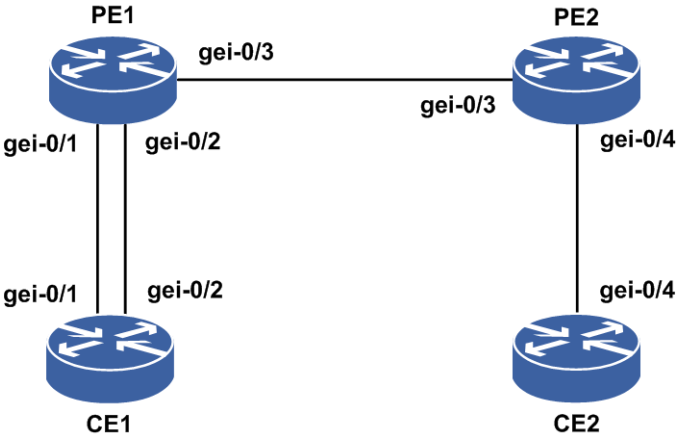
PE1上VPN的FRR关系就会从主链路切换到备用链路，从而达到快速切换的目的。

7.3.5.3 L3VPN 接入侧 FRR 配置实例

配置说明

如*图 7-24*所示，CE1通过IS-IS接入到PE1上的VRF inspur, CE2通过IS-IS接入到PE2上的VRF inspur，分别在PE1、PE2上的VRF地址族下重分发IS-IS。PE1与PE2建立LDP/MPBGP的邻居。

图 7-24 L3VPN 接入侧 FRR 配置实例组网图



配置思路

1.按上图所示搭建环境，PE1与PE2搭建MP-IBGP环境

2.CE1、CE2分别与PE1、PE2的VRF接入接口创建IS-IS邻居

3.分别在PE1、PE2上的VRF地址族下重分发IS-IS

4.在PE1的vrf下配置FRR

配置过程

CE1上的配置如下：

```
/*配置接口IP地址*/
CE1(config)#interface gei-0/1
CE1(config-if-gei-0/1)#no shutdown
CE1(config-if-gei-0/1)#ip address 100.101.1.11 255.255.255.0
CE1(config-if-gei-0/1)#exit
CE1(config)#interface gei-0/2
CE1(config-if-gei-0/2)#no shutdown
CE1(config-if-gei-0/2)#ip address 100.101.2.11 255.255.255.0
CE1(config-if-gei-0/2)#exit
```

```
/*配置IS-IS邻居*/
CE1(config)#router isis 2
CE1(config-isis-2)#area 00
CE1(config-isis-2)#system-id 2002.1234.2CE1
CE1(config-isis-2)#interface gei-0/1
CE1(config-isis-2-if-gei-0/1)#ip router isis
CE1(config-isis-2-if-gei-0/1)#exit
CE1(config-isis-2)#interface gei-0/2
CE1(config-isis-2-if-gei-0/2)#ip router isis
CE1(config-isis-2-if-gei-0/2)#metric 15
CE1(config-isis-2-if-gei-0/2)#exit
CE1(config-isis-2)#exit
```

PE1的配置如下：

```
/*配置VRF*/
PE1(config)#ip vrf inspur
PE1(config-vrf-inspur)#rd 1:50
PE1(config-vrf-inspur)#route-target both 1:50
PE1(config-vrf-inspur)#address-family ipv4
PE1(config-vrf-inspur-af-ipv4)#exit
PE1(config-vrf-inspur)#exit

/*配置接口IP地址*/
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
PE1(config-if-loopback1)#exit
PE1(config)#interface gei-0/1
PE1(config-if-gei-0/1)#no shutdown
PE1(config-if-gei-0/1)#ip vrf forwarding inspur
PE1(config-if-gei-0/1)#ip address 100.101.1.1 255.255.255.0
PE1(config-if-gei-0/1)#exit
PE1(config)#interface gei-0/2
PE1(config-if-gei-0/2)#no shutdown
PE1(config-if-gei-0/2)#ip vrf forwarding inspur
PE1(config-if-gei-0/2)#ip address 100.101.2.1 255.255.255.0
PE1(config-if-gei-0/2)#exit
PE1(config)#interface gei-0/3
PE1(config-if-gei-0/3)#no shutdown
PE1(config-if-gei-0/3)#ip address 100.101.3.1 255.255.255.0
PE1(config-if-gei-0/3)#exit

/*配置接入侧IS-IS邻居*/
PE1(config)#router isis 2 vrf inspur
PE1(config-isis-2)#area 00
PE1(config-isis-2)#system-id 2002.1234.2PE1
PE1(config-isis-2)#interface gei-0/1
PE1(config-isis-2-if-gei-0/1)#ip router isis
PE1(config-isis-2-if-gei-0/1)#exit
PE1(config-isis-2)#interface gei-0/2
PE1(config-isis-2-if-gei-0/2)#ip router isis
PE1(config-isis-2-if-gei-0/2)#exit
PE1(config-isis-2)#exit

/*PE间用IS-IS邻居打通*/
PE1(config)#router isis 1
PE1(config-isis-1)#area 00
PE1(config-isis-1)#system-id 1001.1234.1PE1
PE1(config-isis-1)#interface gei-0/3
PE1(config-isis-1-if-gei-0/3)#ip router isis
PE1(config-isis-1-if-gei-0/3)#exit
PE1(config-isis-1)#interface loopback1
PE1(config-isis-1-if-loopback1)#ip router isis
PE1(config-isis-1-if-loopback1)#exit
PE1(config-isis-1)#exit
```

```
/*配置LDP邻居*/
PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#interface gei-0/3
PE1(config-ldp-1-if-gei-0/3)#exit
PE1(config-ldp-1)#exit

/*配置MIBGP邻居*/
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 1.1.1.2 remote-as 100
PE1(config-bgp)#neighbor 1.1.1.2 update-source loopback1
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 1.1.1.2 activate
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#address-family ipv4 vrf inspur
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#redistribute isis-1-2 2
PE1(config-bgp-af-ipv4-vrf)#bgp frr
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#exit
```

PE2上的配置如下：

```
/*配置VRF*/
PE2(config)#ip vrf inspur
PE2(config-vrf-inspur)#rd 1:50
PE2(config-vrf-inspur)#route-target both 1:50
PE2(config-vrf-inspur)#address-family ipv4
PE2(config-vrf-inspur-af-ipv4)#exit
PE2(config-vrf-inspur)#exit

/*配置接口IP地址*/
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 1.1.1.2 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#interface gei-0/3
PE2(config-if-gei-0/3)#no shutdown
PE2(config-if-gei-0/3)#ip address 100.101.3.2 255.255.255.0
PE2(config-if-gei-0/3)#exit
PE2(config)#interface gei-0/4
PE2(config-if-gei-0/4)#no shutdown
PE2(config-if-gei-0/4)#ip vrf for inspur
PE2(config-if-gei-0/4)#ip address 100.101.4.2 255.255.255.252
PE2(config-if-gei-0/4)#exit

/*配置接入侧IS-IS邻居*/
PE2(config)#router isis 2 vrf inspur
PE2(config-isis-2)#area 00
PE2(config-isis-2)#system-id 2002.1234.2PE2
PE2(config-isis-2)#interface gei-0/4
PE2(config-isis-2-if-gei-0/4)#ip router isis
PE2(config-isis-2-if-gei-0/4)#exit
PE2(config-isis-2)#exit

/*PE间用IS-IS邻居打通*/
PE2(config)#router isis 1
PE2(config-isis-1)#area 00
PE2(config-isis-1)#system-id 1001.1234.1PE2
PE2(config-isis-1)#interface gei-0/3
PE2(config-isis-1-if-gei-0/3)#ip router isis
PE2(config-isis-1-if-gei-0/3)#exit
PE2(config-isis-1)#exit

/*配置LDP邻居*/
PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
```

```
PE2(config-ldp-1)#interface gei-0/3
PE2(config-ldp-1-if-gei-0/3)#exit
PE2(config-ldp)#exit

/*配置MIBGP邻居*/
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 18004
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback1
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 1.1.1.1  activate
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#address-family ipv4 vrf inspur
PE2(config-bgp-af-ipv4-vrf)#redistribute connected
PE2(config-bgp-af-ipv4-vrf)#redistribute isis-1-2 2
PE2(config-bgp-af-ipv4-vrf)#exit
PE2(config-bgp)#exit
```

CE2上的配置如下：

```
/*配置接口IP地址*/
CE2(config)#interface gei-0/4
CE2(config-if-gei-0/4)#no shutdown
CE2(config-if-gei-0/4)#ip address 100.101.4.22  255.255.255.0
CE2(config-if-gei-0/4)#exit

/*配置IS-IS邻居*/
CE2(config)#router isis 2
CE2(config-isis-2)#area 00
CE2(config-isis-2)#system-id 2002.1234.2CE2
CE2(config-isis-2)#interface gei-0/4
CE2(config-isis-2-if-gei-0/4)#ip router isis
CE2(config-isis-2-if-gei-0/4)#exit
CE2(config-isis-2)#exit
```

7.3.6 MPLS L3VPN 负荷分担

在实际应用中，根据不同的路由建立多条LSP，并且通过一定的规则将数据流量进行均衡，分配到不同的链路上进行转发，从而实现MPLS负荷分担的功能。

7.3.6.1 配置 MPLS L3VPN VRF 负荷分担

本节介绍MPLS L3VPN的VRF负荷分担的配置步骤和命令。

1.配置负荷分担模式。

步骤	命令	功能
1	inspur(config)#**interface** {<*interface-name*>| **byname** <*byname*>}	进入接口配置模式
2	inspur(config-if-interface-name)#**ip load-sharing** [per-packet|per-destination]	配置负荷分担模式

per-packet：负荷分担流量基于包转发。

per-destination：负荷分担流量基于目的地转发。

2.配置MPLS L3VPN VRF负荷分担。

配置静态路由的负荷分担：

命令	功能
inspur(config)#**ip route vrf** <*vrf-name*><*ip-address*><*net-mask*><*next-hop address*>[<*1~255*>| **global**	**tag**<*1~4294967295*>]	在PE上全局模式下配置负荷分担的VRF静态路由

<*1~255*>：目的路由的metric值，范围1~255。

配置RIP路由的负荷分担：

步骤	命令	功能
1	inspur(config-rip)#**address-family ipv4 vrf** <*vrf-name*>	进入RIP协议中的address-family IPv4 vrf地址族下
2	inspur(config-rip-af)#**maximum-paths** <*1~32*>	在PE上的RIP协议中的address-family IPv4 vrf地址族下面配置负荷分担命令

<*1~32*>：需要形成的负荷分担的条目数。

配置BGP路由的负荷分担：

步骤	命令	功能
1	inspur(config-bgp)#**address-family ipv4 vrf** <*vrf-name*>	进入BGP协议中的address-family IPv4 vrf地址族下
2	inspur(config-bgp-af-ipv4-vrf)#**maximum-paths**[**ibgp**] <*1~64*>	在PE的BGP的address-family IPv4 vrf地址族下面配置负荷分担命令

配置IS-IS路由的负荷分担：

命令	功能
inspur(config-isis-process-id)#**maximum-paths** <*1~64*>	在PE上的IS-IS协议中的VRF实例的路由模式下配置负荷分担命令

配置OSPF路由的负荷分担：

命令	功能
inspur(config-ospf-process-id)#**maximum-paths** <*1~64*>	在PE上的OSPF协议中的VRF实例的路由模式下配置负荷分担命令

3.验证配置结果。

命令	功能
inspur#**show ip forwarding route vrf** <*vrf-name*>{[{<*Network to display information*>}[<*Network mask*>{**weak-match**|**exact-match**}]]|[<*Protocol name*>]}	显示指定VPN中的路由

7.3.6.2 配置 MPLS L3VPN MPBGP 负荷分担

本节介绍MPLS L3VPN MPBGP负荷分担的配置步骤和命令。

1.配置负荷分担模式。

步骤	命令	功能
1	inspur(config)#**interface** {<*interface-name*>| **byname** <*byname*>}	进入接口配置模式
2	inspur(config-if-interface-name)#**ip load-sharing** [**per-packet** | **per-destination**]	配置负荷分担模式

per-packet：负荷分担流量基于包转发。

per-destination：负荷分担流量基于目的地转发。

2.配置负荷分担。

步骤	命令	功能
1	inspur(config)#**router bgp** <*as-number*>	启用BGP进程并指定本路由器所在的AS号
2	inspur(config-bgp)#**address-family ipv4 vrf** <*vrf-name*>	激活IPv4地址族
3	inspur(config-bgp-af-ipv4-vrf)#**maximum-paths**[**ibgp**]<*1~64*>	在PE的BGP的address-family IPv4 vrf地址族下面配置负荷分担命令

3.验证配置结果。

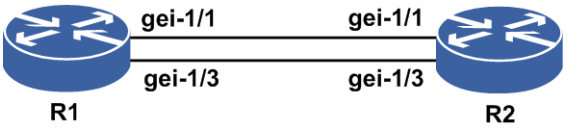
命令	功能
inspur#**show bgp vpnv4 unicast detail** <*VPN Route Distinguisher*><*ip-address*><*mask*>	显示指定VPN路由的详细信息

7.3.6.3 MPLS L3VPN 公网 LDP 负荷分担配置实例

配置说明

如*图 7-25*所示是一个LDP负荷分担配置实例。R1和R2之间存在两条链路。

图 7-25 MPLS L3VPN 公网 LDP 负荷分担配置实例示意图



以OSPF路由负荷分担为例，两台路由器的配置任务如下：

路由器	接口及地址	接口及地址	环回接口及地址
R1	gei-1/1 1.1.1.1/24	gei-1/3 2.2.2.2/24	loopback1 4.4.4.4
R2	gei-1/1 1.1.1.2/24	gei-1/3 2.2.2.3/24	loopback1 5.5.5.5

配置思路

1.配置好各LSR上的接口地址。

2.在两个LSR上配置本地的OSPF规则。

3.配置MPLS LDP功能，并向LDP添加相应的接口。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ip address 1.1.1.1 255.255.255.0
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#ip address 2.2.2.2 255.255.255.0
R1(config-if-gei-1/3)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 4.4.4.4  255.255.255.255
R1(config-if-loopback1)#exit

R1(config)#router ospf 1
R1(config-ospf-1)#router-id 4.4.4.4
R1(config-ospf-1)#maximum-paths 2
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 4.4.4.4  0.0.0.0
R1(config-ospf-1-area-0)#network 1.1.1.0 0.0.0.255
R1(config-ospf-1-area-0)#network 2.2.2.0 0.0.0.255
R1(config-ospf-1-area-0)#exit

R1(config)#mpls ldp instance 1
```

```
R1(config-ldp-1)#router-id loopback1
R1(config-ldp-1)#interface gei-1/1
R1(config-ldp-1-if-gei-1/1)#exit
R1(config-ldp-1)#interface gei-1/3
R1(config-ldp-1-if-gei-1/3)#exit
R1(config-ldp-1)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 1.1.1.2 255.255.255.0
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#no shutdown
R2(config-if-gei-1/3)#ip address 2.2.2.3 255.255.255.0
R2(config-if-gei-1/3)#exit
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 5.5.5.5 255.255.255.255
R2(config-if-loopback1)#exit

R2(config)#router ospf 1
R2(config-ospf-1)#router-id 5.5.5.5
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 1.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#network 2.2.2.0 0.0.0.255
R2(config-ospf-1-area-0)#network 5.5.5.5 0.0.0.0
R2(config-ospf-1-area-0)#exit

R2(config)#mpls ldp instance 1
R2(config-ldp-1)#interface gei-1/1
R2(config-ldp-1-if-gei-1/1)#exit
R2(config-ldp-1)#interface gei-1/3
R2(config-ldp-1-if-gei-1/3)#exit
R2(config-ldp-1)#router-id loopback1
R2(config-ldp-1)#exit
```

至此，已经实现路由负载均衡。接下来创建负载均衡的LSP链路，以达到LDP负荷分担的目的。

配置验证

查看R1上的路由转发表：

```
R1(config)#show ip forwarding route 5.5.5.5
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
status codes: *valid, >best
Dest        Gw          Interface       Owner       Pri Metric
*>5.5.5.5/32   2.2.2.3     gei-1/3       OSPF         110  2
*>5.5.5.5/32   1.1.1.2     gei-1/1       OSPF         110  2
```

从转发表最后可以看到对于目的地址为5.5.5.5，掩码为255.255.255.255的网段，有两个下一跳：

- 通过接口gei-1/3到2.2.2.3。
- 通过接口gei-1/1到1.1.1.2。

在R1上运行show mpls forwarding-table命令：

```
R1(config)#show mpls forwarding-table 5.5.5.5
Local     Outgoing       Prefix or        Outgoing       Next Hop   M/S
label      label          Tunnel Id        interface
16402      Poptag          5.5.5.5/32      gei-1/3        2.2.2.3   M
16402      Poptag          5.5.5.5/32      gei-1/1        1.1.1.2   M
```

可以看到对于目的地址为5.5.5.5，掩码为255.255.255.255网段的标签表里面有2个下一跳，说明对于该网段的FEC，本地和远端之间存在两个会话，即两条LSP。这两条LSP就是**show ip forwarding route**命令显示的两个下一跳形成的。

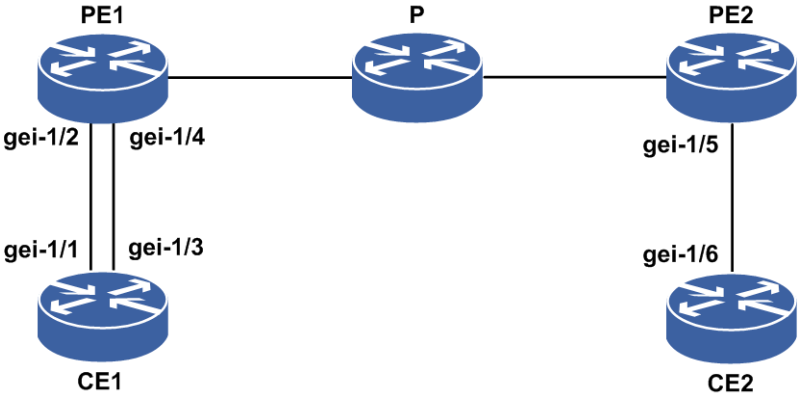
此时，已实现负载均衡，可以通过接口流量统计查看MPLS负荷分担的情况。

7.3.6.4 MPLS L3VPN VRF 负荷分担配置实例

配置说明

如*图 7-26*所示，搭建L3VPN的环境。

图 7-26 MPLS L3VPN VRF 负荷分担配置实例示意图



在PE1和PE2上存在VRF，命名为inspur，RD为1：1，RT为1：1，接口gei-1/2、gei-1/4、gei-1/5全部绑定到VRF inspur中，接口地址分别设置为：

路由器	接口	地址
PE1	gei-1/2	10.1.1.2/24
	gei-1/4	10.1.2.2/24
CE1	gei-1/1	10.1.1.1/24
	gei-1/3	10.1.2.1/24
PE2	gei-1/5	10.1.3.1/24
CE2	gei-1/6	10.1.3.2/24

配置思路

1.将接口gei-1/2、gei-1/4、gei-1/5全部绑定到VRF inspur中。

2.PE1和P、P和PE2之间分别建立IGP和LDP邻居关系，并互相通告loopback地址。

3.PE1和PE2之间使用loopback地址建立MPBGP邻居。

4.在接口gei-1/1、gei-1/2、gei-1/3、gei-1/4上配置VRF负荷分担，在VRF模式下配置负荷分担命令。

配置过程

1.CE1和PE1之间建立OSPF邻居。

CE1的配置如下：

```
CE1(config)#interface loopback1
CE1(config-if-loopback1)#ip address 20.1.1.1 255.255.255.255
CE1(config-if-loopback1)#exit

CE1(config)#router ospf 10
CE1(config-ospf-10)#maximum-paths 2
CE1(config-ospf-10)#area 0
CE1(config-ospf-10-area-0)#network 10.1.1.0 0.0.0.255
CE1(config-ospf-10-area-0)#network 10.1.2.0 0.0.0.255
CE1(config-ospf-10-area-0)#network 20.1.1.1 0.0.0.0
CE1(config-ospf-10-area-0)#exit
```

PE1的配置如下：

```
PE1(config)#router ospf 10 vrf inspur
PE1(config-ospf-10)#redistribute bgp-int
PE1(config-ospf-10)#area 0
PE1(config-ospf-10-area-0)#network 10.1.1.0 0.0.0.255
PE1(config-ospf-10-area-0)#network 10.1.2.0 0.0.0.255
PE1(config-ospf-10-area-0)#exit
```

在PE1上BGP的IPv4 vrf模式下重新分配OSPF路由和直连路由：

```
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf inspur
PE1(config-bgp-af-ipv4-vrf)#redistribute ospf-int 10
PE1(config-bgp-af-ipv4-vrf)#redistribute connect
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#exit
```

在PE1的VRF模式下配置负荷分担命令：

```
PE1(config)#router ospf 10 vrf inspur
PE1(config-ospf-10)#maximum-paths 2
PE1(config-ospf-10)#exit
```

2.CE2和PE2之间建立OSPF邻居。

CE2的配置如下：

```
CE2(config)#router ospf 10
CE2(config-ospf-10)#area 0
CE2(config-ospf-10-area-0)#network 10.1.3.0 0.0.0.255
CE2(config-ospf-10-area-0)#exit
```

PE2的配置如下：

```
PE2(config)#router ospf 10 vrf inspur
PE2(config-ospf-10)#redistribute bgp-int
PE2(config-ospf-10)#area 0
PE2(config-ospf-10-area-0)#network 10.1.3.0 0.0.0.255
PE2(config-ospf-10-area-0)#exit
```

在PE2上BGP的IPv4 vrf模式下配置重新分配直连命令：

```
PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv4 vrf inspur
PE2(config-bgp-af-ipv4-vrf)#redistribute connect
PE2(config-bgp-af-ipv4-vrf)#exit
PE2(config-bgp)#exit
```

3.在接口gei-1/1、gei-1/2、gei-1/3、gei-1/4上分别配置负荷分担命令。

CE1的配置如下：

```
CE1(config)#interface gei-1/1
CE1(config-if-gei-1/1)#no shutdown
CE1(config-if-gei-1/1)#ip load-sharing per-packet
CE1(config-if-gei-1/1)#exit
CE1(config)#interface gei-1/3
CE1(config-if-gei-1/3)#no shutdown
CE1(config-if-gei-1/3)#ip load-sharing per-packet
CE1(config-if-gei-1/3)#exit
```

PE1的配置如下：

```
PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#no shutdown
PE1(config-if-gei-1/2)#ip load-sharing per-packet
PE1(config-if-gei-1/2)#exit
PE1(config)#interface gei-1/4
PE1(config-if-gei-1/4)#no shutdown
PE1(config-if-gei-1/4)#ip load-sharing per-packet
PE1(config-if-gei-1/4)#exit
```

配置验证

在PE1上使用命令**show ip protocol routing vrf inspur**，可以查看到CE1通告给PE1的IP地址为20.1.1.1，子网掩码为255.255.255.255的两条路由，并且都为其分配了标签：

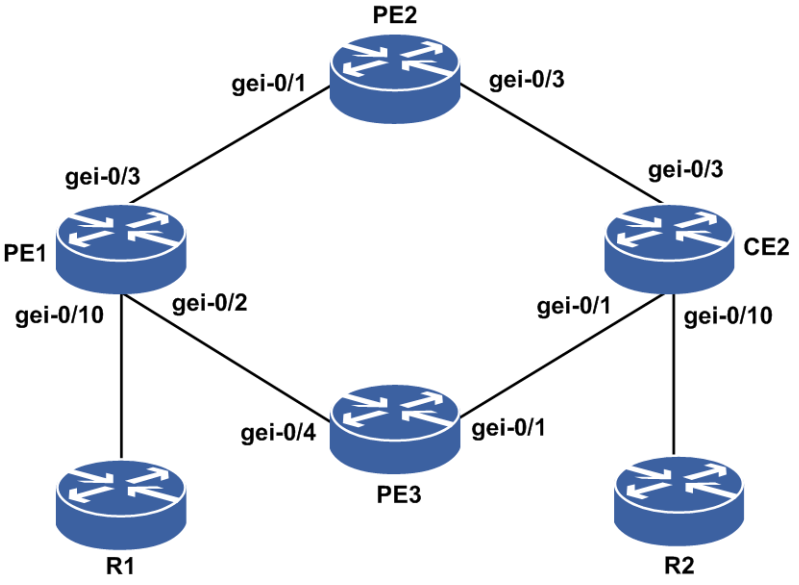
```
PE1#show ip protocol routing vrf inspur
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale
Dest            NextHop    Intag    Outtag   RtPrf   Protocol
*>  20.1.1.1/32   10.1.1.1   163840   notag    110     OSPF
*>  20.1.1.1/32   10.1.2.1   163840   notag    110     OSPF
```

7.3.6.5 MPLS L3VPN MPBGP 负荷分担配置实例

配置说明

如*图 7-27*所示，PE1分别与PE2、PE3搭建L3VPN的环境。

图 7-27 MPLS L3VPN MPBGP 负荷分担配置实例示意图



配置思路

1.PE1分别与PE2、PE3搭建MPIBGP环境。

2.CE2分别与PE2、PE3的VRF接入接口创建OSPF邻居，CE2与R2创建OSPF邻居。

3.分别在PE2、PE3上的VRF地址族下重分发OSPF。

4.在PE1的VRF下配置IBGP的负荷分担。

配置过程

PE与PE之间的OSPF和LDP配置参见"MPLS L3VPN公网LDP负荷分担配置实例"。

PE1的配置如下：

```
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 172.20.96.2 255.255.255.255
PE1(config-if-loopback1)#exit

PE1(config)#ip vrf inspur
PE1(config-vrf-inspur)#rd 1:50
PE1(config-vrf-inspur)#route-target both 1:50
PE1(config-vrf-inspur)#address-family ipv4
PE1(config-vrf-inspur-af-ipv4)#exit
PE1(config-vrf-inspur)#exit
```

```
PE1(config)#router bgp 18004
PE1(config-bgp)#neighbor 172.20.96.1 remote-as 18004
PE1(config-bgp)#neighbor 172.20.96.1 update-source loopback1
PE1(config-bgp)#neighbor 172.20.108.2 remote-as 18004
PE1(config-bgp)#neighbor 172.20.108.2 update-source loopback1
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 172.20.96.1 activate
PE1(config-bgp-af-vpnv4)#neighbor 172.20.108.2 activate
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#address-family ipv4 vrf inspur
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#maximum-paths ibgp 2
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#exit

PE1(config)#interface gei-0/10
PE1(config-if-gei-0/10)#no shutdown
PE1(config-if-gei-0/10)#ip vrf forwarding inspur
PE1(config-if-gei-0/10)#ip address 202.10.10.61 255.255.255.0
PE1(config-if-gei-0/10)#exit
```

PE2的配置如下：

```
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 172.20.96.1 255.255.255.255
PE2(config-if-loopback1)#exit

PE2(config)#ip vrf inspur
PE2(config-vrf-inspur)#rd 1:50
PE2(config-vrf-inspur)#route-target both 1:50
PE2(config-vrf-inspur)#address-family ipv4
PE2(config-vrf-inspur-af-ipv4)#exit
PE2(config-vrf-inspur)#exit

PE2(config)#router bgp 18004
PE2(config-bgp)#neighbor 172.20.96.2 remote-as 18004
PE2(config-bgp)#neighbor 172.20.96.2 update-source loopback1
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 172.20.96.2 activate
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#address-family ipv4 vrf inspur
PE2(config-bgp-af-ipv4-vrf)#redistribute ospf-int 100
PE2(config-bgp-af-ipv4-vrf)#exit
PE2(config-bgp)#exit

PE2(config)#interface gei-0/3
PE2(config-if-gei-0/3)#no shutdown
PE2(config-if-gei-0/3)#ip vrf forwarding inspur
PE2(config-if-gei-0/3)#ip address 200.1.1.60 255.255.255.0
PE2(config-if-gei-0/3)#exit

PE2(config)#router ospf 100 vrf inspur
PE2(config-ospf-100)#area 0
PE2(config-ospf-100-area-0)#network 200.1.1.0 0.0.0.255
PE2(config-ospf-100-area-0)#exit
```

PE3的配置如下：

```
PE3(config)#interface loopback1
PE3(config-if-loopback1)#ip address 172.20.108.2 255.255.255.255
PE3(config-if-loopback1)#exit

PE3(config)#ip vrf inspur
PE3(config-vrf-inspur)#rd 1:50
PE3(config-vrf-inspur)#route-target both 1:50
PE3(config-vrf-inspur)#address-family ipv4
PE3(config-vrf-inspur-af-ipv4)#exit
PE3(config-vrf)#exit
```

```
PE3(config)#router  bgp 18004
PE3(config-bgp)#neighbor 172.20.96.2 remote-as 18004
PE3(config-bgp)#neighbor 172.20.96.2 update-source loopback1
PE3(config-bgp)#address-family vpnv4
PE3(config-bgp-af-vpnv4)#neighbor 172.20.96.2 activate
PE3(config-bgp-af-vpnv4)#exit
PE3(config-bgp)#address-family ipv4 vrf inspur
PE3(config-bgp-af-ipv4-vrf)#redistribute ospf-int 100
PE3(config-bgp-af-ipv4-vrf)#exit
PE3(config-bgp)#exit

PE3(config)#interface gei-0/1
PE3(config-if-gei-0/1)#no shutdown
PE3(config-if-gei-0/1)#ip vrf forwarding inspur
PE3(config-if-gei-0/1)#ip address 100.1.1.63 255.255.255.0
PE3(config-if-gei-0/1)#exit

PE3(config)#router ospf 100 vrf inspur
PE3(config-ospf-100)#area 0
PE3(config-ospf-100-area-0)#network 100.1.1.0 0.0.0.255
PE3(config-ospf-100-area-0)#exit
```

CE2的配置如下：

```
CE2(config)#interface gei-0/10
CE2(config-if-gei-0/10)#no shutdown
CE2(config-if-gei-0/10)#ip address 192.1.1.64 255.255.255.0
CE2(config-if-gei-0/10)#exit
CE2(config)#interface gei-0/1
CE2(config-if-gei-0/1)#no shutdown
CE2(config-if-gei-0/1)#ip address 100.1.1.64 255.255.255.0
CE2(config-if-gei-0/1)#exit
CE2(config)#interface gei-0/3
CE2(config-if-gei-0/3)#no shutdown
CE2(config-if-gei-0/3)#ip address 200.1.1.64 255.255.255.0
CE2(config-if-gei-0/3)#exit

CE2(config)#router ospf 1
CE2(config-ospf-1)#area 0
CE2(config-ospf-1-area-0)#network 100.1.1.0 0.0.0.255
CE2(config-ospf-1-area-0)#network 200.1.1.0 0.0.0.255
CE2(config-ospf-1-area-0)#network 192.1.1.0 0.0.0.255
CE2(config-ospf-1-area-0)#exit
```

配置验证

在PE1上使用命令**show ip protocol routing vrf**查看相关信息：

```
PE1(config)#show ip protocol routing vrf inspur network 192.1.1.0
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale
    Dest            NextHop        Intag    Outtag    RtPrf    Protocol
*>  192.1.1.0/24      172.20.108.2    213003    229125    200      BGP-INT
*>  192.1.1.0/24      172.20.96.1     213003    212998    200      BGP-INT
```

此时BGP已经为这些路由分配好了标签。

```
PE1(config)#show ip forwarding route vrf inspur 192.1.1.0
IPv4 Routing Table:
```

```
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest              Gw            Interface         Owner     Pri Metric
192.1.1.0/24      172.20.108.2    gei-0/2       BGP      200 3
192.1.1.0/24      172.20.96.1     gei-0/3       BGP      200 3

PE1(config)#show bgp vpnv4 unicast
Status codes: *valid, >best, i-internal, s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete
    Network          Next Hop       Metric     Locprf     Path

Route Distinguisher: 1:50 (default for vrf inspur)
*>i  192.1.1.0/24      172.20.108.2     3         100        200    ?
*>i  192.1.1.0/24      172.20.96.1      3         100        200    ?
```

MPBGP学习到远端2个PE的VPN路由，当以下属性一样时，才能形成负荷分担的等价路由。

•AS号

•origin

•local-pref

•AS-path

```
PE1(config)#show
bgp vpnv4 unicast detail 1:50 192.1.1.0 255.255.255.0
BGP routing table entry for 1:50:192.1.1.0/24
  01:38:07 received from 172.20.108.2 (172.20.108.2)
   origin ?,nexthop 172.20.108.2,metric 3,localpref 100, rtpref 200,best,
   as path
   as4 path
   extended Community:RT:1:50
 received label
220712
  01:38:06 received from 172.20.96.1 (172.20.96.1)
   origin ?,nexthop 172.20.96.1,metric 3,localpref 100, rtpref 200,best,
   as path
   as4 path
   extended Community:RT:1:50
 received label
 212998
```

7.3.7 MPLS L3VPN 跨域

随着MPLS L3VPN解决方案的广泛应用，运营商的不同城域网之间，或相互协作的运营商的骨干网之间都存在跨越不同自治域的情况。

一般的MPLS L3VPN体系结构都是在一个自治系统内运行，任何VPN的路由信息只能在一个自治系统内按需扩散，没有提供自治系统内的VPN信息向其他自治系统扩散的功能。跨域（Inter-AS）的MPLS L3VPN功能支持运营商之间的VPN路由信息交换，可以穿过运营商间的链路来发布路由前缀和标签信息。

IR12000智能路由器支持3种跨域VPN解决方案：

•跨域VPN-OptionA方式，需要跨域的VPN在ASBR间通过专用的接口管理自己的VPN路由，也称之为VRF-to-VRF。

·跨域VPN-OptionB方式，ASBR间通过MP-EBGP发布标签VPN-IPv4路由。

·跨域VPN-OptionC方式，PE间通过Multi-hop MP-EBGP发布VPN-IPv4路由。

7.3.7.1 配置 MPLS L3VPN 跨域

本节介绍MPLS L3VPN跨域的配置步骤和命令。

1.配置MPLS L3VPN跨域。

配置MPLS L3VPN跨域参见MPLS L3VPN基本功能。

2.验证配置结果。

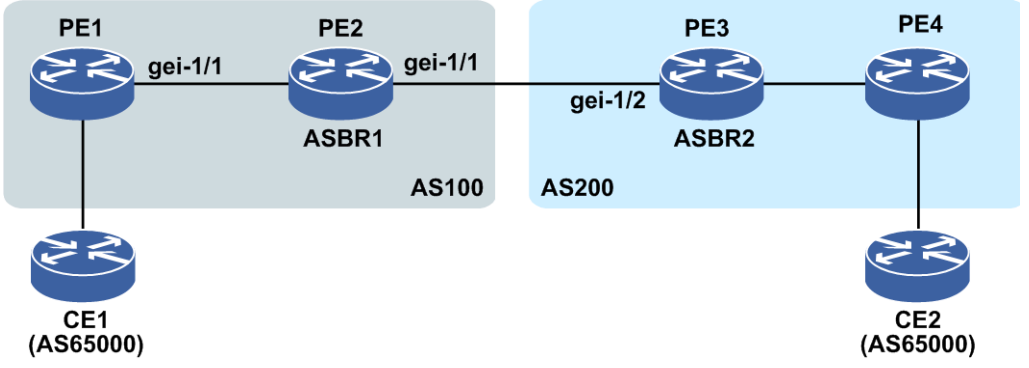
MPLS L3VPN跨域的配置结果验证参见MPLS L3VPN基本功能。

7.3.7.2 MPLS L3VPN 跨域 OptionA 配置实例

配置说明

如*图 7-28*所示，客户的两个站点之间需要有VPN连接。但是，站点1（CE1）连接到AS100，而站点2（CE2）连接到AS200，两个站点都提供MPLS VPN。为了建立两个站点间的MPLS VPN的连接性，运用MPLS L3VPN跨域OptionA的方法，这是实现AS间的VPN的最简单的办法。

图 7-28 MPLS L3VPN 跨域 OptionA 配置实例示意图



配置思路

1.PE1、PE2、PE3和PE4皆有VPN1，设置其RD和RT均为1:1。

2.PE1与PE2之间、PE3和PE4之间建立LDP、IGP、MP-IBGP邻居关系，Loopback地址采用IGP协议通告。

3.两个ASBR之间是背靠背的vrf，并通过vrf接口建立EBGP。

配置过程

1.将PE1与CE1对接的接口划分到VPN1中，PE1-CE1间采用EBGP接入：

```
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf vpn1
PE1(config-bgp-af-ipv4-vrf)#neighbor 100.1.1.2 remote-as 65000
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#exit
```

2.PE1和PE2间分别用Loopback1地址1.2.3.4、2.3.4.5建立MP-IBGP：

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 2.3.4.5  remote-as 100
PE1(config-bgp)#neighbor 2.3.4.5 update-source loopback1
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 2.3.4.5 activate
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#exit

PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.2.3.4 remote-as 100
PE2(config-bgp)#neighbor 1.2.3.4 update-source loopback1
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 1.2.3.4 activate
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#exit
```

3.将PE4与CE2对接的接口划分到VPN1中，PE4-CE2间采用EBGP接入：

```
PE4(config)#router bgp 200
PE4(config-bgp)#address-family ipv4 vrf vpn1
PE4(config-bgp-af-ipv4-vrf)#neighbor 200.1.1.2 remote-as 65000
PE4(config-bgp-af-ipv4-vrf)#exit
PE4(config-bgp)#exit
```

PE间皆有IPv4和VPNv4能力。

4.PE3和PE4间分别用Loopback1地址3.4.5.6、4.5.6.7建立MP-IBGP：

```
PE3(config)#router bgp 200
PE3(config-bgp)#neighbor 4.5.6.7 remote-as 200
PE3(config-bgp)#neighbor 4.5.6.7 update-source loopback1
PE3(config-bgp)#address-family vpnv4
PE3(config-bgp-af-vpnv4)#neighbor 4.5.6.7 activate
PE3(config-bgp-af-vpnv4)#exit
PE3(config-bgp)#exit

PE4(config)#router bgp 200
PE4(config-bgp)#neighbor 3.4.5.6 remote-as 200
PE4(config-bgp)#neighbor 3.4.5.6  update-source loopback1
PE4(config-bgp)#address-family vpnv4
PE4(config-bgp-af-vpnv4)#neighbor 3.4.5.6  activate
PE4(config-bgp-af-vpnv4)#exit
PE4(config-bgp)#exit
```

5.PE2在BGP的**address-family ipv4 vrf vpn1**模式下指定PE3为EBGP邻居，其中gei-1/2的地址为150.3.2.3：

```
PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv4 vrf vpn1
PE2(config-bgp-af-ipv4-vrf)#neighbor 150.3.2.3 remote-as 200
PE2(config-bgp-af-ipv4-vrf)#exit
PE2(config-bgp)#exit
```

6.将PE3上与PE2对接的接口划分到VPN1中：

```
PE3(config)#interface gei-1/2
PE3(config-if-gei-1/2)#no shutdown
PE3(config-if-gei-1/2)#ip vrf forwarding vpn1
PE3(config-if-gei-1/2)#ip address 150.3.2.3 255.255.255.0
PE3(config-if-gei-1/2)#exit
```

7.将PE2上与PE3对接的接口划分到VPN1中：

```
PE2(config)#interface gei-1/1
PE2(config-if-gei-1/1)#no shutdown
PE2(config-if-gei-1/1)#ip vrf forwarding vpn1
PE2(config-if-gei-1/1)#ip address 150.3.2.2 255.255.255.0
PE2(config-if-gei-1/1)#exit
```

8.PE3在BGP的**address-family ipv4 vrf vpn1**模式下指定PE2为EBGP邻居，其中gei-1/2的地址为150.3.2.2：

```
PE3(config)#router bgp 200
PE3(config-bgp)#address-family ipv4 vrf vpn1
PE3(config-bgp-af-ipv4-vrf)#neighbor 150.3.2.2 remote-as 100
PE3(config-bgp-af-ipv4-vrf)#exit
PE3(config-bgp)#exit
```

9.PE1在**address-family ipv4 vrf vpn1**模式下重分配直连路由：

```
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf vpn1
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#exit
```

10.PE4在**address-family ipv4 vrf vpn1**模式下通告200.1.1.0/24网段路由：

```
PE4(config)#router bgp 200
PE4(config-bgp)#address-family ipv4 vrf vpn1
PE4(config-bgp-af-ipv4-vrf)#network 200.1.1.0 255.255.255.0
PE4(config-bgp-af-ipv4-vrf)#exit
PE4(config-bgp)#exit
```

11.PE1和PE2间启用LDP建立LSP，其中PE1上和PE2连接的接口是gei-1/1：

```
PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#interface gei-1/1
PE1(config-ldp-1-if-gei-1/1)#exit
PE1(config-ldp-1)#exit
```

PE3和PE4间启用LDP建立LSP，配置同上。

配置验证

在PE1上使用**show bgp vpnv4 unicast vrf-summary vpn1**命令查看与100.1.1.2 EBGP邻居建立的结果：

```
PE1#show bgp vpnv4 unicast vrf-summary vpn1
Neighbor   Ver  As MsgRcvd MsgSend   Up/Down      State/PfxRcd

100.1.1.2 4    65000  0         0     00:10:00       2
```

在PE1上查看私网vrf的协议路由表：

```
PE1#show ip protocol routing vrf vpn1 network 200.1.1.0
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
```

```
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale

   Dest            NextHop       Intag    Outtag    RtPrf     Protocol
*>  200.1.1.0/24     2.3.4.5       213055   213012    200       BGP-INT
```

在PE2上使用**show bgp vpnv4 unicast neighbor 1.2.3.4**命令查看：

```
PE2#show bgp vpnv4 unicast neighbor 1.2.3.4
  BGP neighbor is 1.2.3.4, remote AS 100, internal link
  BGP version 4, remote router ID 1.2.3.4
  BGP state = Established, up for 22:27:17
  Last read update 00:18:51, hold time is 90 seconds, keepalive interval is 30
seconds
  Neighbor capabilities:
   Route refresh: advertised and received
   New ASN capability: advertised and received
   Address family IPv4 Unicast: advertised and received
   Address family VPNv4 Unicast: advertised and receivedRestart Capability:
   advertised and received
```

在PE2上查看私网vrf的协议路由表和私网转发表：

```
PE2#show ip protocol routing vrf vpn1 network 200.1.1.0
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale

   Dest            NextHop       Intag    Outtag    RtPrf    Protocol
*>  200.1.1.0/24     150.3.2.3     213012    notag    20       bgp-ext

PE2#show ip forwarding route vrf  vpn1 200.1.1.0
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
status codes: *valid, >best;
   Dest            Gw            Interface       Owner    Pri Metric
*> 200.1.1.0/24     150.3.2.3     gei-1/1          BGP      20  0
```

在PE4上使用**show bgp vpnv4 unicast vrf-summary vpn1**命令查看与200.1.1.2 EBGP邻居建立的结果：

```
PE4#show bgp vpnv4 unicast vrf-summary vpn1
Neighbor   Ver  As MsgRcvd MsgSend    Up/Down      State/PfxRcd

200.1.1.2   4    65000   0         0       00:15:00    2
```

在PE2上使用**show bgp vpnv4 unicast neighbor 4.5.6.7**命令查看：

```
PE2#show bgp vpnv4 unicast neighbor 4.5.6.7
  BGP version 4, remote router ID 4.5.6.7
  BGP state = Established, up for 22:27:17
  Last read update 00:18:51, hold time is 90 seconds, keepalive interval is 30
seconds
capabilities:
   Route refresh: advertised and received
```

```
Address family IPv4 Unicast: advertised and received
Address family VPNv4 Unicast: advertised and receivedRestart Capability:
advertised and received
```

在PE2上使用**show bgp vpnv4 unicast vrf-summary vpn1**命令查看与150.3.2.3（PE3）邻居建立的结果：

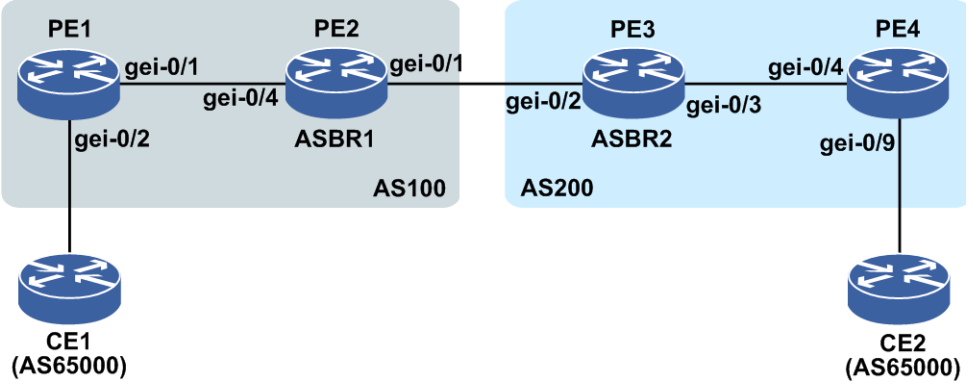
```
PE2#show bgp vpnv4 unicast vrf-summary vpn1
Neighbor   Ver  As MsgRcvd MsgSend   Up/Down      State/PfxRcd
150.3.2.3   4   200    0         0    00:22:35       2
```

7.3.7.3 MPLS L3VPN 跨域 OptionB 配置实例

配置说明

如*图 7-29*所示，客户的两个站点之间需要有VPN连接。但是，站点1（CE1）连接到AS100，而站点2（CE2）连接到AS200，两个站点都提供MPLS VPN。为了建立两个站点间的MPLS VPN的连接性，运用跨域OptionB的方法。

图 7-29 MPLS L3VPN 跨域 OptionB 配置实例示意图



配置思路

1.配置接口地址：

- PE1的左接口：gei-0/2，PE1的右接口：gei-0/1
- PE2的左接口：gei-0/4，PE2的右接口：gei-0/1
- PE3的左接口：gei-0/2，PE3的右接口：gei-0/3
- PE4的左接口：gei-0/4，PE4的右接口：gei-0/9

2.PE1、PE2、PE3和PE4皆有VPN1，设置其RD和RT均为1：10。

3.PE1与PE2之间、PE3和PE4之间建立LDP、IGP和MP-IBGP邻居关系，Loopback地址采用IGP协议通告。

4.PE2与PE3之间建立MP-EBGP。

配置过程

1.将PE1与CE1对接的接口划分到VPN1中，PE1-CE1间采用直连重分发。

2.PE1和PE2间分别用Loopback1地址1.2.3.1和1.2.3.2建立MP-IBGP。

PE1的配置如下：

```
PE1(config)#ip vrf vpn1
PE1(config-vrf-vpn1)#rd 1:10
PE1(config-vrf-vpn1)#route-target both 1:10
PE1(config-vrf-vpn1)#address-family ipv4
PE1(config-vrf-vpn1-af-ipv4)#exit
PE1(config-vrf-vpn1)#exit

PE1(config)#interface gei-0/2
PE1(config-if-gei-0/2)#no shutdown
PE1(config-if-gei-0/2)#ip vrf forwarding vpn1
PE1(config-if-gei-0/2)#ip address 32.1.1.1 255.255.255.0
PE1(config-if-gei-0/2)#exit
PE1(config)#interface gei-0/1
PE1(config-if-gei-0/1)#no shutdown
PE1(config-if-gei-0/1)#ip address 37.64.1.1 255.255.255.0
PE1(config-if-gei-0/1)#exit
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 1.2.3.1 255.255.255.255
PE1(config-if-loopback1)#exit
```

OSPF打通IGP路由：

```
PE1(config)#router ospf 1
PE1(config-ospf-1)#router-id 1.2.3.1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 37.64.1.0 0.0.0.255
PE1(config-ospf-1-area-0)#network 1.2.3.1  0.0.0.0
PE1(config-ospf-1-area-0)#exit
```

配置LDP：

```
PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#interface gei-0/1
PE1(config-ldp-1-if-gei-0/1)#exit
PE1(config-ldp-1)#exit
```

PE1与PE2建立MP-IBGP：

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 1.2.3.2 remote-as 100
PE1(config-bgp)#no neighbor 1.2.3.2 activate
PE1(config-bgp)#neighbor 1.2.3.2 update-source loopback1
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 1.2.3.2 activate
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#address-family ipv4 vrf vpn1
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#exit
```

PE2的配置如下：

PE2与PE1之间配置OSPF打通IGP：

```
PE2(config)#interface gei-0/4
PE2(config-if-gei-0/4)#no shutdown
PE2(config-if-gei-0/4)#ip address 37.64.1.2 255.255.255.0
PE2(config-if-gei-0/4)#exit
PE2(config)#interface gei-0/1
```

```
PE2(config-if-gei-0/1)#no shutdown
PE2(config-if-gei-0/1)#ip address 109.65.1.1 255.255.255.0
PE2(config-if-gei-0/1)#exit
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 1.2.3.2 255.255.255.255
PE2(config-if-loopback1)#exit

PE2(config)#router ospf 1
PE2(config-ospf-1)#router-id 1.2.3.2
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 37.64.1.0 0.0.0.255
PE2(config-ospf-1-area-0)#network 1.2.3.2 0.0.0.0
PE2(config-ospf-1-area-0)#exit
```

配置LDP：

```
PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#interface gei-0/4
PE2(config-ldp-1-if-gei-0/4)#exit
PE2(config-ldp-1)#exit
```

PE2与PE1之间配置MP-IBGP：

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.2.3.1 remote-as 100
PE2(config-bgp)#no neighbor 1.2.3.1 activate
PE2(config-bgp)#neighbor 1.2.3.1 update-source loopback1
PE2(config-bgp)#no synchronization            /*关闭BGP同步*/
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 1.2.3.1 activate
PE2(config-bgp-af-vpnv4)#neighbor 1.2.3.1 next-hop-self  /*将下一跳设为自己*/
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#no bgp default route-target filte
PE2(config-bgp)#exit
```

在两ASBR之间用直连接口建立MP-EBGP：

```
PE2(config-bgp)#neighbor 109.65.1.2 remote-as 200
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 109.65.1.2 activate
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#exit
```

PE3的配置如下：

配置OSPF打通PE3与PE4之间的IGP：

```
PE3(config)#interface gei-0/2
PE3(config-if-gei-0/2)#no shutdown
PE3(config-if-gei-0/2)#ip address ip address 109.65.1.2 255.255.255.0
PE3(config-if-gei-0/2)#exit
PE3(config)#interface gei-0/3
PE3(config-if-gei-0/3)#no shutdown
PE3(config-if-gei-0/3)#ip address 63.44.1.1 255.255.255.0
PE3(config-if-gei-0/3)#exit
PE3(config)#interface loopback1
PE3(config-if-loopback1)#ip address 1.2.3.3 255.255.255.255
PE3(config-if-loopback1)#exit

PE3(config)#router ospf 1
PE3(config-ospf-1)#router-id 1.2.3.3
PE3(config-ospf-1)#area 0
PE3(config-ospf-1-area-0)#network 63.44.1.0 0.0.0.255
PE3(config-ospf-1-area-0)#network 1.2.3.3 0.0.0.0
PE3(config-ospf-1-area-0)#exit
```

PE3与PE4之间配置LDP：

```
PE3(config)#mpls ldp instance 1
```

```
PE3(config-ldp-1)#router-id loopback1
PE3(config-ldp-1)#interface gei-0/3
PE3(config-ldp-1-if-gei-0/3)#exit
PE3(config-ldp-1)#exit
```

PE3与PE4之间配置MP-IBGP：

```
PE3(config)#router bgp 200
PE3(config-bgp)#neighbor 1.2.3.4 remote-as 200
PE3(config-bgp)#no neighbor 1.2.3.4 activate
PE3(config-bgp)#neighbor 1.2.3.4 update-source loopback1
PE3(config-bgp)#no synchronizatio
PE3(config-bgp)#address-family vpnv4
PE3(config-bgp-af-vpnv4)#neighbor 1.2.3.4 activate
PE3(config-bgp-af-vpnv4)#neighbor 1.2.3.4 next-hop-self
PE3(config-bgp-af-vpnv4)#exit
PE3(config-bgp)#no bgp default route-target filte
PE3(config-bgp)#exit
```

在两ASBR之间用直连接口建立MP-EBGP：

```
PE3(config-bgp)#neighbor 109.65.1.1 remote-as 100
PE3(config-bgp)#address-family vpnv4
PE3(config-bgp-af-vpnv4)#neighbor 109.65.1.1 activate
PE3(config-bgp-af-vpnv4)#exit
PE3(config-bgp)#exit
```

PE4的配置如下：

```
PE4(config)#ip vrf vpn1
PE4(config-vrf-vpn1)#rd 1:10
PE4(config-vrf-vpn1)#route-target both 1:10
PE4(config-vrf-vpn1)#address-family ipv4
PE4(config-vrf-vpn1-af-ipv4)#exit
PE4(config-vrf-vpn1)#exit

PE4(config)#interface gei-0/9
PE4(config-if-gei-0/9)#no shutdown
PE4(config-if-gei-0/9)#ip vrf forwarding vpn1
PE4(config-if-gei-0/9)#ip address 44.1.1.1 255.255.255.0
PE4(config-if-gei-0/9)#exit
PE4(config)#interface gei-0/4
PE4(config-if-gei-0/4)#no shutdown
PE4(config-if-gei-0/4)#ip address 63.44. 1.2 255.255.255.0
PE4(config-if-gei-0/4)#exit
PE4(config)#interface loopback1
PE4(config-if-loopack1)#ip address 1.2.3.4 255.255.255.255
PE4(config-if-loopback1)#exit

PE4(config)#router ospf 1          /*配置OSPF并通告路由*/
PE4(config-ospf-1)#router-id 1.2.3.4
PE4(config-ospf-1)#area 0
PE4(config-ospf-1-area-0)#network 63.44.1.0 0.0.0.255
PE4(config-ospf-1-area-0)#network 1.2.3.4  0.0.0.0
PE4(config-ospf-1-area-0)#exit

PE4(config)#mpls ldp instance 1         /*接口起LDP协议*/
PE4(config-ldp-1)#router-id loopback1
PE4(config-ldp-1)#interface gei-0/4
PE4(config-ldp-1-if-gei-0/4)#exit
PE4(config-ldp-1)#exit

PE4(config)#router bgp 200             /*配置BGP协议*/
PE4(config-bgp)#neighbor 1.2.3.3 remote-as 200
PE4(config-bgp)#no neighbor 1.2.3.3 activat
PE4(config-bgp)#neighbor 1.2.3.3 update-source loopback1
PE4(config-bgp)#address-family vpnv4          /*使能MP-BGP*/
PE4(config-bgp-af-vpnv4)#neighbor 1.2.3.3 activat
```

```
PE4(config-bgp-af-vpnv4)#exit
PE4(config-bgp)#address-family ipv4 vrf vpn1
PE4(config-bgp-af-ipv4-vrf)#redistribute connected     /*重分发直连，如果PE与CE
之间是
通过动态路由协议，也需要重分发该动态路由协议*/
PE4(config-bgp-af-ipv4-vrf)#exit
PE4(config-bgp)#exit
```

配置验证

在PE1上查看私网协议路由表以及公网标签信息：

```
PE1(config)#show ip protocol routing vrf vpn1
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale
   Dest             NextHop      Intag    Outtag    RtPrf     Protocol
*>  32.1.1.0/24       32.1.1.1     213002    notag     0         Direct
*>  32.1.1.1/32       32.1.1.1     213001    notag     0         Address
*>  44.1.1 .0/24      1.2.3.2      213003    213019    200       BGP-INT

PE1(config)#show mpls forwarding-table 1.2.3.2
Local     Outgoing  Prefix or         Outgoing          Next Hop     M/S
label     label     Tunnel Id         interface
16408     0        1.2.3.2/32        gei-0/1           37.64.1.2    M
```

在PE1上用**show bgp vpnv4 unicast neighbor 1.2.3.2**命令查看：

```
PE1#show bgp vpnv4 unicast neighbor 1.2.3.2
BGP neighbor is 1.2.3.2, remote AS 100, internal link
  BGP version 4, remote router ID 1.2.3.2
  BGP state = Established, up for 22:27:17
  Last read update 00:18:51, hold time is 90 seconds, keepalive interval
is 30 seconds
  Neighbor capabilities:
   Route refresh: advertised and received
New ASN capability: advertised and received
   Address family IPv4 Unicast: advertised and received
   Address family VPNv4 Unicast: advertised and receivedRestart Capability:
   advertised and received
```

在PE2上查看私网协议路由表信息：

```
PE2(config)#show ip protocol routing vrf vpn1
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale

   Dest             NextHop      Intag    Outtag    RtPrf     Protocol
*>  32.1.1.0/24       1.2.3.1      213020    213002    200       BGP-INT
*>  44.1.1.0/24       109.65.1.2   213019    213006    20        BGP-EXT
```

在PE2上使用**show bgp vpnv4 unicast neighbor 1.2.3.1**命令查看：

```
PE2#show bgp vpnv4 unicast neighbor 1.2.3.1
BGP neighbor is 1.2.3.1, remote AS 100, internal link
  BGP version 4, remote router ID 1.2.3.1
  BGP state = Established, up for 22:27:17
  Last read update 00:18:51, hold time is 90 seconds, keepalive interval
is 30 seconds
capabilities:
   Route refresh: advertised and received
New ASN capability: advertised and received
   Address family IPv4 Unicast: advertised and received
   Address family VPNv4 Unicast: advertised and receivedRestart Capability:
   advertised and received
```

在PE3上查看私网路由表信息：

```
PE3(config)#show ip protocol routing vrf vpn1
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale

    Dest           NextHop       Intag     Outtag    RtPrf    Protocol
*>  32.1.1.0/24     109.65.1.1     213007    213020    20       BGP-EXT
*>  44.1.1.0/24     1.2.3.4       213006    213017    200      BGP-INT
```

在PE3上使用**show bgp vpnv4 unicast neighbor 1.2.3.4**命令查看：

```
PE3#show bgp vpnv4 unicast neighbor 1.2.3.4
BGP neighbor is 1.2.3.4, remote AS 200, internal link
  BGP version 4, remote router ID 1.2.3.4
  BGP state = Established, up for 22:27:17
  Last read update 00:18:51, hold time is 90 seconds, keepalive interval
is 30 seconds
capabilities:
   Route refresh: advertised and received
New ASN capability: advertised and received
   Address family IPv4 Unicast: advertised and received
   Address family VPNv4 Unicast: advertised and receivedRestart Capability:
   advertised and received
```

在PE1上可以使用**show bgp vpnv4 unicast label**命令查看前缀44.1.1.0和VPN出标签。

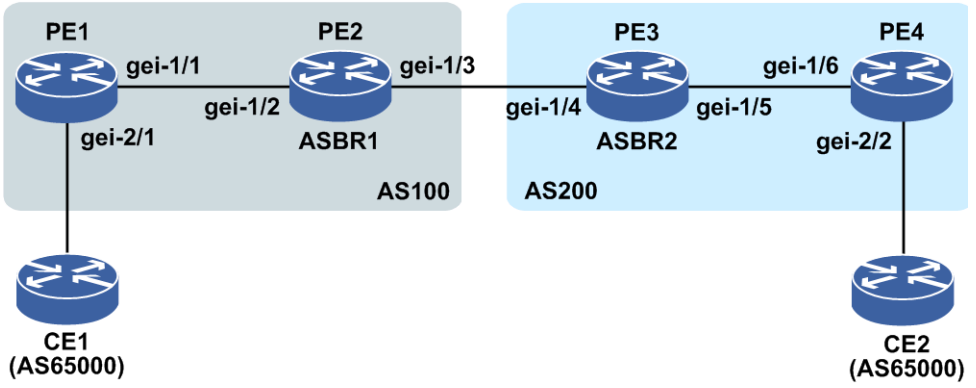
在PE4上可以使用**show bgp vpnv4 unicast label**命令查看前缀44.1.1.0和VPN入标签。

7.3.7.4 MPLS L3VPN 跨域 OptionC（PE 与 ASBR 之间采用 IBGP）配置实例

配置说明

如*图 7-30*所示，客户的两个站点之间需要有VPN连接。但是，站点1（CE1）连接到AS100，而站点2（CE2）连接到AS200，两个站点都提供MPLS VPN。为了建立两个站点间的MPLS VPN的连接性，运用跨域OptionC（PE与ASBR之间采用IBGP）的方法。

图 7-30 MPLS L3VPN 跨域 OptionC（PE 与 ASBR 之间采用 IBGP）配置实例示意图



配置思路

1.按*图 7-30*所示搭建环境，配置接口地址：

PE1的左接口：gei-2/1 20.1.1.1/24；PE1的右接口：gei-1/1 100.1.12.1/24。

ASBR1的左接口：gei-1/2 100.1.12.2/24；ASBR1的右接口：gei-1/3 100.1.23.2/24。

ASBR2的左接口：gei-1/4 100.1.23.3/24；ASBR2的右接口：gei-1/5 100.1.34.3/24。

PE4的左接口：gei-1/6 100.1.34.4/24；PE4的右接口：gei-2/2 30.1.1.1/24。

2.每个路由器上配置一个Loopback地址，自左向右依次为100.1.5.1/32，100.1.5.2/32，100.1.5.3/32，100.1.5.4/32。

3.PE1和ASBR1处于AS100中，PE4和ASBR2处于AS200中。

4.PE与ASBR间建立IBGP邻居并且互相配置**send-lable**能力；PE1与PE4间建立MPEBGP邻居通告VPNv4路由，同时不要激活IPv4邻居。

5.ASBR间使用直连接口建立普通的EBGP邻居，并使用**network**命令通告PE的Loopback地址到对端ASBR，BGP下配置到邻居的send-lable能力，并配置route-map，route-map配置**set mpls lable**并配置匹配前缀过滤路由。

6.PE与ASBR间建立IGP+LDP标签分发隧道。

7.CE侧通过EBGP协议接入PE。

配置过程

PE1的配置如下：

```
PE1(config)#ip vrf vpn1
PE1(config-vrf-vpn1)#rd 100:1
PE1(config-vrf-vpn1)address-family ipv4
PE1(config-vrf-vpn1-af-ipv4)#route-target 100:1
PE1(config-vrf-vpn1-af-ipv4)#exit
PE1(config-vrf-vpn1)#exit

PE1(config)#interface gei-2/1
PE1(config-if-gei-2/1)#no shutdown
```

```
PE1(config-if-gei-2/1)#ip vrf forwarding vpn1
PE1(config-if-gei-2/1)#ip address 20.1.1.1 255.255.255.0
PE1(config-if-gei-2/1)#exit
PE1(config)#interface loopback10
PE1(config-if-loopback10)#ip address 100.1.5.1  255.255.255.255
PE1(config-if-loopback10)#exit

PE1(config)#router ospf 10
PE1(config-ospf-10)#router-id 100.1.5.1
PE1(config-ospf-10)#area 0
PE1(config-ospf-10-area-0)#network 100.1.0.0 0.0.255.255
PE1(config-ospf-10-area-0)#exit
```

PE1与PE4之间建立MP-EBGP：

```
PE1(config)#router bgp 100
PE1(config-bgp)#no synchronization
PE1(config-bgp)#neighbor 100.1.5.2 remote-as 100
PE1(config-bgp)#neighbor 100.1.5.2 update-source loopback10
PE1(config-bgp)#neighbor 100.1.5.2 send-label
PE1(config-bgp)#neighbor 100.1.5.4 remote-as 200
PE1(config-bgp)#neighbor 100.1.5.4 update-source loopback10
PE1(config-bgp)#neighbor 100.1.5.4 ebgp-multihop
PE1(config-bgp)#no neighbor 100.1.5.4 activate
PE1(config-bgp)#address-family ipv4 vrf vpn1
PE1(config-bgp-af-ipv4-vrf)#neighbor 20.1.1.2 remote-as 1
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 100.1.5.4 activate
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#exit

PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback10
PE1(config-ldp-1)#interface gei-1/1
PE1(config-ldp-1-if-gei-1/1)#exit
PE1(config-ldp-1)#exit
```

PE2的配置如下：

```
PE2(config)#interface loopback10
PE2(config-if-loopback10)#ip address 100.1.5.2 255.255.255.255
PE2(config-if-loopback10)#exit

PE2(config)#router ospf 10
PE2(config-ospf-10)#router-id 100.1.5.2
PE2(config-ospf-10)#area 0
PE2(config-ospf-10-area-0)#network 100.1.0.0 0.0.255.255
PE2(config-ospf-10-area-0)#exit

PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback10
PE2(config-ldp-1)#interface gei-1/2
PE2(config-ldp-1-gei-1/2)#exit
PE2(config-ldp-1)#access-fec bgp
PE2(config-ldp-1)#exit

PE2(config)#ipv4-access-list inspur
PE2(config-ipv4-acl)#rule 1 permit 100.1.5.1 0.0.0.0
PE2(config-ipv4-acl)#exit
PE2(config)#route-map inspur
PE2(config-route-map)#match ip address inspur
PE2(config-route-map)#set mpls-label
PE2(config-route-map)#exit

PE2(config)#router bgp 100
PE2(config-bgp)#no synchronization
PE2(config-bgp)#neighbor 100.1.23.3 remote-as 200
```

```
PE2(config-bgp)#neighbor 100.1.23.3 route-map inspur out
PE2(config-bgp)#neighbor 100.1.23.3 send-label
PE2(config-bgp)#neighbor 100.1.5.1 remote-as 100
PE2(config-bgp)#neighbor 100.1.5.1 update-source loopback10
PE2(config-bgp)#neighbor 100.1.5.1 next-hop-self
PE2(config-bgp)#neighbor 100.1.5.1 send-label
PE2(config-bgp)#network 100.1.5.1 255.255.255.255
PE2(config-bgp)#exit
```

PE3的配置如下：

```
PE3(config)#interface loopback10
PE3(config-if-loopback10)#ip address 100.1.5.3  255.255.255.255
PE3(config-if-loopback10)#exit

PE3(config)#router ospf 10
PE3(config-ospf-10)#router-id 100.1.5.3
PE3(config-ospf-10)#area 0
PE3(config-ospf-10-area-0)#network 100.1.0.0 0.0.255.255
PE3(config-ospf-10-area-0)#exit

PE3(config)#mpls ldp instance 1
PE3(config-ldp-1)#router-id loopback10
PE3(config-ldp-1)#interface gei-1/5
PE3(config-ldp-1-gei-1/5)#exit
PE3(config-ldp-1)#access-fec bgp
PE3(config-ldp-1)#exit

PE3(config)#ipv4-access-list inspur
PE3(config-ipv4-acl)#rule 1 permit 100.1.5.4 0.0.0.0
PE3(config-ipv4-acl)#exit
PE3(config)#route-map inspur
PE3(config-route-map)#match ip address inspur
PE3(config-route-map)#set mpls-label
PE3(config-route-map)#exit

PE3(config)#router bgp 200
PE3(config-bgp)#no synchronization
PE3(config-bgp)#neighbor 100.1.23.2 remote-as 100
PE3(config-bgp)#neighbor 100.1.23.2 route-map inspur out
PE3(config-bgp)#neighbor 100.1.23.2 send-label
PE3(config-bgp)#neighbor 100.1.5.4 remote-as 200
PE3(config-bgp)#neighbor 100.1.5.4 update-source loopback10
PE3(config-bgp)#neighbor 100.1.5.4 next-hop-self
PE3(config-bgp)#neighbor 100.1.5.4 send-label
PE3(config-bgp)#network 100.1.5.4 255.255.255.255
PE3(config-bgp)#exit
```

PE4的配置如下：

```
PE4(config)#ip vrf vpn1
PE4(config-vrf-vpn1)#rd 100:1
PE4(config-vrf-vpn1)address-family ipv4
PE4(config-vrf-vpn1-af-ipv4)#route-target 100:1
PE4(config-vrf-vpn1-af-ipv4)#exit
PE4(config-vrf-vpn1)#exit

PE4(config)#interface gei-2/2
PE4(config-if-gei-2/2)#no shutdown
PE4(config-if-gei-2/2)#ip vrf forwarding vpn1
PE4(config-if-gei-2/2)#ip address 30.1.1.1 255.255.255.0
PE4(config-if-gei-2/2)#exit

PE4(config)#interface loopback10
PE4(config-if-loopback10)#ip address 100.1.5.4  255.255.255.255
PE4(config-if-loopback10)#exit

PE4(config)#router ospf 10
PE4(config-ospf-10)#router-id 100.1.5.4
```

```
PE4(config-ospf-10)#area 0
PE4(config-ospf-10-area-0)#network 100.1.0.0 0.0.255.255
PE4(config-ospf-10-area-0)#exit

PE4(config)#mpls ldp instance 1
PE4(config-ldp-1)#router-id loopback10
PE4(config-ldp-1)#interface gei-1/6
PE4(config-ldp-1-gei-1/6)#exit
PE4(config-ldp-1)#exit

PE4(config)#router bgp 200
PE4(config-bgp)#no synchronization
PE4(config-bgp)#neighbor 100.1.5.3 remote-as 200
PE4(config-bgp)#neighbor 100.1.5.3 update-source loopback10
PE4(config-bgp)#neighbor 100.1.5.3 send-label
PE4(config-bgp)#neighbor 100.1.5.1 remote-as 100
PE4(config-bgp)#neighbor 100.1.5.1 update-source loopback10
PE4(config-bgp)#neighbor 100.1.5.1 ebgp-multihop
PE4(config-bgp)#no neighbor 100.1.5.1 activate
PE4(config-bgp)#address-family ipv4 vrf vpn1
PE4(config-bgp-af-ipv4-vrf)#neighbor 30.1.1.2 remote-as 1
PE4(config-bgp-af-ipv4-vrf)#exit
PE4(config-bgp)#address-family vpnv4
PE4(config-bgp-af-vpnv4)#neighbor 100.1.5.1 activate
PE4(config-bgp-af-vpnv4)#exit
PE4(config-bgp)#exit
```

配置验证

在PE1上使用**show bgp vpnv4 unicast summary**命令查看PE1和PE4间VPNv4邻居的建立情况：

```
PE1(config)#show bgp vpnv4 unicast summary
Neighbor     Ver  As      MsgRcvd    MsgSend    Up/Down      State/PfxRcd
100.1.5.4    4    200     48         47         00:23:27          2
```

在PE1上查看到ASBR1的LDP标签信息：

```
PE1(config)#show mpls forwarding-table 100.1.5.2
Local     Outgoing  Prefix or        Outgoing       Next Hop      M/S
label     label     Tunnel Id        interface
16389     0         100.1.5.2/32     gei-1/1        100.1.12.2    M
```

在PE1查看到其他设备的BGP标签信息：

```
PE1(config)#show ip bgp labels
  Network          Next Hop      In Label/Out Label
 100.1.5.1/32      100.1.5.2        notag/notag
 100.1.5.2/32      100.1.5.2        213006/213024
 100.1.5.3/32      100.1.5.2        213007/213025
 100.1.5.4/32      100.1.5.2        notag/notag
```

在PE1上使用**show bgp vpnv4 unicast label**命令可看到前缀20.1.1.0、30.1.1.0的信息：

```
PE1(config)#show bgp vpnv4 unicast labels
Network          Next Hop     In Label/Out Label

Route Distinguisher: 65535:0 (default for vrf vpn1)
 20.1.1.0/24      20.1.1.1       213003/notag
 30.1.1.0/24      100.1.5.4      213008/213013
```

在PE4上使用**show bgp vpnv4 unicast label**命令可看到前缀20.1.1.0、30.1.1.0的信息：

```
PE4#show bgp vpnv4 unicast labels
```

```
 Network          Next Hop      In Label/Out Label

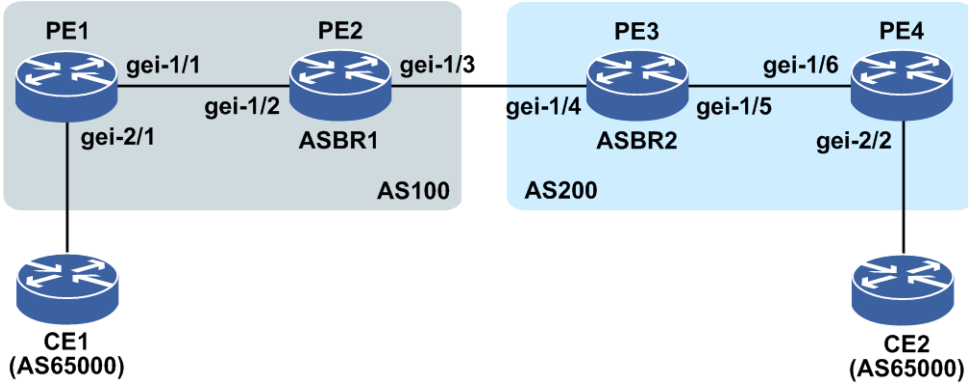
Route Distinguisher: 65535:0 (default for vrf vpn1)
 20.1.1.0/24      1.1.1.64       213018/213003
 30.1.1.0/24      31.1.1.1       213013/notag
```

7.3.7.5 MPLS L3VPN 跨域 OptionC（PE 与 ASBR 之间采用 IGP）配置实例

配置说明

如*图 7-31*所示，客户的两个站点之间需要有VPN连接。但是，站点1（CE1）连接到AS100，而站点2（CE2）连接到AS200，两个站点都提供MPLS VPN。为了建立两个站点间的MPLS VPN的连接性，运用跨域OptionC（PE与ASBR之间采用IGP）的方法，这是实现AS间的VPN的最简单的办法。

图 7-31 MPLS L3VPN 跨域 OptionC（PE 与 ASBR 之间采用 IGP）配置实例示意图



配置思路

1.按*图 7-31*所示搭建环境，配置接口地址：

PE1的左接口：gei-2/1 20.1.1.1/24，PE1的右接口：gei-1/1 100.1.12.1/24。

ASBR1的左接口：gei-1/2 100.1.12.2/24，ASBR1的右接口：gei-1/3 100.1.23.2/24。

ASBR2的左接口：gei-1/4 100.1.23.3/24，ASBR2的右接口：gei-1/5 100.1.34.3/24。

PE4的左接口：gei-1/6 100.1.34.4/24，PE4的右接口：gei-2/2 30.1.1.4/24。

2.每个路由器上配置一个Loopback地址，自左向右依次为100.1.5.1/32，100.1.5.2/32，100.1.5.3/32，100.1.5.4/32。

3.PE1和ASBR1处于AS100中，PE4和ASBR2处于AS200中。

4.PE1与PE4间建立MPEBGP邻居通告VPNv4路由，同时不要激活IPv4邻居。

5.ASBR间使用直连接口建立普通的EBGP邻居，并使用**network**通告PE的Loopback地址到对端ASBR。ASBR的LDP下要配置**access-fec bgp**，为BGP路由分标签。

6.PE与ASBR间建立OSPF邻居，PE与ASBR间建立IGP+LDP标签分发隧道，IGP下要

重分发BGP路由。

配置过程

PE与PE之间的OSPF和LDP配置参见"MPLS L3VPN公网LDP负荷分担配置实例"小节。

PE1的配置如下：

```
PE1(config)#ip vrf vpn1
PE1(config-vrf-vpn1)#rd 100:1
PE1(config-vrf-vpn1)#address-family ipv4
PE1(config-vrf-vpn1-af-ipv4)#route-target 100:1
PE1(config-vrf-vpn1-af-ipv4)#exit
PE1(config-vrf-vpn1)#exit

PE1(config)#interface gei-2/1
PE1(config-if-gei-2/1)#no shutdown
PE1(config-if-gei-2/1)#ip vrf forwarding vpn1
PE1(config-if-gei-2/1)#ip address 20.1.1.1 255.255.255.0
PE1(config-if-gei-2/1)#exit

PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 100.1.5.1  255.255.255.255
PE1(config-if-loopback1)#exit

PE1(config)#router ospf 10
PE1(config-ospf-10)#router-id 100.1.5.1
PE1(config-ospf-10)#area 0
PE1(config-ospf-10-area-0)#network 100.1.0.0 0.0.255.255
PE1(config-ospf-10-area-0)#exit
```

PE1与PE4间建立MPEBGP邻居通告VPNv4路由，同时不要激活IPv4邻居。

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 100.1.5.4 remote-as 200
PE1(config-bgp)#no neighbor 100.1.5.4 activate
PE1(config-bgp)#neighbor 100.1.5.4 update-source loopback1
PE1(config-bgp)#neighbor 100.1.5.4 ebgp-multihop
PE1(config-bgp)#address-family ipv4 vrf vpn1
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 100.1.5.4 activate
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#exit

PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#interface gei-1/1
PE1(config-ldp-1-if-gei-1/1)#exit
PE1(config-ldp-1)#exit
```

PE2的配置如下：

```
PE2(config)#ipv4-access-list inspur
PE2(config-ipv4-acl)#rule 1 permit 100.1.5.1 0.0.0.0
PE2(config-ipv4-acl)#exit
PE2(config)#route-map inspur
PE2(config-route-map)#match ip address inspur
PE2(config-route-map)#set mpls-label
PE2(config-route-map)#exit

PE2(config)#interface loopback1
```

```
PE2(config-if-loopback1)#ip address 100.1.5.2  255.255.255.255
PE2(config-if-loopback1)#exit

PE2(config)#router ospf 10
PE2(config-ospf-10)#router-id 100.1.5.2
PE2(config-ospf-10)#redistribute bgp-ext
PE2(config-ospf-10)#area 0
PE2(config-ospf-10-area-0)#network 100.1.0.0 0.0.255.255
PE2(config-ospf-10-area-0)#exit

PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#access-fec bgp
PE2(config-ldp-1)#interface gei-1/2
PE2(config-ldp-1-if-gei-1/2)#exit
PE2(config-ldp-1)#exit

PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 100.1.23.3 remote-as 200
PE2(config-bgp)#neighbor 100.1.23.3 route-map inspur out
PE2(config-bgp)#neighbor 100.1.23.3 send-label
PE2(config-bgp)#network 100.1.5.1 255.255.255.255
PE2(config-bgp)#network 100.1.5.2 255.255.255.255
PE2(config-bgp)#exit
```

PE3的配置如下：

```
PE3(config)#interface loopback1
PE3(config-if-loopback1)#ip address 100.1.5.3  255.255.255.255
PE3(config-if-loopback1)#exit

PE3(config)#router ospf 10
PE3(config-ospf-10)#router-id 100.1.5.3
PE3(config-ospf-10)#redistribute bgp-ext
PE3(config-ospf-10)#area 0
PE3(config-ospf-10-area-0)#network 100.1.0.0 0.0.255.255
PE3(config-ospf-10-area-0)#exit

PE3(config)#mpls ldp instance 1
PE3(config-ldp-1)#router-id loopback1
PE3(config-ldp-1)#access-fec bgp
PE3(config-ldp-1)#interface gei-1/5
PE3(config-ldp-1-if-gei-1/5)#exit
PE3(config-ldp-1)#exit

PE3(config)#ipv4-access-list inspur
PE3(config-ipv4-acl)#rule 1 permit 100.1.5.4 0.0.0.0
PE3(config-ipv4-acl)#exit
PE3(config)#route-map inspur
PE3(config-route-map)#match ip address inspur
PE3(config-route-map)#set mpls-label
PE3(config-route-map)#exit

PE3(config)#router bgp 200
PE3(config-bgp)#neighbor 100.1.23.2 remote-as 100
PE3(config-bgp)#neighbor 100.1.23.2 route-map inspur out
PE3(config-bgp)#neighbor 100.1.23.2 send-label
PE3(config-bgp)#network 100.1.5.3 255.255.255.255
PE3(config-bgp)#network 100.1.5.4 255.255.255.255
PE3(config-bgp)#exit
```

PE4的配置如下：

```
PE4(config)#ip vrf vpn1
PE4(config-vrf-vpn1)#rd 100:1
PE4(config-vrf-vpn1)#address-family ipv4
PE4(config-vrf-vpn1-af-ipv4)#route-target 100:1
PE4(config-vrf-vpn1-af-ipv4)#exit
PE4(config-vrf-vpn1)#exit
```

```
PE4(config)#interface loopback1
PE4(config-if-loopback1)#ip address 100.1.5.4  255.255.255.255
PE4(config-if-loopback1)#exit

PE4(config)#router ospf 10
PE4(config-ospf-10)#router-id 100.1.5.4
PE4(config-ospf-10)#area 0
PE4(config-ospf-10-area-0)#network 100.1.0.0 0.0.255.255
PE4(config-ospf-10-area-0)#exit

PE4(config)#mpls ldp instance 1
PE4(config-ldp-1)#router-id loopback1
PE4(config-ldp-1)#interface gei-1/6
PE4(config-ldp-1-if-gei-1/6)#exit
PE4(config-ldp-1)#exit

PE4(config)#router bgp 200
PE4(config-bgp)#neighbor 100.1.5.1 remote-as 100
PE4(config-bgp)#no neighbor 100.1.5.1 activate
PE4(config-bgp)#neighbor 100.1.5.1 update-source loopback1
PE4(config-bgp)#neighbor 100.1.5.1 ebgp-multihop
PE4(config-bgp)#address-family ipv4 vrf vpn1
PE4(config-bgp-af-ipv4-vrf)#redistribute connected
PE4(config-bgp-af-ipv4-vrf)#exit
PE4(config-bgp)#address-family vpnv4
PE4(config-bgp-af-vpnv4)#neighbor 100.1.5.1 activate
PE4(config-bgp-af-vpnv4)#exit
PE4(config-bgp)#exit
```

配置验证

在PE1上使用**show bgp vpnv4 unicast summary**命令查看PE1和PE4间VPNv4邻居的建立情况：

```
PE1#show bgp vpnv4 unicast summary
Neighbor      Ver  As      MsgRcvd    MsgSend    Up/Down      State/PfxRcd
100.1.5.4     4    200       18         7       00:03:24          2
```

在PE1上查看私网协议路由表：

```
PE1#show ip protocol routing vrf vpn1 network 30.1.1.0
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale

   Dest           NextHop       Intag     Outtag    RtPrf    Protocol
*>  30.1.1.0/24     100.1.5.4     214007    213011    20       BGP-EXT
```

查看公网LDP和BGP标签信息：

```
PE1#show mpls forwarding-table 100.1.5.4
Local     Outgoing  Prefix or         Outgoing        Next Hop      M/S
label     label     Tunnel Id         interface
16396     16389     100.1.5.4/32       gei-1/1     100.1.12.2    M
```

ASBR1上查看LDP和BGP标签信息：

```
ASBR1#show mpls forwarding-table 100.1.5.4
Local     Outgoing  Prefix or         Outgoing        Next Hop      M/S
```

```
label     label     Tunnel Id         interface
16389     Untagged  100.1.5.4/32      gei-1/3         100.1.23.3    M
ASBR1#show ip bgp labels
  Network          Next Hop      In Label/Out Label

 100.1.5.1/32       100.1.12.1     notag/notag
 100.1.5.2/32       100.1.5.2      notag/notag
 100.1.5.4/32       100.1.23.3    213005/213072
 100.1.5.3/32       100.1.23.3    213006/213076
```

ASBR2上查看LDP和BGP标签信息：

```
ASBR2#show mpls forwarding-table
Local     Outgoing  Prefix or         Outgoing        Next Hop      M/S
label     label     Tunnel Id         interface
16446     Poptag    100.1.5.4/32      gei-1/5         100.1.34.4     M
```

7.3.8 MPLS L3VPN 每 VPN 每标签

目前VPN路由的标签分配模式有两种：

- 每前缀分配，指给每条前缀都分配不同的私网标签。
- 每VRF分配，允许属于同一个VRF的所有前缀使用相同的私网标签，并且可以通过配置命令单独设置每个VRF的标签分配模式或者一次指定所有VRF的标签分配模式。

PE路由器上会保存所有VPN路由，包括本地产生和从远端接收，并且每条路由前缀都会携带一个私网标签，这些标签将消耗内存。如果是每前缀方式分配标签，当PE上有很多VRF和路由，每前缀标签消耗的内存将是很大的开销。

每VRF标签功能用于解决上述问题，每VRF标签允许同一个VRF下所有本地路由都是用相同的私网标签，这个新的标签将用于决定向PE或CE的哪个接口转发报文。

7.3.8.1 配置 MPLS L3VPN 每 VRF 每标签

本节介绍MPLS L3VPN每VRF每标签的配置步骤和命令。

1.配置MPLS L3VPN每VRF每标签。

命令	功能
inspur(config-vrf-vrf-name)#**mpls label mode** [**ipv6**]{**per-prefix** | **per-vrf**}	配置私网标签的分配方式

per-prefix：每前缀每标签分配方式（默认情况）。

per-vrf：每VRF每标签分配方式。

2.验证配置结果。

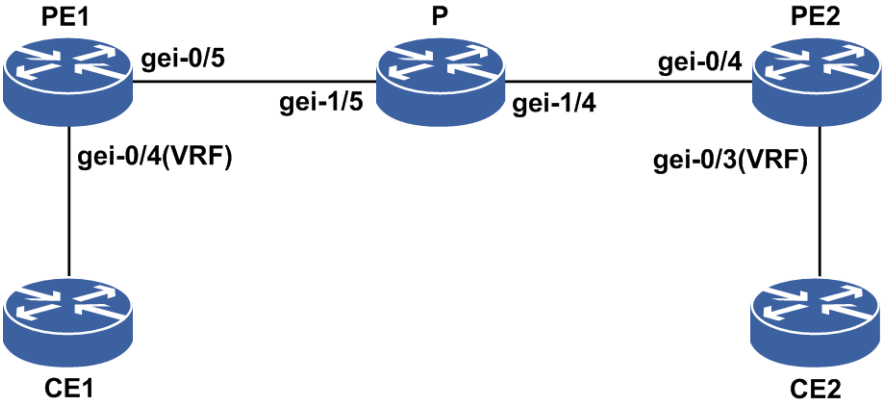
命令	功能
inspur(config)#**show ip vrf detail** [<*vrf-name*>]	查看VRF实例的详细信息
inspur(config)#**show ip protocol routing vrf** <*vrf-name*>	查看VRF协议路由表信息

7.3.8.2 MPLS L3VPN 每 VPN 每标签配置实例

配置说明

如*图 7-32*所示，搭建L3VPN环境。

图 7-32 MPLS L3VPN 每 VPN 每标签配置实例示意图



配置思路

1.按*图 7-32*所示搭建环境，PE1与PE2搭建L3VPN环境。

2.CE1与PE1的VRF接入接口创建IS-IS邻居，并通告1000条IS-IS路由。

3.在PE1的vrf inspur下配置每VPN每标签。

配置过程

PE与PE之间的IS-IS、LDP配置请参考“配置MPLS L3VPN公网LDP负荷分担”。

PE1的配置如下：

```
PE1(config)#interface loopback1
PE1(config-if-loopbck1)#ip address 100.1.1.2 255.255.255.255
PE1(config-if-loopback1)#exit

PE1(config)#ip vrf inspur
PE1(config-vrf-inspur)#rd 1:100
PE1(config-vrf-inspur)#route-target both 1:100
PE1(config-vrf-inspur)#address-family ipv4
PE1(config-vrf-inspur-af-ipv4)#exit
PE1(config-vrf-inspur)#exit

PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 100.1.1.1 remote-as 100
PE1(config-bgp)#neighbor 100.1.1.1 update-source loopback1
PE1(config-bgp)#address-family vpnv4
```

```
PE1(config-bgp-af-vpnv4)#neighbor 100.1.1.1 activate
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#address-family ipv4 vrf inspur
PE1(config-bgp-af-ipv4-vrf)#redistribute isis-l-2 100
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#exit

PE1(config)#interface gei-0/4
PE1(config-if-gei-0/4)#no shutdown
PE1(config-if-gei-0/4)#ip vrf  forwarding inspur
PE1(config-if-gei-0/4)#ip address 192.1.1.1 255.255.255.0
PE1(config-if-gei-0/4)#exit

PE1(config)#router isis 100 vrf inspur
PE1(config-isis-100)#area 47.0005
PE1(config-isis-100)#system-id 0000.0022.2222
PE1(config-isis-100)#interface gei-0/4
PE1(config-isis-100-if-gei-0/4)#ip router isis
PE1(config-isis-100-if-gei-0/4)#exit
PE1(config-isis-100)#exit

PE1(config)#ip vrf inspur
PE1(config-vrf-inspur)#mpls label mode per-vrf /*配置每VRF每标签分配方式*/
PE1(config-vrf-inspur)#exit
```

PE2的配置如下：

```
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 100.1.1.1 255.255.255.255
PE2(config-if-loopback1)#exit

PE2(config)#ip vrf inspur
PE2(config-vrf-inspur)#rd 1:100
PE2(config-vrf-inspur)#route-target both 1:100
PE2(config-vrf-inspur)#address-family ipv4
PE2(config-vrf-inspur-af-ipv4)#exit
PE2(config-vrf-inspur)#exit

PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 100.1.1.2 remote-as 100
PE2(config-bgp)#neighbor 100.1.1.2  update-source loopback1
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 100.1.1.2 activate
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#address-family ipv4 vrf inspur
PE2(config-bgp-af-ipv4-vrf)#redistribute connect
PE2(config-bgp-af-ipv4-vrf)#exit
PE2(config-bgp)#exit

PE2(config)#interface gei-0/3
PE2(config-if-gei-0/3)#no shutdown
PE2(config-if-gei-0/3)#ip vrf forwarding inspur
PE2(config-if-gei-0/3)#ip address 193.1.1.1 255.255.255.0
PE2(config-if-gei-0/3)#exit
```

配置验证

PE1上验证情况：

```
PE1(config)#show ip protocol routing vrf inspur
/*PE1只会为这1000条私网路由分配一个标签212994*/
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
 OSPF-7D = ospf-type7-discard, OSPF-E = ospf-ext, RIP-D = rip-discard,
 BGP-AD = bgp-aggr-discard, ISIS-1D = isis-l1-discard, DHCP-D = dhcp-dft,
 ISIS-2D = isis-l2-discard, REDIST = redistribute, DHCP-S = dhcp-static,
```

```
 STAT-A = static-all, BGP-CE = bgp-confed-ext, ASBR-V = asbr-vpn,
 P-SPEC = prot-special, USER-I = user-ipaddr, USER-N = user-network,
 NAT64 = sl-nat64-v4, OSPF-A = ospf-all, USER-S = user-special,
 GW-FWD = ps-busi, GW-UE = ps-user
Marks: *valid, >best, s-stale

   Dest             NextHop      Intag    Outtag    RtPrf      Protocol
*>  80.80.80.0/24    192.1.1.2    212994    notag     115        ISIS-L2
*>  80.80.81.0/24    192.1.1.2    212994    notag     115        ISIS-L2
*>  80.80.82.0/24    192.1.1.2    212994    notag     115        ISIS-L2
*>  80.80.83.0/24    192.1.1.2    212994    notag     115        ISIS-L2
*>  80.80.84.0/24    192.1.1.2    212994    notag     115        ISIS-L2
*>  80.80.85.0/24    192.1.1.2    212994    notag     115        ISIS-L2
*>  80.80.86.0/24    192.1.1.2    212994    notag     115        ISIS-L2
*>  80.80.87.0/24    192.1.1.2    212994    notag     115        ISIS-L2
*>  80.80.88.0/24    192.1.1.2    212994    notag     115        ISIS-L2
*>  80.80.89.0/24    192.1.1.2    212994    notag     115        ISIS-L2
*>  80.80.90.0/24    192.1.1.2    212994    notag     115        ISIS-L2
*>  80.80.91.0/24    192.1.1.2    212994    notag     115        ISIS-L2
*>  80.80.92.0/24    192.1.1.2    212994    notag     115        ISIS-L2
*>  80.80.93.0/24    192.1.1.2    212994    notag     115        ISIS-L2
......
```

7.3.9 MPLS L3VPN GR

MPLS L3VPN Graceful Restart（GR）功能指在L3VPN环境里出现主备倒换时，路由能保持住，使流量不中断。MPLS L3VPN的组成包括LDP和MPBGP两部分，因此在配置GR时关注的重点是：

·在LDP的Router-ID的路由协议上启用GR功能、启用LDP-GR功能

·在MPBGP的建链地址的路由协议上启用GR功能、启用BGP-GR功能

LDP的Router-ID的通告方式可以为IS-IS或OSPF，所以IS-IS协议或OSPF协议需要启用GR。LDP自身需要启用GR。

MPBGP采用LDP的Router-ID作为建链地址，GR能力在之前的LDP-GR的配置过程已经得到满足。MPBGP的GR主要是指在BGP中需启用GR。

7.3.9.1 配置 MPLS L3VPN GR

本节分别介绍IS-IS Graceful Restart（GR）、OSPF Graceful Restart、BGP Graceful Restart和LDP Graceful Restart的配置步骤和命令。

1.配置IS-IS Graceful Restart。

i.开启IS-IS的Graceful Restart功能。

步骤	命令	功能
1	inspur(config)#**router isis** *<process-id>*	进入IS-IS配置模式
2	inspur(config-isis-id)#**restart enable**	开启IS-IS的GR功能

ii.（可选）调整IS-IS Graceful Restart属性。

命令	功能
inspur(config-isis-id)#**restart t2-timer** <*t2-interval*>[**level-1** | **level-2**]	配置IS-IS T2（Graceful Restart的数据库同步定时器）时间间隔，范围：5~65535，单位：秒
inspur(config-isis-id)#**restart t3-timer** {**adjacency** | **manual** <*t3-interval*>}	配置IS-IS T3（设置graceful Restart的完成时间定时器）时间间隔，范围：1~65535，单位：秒
inspur(config-isis-id-if-interface)#**hello-multiplier** <*multiplier*>[**level-1** | **level-2**]	配置IS-IS邻居关系保活乘数，缺省为3，范围：3~1000
inspur(config-isis-id-if-interface)#**restart t1-retry** <*retry-timers*>[**level-1** | **level-2**]	配置IS-IS接口T1定时器重置最大次数，缺省为3次，范围：1~65535
inspur(config-isis-id-if-interface)#**restart t1-timer** <*interval*>[**level-1** | **level-2**]	配置IS-IS接口T1定时器时间间隔，单位：秒，缺省为3秒，范围：1~65535

adjacency：根据邻居通告的hello报文中设置的保持时间确定T3。

manual：根据手工配置的值确定T3。

2.配置OSPF Graceful Restart。

i.开启OSPF的Graceful Restart功能。

步骤	命令	功能
1	inspur(config)#**router ospf**<*process-id*>	进入OSPF配置模式
2	inspur(config-ospf-id)#**nsf**	开启OSPF的GR功能，如果是help方的话，表示激活支持邻居倒换的功能

ii.（可选）调整OSPF的Graceful Restart属性。

命令	功能
inspur(config-ospf-id)#**grace-period** <*time*>	配置OSPF GR时间，默认是120秒，如果倒换方路由条目较多时，可将此时间设置稍长些
inspur(config-ospf-id-if-interface)#**dead-interval** <*time*>	在设备倒换时间性能较长时需配置这个命令

3.配置BGP Graceful Restart。

i.开启BGP的Graceful Restart功能。

步骤	命令	功能
1	inspur(config)#**router bgp**<*as-number*>	进入BGP配置模式

步骤	命令	功能
2	inspur(config-bgp)#**bgp graceful-restart**	开启BGP的GR功能

ii.（可选）调整BGP的Graceful Restart属性。

命令	功能
inspur(config-bgp)#**bgp graceful-restart restart-time** <*time*>	设置Graceful Restart的完成时间间隔，范围：1~3600，默认值120，单位：秒
inspur(config-bgp)#**bgp graceful-restart stalepath-time** <*time*>	设置Graceful Restart的数据库同步时间间隔，范围：1~3600，默认值360，单位：秒

4.配置LDP Graceful Restart。

i.开启LDP的Graceful Restart功能。

步骤	命令	功能
1	inspur(config)#**mpls ldp instance** <*instance-id*>	进入LDP配置模式
2	inspur(config-ldp-id)#**graceful-restart**	开启LDP的GR功能

ii.（可选）调整LDP的Graceful Restart属性。

命令	功能
inspur(config-ldp-id)#**graceful-restart timers neighbor-liveness** <*time*>	设置Graceful Restart的邻居保持时间间隔，单位：秒，缺省值为120，该参数需要协商
inspur(config-ldp-id)#**graceful-restart timers max-recovery** <*time*>	设置Graceful Restart的完成时间间隔，单位：秒，缺省值为120，该参数需要协商

5.验证配置结果。

命令	功能
inspur#**show mpls ldp graceful-restart instance** <*instance-id*>	查看LDP GR配置信息
inspur#**show mpls ldp neighbor graceful-restart instance** <*instance-id*>	查看LDP GR的邻居信息
inspur#**show ip ospf nsf process** <*process-id*>	查看OSPF GR信息
inspur#**show isis nsf process-id** <*process-id*>	查看IS-IS GR信息

6.维护MPLS L3VPN GR。

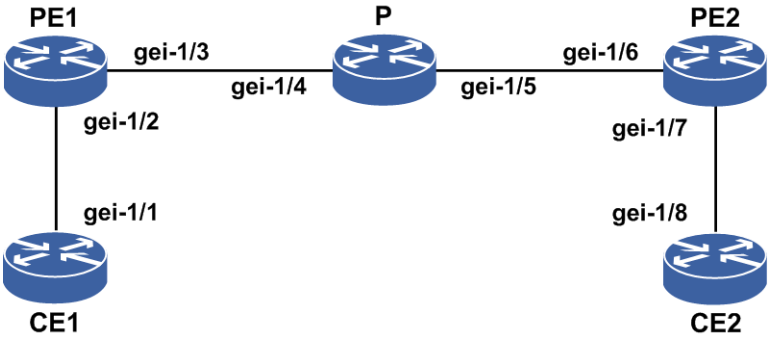
命令	功能
inspur#**debug ldp graceful-restart instance** <*instance-id*>	打开LDP GR诊断开关
inspur#**debug ip ospf nsf** <*process-id*>	打开OSPF GR诊断开关
inspur#**debug isis nsf-events** [**process-id** <*process-id*>]	打开IS-IS GR诊断开关

7.3.9.2 MPLS L3VPN GR 配置实例

配置说明

如*图 7-33*所示，CE1和CE2在同一个VPN中，PE1和PE2通过OSPF路由协议互通，CE1与PE1之间运行OSPF协议，CE2与PE2之间运行OSPF协议，使得CE1与CE2能够互相学到对方的路由。CE1和CE2上启用OSPF GR；PE1和PE2启用OSPF GR、LDP GR和BGP GR；P上启用OSPF GR、BGP GR和LDP GR。

图 7-33 MPLS L3VPN GR 配置拓扑图



配置思路

1.按上图所示搭建环境，PE1与PE2之间通过OSPF搭建L3VPN环境

2.CE1与PE1，CE2与PE2之间建立OSPF邻居

3.在CE1和CE2上配置启用OSPF GR；在PE1和PE2 上配置启用OSPF GR、LDP GR和BGP GR；在P上配置启用OSPF GR和LDP GR

配置过程

PE与PE之间的OSPF、LDP和BGP配置参见MPLS L3VPN基本功能。

CE1上的GR配置如下：

```
CE1(config)#router ospf 2
CE1(config-ospf-2)#nsf
CE1(config-ospf-2)#exit
```

PE1上的GR配置如下：

```
PE1(config)#router ospf 1
PE1(config-ospf-1)#nsf
PE1(config-ospf-1)#exit

PE1(config)#router ospf 2 vrf inspur
PE1(config-ospf-2)#nsf
PE1(config-ospf-2)#exit

PE1(config)#router bgp 1
PE1(config-bgp)#bgp graceful-restart
PE1(config-bgp)#exit

PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#graceful-restart
PE1(config-ldp-1)#exit
```

P上的GR配置如下：

```
P(config)#router ospf 1
P(config-ospf-1)#nsf
P(config-ospf-1)#exit

P(config)#mpls ldp instance 1
P(config-ldp-1)#graceful-restart
P(config-ldp-1)#exit

P(config)#router bgp 1
P(config-bgp)#bgp graceful-restart
P(config-bgp)#exit
```

PE2上的GR配置如下：

```
PE2(config)#router ospf 1
PE2(config-ospf-1)#nsf
PE2(config-ospf-1)#exit

PE2(config)#router ospf 2 vrf inspur
PE2(config-ospf-2)#nsf
PE2(config-ospf-2)#exit

PE2(config)#router bgp 1
PE2(config-bgp)#bgp graceful-restart
PE2(config-bgp)#exit

PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#graceful-restart
PE2(config-ldp-1)#exit
```

CE2上的GR配置如下：

```
CE2(config)#router ospf 2
CE2(config-ospf-2)#nsf
CE2(config-ospf-2)#exit
```

配置验证

在PE1上查看相关信息：

```
R1(config-ldp)#show bgp all summary
Neighbor     Ver   As   MsgRcvd  MsgSend     Up/Down   State
1.1.1.2       4    1    681      680       05:40:18  Established
```

```
/*PE1上MPBGP邻居建立*/

PE1(config-ldp)#show ip forwarding route vrf inspur
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
status codes: *valid, >best;
   Dest             Gw      Interface     Owner   Pri Metric
*> 10.11.1.2/24     1.1.1.2     gei-1/3    BGP     200 0
*> 10.11.2.2/24     1.1.1.2     gei-1/3    BGP     200 0
*> 10.11.3.2/24     1.1.1.2     gei-1/3    BGP     200 0
*> 10.11.4.2/24     1.1.1.2     gei-1/3    BGP     200 0

PE1#show mpls ldp graceful-restart instance 1
 LDP Graceful Restart is enabled
 Neighbor Liveness Timer: 120 seconds
 Max Recovery Timer: 120 seconds
 Graceful Restart enabled Sessions:
  Peer LDP Ident: 1.1.1.2:0;State:Oper

PE1#show mpls ldp neighbor graceful-restart instance 1
Peer LDP Ident: 1.1.1.2:0; Local LDP Ident: 1.1.1.1:0
       TCP connection: 1.1.1.2.25911 - 1.1.1.1.646
       State: Oper; Msgs sent/rcvd: 1652/1547; Downstream
       Up Time: 1d1h
       LDP discovery sources:
         gei-1/1; Src IP addr: 104.110.111.2
       Addresses bound to peer LDP Ident:
         1.1.1.2  2.1.1.1  2.1.1.3  2.1.1.4
         104.110.111.2
       Graceful Restart enable d; Peer reconnect time (msecs): 120000
```

主备倒换PE1设备后：

1.在PE2上执行命令**show ip protocol route vrf** <*vrf-name*>查看到从PE1学习的路由，发现打上了**stale**标记。在PE2上执行命令**show ip forwarding route vrf** <*vrf-name*>查看到从PE1学习的路由始终存在，出接口信息始终存在。

2.在PE2上长ping vrf远端PE1的私网地址，整个主备倒换过程中及倒换完成后ping不丢包。

3.如果有双向的流量转发，整个主备倒换过程及倒换完成后均不丢包。

主备倒换P设备后：

1.在PE2上执行命令**show ip protocol route vrf** <*vrf-name*>查看到从PE1学习的路由，打上了**stale**标记。在PE2上执行命令**show ip forwarding route vrf** <*vrf-name*>查看到从PE1学习的路由始终存在，出接口信息始终存在。

2.在PE1上执行命令**show ip protocol route vrf** <*vrf-name*>查看到从PE2学习的路由，打上了**stale**标记。在PE1上执行命令**show ip forwarding route vrf** <*vrf-name*>查看到从PE2学习的路由始终存在，出接口信息始终存在。

3.在PE2上长ping vrf远端PE1的私网地址，整个主备倒换过程中及倒换完成后ping不丢包。

4.在PE1上长ping vrf远端PE2的私网地址，整个主备倒换过程中及倒换完成后ping不丢包。

5.如果有双向的流量转发，整个主备倒换过程及倒换完成后均不丢包。

主备倒换PE2设备后：

1.在PE1上执行命令**show ip protocol route vrf** <*vrf-name*>查看到从PE2学习的路由，打上了**stale**标记。在PE1上执行命令**show ip forwarding route vrf** <*vrf-name*>查看到从PE2学习的路由始终存在，出接口信息始终存在。

2.在PE1上长ping vrf远端PE2的私网地址，整个主备倒换过程中及倒换完成后ping不丢包。

3.如果有双向的流量转发，整个主备倒换过程及倒换完成后均不丢包。

7.3.10 MPLS L3VPN HoPE

MPLS L3VPN网络分层结构是为了适应当前城域网典型的**接入网—汇聚网—核心网**的网络层次结构，设计思路是：

•将PE分为多个层次，共同完成一台PE的功能

•与分层分级网络相适应，网络层次越高的PE容量和性能要求越高，网络层次越低的PE容量和性能要求越低

•网络层次越低，PE数量越大，用户接入能力越强

•网络框架可以支持网络的分层扩展、无限延伸的要求

•在框架中充分考虑跨AS连接

上述功能即HoPE（Hierarchy of PE），将PE分为任意多个层次，实现无限扩展和延伸。

7.3.10.1 配置 MPLS L3VPN HoPE

本节介绍了MPLS L3VPN HoPE的配置步骤和命令。

前提

先配置好VRF实例。

1.配置MPLS L3VPN HoPE。

步骤	命令	功能
1	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**address-family vpnv4**	进入IPv4 vpnv4地址族配置模式
3	inspur(config-bgp-af-vpnv4)#**neighbor** {<*ipv4-address*>|<*peer-group-name*>} **default-originate** [**all** | **vrf** <*vrf-name*>]	在某个VRF或所有VRF下，配置向某个邻居或邻居对等体通告缺省路由
4	inspur(config-bgp-af-vpnv4)#**neighbor** {<*ipv4-address*>|<*peer-group-name*>} **virtual-spoke** [**reflect-next-hop-self**]	BGP vpnv4地址族下配置邻居或邻居对等体为自己的UPE（spoke-PE）

配置了邻居或者邻居对等体为自己的UPE（spoke-PE）后，收到UPE的VPN路由会自动向其他非UPE（spoke-PE）反射路由。

2.验证配置结果。

命令	功能
inspur#**show running-config bgp**	查看BGP配置信息
inspur#**show bgp vpnv4 unicast summary**	查看所有BGP vpnv4邻居信息
inspur#**show ip forwarding route vrf** <*vrf-name*>{[{<*Network to display informatio*>}[<*Network mask*>{**weak-match**|**exact-match**}]]|[<*Protocol name*>]}	查看VRF私网路由转发表
inspur#**show ip protocol routing vrf** <*vrf-name*>	查看VRF私网路由协议表
inspur#**show bgp vpnv4 unicast detail** {<*0-65535*>**:**<*0-4294967295*>|<*1-65535*>**.**<*0-65535*>**:**<*0-65535*>| **A.B.C.D:**<*0-65535*>}<*ipv4-address*><*ipv4-mask*>	查看vpnv4路由接受和通告的信息信息
inspur#**debug ip bgp update**	查看BGP路由更新消息

7.3.10.2 单级 HoPE 配置实例

配置说明

在如*图 7-34*所示的网络中，配置单级HoPE功能。

图 7-34 单级 HoPE 配置实例组网图



配置思路

1.全网配置OSPF，使OSPF邻居正确建立。

2.全网启用LDP，使邻居正确建立。

3.在各设备上配置具有相同RT属性的VRF实例。

4.在UPE1和SPE1之间建立MPBGP邻居；在SPE1和SPE2之间建立MPBGP邻居；在SPE2和UPE2之间建立MPBGP邻居。

5.在SPE1上配置UPE1为自己的UPE；在SPE2上配置UPE2为自己的UPE。

6.4个CE接入到各PE路由器的VRF。

配置过程

OSPF和LDP的一般配置省略。

UPE1上配置过程如下：

```
UPE1(config)#ip vrf hpe
UPE1(config-vrf-hpe)#rd 4:4
UPE1(config-vrf-hpe)#address-family ipv4
UPE1(config-vrf-hpe-af-ipv4)#route-target 4:4
UPE1(config-vrf-hpe-af-ipv4)#exit
UPE1(config-vrf-hpe)#exit
UPE1(config)#interface gei-0/3.1
UPE1(config-if-gei-0/3.1)#ip vrf forwarding hpe
UPE1(config-if-gei-0/3.1)#ip address 37.0.1.1 255.255.255.0
UPE1(config-if-gei-0/3.1)#exit

UPE1(config)#vlan-configuration
UPE1(config-vlan)#interface gei-0/3.1
UPE1(config-vlan-if-gei-0/3.1)#encapsulation-dot1q 1
UPE1(config-vlan-if-gei-0/3.1)#exit
UPE1(config-vlan)#exit

UPE1(config)#router bgp 200
UPE1(config-bgp)#no synchronization
UPE1(config-bgp)#neighbor 11.11.11.51 remote-as 200
UPE1(config-bgp)#neighbor 11.11.11.51 update-source loopback11
UPE1(config-bgp)#no neighbor 11.11.11.51 activate
UPE1(config-bgp)#address-family vpnv4
UPE1(config-bgp-af-vpnv4)#neighbor 11.11.11.51 activate
UPE1(config-bgp-af-vpnv4)#exit
UPE1(config-bgp)#address-family ipv4 vrf hpe
UPE1(config-bgp-af-ipv4-vrf)#redistribute connected
UPE1(config-bgp-af-ipv4-vrf)#exit
UPE1(config-bgp)#exit
```

SPE1上的配置如下：

```
SPE1(config)#ip vrf hpe
SPE1(config-vrf-hpe)#rd 4:4
SPE1(config-vrf-hpe)#address-family ipv4
SPE1(config-vrf-hpe-af-ipv4)#route-target 4:4
SPE1(config-vrf-hpe-af-ipv4)#exit
SPE1(config-vrf-hpe)#exit

SPE1(config)#interface gei-0/1.100
SPE1(config-if-gei-0/1.100)#ip vrf forwarding hpe
SPE1(config-if-gei-0/1.100)#ip address 51.0.1.1 255.255.255.0
SPE1(config-if-gei-0/1.100)#exit

SPE1(config)#vlan-configuration
SPE1(config-vlan)#interface gei-0/1.100
SPE1(config-vlan-if-gei-0/1.100)#encapsulation-dot1q 100
SPE1(config-vlan-if-gei-0/1.100)#exit
SPE1(config-vlan)#exit

SPE1(config)#router bgp 200
SPE1(config-bgp)#no synchronization
SPE1(config-bgp)#neighbor 11.11.11.37 remote-as 200
SPE1(config-bgp)#neighbor 11.11.11.37 update-source loopback11
```

```
SPE1(config-bgp)#no neighbor 11.11.11.37 activate
SPE1(config-bgp)#neighbor 11.11.11.52 remote-as 200
SPE1(config-bgp)#neighbor 11.11.11.52 update-source loopback11
SPE1(config-bgp)#no neighbor 11.11.11.52 activate
SPE1(config-bgp)#address-family vpnv4
SPE1(config-bgp-af-vpnv4)#neighbor 11.11.11.37 activate
SPE1(config-bgp-af-vpnv4)#neighbor 11.11.11.37 default-originate vrf hpe
SPE1(config-bgp-af-vpnv4)#neighbor        11.11.11.37        virtual-spoke
reflect-next-hop-self
SPE1(config-bgp-af-vpnv4)#neighbor 11.11.11.52 activate
SPE1(config-bgp-af-vpnv4)#exit
SPE1(config-bgp)#address-family ipv4 vrf hpe
SPE1(config-bgp-af-ipv4-vrf)#redistribute connected
SPE1(config-bgp-af-ipv4-vrf)#exit
SPE1(config-bgp)#exit
```

SPE2上的配置如下：

```
SPE2(config)#ip vrf hpe
SPE2(config-vrf-hpe)#rd 4:4
SPE2(config-vrf-hpe)#address-family ipv4
SPE2(config-vrf-hpe-af-ipv4)#route-target 4:4
SPE2(config-vrf-hpe-af-ipv4)#exit
SPE2(config-vrf-hpe)#exit

SPE2(config)#interface gei-0/7.1
SPE2(config-if-gei-0/7.1)#ip vrf forwarding hpe
SPE2(config-if-gei-0/7.1)#ip address 52.0.1.1 255.255.255.0
SPE2(config-if-gei-0/7.1)#exit

SPE2(config)#vlan-configuration
SPE2(config-vlan)#interface gei-0/7.1
SPE2(config-vlan-if-gei-0/7.1)#encapsulation-dot1q 1
SPE2(config-vlan-if-gei-0/7.1)#exit
SPE2(config-vlan)#exit

SPE2(config)#router bgp 200
SPE2(config-bgp)#no synchronization
SPE2(config-bgp)#neighbor 11.11.11.51 remote-as 200
SPE2(config-bgp)#neighbor 11.11.11.51 update-source loopback11
SPE2(config-bgp)#no neighbor 11.11.11.51 activate
SPE2(config-bgp)#neighbor 11.11.11.53 remote-as 200
SPE2(config-bgp)#neighbor 11.11.11.53 update-source loopback11
SPE2(config-bgp)#no neighbor 11.11.11.53 activate
SPE2(config-bgp)#address-family vpnv4
SPE2(config-bgp-af-vpnv4)#neighbor 11.11.11.53 activate
SPE2(config-bgp-af-vpnv4)#neighbor 11.11.11.53 default-originate vrf hpe
SPE2(config-bgp-af-vpnv4)#neighbor        11.11.11.53        virtual-spoke
reflect-next-hop-self
SPE2(config-bgp-af-vpnv4)#neighbor 11.11.11.51 activate
SPE2(config-bgp-af-vpnv4)#exit
SPE2(config-bgp)#address-family ipv4 vrf hpe
SPE2(config-bgp-af-ipv4-vrf)#redistribute connected
SPE2(config-bgp-af-ipv4-vrf)#exit
SPE2(config-bgp)#exit
```

UPE2上配置过程如下：

```
UPE2(config)#ip vrf hpe
UPE2(config-vrf-hpe)#rd 4:4
UPE2(config-vrf-hpe)#address-family ipv4
UPE2(config-vrf-hpe-af-ipv4)#route-target 4:4
UPE2(config-vrf-hpe-af-ipv4)#exit
UPE2(config-vrf-hpe)#exit

UPE2(config)#interface gei-0/11.1
UPE2(config-if-gei-0/11.1)#ip vrf forwarding hpe
UPE2(config-if-gei-0/11.1)#ip address 53.0.1.1 255.255.255.0
UPE2(config-if-gei-0/11.1)#exit
```

```
UPE2(config)#vlan-configuration
UPE2(config-vlan)#interface gei-0/11.1
UPE2(config-vlan-if-gei-0/11.1)#encapsulation-dot1q 1
UPE2(config-vlan-if-gei-0/11.1)#exit
UPE2(config-vlan)#exit

UPE2(config)#router bgp 200
UPE2(config-bgp)#no synchronization
UPE2(config-bgp)#neighbor 11.11.11.52 remote-as 200
UPE2(config-bgp)#neighbor 11.11.11.52 update-source loopback11
UPE2(config-bgp)#no neighbor 11.11.11.52 activate
UPE2(config-bgp)#address-family vpnv4
UPE2(config-bgp-af-vpnv4)#neighbor 11.11.11.52 activate
UPE2(config-bgp-af-vpnv4)#exit
UPE2(config-bgp)#address-family ipv4 vrf hpe
UPE2(config-bgp-af-ipv4-vrf)#redistribute connected
UPE2(config-bgp-af-ipv4-vrf)#exit
UPE2(config-bgp)#exit
```

配置验证

在UPE1上查看相应的信息：

```
UPE1#show ip forwarding route vrf hpe
/*查看私网路由转发表，UPE上只维护本地路由和缺省路由；缺省路由下一跳为SPE1*/
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
  GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
   Dest             Gw            Interface          Owner      Pri Metric
*> 0.0.0.0/0         11.11.11.51     smartgroup60       BGP        200 0
*> 37.0.1.0/24       37.0.1.1        gei-0/3.1          Direct     0   0
*> 37.0.1.1/32       37.0.1.1        gei-0/3.1          Address    0   0

UPE1#show bgp vpnv4 unicast summary
/*查看BGP vpnv4邻居，和SPE1建立MPBGP邻居*/
Neighbor              Ver   As              MsgRcvd      MsgSend      Up/Down
State/PfxRcd
11.11.11.51      4    200        9         16        00:04:27         1

UPE1#show bgp vpnv4 unicast detail 4:4 0.0.0.0 0.0.0.0
/*查看接收和通告缺省路由的详细信息；SPE1通告缺省路由给UPE1，下一跳修改为SPE1自己*/
BGP routing table entry for 4:4 0.0.0.0/0
  2d2h received from 11.11.11.51 (1.1.1.51)
   origin i,nexthop 11.11.11.51,localpref 100,rtpref 200,
   as path
   as4 path
   extended Community:RT:4:4
   received label  157472

UPE1#show bgp vpnv4 unicast detail 4:4 37.0.1.0 255.255.255.0
/*查看接收和通告本地直连路由的详细信息；UPE1通告明细路由给SPE1*/;
BGP routing table entry for 4:4 37.0.1.0/24
Local
   origin ?,nexthop 37.0.1.1,metric 0,rtpref 0,
   as path
   as4 path
   extended Community:RT:4:4
   received label  notag
```

```
  2d2h advertised to 11.11.11.51 (1.1.1.51)
   origin ?,nexthop 11.11.11.37,localpref 100,
   as path
   as4 path
   extended Community:RT:4:4
   sent label  213005

UPE1#ping vrf hpe 51.0.1.1
/*ping SPE1下直连地址，通过缺省路由，能ping通*/
sending 5,100-byte ICMP echoes to 51.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 6/6/8 ms.

UPE1#ping vrf hpe 52.0.1.1
/*ping SPE2下直连地址，通过缺省路由，能ping通*/
sending 5,100-byte ICMP echoes to 52.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 6/6/8 ms.

UPE1#ping vrf hpe 53.0.1.1
/*ping UPE2下直连地址，通过缺省路由，能ping通*/
sending 5,100-byte ICMP echoes to 53.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 6/6/8 ms.

/*Tester1(CE1)发流，目的IP为Tester2(CE2),流量正确转发*/
```

在SPE1上查看相应的信息：

```
SPE1#show ip forwarding route vrf hpe
/*查看私网路由转发表，SPE上维护UPE和非UPE上所有明细路由*/
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
   Dest             Gw            Interface          Owner      Pri Met
*> 37.0.1.0/24       11.11.11.37    smartgroup60       BGP        200 0
*> 51.0.1.0/24       51.0.1.1       gei-0/1.100        Direct     0   0
*> 51.0.1.1/32       51.0.1.1       gei-0/1.100        Address    0   0
*> 52.0.1.0/24       11.11.11.52    gei-0/3            BGP        200 0
*> 53.0.1.0/24       11.11.11.52    gei-0/3            BGP        200 0

SPE1#show bgp vpnv4 unicast summary
/*查看BGP vpnv4邻居，SPE1和UPE1&SPE2建立MPBGP邻居*/
Neighbor         Ver  As         MsgRcvd    MsgSend    Up/Down    State/PfxRcd
11.11.11.37      4    200        19         13         00:05:34           1
11.11.11.52      4    65002      14         26         00:05:34           2

SPE1#show bgp vpnv4 unicast detail 4:4 0.0.0.0 0.0.0.0
/*查看接收和通告缺省路由的详细信息；SPE通告缺省路由给UPE*/
BGP routing table entry for 4:4 0.0.0.0/0
  02:34:05 advertised to 11.11.11.37 (1.1.1.37)
   origin i,nexthop 11.11.11.51,localpref 100,
   as path
   as4 path
   extended Community:RT:4:4
   sent label  157472

SPE1#show bgp vpnv4 unicast detail 4:4 37.0.1.0 255.255.255.0
/*查看接收和通告UPE1下直连路由的详细信息，SPE会自动反射UPE1的路由给其他非UPE邻居*/
BGP routing table entry for 4:4 37.0.1.0/24
  02:35:35 received from 11.11.11.37 (1.1.1.37)
   origin ?,nexthop 11.11.11.37,localpref 100,rtpref 200,
```

```
   as path
   as4 path
   extended Community:RT:4:4
   received label  213005
  02:35:36 advertised to 11.11.11.52 (1.1.1.52)
   origin ?,nexthop 11.11.11.51,
   as path [200]
   as4 path
   extended Community:RT:4:4
   sent label  157625

SPE1#show bgp vpnv4 unicast detail 4:4 51.0.1.0 255.255.255.0
/*查看接收和通告本地直连路由的详细信息，SPE会通告自己路由给其他非UPE邻居*/
BGP routing table entry for 4:4 51.0.1.0/24
Local
   origin ?,nexthop 51.0.1.1,metric 0,rtpref 0,
   as path
   as4 path
   extended Community:RT:4:4
   received label  notag
  02:34:05 advertised to 11.11.11.52 (1.1.1.52)
   origin ?,nexthop 11.11.11.51,
   as path [200]
   as4 path
   extended Community:RT:4:4
   sent label  157528

SPE1#show bgp vpnv4 unicast detail 4:4 52.0.1.0 255.255.255.0
/*查看接收 和 通告SPE2下直连路由的详细信息，明细路由不会通告给UPE*/
BGP routing table entry for 4:4 52.0.1.0/24
  02:40:43 received from 11.11.11.52 (1.1.1.52)
   origin ?,nexthop 11.11.11.52,rtpref 20,
   as path [200]
   as4 path
   extended Community:RT:4:4
   received label  213013

SPE1#show bgp vpnv4 unicast detail 4:4 53.0.1.0 255.255.255.0
/*查看接收 和 通告UPE2下直连路由的详细信息，明细路由不会通告给UPE*/
BGP routing table entry for 4:4 53.0.1.0/24
  02:41:29 received from 11.11.11.52 (1.1.1.52)
   origin ?,nexthop 11.11.11.52,rtpref 20,
   as path [200]
   as4 path
   extended Community:RT:4:4
   received label  213129

SPE1#ping vrf hpe 37.0.1.1
/*ping UPE，通过明细路由，能ping通*/
sending 5,100-byte ICMP echoes to 37.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/3 ms.

SPE1#ping vrf hpe 52.0.1.1
/*ping SPE2，通过明细路由，能ping通*/
sending 5,100-byte ICMP echoes to 52.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.

SPE1#ping vrf hpe 53.0.1.1
/*ping UPE2，通过明细路由，能ping通*/
sending 5,100-byte ICMP echoes to 53.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/1 ms.
```

在SPE2上查看相应信息：

```
SPE2#show ip forwarding route vrf hpe
/*查看私网路由转发表；SPE2上维护所有UPE和非UPE的路由明细信息*/
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
status codes: *valid, >best;
   Dest             Gw            Interface          Owner      Pri Metric
*> 37.0.1.0/24       11.11.11.51    gei-0/4           BGP        20  0
*> 51.0.1.0/24       11.11.11.51    gei-0/4           BGP        20  0
*> 52.0.1.0/24       52.0.1.1       gei-0/3.1         Direct     0   0
*> 52.0.1.1/32       52.0.1.1       gei-0/3.1         Address    0   0
*> 53.0.1.0/24       11.11.11.53    smartgroup44.100   BGP        200 0

SPE2#show bgp vpnv4 unicast summary
/*查看BGP vpnv4邻居，SPE2和SPE1 & UPE2建立MPBGP邻居*/
Neighbor              Ver   As              MsgRcvd      MsgSend      Up/Down
State/PfxRcd
11.11.11.51      4    200        35        28        00:10:11          22
11.11.11.53      4    200        391       330       02:41:48          113

SPE2#show bgp vpnv4 unicast detail 4:4 0.0.0.0 0.0.0.0
/*查看接收 和 通告缺省路由的详细信息*/
BGP routing table entry for 4:4 0.0.0.0/0
  2d23h advertised to 11.11.11.53 (145.0.214.1)
   origin i,nexthop 11.11.11.52,localpref 100,
   as path
   as4 path
   extended Community:RT:4:4
   sent label  212993

SPE2#show bgp vpnv4 unicast detail 4:4 37.0.1.0 255.255.255.0
/*查看接收 和 通告UPE1下直连路由的详细信息*/
BGP routing table entry for 4:4 37.0.1.0/24
  3d2h received from 11.11.11.51 (1.1.1.51)
   origin ?,nexthop 11.11.11.51,rtpref 20,
   as path [200]
   as4 path
   extended Community:RT:4:4
   received label  157625

SPE2#show bgp vpnv4 unicast detail 4:4 51.0.1.0 255.255.255.0
/*查看接收和通告SPE1下直连路由的详细信息*/
BGP routing table entry for 4:4 51.0.1.0/24
  3d2h received from 11.11.11.51 (1.1.1.51)
   origin ?,nexthop 11.11.11.51,rtpref 20,
   as path [200]
   as4 path
   extended Community:RT:4:4
   received label  157528

SPE2#show bgp vpnv4 unicast detail 4:4 52.0.1.0 255.255.255.0
/*查看接收和通告SPE2下直连路由的详细信息*/
BGP routing table entry for 4:4 52.0.1.0/24
Local
   origin ?,nexthop 52.0.1.1,metric 0,rtpref 0,
   as path
   as4 path
   extended Community:RT:4:4
   received label  notag
  3d2h advertised to 11.11.11.51 (1.1.1.51)
   origin ?,nexthop 11.11.11.52,
   as path [200]
   as4 path
```

```
   extended Community:RT:4:4
   sent label  213013

SPE2#sho bgp vpnv4 unicast detail 4:4 53.0.1.0 255.255.255.0
/*查看接收和通告UPE2下直连路由的详细信息*/;
BGP routing table entry for 4:4 53.0.1.0/24
  3d2h received from 11.11.11.53 (145.0.214.1)
   origin ?,nexthop 11.11.11.53,localpref 100,rtpref 200,
   as path
   as4 path
   extended Community:RT:4:4
   received label  120025
  3d2h advertised to 11.11.11.51 (1.1.1.51)
   origin ?,nexthop 11.11.11.52,
   as path [200]
   as4 path
   extended Community:RT:4:4
   sent label  213129

SPE2#ping vrf hpe 37.0.1.1
/*ping UPE1，通告明细路由，能ping通*/
sending 5,100-byte ICMP echoes to 37.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.

SPE2#ping vrf hpe 51.0.1.1
/*ping SPE1，通告明细路由，能ping通*/
sending 5,100-byte ICMP echoes to 51.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.

SPE2#ping vrf hpe 53.0.1.1
/*ping SPE1，通告明细路由，能ping通*/
sending 5,100-byte ICMP echoes to 53.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.
```

在UPE2上查看相应信息：

```
UPE2#show ip forwarding route vrf hpe
/*查看私网路由转发信息表*/
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
status codes: *valid, >best;
   Dest             Gw            Interface          Owner      Pri Metric
*> 0.0.0.0/0         11.11.11.52     smartgroup44.100    BGP        200 0
*> 5.5.5.53/32       5.5.5.53        loopback55          Address    0   0
*> 53.0.1.0/24       53.0.1.1        gei-0/11.1          Direct     0   0
*> 53.0.1.1/32       53.0.1.1        gei-0/11.1          Address    0   0

UPE2#show bgp vpnv4 unicast summary
/*查看BGP vpnv4邻居信息，UPE2和SPE2建立MPBGP邻居*/
Neighbor                Ver    As            MsgRcvd      MsgSend      Up/Down
State/PfxRcd
11.11.11.52      4    200      337       398       02:45:00        2

UPE2#show bgp vpnv4 unicast detail 4:4 0.0.0.0 0.0.0.0
/*查看接收和通告缺省路由的详细信息；UPE2上只接收缺省路由；
BGP routing table entry for 4:4 0.0.0.0/0
  2d20h received from 11.11.11.52 (1.1.1.52)
   origin i,nexthop 11.11.11.52,localpref 100,rtpref 200,
   as path
```

```
   as4 path
   extended Community:RT:4:4
   received label  212993

UPE2#show bgp vpnv4 unicast detail 4:4 37.0.1.0 255.255.255.0
/*查看接收和通告UPE1下直连路由的详细信息；UPE2上只接收缺省路由*/
UPE2#show bgp vpnv4 unicast detail 4:4 51.0.1.0 255.255.255.0
/*查看接收和通告SPE1下直连路由的详细信息；UPE2上只接收缺省路由*/
UPE2#show bgp vpnv4 unicast detail 4:4 52.0.1.0 255.255.255.0
/*查看接收和通告SPE2下直连路由的详细信息；UPE2上只接收缺省路由*/
UPE2#show bgp vpnv4 unicast detail 4:4 53.0.1.0 255.255.255.0
/*查看接收和通告本地直连路由的详细信息*/
BGP routing table entry for 4:4 53.0.1.0/24
Local
   origin ?,nexthop 53.0.1.1,metric 0,rtpref 0,
   as path
   as4 path
   extended Community:RT:4:4
   received label  notag
  2d22h advertised to 11.11.11.52 (1.1.1.52)
   origin ?,nexthop 11.11.11.53,localpref 100,
   as path
   as4 path
   extended Community:RT:4:4
   sent label  120025

UPE2#ping vrf hpe 37.0.1.1
/*ping UPE1，通告缺省路由，能ping通*/
sending 5,100-byte ICMP echoes to 37.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.

UPE2#ping vrf hpe 51.0.1.1
/*ping SPE1，通告缺省路由，能ping通*/
sending 5,100-byte ICMP echoes to 51.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/1 ms.

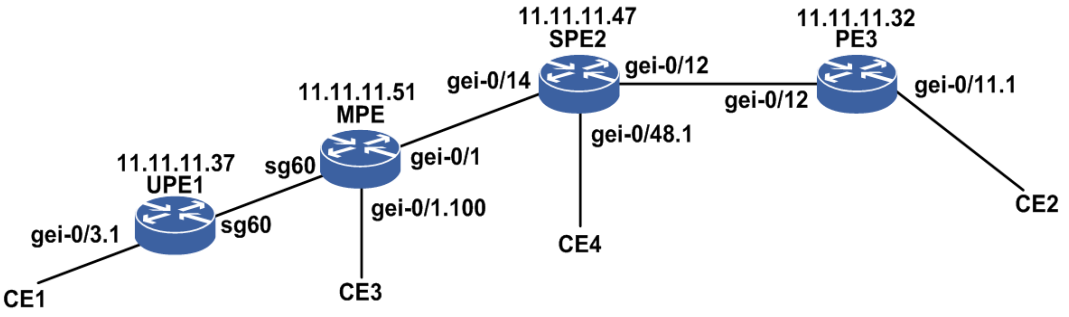
UPE2#ping vrf hpe 52.0.1.1
/*ping SPE2，通告缺省路由，能ping通*/
sending 5,100-byte ICMP echoes to 52.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/1 ms
.
/*Tester2(CE2)发流，流量目的IP为Tester1(CE1)，流量正确转发*/
```

7.3.10.3 多级 HoPE 配置实例

配置说明

在如*图 7-35*所示的网络中，配置多级HoPE功能。

图 7-35 多级 HoPE 配置实例组网图



配置思路

1.全网配置OSPF，使邻居正常建立。

2.全网开启LDP功能，使邻居正常建立。

3.各设备上配置具有相同RT属性的VRF实例。

4.在UPE1和MPE之间建立MPBGP邻居；在MPE和SPE2之间建立MPBGP邻居；在SPE2和PE3之间建立MPBGP邻居。

5.在SPE2上配置MPE为自己的UPE；在MPE上配置UPE1为自己的UPE。

6.在SPE2上通告缺省路由给MPE，MPE上收到IBGP属性的缺省路由，不会通告给UPE1，故需要在MPE上增加配置：MPE为RR，UPE1为MPE的RRC。

7.4个CE接入到各PE路由器的VRF。

配置过程

OSPF、LDP和VRF的配置略。

在MPE上的BGP vpnv4地址族下相关配置：

```
MPE(config-bgp-af-vpnv4)#neighbor 11.11.11.37 active
MPE(config-bgp-af-vpnv4)#neighbor 11.11.11.37 default-originate vrf hpe
MPE(config-bgp-af-vpnv4)#neighbor          11.11.11.37          virtual-spoke
reflect-next-hop-self
MPE(config-bgp-af-vpnv4)#neighbor 11.11.11.37 route-reflector-client
MPE(config-bgp-af-vpnv4)#neighbor 11.11.11.47 active
```

SPE2上BGP vpnv4地址族下相关配置：

```
SPE2(config-bgp-af-vpnv4)#neighbor 11.11.11.51active
SPE2(config-bgp-af-vpnv4)#neighbor 11.11.11.51 default-originate vrf hpe
SPE2(config-bgp-af-vpnv4)#neighbor          11.11.11.51          virtual-spoke
reflect-next-hop-self
SPE2(config-bgp-af-vpnv4)#neighbor 11.11.11.32 active
```

配置验证

在UPE1上查看相关命令：

```
UPE1#show ip forwarding route vrf hpe
/*查看私网路由转发表，UPE上只维护本地路由和缺省路由；此时缺省路由下一跳为SPE2
因为此时的缺省路由是通过RR反射过来的，RR反射路由时不改变下一跳信息*/
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
   Dest             Gw            Interface          Owner      Pri Metric
*> 0.0.0.0/0         11.11.11.47     smartgroup60       BGP        200 0
*> 37.0.1.0/24       37.0.1.1        gei-0/1.1          Direct     0   0
*> 37.0.1.1/32       37.0.1.1        gei-0/1.1          Address    0   0

UPE1#show bgp vpnv4 unicast summary
/*查看BGP vpnv4邻居，和MPE建立MPBGP邻居*/
Neighbor              Ver    As              MsgRcvd      MsgSend      Up/Down
State/PfxRcd
11.11.11.51      4    200        518       527       04:17:30        1

UPE1#show bgp vpnv4 unicast detail 4:4 0.0.0.0 0.0.0.0
/*查看接收和通告缺省路由的详细信息；MPE发射缺省路由给UPE1，下一跳不变仍然为SPE2，即使MPE
上配置了
命令neighbor 11.11.11.37 virtual-spoke reflect-next-hop-self也没用，因为此条缺
省路由是通过
RR反射过来的*/
BGP routing table entry for 4:4 0.0.0.0/0
  2d6h received from 11.11.11.51 (1.1.1.51)
   origin  i,nexthop  11.11.11.47,localpref  100,rtpref  200,originator_id
1.1.1.47,
   cluster list: 1.1.1.51
   as path
   as4 path
   extended Community:RT:4:4
   received label  950819

UPE1#ping vrf hpe 51.0.1.1
/*ping MPE，通过缺省路由，能ping通*/
sending 5,100-byte ICMP echoes to 51.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 6/6/7 ms.

UPE1#ping vrf hpe 47.0.1.1
/*ping SPE2，通过缺省路由，能ping通*/
sending 5,100-byte ICMP echoes to 47.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 4/4/4 ms.

UPE1#ping vrf hpe 32.0.1.1
/*ping PE3，通过缺省路由，能ping通*/
sending 5,100-byte ICMP echoes to 32.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 6/6/7 ms
```

在MPE上查看相关命令：

```
MPE#show ip forwarding route vrf hpe
/*查看私网路由转发表；MPE上的缺省路由是SPE2通告过来的，路由下一跳为SPE2*/
IPv4 Routing Table:
status codes: *valid, >best
   Dest             Gw            Interface          Owner      Pri Metric
*> 0.0.0.0/0         11.11.11.47     gei-0/1            BGP        200 0
*> 37.0.1.0/24       11.11.11.37     smartgroup60       BGP        200 0
*> 51.0.1.0/24       51.0.1.1        gei-0/1.100        Direct     0   0
```

```
*> 51.0.1.1/32       51.0.1.1       gei-0/1.100        Address     0   0

MPE#show bgp vpnv4 unicast summary
/*查看BGP vpnv4邻居，MPE和UPE1&SPE2建立L3VPN邻居*/
Neighbor              Ver   As              MsgRcvd      MsgSend      Up/Down
State/PfxRcd
11.11.11.37      4    200        528       521       04:18:27           9
11.11.11.47      4    200        3         12        00:01:12           1

MPE#show bgp vpnv4 unicast detail 4:4 0.0.0.0 0.0.0.0
/*查看接收和通告缺省路由的详细信息；缺省路由是SPE2通告过来的，为IBGP属性，IBGP路由不会向
MPIBGP邻居通告，故此处需配置RR，UPE1为RRC，反射IBGP属性的缺省路由给UPE1，路由下一跳不变*/
BGP routing table entry for 4:4 0.0.0.0/0
  06:51:21 received from 11.11.11.47 (1.1.1.47)
   origin i,nexthop 11.11.11.47,localpref 100,rtpref 200,
   as path
   as4 path
   extended Community:RT:4:4
   received label  950819
  06:51:22 advertised to 11.11.11.37 (1.1.1.37)
   origin i,nexthop 11.11.11.47,localpref 100,originator_id 1.1.1.47,
   cluster list: 1.1.1.51
   as path
   as4 path
   extended Community:RT:4:4
   sent label  950819

MPE#show bgp vpnv4 unicast detail 4:4 37.0.1.0 255.255.255.0
/*查看接收 和 通告UPE1下直连路由的详细信息*/
BGP routing table entry for 4:4 37.0.1.0/24
  04:33:41 received from 11.11.11.37 (1.1.1.37)
   origin ?,nexthop 11.11.11.37,localpref 100,rtpref 200,
   as path
   as4 path
   extended Community:RT:4:4
   received label  213005
  06:51:20 advertised to 11.11.11.47 (1.1.1.47)
   origin ?,nexthop 11.11.11.51,localpref 100,originator_id 1.1.1.37,
   cluster list: 1.1.1.51
   as path
   as4 path
   extended Community:RT:4:4
   sent label  157621


MPE#show bgp vpnv4 unicast detail 4:4 51.0.1.0 255.255.255.0
/*查看接收 和 通告MPE下直连路由的详细信息*/
BGP routing table entry for 4:4 51.0.1.0/24
Local
   origin ?,nexthop 51.0.1.1,metric 0,rtpref 0,
   as path
   as4 path
   extended Community:RT:4:4
   received label  notag
  06:51:20 advertised to 11.11.11.47 (1.1.1.47)
   origin ?,nexthop 11.11.11.51,localpref 100,
   as path
   as4 path
   extended Community:RT:4:4
   sent label  157528


MPE#show bgp vpnv4 unicast detail 4:4 47.0.1.0 255.255.255.0
/*查看接收 和 通告SPE2下直连路由的详细信息，MPE是SPE2的UPE，故不通告明细路由*/
```

```
MPE#show bgp vpnv4 unicast detail 4:4 32.0.1.0 255.255.255.0
/*查看接收 和 通告PE3下直连路由的详细信息，MPE是SPE2的UPE，故不通告明细路由*/
MPE#ping vrf hpe 37.0.1.1
/*ping UPE1，通过明细路由，能ping通*/
sending 5,100-byte ICMP echoes to 37.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.

MPE#ping vrf hpe 47.0.1.1
/*ping SPE2，通告缺省路由，能ping通*/
sending 5,100-byte ICMP echoes to 47.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.

MPE#ping vrf hpe 32.0.1.1
/*ping PE3，通过缺省路由，能ping通*/
sending 5,100-byte ICMP echoes to 32.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.
```

在SPE2上查看相关命令：

```
SPE2#show ip forwarding route vrf hpe
/*查看私网路由转发表；SPE2上维护所有路由的明细信息*/
IPv4 Routing Table:
status codes: *valid, >best
   Dest             Gw            Interface      Owner      Pri Metric
*> 32.0.1.0/24       11.11.11.32     gei-0/12       BGP        200  0
*> 32.0.1.1/32       11.11.11.32     gei-0/12       BGP        200  0
*> 37.0.1.0/24       11.11.11.51     gei-0/14       BGP        100 0
*> 47.0.1.0/24       47.0.1.1       gei-0/48.1     Direct      0   0
*> 47.0.1.1/32       47.0.1.1       gei-0/48.1     Address     0   0
*> 51.0.1.0/24       11.11.11.51     gei-0/14       BGP        100 0

SPE2#show bgp vpnv4 unicast summary
/*查看BGP vpnv4邻居，SPE2和MPE&PE3建立MPBGP邻居*/
Neighbor              Ver   As              MsgRcvd      MsgSend      Up/Down
State/PfxRcd
11.11.11.32      4    200        149       179       01:05:54           10
11.11.11.51      4    200        14        5         00:02:23           9


SPE2#show bgp vpnv4 unicast detail 4:4 0.0.0.0 0.0.0.0
/*查看接收和通告缺省路由的详细信息*/
BGP routing table entry for 4:4 0.0.0.0/0
  1d1h advertised to 11.11.11.51 (1.1.1.51)
   origin i,nexthop 11.11.11.47,localpref 100,
   as path
   as4 path
   extended Community:RT:4:4
   sent label  950819

SPE2#show bgp vpnv4 unicast detail 4:4 37.0.1.0 255.255.255.0
/*查看接收和通告UPE1下直连路由的详细信息*/
BGP routing table entry for 4:4 37.0.1.0/24
  1d1h received from 11.11.11.51 (1.1.1.51)
   origin  ?,nexthop  11.11.11.51,localpref  100,rtpref  100,originator_id
1.1.1.37,
   cluster list: 1.1.1.51
   as path
   as4 path
   extended Community:RT:4:4
   received label  157621
  1d1h advertised to 11.11.11.32 (0.0.0.1)
   origin ?,nexthop 11.11.11.47,
   as path [200]
   as4 path
```

```
   extended Community:RT:4:4
   sent label  951026


SPE2#show bgp vpnv4 unicast detail 4:4 51.0.1.0 255.255.255.0
/*查看接收和通告MPE下直连路由的详细信息*/
BGP routing table entry for 4:4 51.0.1.0/24
  1d1h received from 11.11.11.51 (1.1.1.51)
   origin ?,nexthop 11.11.11.51,localpref 100,rtpref 100,
   as path
   as4 path
   extended Community:RT:4:4
   received label  157528
  1d1h advertised to 11.11.11.32 (0.0.0.1)
   origin ?,nexthop 11.11.11.47,
   as path [200]
   as4 path
   extended Community:RT:4:4
   sent label  951060

SPE2#show bgp vpnv4 unicast detail 4:4 32.0.1.0 255.255.255.0
/*查看接收和通告PE3下直连路由的详细信息*/
BGP routing table entry for 4:4 32.0.1.0/24
  1d0h received from 11.11.11.32 (0.0.0.1)
   origin ?,nexthop 11.11.11.32,rtpref 20,
   as path [300]
   as4 path
   extended Community:RT:4:4
   received label  217113
SPE2#ping vrf hpe 37.0.1.1
/*ping UPE1，通告明细路由 ，能ping通*/
sending 5,100-byte ICMP echoes to 37.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.

SPE2#ping vrf hpe 51.0.1.1
/*ping MPE，通过明细路由，能ping通*/
sending 5,100-byte ICMP echoes to 51.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.

SPE2#ping vrf hpe 32.0.1.1
/*ping PE3，通告明细路由，能ping通*/
sending 5,100-byte ICMP echoes to 32.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/3 ms.
```

在PE3上查看相关命令：

```
PE3#show ip for route vrf hpe
/*查看私网路由转发表*/
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
status codes: *valid, >best;
   Dest             Gw            Interface      Owner      Pri Metric
*> 32.0.1.0/24       32.0.1.1       gei-0/11.1     Direct     0   0
*> 32.0.1.1/32       32.0.1.1       gei-0/11.1     Address    0   0
*> 37.0.1.0/24       11.11.11.47    gei-0/12       BGP        20  0
*> 47.0.1.0/24       11.11.11.47    gei-0/12       BGP        20  0
*> 51.0.1.0/24       11.11.11.47    gei-0/12       BGP        20  0

PE3#shwo bgp vpnv4 unicast summary
```

```
/*查看BGP vpnv4邻居，PE3和SPE2建立MPBGP邻居*/
Neighbor              Ver   As              MsgRcvd      MsgSend      Up/Down
State/PfxRcd
11.11.11.47      4    200        182       152       01:07:11         28

PE3#show bgp vpnv4 unicast detail 4:4 0.0.0.0 0.0.0.0
/*查看接收和通告缺省路由的详细信息*/
BGP routing table entry for 4:4 0.0.0.0/0

PE3#show bgp vpnv4 unicast detail 4:4 37.0.1.0 255.255.255.0
/*查看接收和通告UPE1下直连路由的详细信息*/
BGP routing table entry for 4:4 37.0.1.0/24
  3d6h received from 11.11.11.47 (1.1.1.47)
   origin ?,nexthop 11.11.11.47,rtpref 20,
   as path [200]
   as4 path
   extended Community:RT:4:4
   received label  951026

PE3#show bgp vpnv4 unicast detail 4:4 51.0.1.0 255.255.255.0
/*查看接收和通告MPE下直连路由的详细信息*/
BGP routing table entry for 4:4 51.0.1.0/24
  3d6h received from 11.11.11.47 (1.1.1.47)
   origin ?,nexthop 11.11.11.47,rtpref 20,
   as path [200]
   as4 path
   extended Community:RT:4:4
   received label  951060

PE3#show bgp vpnv4 unicast detail 4:4 47.0.1.0 255.255.255.0
/*查看接收和通告SPE2下直连路由的详细信息*/
BGP routing table entry for 4:4 47.0.1.0/24
  3d5h received from 11.11.11.47 (1.1.1.47)
   origin ?,nexthop 11.11.11.47,rtpref 20,
   as path [200]
   as4 path
   extended Community:RT:4:4
   received label  950829

PE3#show bgp vpnv4 unicast detail 4:4 32.0.1.0 255.255.255.0
/*查看接收和通告PE3下直连路由的详细信息*/
BGP routing table entry for 4:4 32.0.1.0/24
Local
   origin ?,nexthop 32.0.1.1,metric 0,rtpref 0,
   as path
   as4 path
   extended Community:RT:4:4
   received label  notag
  3d5h advertised to 11.11.11.47 (1.1.1.47)
   origin ?,nexthop 11.11.11.32,
   as path [300]
   as4 path
   extended Community:RT:4:4
   sent label  217113

PE3#ping vrf hpe 37.0.1.1
/*ping UPE1，通告明细路由，能ping通*/
sending 5,100-byte ICMP echoes to 37.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.

PE3#ping vrf hpe 51.0.1.1
/*ping MPE，通告明细路由，能ping通*/
sending 5,100-byte ICMP echoes to 51.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.
```

```
PE3#ping vrf hpe 47.0.1.1
/*ping SPE2，通过明细路由，能ping通*/
sending 5,100-byte ICMP echoes to 47.0.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.
```

7.3.11 L3VPN 隧道策略选择

隧道策略选择功能根据用户配置，负责为L2VPN/L3VPN业务选择公网隧道，实现公网转发路径的可控管理。

隧道策略通过以下方式为业务选择公网隧道：

•强制指定TE隧道。

•优选指定TE隧道。

•采用路由迭代选择TE隧道/LDP隧道。

•通过优先级控制TE隧道/LDP隧道的选择。

7.3.11.1 配置 L3VPN 与隧道策略状态一致

本节介绍L3VPN与隧道策略状态一致的配置步骤和命令。

1.创建隧道策略实例。

命令	功能
inspur(config)#**tunnel-policy** {*<policy-name>*}	配置名为policy-name的隧道策略实例

若系统中存在相同名称的隧道策略，直接进入隧道策略模式；若不存在，创建实例后（默认为自动类型，LSP选择顺序为TE优先），进入隧道策略模式。

2.配置隧道策略实例的属性。

步骤	命令	功能
1	inspur(config-tunnel-policy-policy-name)#**tunnel preferring mpls-te** *<interface-name>*[**disable-fallback**]	配置隧道策略的类型为优选类型，并指定优选隧道的隧道接口，缺省开启回切功能
2	inspur(config-tunnel-policy-policy-name)#**tunnel selecting** {**auto** | **mpls-te** *<interface-name>*}	配置隧道策略的类型为自动或者强制指定类型，同时为强制指定类型指定MPLS TE tunnel接口
3	inspur(config-tunnel-policy-policy-name)#**tunnel select-seq** {**te-lsp ldp-lsp** | **ldp-lsp te-lsp**}	配置业务应用该隧道策略时，LSP的选择顺序 LSP缺省的选择顺序：TE-LSP>LDP-LSP，即TE优先

<*interface-name*>：MPLE TE tunnel接口。

disable-fallback：关闭回切功能，默认开启回切功能。

ldp-lsp：LSP的选择顺序以LDP优先。

te-lsp：LSP的选择顺序以TE优先。

3.验证配置结果。

命令	功能
inspur#**show tunnel-policy instance-info** [<*policy-name*>]	显示系统中配置的隧道策略的信息，缺省显示所有的实例的信息
inspur#**show tunnel-policy selecting-result** [{**pseudo-wire** <*pw-name*>| **vrf** <*vrf-name*> **peer** <*ipv4-address*>}]	显示业务应用隧道策略的选择结果信息，缺省显示所有业务应用隧道策略的结果信息

举例

配置名为inspur_1的隧道策略实例：

```
inspur(config)#tunnel-policy inspur_1
inspur(config-tunnel-policy-inspur_1)#exit
```

配置名为inspur_1隧道策略的类型为优选的，指定优选的隧道出接口为te_tunnel1，且是禁止回切：

```
inspur(config)#tunnel-policy inspur_1
inspur(config-tunnel-policy-inspur_1)#tunnel preferring mpls-te te_tunnel1
disable-fallback
inspur(config-tunnel-policy-inspur_1)#exit
```

配置名为inspur_2隧道策略的类型为优选的，指定优选的隧道出接口为te_tunnel1，默认启用回切：

```
inspur(config)#tunnel-policy inspur_2
inspur(config-tunnel-policy-inspur_2)#tunnel preferring mpls-te te_tunnel1
inspur(config-tunnel-policy-inspur_2)#exit
```

配置名为inspur_4的隧道策略的类型为自动类型：

```
inspur(config)#tunnel-policy inspur_4
inspur(config-tunnel-policy-inspur_4)#tunnel selecting auto
inspur(config-tunnel-policy-inspur_4)#exit
```

配置名为inspur_5的隧道策略的类型为强制指定类型，且指定隧道出接口为te_tunnel1：

```
inspur(config)#tunnel-policy inspur_5
inspur(config-tunnel-policy-inspur_5)#tunnel selecting mpls-te te_tunnel1
inspur(config-tunnel-policy-inspur_5)#exit
```

配置名为inspur_1的隧道策略，指定其LSP的选择顺序为LDP优先：

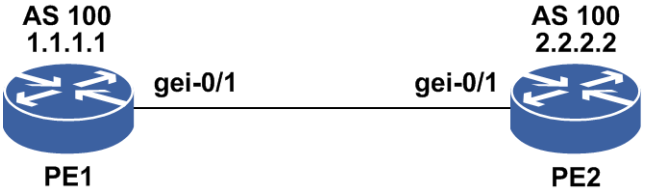
```
inspur(config)#tunnel-policy inspur_1
inspur(config-tunnel-policy-inspur_1)#tunnel select-seq ldp-lsp te-lsp
inspur(config-tunnel-policy-inspur_1)#exit
```

7.3.11.2 L3VPN 与隧道策略状态一致配置实例

配置说明

L3VPN与隧道策略状态一致配置实例的拓扑如*图 7-36*所示，PE1和PE2通过gei-0/1互联。

图 7-36 L3VPN 与隧道策略状态一致配置实例示意图



配置思路

1.配置设备接口IP地址和loopback环回地址，PE1和PE2的gei-0/1先建立OSPF邻居打通环回地址路由，并在直连接口上建立LDP邻居。

2.PE1与PE2之间配置BGP VPNv4邻居，确保邻居建链成功。

3.PE1和PE2上配置loopback环回接口绑定VRF，并将VRF直连路由重分配进BGP。

4.隧道策略优先选择流量通过LDP隧道转发，外层隧道指定为静态TE隧道。

配置过程

PE1上的配置如下：

```
PE1(config)#interface gei-0/1
PE1(config-if-gei-0/1)#ip address 190.1.1.1 255.255.255.0
PE1(config-if-gei-0/1)#no shutdown
PE1(config-if-gei-0/1)#exit
PE1(config)#interface loopback11
PE1(config-if-loopback11)#ip address 1.1.1.1 255.255.255.255
PE1(config-if-loopback11)#exit

PE1(config)#router ospf 11
PE1(config-ospf-11)#router-id 190.1.1.1
PE1(config-ospf-11)#area 0
PE1(config-ospf-11-area-0)#network 190.1.1.0 0.0.0.255
PE1(config-ospf-11-area-0)#network 1.1.1.1 0.0.0.0
PE1(config-ospf-11-area-0)#exit
PE1(config-ospf-11)#exit

PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#interface gei-0/1
PE1(config-ldp-1-if-gei-0/1)#exit
PE1(config-ldp-1)#router-id loopback11
PE1(config-ldp-1)#exit

PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 2.2.2.2 remote-as 100
```

```
PE1(config-bgp)#neighbor 2.2.2.2 update-source loopback11
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 2.2.2.2 activate
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#exit

PE1(config)#tunnel-policy abc
PE1(config-tunnel-policy-abc)#tunnel select-seq ldp-lsp te-lsp
PE1(config-tunnel-policy-abc)#exit

PE1(config)#ip vrf test
PE1(config-vrf-test)#rd 1:100
PE1(config-vrf-test)#address-family ipv4
PE1(config-vrf-test-af-ipv4)#peer 2.2.2.2 tunnel-policy abc
PE1(config-vrf-test-af-ipv4)#route-target import 1:100
PE1(config-vrf-test-af-ipv4)#route-target export 1:100
PE1(config-vrf-test-af-ipv4)#exit
PE1(config-vrf-test)#exit

PE1(config)#interface Loopback1
PE1(config-if-loopback1)#ip vrf forwarding test
PE1(config-if-loopback1)#ip address 11.1.1.1 255.255.255.255
PE1(config-if-loopback1)exit

PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv4 vrf test
PE1(config-bgp-af-ipv4-vrf)#redistribute connect
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#exit

PE1(config)#interface te_tunnel1
PE1(config-if-te_tunnel1)#exit

PE1(config)#mpls traffic-eng
PE1(config-mpls-te)#router-id 1.1.1.1
PE1(config-mpls-te)#interface loopback11
PE1(config-mpls-te-if-loopback11)#exit
PE1(config-mpls-te)#interface gei-0/1
PE1(config-mpls-te-if-gei-0/1)#exit
PE1(config-mpls-te)#static te_tunnel1
PE1(config-mpls-te-static-te_tunnel1)#role ingress type unidirectional
PE1(config-mpls-te-static-te_tunnel1)#ingress-tunnel-id 1 ingress 1.1.1.1
 egress 2.2.2.2
PE1(config-mpls-te-static-te_tunnel1)#lsp 1
PE1(config-mpls-te-static-te_tunnel1-lsp)#out-seg-info out-port gei-0/1
 out-label 3 next-hop 190.1.1.2
PE1(config-mpls-te-static-te_tunnel1-lsp)#exit
PE1(config-mpls-te-static-te_tunnel1)#exit
PE1(config-mpls-te)#exit
```

PE2上的配置如下：

```
PE2(config)#interface gei-0/1
PE2(config-if-gei-0/1)#ip address 190.1.1.2 255.255.255.0
PE2(config-if-gei-0/1)#no shutdown
PE2(config-if-gei-0/1)#exit
PE2(config)#interface loopback12
PE2(config-if-loopback11)#ip address 2.2.2.2 255.255.255.255
PE2(config-if-loopback11)#exit

PE2(config)#router ospf 11
PE2(config-ospf-11)#router-id 190.1.1.2
PE2(config-ospf-11)#area 0
PE2(config-ospf-11-area-0)#network 190.1.1.0 0.0.0.255
PE2(config-ospf-11-area-0)#network 2.2.2.2 0.0.0.0
PE2(config-ospf-11-area-0)#exit
PE2(config-ospf-11)#exit
```

```
PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#interface gei-0/1
PE2(config-ldp-1-if-gei-0/1)#exit
PE2(config-ldp-1)#router-id loopback12
PE2(config-ldp-1)#exit

PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback12
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 1.1.1.1 activate
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#exit

PE2(config)#ip vrf test
PE2(config-vrf-test)#rd 1:100
PE2(config-vrf-test)#address-family ipv4
PE2(config-vrf-test-af-ipv4)#route-target import 1:100
PE2(config-vrf-test-af-ipv4)#route-target export 1:100
PE2(config-vrf-test-af-ipv4)#exit
PE2(config-vrf-test)#exit

PE2(config)#interface Loopback1
PE2(config-if-loopback1)#ip vrf forwarding test
PE2(config-if-loopback1)#ip address 22.1.1.1 255.255.255.255
PE2(config-if-loopback1)#exit

PE2(config)#router bgp 100
PE2(config-bgp)#address-family ipv4 vrf test
PE2(config-bgp-af-ipv4-vrf)#redistribute connect
PE2(config-bgp-af-ipv4-vrf)#exit
PE2(config-bgp)#exit

PE2(config)#interface te_tunnel32775
PE2(config-if-te_tunnel32775)#exit

PE2(config)#mpls traffic-eng
PE2(config-mpls-te)#router-id 2.2.2.2
PE2(config-mpls-te)#interface loopback12
PE2(config-mpls-te-if-loopback12)#exit
PE2(config-mpls-te)#interface gei-0/1
PE2(config-mpls-te-if-gei-0/1)#exit
PE2(config-mpls-te)#static te_tunnel32775
PE2(config-mpls-te-static-te_tunnel32775)#role egress type unidirectional
PE2(config-mpls-te-static-te_tunnel32775)#ingress-tunnel-id    1    ingress
1.1.1.1
 egress 2.2.2.2
PE2(config-mpls-te-static-te_tunnel32775)#lsp 1
PE2(config-mpls-te-static-te_tunnel32775-lsp)#in-seg-info in-port gei-0/1
 in-label 3
PE2(config-mpls-te-static-te_tunnel32775-lsp)#exit
PE2(config-mpls-te-static-te_tunnel32775)#exit
PE2(config-mpls-te)#exit
```

配置验证

查看TE隧道状态：

```
PE1(config-mpls-te)#show mpls traffic-eng static

Name: tunnel_1
  Status:
    Admin Status: up  Protocol Status: up
```

```
    Actual Bandwidth: N/A
  Basic Config Parameters:
    Ingress-TnnlID:1  IngressID:1.1.1.1        EgressID:2.2.2.2
    Tunnel Type: Unidirect    Role: Ingress
    Policy Class:
    Perf Switch: off
  Binded LSP 1
  Positive Forward Info:
    in-port:
    in-label:
    out-port: gei-0/1
    out-label:3
    next-hop: 190.1.1.2
    bandwidth: 0
    burst: 0
    peak: 0
    excess-burst: 0
```

查看VRF下指定的策略最终选择的隧道类型：

```
PE1#show tunnel-policy selecting-result
The tunnel policy's tunnel selecting result:

Code   : l: means select ldp lsp, t: means select te lsp.
------------------------------------------------------------------------------
------
--
Type    InstanceName       PWName/Peer        F  ResultTE           Bandwidth
TunnelPolicyNa
me
VRF   test          2.2.2.2        t te_tunnel1     0         abc
```

查看协议和转发表路由：

```
PE1#show ip protocol routing vrf test all
Codes: OSPF-3D = ospf-type3-discard, OSPF-5D = ospf-type5-discard, TE = rsvpte,
       OSPF-7D = ospf-type7-discard, USER-I = user-ipaddr, RIP-D = rip-discard,
       OSPF-E = ospf-ext, ASBR-V = asbr-vpn, GW-FWD = ps-busi, GW-UE = ps-user,
       BGP-AD = bgp-aggr-discard, BGP-CE = bgp-confed-ext, NAT64 = sl-nat64-v4,
       USER-N = user-network, USER-S = user-special, DHCP-S = dhcp-static,
       DHCP-D = dhcp-dft
Marks: *valid, >best, s-stale

    Dest            NextHop        Intag     Outtag    RtPrf      Protocol
*>  11.1.1.1/32       11.1.1.1       212995    notag     0          Address
 *  11.1.1.1/32       11.1.1.1       212995    notag     0          Direct
*>  22.1.1.1/32       2.2.2.2        notag     212992    200        BGP-INT

PE1#show ip forwarding route vrf test
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
status codes: *valid, >best;
   Dest             Gw             Interface          Owner    Pri Metric
*> 11.1.1.1/32       11.1.1.1       loopback1          Address   0   0
*> 22.1.1.1/32       2.2.2.2        te_tunnel1         BGP      200 0
```

7.4 VPN 组播

组播VPN是一项在现有BGP/MPLS IP VPN基础上支持组播业务的技术，该技术通过对私网组播报文进行封装，并将报文由各站点间建立的组播隧道进行传递，以完成组播数据在私网之间的传送。

7.4.1 配置 VPN 组播

本节介绍VPN组播的配置步骤和命令。

1.启动PIM-SM。

步骤	命令	功能
1	inspur(config)#**ip multicast-routing**	启用IP组播路由功能
2	inspur(config-mcast)#**router pim**	启动PIM-SM模式
3	inspur(config-mcast-pim)#**exit**	退出PIM-SM模式

2.启动Option B跨域。

命令	功能
inspur(config-mcast)#**rpf-proxy-vector** {**mbgp** <*acl-name*>| **mdt**}	控制收发携带vector参数的组播加入报文，同时控制接口proxy选项的发送

3.在组播VRF模式下配置接口和实例。

步骤	命令	功能
1	inspur(config-mcast)#**vrf** <*vrf-name*>	进入组播VRF模式
2	inspur(config-mcast-vrf-vrf-name)#**mtunnel** <*interface-name*>	将某接口配置成mtunnel接口
3	inspur(config-mcast-vrf-vrf-name)#**mdt default** {<*group-address*>| **mpls-mldp** <*root-addr*>}	配置组播某实例的mdt default group
4	inspur(config-mcast-vrf-vrf-name)#**mdt data** {<*group-address*><*group-mask*>[<*acl-name*>]| **mpls-mldp** <*num-tree*>}	配置组播某实例的mdt data group

4.配置组播隧道。

步骤	命令	功能

步骤	命令	功能
1	inspur(config-mcast-vrf-vrf-name)#**provider-tunnel** {**mldp-p2mp** | **rsvp-te**}	配置组播隧道
2	inspur(config-mcast-vrf-vrf-name)#**forwarding-policy** {**per-packet** | **per-user** | **per-stream**}[**group-list** <*acl-name*>]	配置组播转发策略区分为逐包和逐用户

5.启动并配置PIM协议。

步骤	命令	功能
1	inspur(config-mcast-vrf-vrf-name)#**router pim**	启动PIM协议
2	inspur(config-mcast-vrf-vrf-name-pim)#**static-rp** <*ip-address*>[**group-list** <*prefix-list-name*>][**priority** <*priority*>]	配置静态RP 优先级参数范围：0~255，默认192
3	inspur(config-mcast-vrf-vrf-name-pim)#**bsr-candidate** <*interface-name*>[**hash-mask-length** <*hash-mask-length*>][**priority** <*priority*>]	配置候选BSR Hash长度的范围：0~32，默认30 优先级的范围：0~255，默认0
4	inspur(config-mcast-vrf-vrf-name-pim)#**rp-candidate** <*interface-name*>[**group-list** <*prefix-list-name*>][**priority** <*priority*>]	配置候选RP 优先级的范围：0~255，默认192

6.配置组播PIM-SM接口。

步骤	命令	功能
1	inspur(config-mcast-vrf-vrf-name-pim)#**interface** <*interface-name*>	配置组播PIM-SM接口
2	inspur(config-mcast-vrf-vrf-name-pim-if-interface-name)#**pimsm**	接口上启动组播路由协议PIM-SM

7.（可选）配置组播负荷分担。

命令	功能
inspur(config-mcast-vrf-vrf-name)#**multipath**	启用负荷分担，使用基于源地址的哈希算法
inspur(config-mcast-vrf-vrf-name)#**multipath s-g-hash basic**	启用负荷分担，使用基于源地址、组播地址的哈希算法
inspur(config-mcast-vrf-vrf-name)#**multipath s-g-hash next-hop-based**	启用负荷分担，使用基于下一跳的哈希算法

8.配置LDP会话。

Inbind signaling进行MLDP带内信令，需要配置MLDP相关配置。

步骤	命令	功能
1	inspur(config)#**mpls ldp instance** <*instance-id*>[**vrf** <*vrf-name*>]	进入LDP配置模式，启用LDP沿着普通的逐跳路由路径建立LSP功能
2	inspur(config-ldp-instance-id)#**router-id** <*interface-name*>	配置LDP实例标识，配置本VPN域中的某一接口地址为LDP实例的路由器标识；为了保证LDP连接的稳定性，推荐选用loopback接口地址作为LDP实例的路由器标识
3	inspur(config-ldp-instance-id)#**interface** <*interface-name*>	在LDP配置模式下添加接口，表示要在此接口上匹配上游会话

9.配置MLDP。

步骤	命令	功能
1	inspur(config)#**mpls ldp instance** <*instance-id*>[**vrf** <*vrf-name*>]	进入LDP配置模式，启用LDP沿着普通的逐跳路由路径建立LSP功能
2	inspur(config-ldp-instance-id)#**mldp**	启用MLDP功能

10.验证配置结果。

命令	功能
inspur#**show ip mroute summary vrf** <*vrf-name*>	显示IP组播路由表的具体数目
inspur#**show ip pim mroute vrf** <*vrf-name*>[**group** <*group-address*>][**source** <*source-address*>]	显示组播PIM-SM路由表的内容
inspur#**show ip pim rp mapping vrf** <*vrf-name*>	显示RP集信息
inspur#**show ip pim bsr vrf** <*vrf-name*>	显示BSR信息
inspur#**show ip pim rp hash vrf** <*vrf-name*><*group-address*>	显示特定组播组选择的RP信息
inspur#**show ip pim interface vrf** <*vrf-name*>[<*interface-name*>]	查看配置的PIM-SM接口情况
inspur#**show ip pim neighbor vrf** <*vrf-name*>[<*interface-name*>]	查看PIM-SM接口的邻居情况
inspur#**show ip pim nexthop** [**vrf**	显示组播PIM-SM到RP或是到组

命令	功能
<*vrf-name*>][**dest-address** <*dest-address*>]	播源的信息

11.清除组播路由。

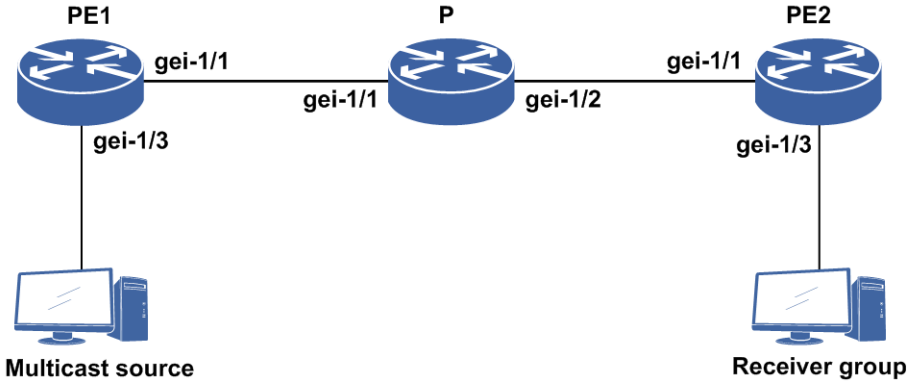
命令	功能
inspur#**clear ip mroute** [**vrf** <*vrf-name*>][**group-address** <*group-address*>][**source-address** <*source-address*>]	清除组播路由

7.4.2 VPN 组播配置实例

配置说明

该实例实现组播VPN的基本功能配置，使得私网的组播数据可以传送，如*图 7-37*所示。

图 7-37 组播 VPN 配置实例



配置思路

1.配置MPLS VPN环境。

2.配置PE1上的公网组播和私网组播。

3.配置P上的公网组播。

4.配置PE2上的公网组播和私网组播。

配置过程

配置过程如下：

1.配置MPLS VPN环境。

▸PE1上的配置：

```
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 1.1.1.17 255.255.255.255
PE1(config-if-loopback1)#exit
PE1(config)#interface gei-1/1
PE1(config-if-gei-1/1)#no shutdown
PE1(config-if-gei-1/1)#ip address 100.101.102.17 255.255.255.0
PE1(config-if-gei-1/1)#exit

PE1(config)#router ospf 1
PE1(config-ospf-1)#router-id 1.1.1.17
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 1.1.1.17 0.0.0.0
PE1(config-ospf-1-area-0)#network 100.101.102.0 0.0.0.255
PE1(config-ospf-1-area-0)#exit

PE1(config)#mpls ldp instance 20
PE1(config-ldp-20)#router-id loopback1
PE1(config-ldp-20)#interface gei-1/1
PE1(config-ldp-20-if-gei-1/1)#exit
PE1(config-ldp-20)#exit

PE1(config)#ip vrf test
PE1(config-vrf-test)#rd 10:10
PE1(config-vrf-test)#route-target 10:10
PE1(config-vrf-test)#address-family ipv4
PE1(config-vrf-test-af-ipv4)#exit
PE1(config-vrf-test)#!

PE1(config)#interface gei-1/3
PE1(config-if-gei-1/3)#no shutdown
PE1(config-if-gei-1/3)#ip vrf forwarding test
PE1(config-if-gei-1/3)#ip address 100.105.102.17 255.255.255.0
PE1(config-if-gei-1/3)#exit

PE1(config)#router bgp 1
/*注：这里一定要使用loopback接口建立BGP邻居*/
PE1(config-bgp)#neighbor 1.1.1.19 remote-as 1
PE1(config-bgp)#neighbor 1.1.1.19 activate
PE1(config-bgp)#neighbor 1.1.1.19 update-source loopback1
PE1(config-bgp)#address-family ipv4 vrf test
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 1.1.1.19 activate
PE1(config-bgp-af-vpnv4)#exit
```

▸P上的配置：

```
P(config)#interface loopback1
P(config-if-loopback1)#ip address 1.1.1.18 255.255.255.255
P(config-if-loopback1)#exit
P(config)#interface gei-1/1
P(config-if-gei-1/1)#no shutdown
P(config-if-gei-1/1)#ip address 100.101.102.18 255.255.255.0
P(config-if-gei-1/1)#exit
P(config)#interface gei-1/2
P(config-if-gei-1/2)#no shutdown
P(config-if-gei-1/2)#ip address 100.103.102.18 255.255.255.0
P(config-if-gei-1/2)#exit
```

```
P(config)#router ospf 1
P(config-ospf-1)#router-id 1.1.1.18
P(config-ospf-1)#area 0
P(config-ospf-1-area-0)#network 1.1.1.18 0.0.0.0
P(config-ospf-1-area-0)#network 100.101.102.0 0.0.0.255
P(config-ospf-1-area-0)#network 100.103.102.0 0.0.0.255
P(config-ospf-1-area-0)#exit

P(config)#mpls ldp instance 20
P(config-ldp-20)#router-id loopback1
P(config-ldp-20)#interface gei-1/1
P(config-ldp-20-if-gei-1/1)#exit
P(config-ldp-20)#interface gei-1/2
P(config-ldp-20-if-gei-1/2)#exit
P(config-ldp-20)#exit
```

▸PE2上的配置：（与PE1上的配置类似）

```
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 1.1.1.19 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#interface gei-1/1
PE2(config-if-gei-1/1)#no shutdown
PE2(config-if-gei-1/1)#ip address 100.103.102.19 255.255.255.0
PE2(config-if-gei-1/1)#exit

PE2(config)#router ospf 1
PE2(config-ospf-1)#router-id 1.1.1.19
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 1.1.1.19 0.0.0.0
PE2(config-ospf-1-area-0)#network 100.103.102.0 0.0.0.255
PE2(config-ospf-1-area-0)#exit

PE2(config)#mpls ldp instance 20
PE2(config-ldp-20)#router-id loopback1
PE2(config-ldp-20)#interface gei-1/1
PE2(config-ldp-20-if-gei-1/1)#exit
PE2(config-ldp-20)#exit

PE2(config)#ip vrf test
PE2(config-vr-testf)#rd 10:10
PE2(config-vrf-test)#route-target 10:10
PE2(config-vrf-test)#address-family ipv4
PE2(config-vrf-test-af-ipv4)#exit
PE2(config-vrf-test)#!

PE2(config)#interface gei-1/3
PE2(config-if-gei-1/3)#no shutdown
PE2(config-if-gei-1/3)#ip vrf forwarding test
PE2(config-if-gei-1/3)#ip address 100.106.102.19 255.255.255.0
PE2(config-if-gei-1/3)#exit

PE2(config)#router bgp 1
PE2(config-bgp)#neighbor 1.1.1.17 remote-as 1
PE2(config-bgp)#neighbor 1.1.1.17 activate
PE2(config-bgp)#neighbor 1.1.1.17 update-source loopback1
PE2(config-bgp)#address-family ipv4 vrf test
PE2(config-bgp-af-ipv4-vrf)#redistribute connected
PE2(config-bgp-af-ipv4-vrf)#exit
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 1.1.1.17 activate
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#exit
```

2.在PE1上配置组播。

▸配置公网组播：

```
PE1(config)#ip multicast-routing
PE1(config-mcast)#router pim
PE1(config-mcast-pim)#interface loopback1
PE1(config-mcast-pim-if-loopback1)#pimsm
PE1(config-mcast-pim-if-loopback1)#exit
PE1(config-mcast-pim)#interface gei-1/1
PE1(config-mcast-pim-if-gei-1/1)#pimsm
PE1(config-mcast-pim-if-gei-1/1)#exit
PE1(config-mcast-pim)#rp-candidate loopback1
/*公网必须有一个RP，也可以配置多个，进行选举*/
PE1(config-mcast-pim)#bsr-candidate loopback1
PE1(config-mcast-pim)#exit
PE1(config-mcast)#exit
```

▸配置私网组播：

```
PE1(config-mcast)#vrf test
PE1(config-mcast-vrf-test)#router pim
PE1(config-mcast-vrf-test-pim)#interface gei-1/3
PE1(config-mcast-vrf-test-pim-if-gei-1/3)#pimsm
PE1(config-mcast-vrf-test-pim-if-gei-1/3)#exit
PE1(config-mcast-vrf-test-pim)#rp-candidate gei-1/3
/*私网也必须有RP*/
PE1(config-mcast-vrf-test-pim)#bsr-candidate gei-1/3
PE1(config-mcast-vrf-test-pim)#exit
PE1(config-mcast-vrf-test)#mdt default 235.1.1.1
/*MDT在PE1和PE2上的配置必须相同*/
PE1(config-mcast-vrf-test)#mtunnel loopback1
/*Mtunnel接口必须是Loopback口，而且必须是BGP的建链接口*/
PE1(config-mcast-vrf-test)#exit
PE1(config-mcast)#exit
```

3.在P上配置组播。

```
P(config)#ip multicast-routing
P(config-mcast)#router pim
P(config-mcast-pim)#interface gei-1/1
P(config-mcast-pim-if-gei-1/1)#pimsm
P(config-mcast-pim-if-gei-1/1)#exit
P(config-mcast-pim)#interface gei-1/2
P(config-mcast-pim-if-gei-1/2)#pimsm
P(config-mcast-pim-if-gei-1/2)#exit
P(config-mcast-pim)#exit
```

4.在PE2上配置组播。

▸配置公网组播：

```
PE2(config)#ip multicast-routing
PE2(config-mcast)#router pim
PE2(config-mcas-pim)#interface loopback1
PE2(config-mcas-pim-if-loopback1)#pimsm
PE2(config-mcas-pim-if-loopback1)#exit
PE2(config-mcas-pim)#interface gei-1/1
PE2(config-mcas-pim-if-gei-1/1)#pimsm
PE2(config-mcas-pim-if-gei-1/1)#exit
PE2(config-mcas-pim)#exit
PE2(config-mcast)#exit
```

▸配置私网组播：

```
PE2(config-mcast)#vrf test
PE2(config-mcast-vrf-test)#router pim
PE2(config-mcast-vrf-test-pim)#interface gei-1/3
PE2(config-mcast-vrf-test-pim-if-gei-1/3)#pimsm
PE2(config-mcast-vrf-test-pim-if-gei-1/3)#exit
```

```
PE2(config-mcast-vrf-test-pim)#exit
PE2(config-mcast-vrf-test)#mdt default 235.1.1.1
/*MDT在PE1和PE2上的配置必须相同*/
PE2(config-mcast-vrf-test)#mtunnel loopback1
/*Mtunnel接口必须是Loopback口，而且必须是BGP的建链接口*/
PE2(config-mcast-vrf-test)#exit
PE2(config-mcast)#exit
```

▸接收端组加入：

```
PE2(config)#ip multicast-routing
PE2(config-mcast)#vrf test
PE2(config-mcast-vrf-test)#router igmp
/*这里接收者可以选择静态组加入，也可以选择动态组加入*/
PE2(config-mcast-vrf-test-igmp)#interface gei-1/3
PE2(config-mcast-vrf-test-igmp-if-gei-1/3)#static-group 225.0.0.1
PE2(config-mcast-vrf-test-igmp-if-gei-1/3)#exit
PE2(config-mcast-vrf-test-igmp)#exit
PE2(config-mcast-vrf-test)#exit
PE2(config-mcast)#exit
```

配置验证

MPLS VPN的环境搭建起来后，在PE1和PE2上执行命令**show ip forwarding route vrf test**看到如下的路由表，并且能够ping通对端：

```
PE1(config)#show ip forwarding route vrf test
IPv4 Routing Table:
Headers: Dest: Destination,Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
status codes: *valid, >bes
Dest             Gw             Interface    Owner    Pri  Metric
100.106.102.0/24   1.1.1.19        gei-1/1      BGP      200    0
100.105.102.0/24   100.105.102.17   gei-1/3      DIRECT    0     0
100.105.102.17/32  100.105.102.17   gei-1/3      ADDRESS   0     0

PE1#ping vrf test 100.106.102.17
sending 5,100-byte ICMP echoes to 125.1.1.1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/2 ms.
```

1.查看公网邻居建立状态：

```
PE1#show ip pim neighbor
Neighbor Address  Interface       DR Priority  Uptime    Expires    Ver
100.101.102.18    gei-1/1         1           00:06:48   00:01:20   V2
```

2.查看私网邻居建立状态：

```
PE1#show ip pim neighbor vrf test
Neighbor Address  Interface       DR Priority  Uptime    Expires    Ver
1.1.1.19          mvpn_tunnel1    1           00:03:28   00:01:17   V2
```

3.查看公网组播接口状态：

```
PE1#show ip pim interface
Address Interface State Nbr Hello DR DR PIM Mode
                            Count Period Priority Silent
1.1.1.17       loopback1    Up    0      30      1    1.1.1.17       Disabled
S
100.101.102.17 gei-1/1      Up    1      30      1    100.101.102.18 Disabled
```

```
S
```

4.查看私网组播接口状态：

```
PE1#show ip pim interface vrf test
Address Interface State Nbr Hello DR DR PIM Mode
                                Count Period Priority Silent
1.1.1.17      mvpn_tunnel1 Up    1     30     1    1.1.1.19      Disabled
S
100.105.102.17 gei-1/3     Up    0     30     1    100.105.102.17 Disabled
S
```

5.查看公网RP：

```
PE1#show ip pim rp mapping
Group(s): 224.0.0.0/4(SM)
RP: 1.1.1.17, v2, Priority:192
  BSR: 1.1.1.17, via bootstrap
       Uptime: 00:13:27, expires: 00:02:03
Group(s): 0.0.0.0/0(NOUSED)
```

6.查看私网RP：

```
PE1#show ip pim rp mapping vrf test
Group(s): 224.0.0.0/4(SM)
  RP: 100.105.102.17, v2, Priority:192
  BSR:  100.105.102.17, via bootstrap
       Uptime: 00:08:17, expires: 00:02:13
Group(s): 0.0.0.0/0(NOUSED)
```

7.查看公网BSR：

```
PE1#show ip pim bsr
BSR address: 1.1.1.17
Uptime: 00:14:30, BSR Priority :0, Hash mask length:30
Expires:00:01:40

This system is a candidate BSR!
  candidate BSR address: 1.1.1.17(loopback1),
              priority: 0,
              hash mask length: 30

This system is a candidate RP!
  candidate RP address: 1.1.1.17(loopback1),priority:192
```

8.查看私网BSR：

```
PE1#show ip pim bsr vrf test
BSR address: 100.105.102.17
Uptime: 00:09:15, BSR Priority :0, Hash mask length:30
Expires:00:01:55


This system is a candidate BSR!
  candidate BSR address: 100.105.102.17(gei-1/3),
              priority: 0,
              hash mask length: 30

This system is a candidate RP!
  candidate RP address: 100.105.102.17(gei-1/3),priority:192
```

9.查看公网路由，一般主要是查看公网和私网路由是否正确生成：

```
PE2#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(*, 235.1.1.1), RP: 1.1.1.17, TYPE: DYNAMIC, FLAGS: NS/MT
   Incoming interface: gei-1/1, flags: NS
   Outgoing interface list:
```

```
    loopback1, mvrf: test, flags: NS/MT/S
(1.1.1.17, 235.1.1.1), TYPE: DYNAMIC, FLAGS: MT
  Incoming interface: gei-1/1, flags: NS
  Outgoing interface list:
    loopback1, mvrf: test, flags: MT/S
(1.1.1.19, 235.1.1.1),  TYPE: DYNAMIC, FLAGS:
  Incoming interface: loopback1, flags:
  Outgoing interface list:
    gei-1/1, flags: F/S

PE2#show ip pim mroute
PIM-SM Multicast Routing Table
Flags: T- SPT-bit set,A- Foward,J- Join SPT,U- Upsend ,
Macro state: Ind- Pim Include Macro,Exd- Pim Exclude Macro,
     Jns- Pim Joins Macro,LAst- Pim Lost_assert Macro,
     Imo- Pim Immediate_olist Macro,Ino- Pim Inherited_olist Macro,

     Lcd- Pim Local_receiver_include Macro
Timers:Uptime/Expires(Upstream State)

(*, 235.1.1.1), 2d17h/00:00:51(JOINED), RP address: 1.1.1.17,
 Ind: 1/Jns: 0/LAst: 0/Imo: 1/Lcd: 1
 Iif: gei-1/1, RPF nbr: 100.103.102.18, AJ
 Oif:
   loopback1,    LocalIn  /  ImoXG
(1.1.1.19, 235.1.1.1), 2d17h/00:00:00(JOINED)/00:03:25,
Reg:PRUNE; RP:1.1.1.17; RT:NULL;
 Ind:0/Exd:0/Jns:1/LAst:0/Imo:1/Ino:2
 Iif: loopback1, RPF nbr:0.0.0.0(S); AT
     RPF nbr:0.0.0.0(D); 00:00:00(FORWARD);
(1.1.1.19, 235.1.1.1, rpt), 2d17h/00:00:00(PRUNED),
 Pru:0/LAst:0/Ino:1
 Iif:gei-1/1; RPF nbr: 100.103.102.18 (RPF'(*, G));
 Oif:
   loopback1,  InheritedFromXG  /  InoSGRpt  /  InoSG
   gei-1/1,  JoinsSG  /  InoSG
(1.1.1.17, 235.1.1.1), 2d17h/00:00:50(JOINED)/00:00:43,
Reg:NO INFO; RP:1.1.1.17; RT:NULL;
 Ind:0/Exd:0/Jns:0/LAst:0/Imo:0/Ino:1
 Iif: gei-1/1, RPF nbr: 100.103.102.18 (S); AT
     RPF nbr: 100.103.102.18 (D); 00:00:00(FORWARD);
 Oif:
   loopback1,  InheritedFromXG  /  InoSGRpt  /  InoSG
```

7.4.3 标签方式 MVPN 配置实例

配置说明

标签方式MVPN的典型组网示意如*图 7-38*所示，其流量转发及配置过程如下：

1.通过BGP新扩展的NLRI、VRF Route Import Extended Community等属性实现各PE间收发AD路由以及控制VPN的导入导出。

2.在各PE上通过BGP通告携带隧道属性的Intra_as AD Route来进行PE间自动发现，各PE收到Intra_as AD Route路由后通告标签模块构建I-PMSI隧道，从而形成全PE互通的一棵分发树。

3.各PE上完成I-PMSI构建后，私网协议报文将封装成标签报文通过I-PMSI收发。私网组播流量在入PE上即可通过MTunnel接口将流量转发到I-PMSI上。私网组播流量加上外层的标签封装后即可在公网通过标签交换转发至出PE。出PE根据流量的外层

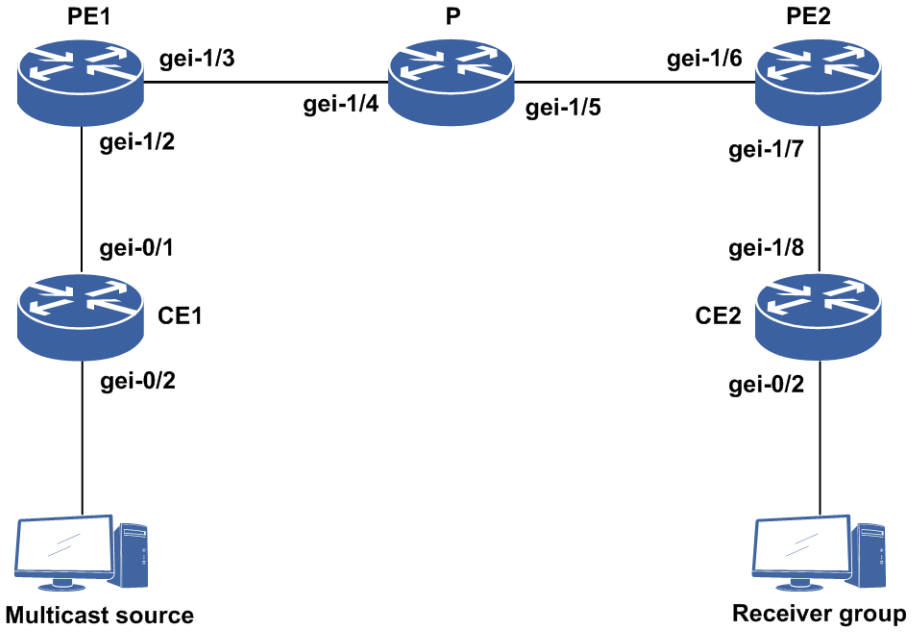
标签在本地查找获取VPN-ID信息后弹出标签，再根据内层（S，G）信息查找组播路由表，完成流量转发。

4.私网流量将触发入PE形成Source Active AD Route并通告到出PE，出PE判断本地有接收者的情况下，会形成SG Join AD Route并通告到入PE。

5.当某条（S，G）在MTunnel上转发的流量超过既定阈值后，需触发I-PMSI向S-PMSI的切换动作。流量在I-PMSI转发时间超过3秒后，自动发起S-PMSI切换动作。

6.为实现S-PMSI功能，在入PE上如果某条（S，G）已形成了本地Source Active AD Route和远端SG Join AD Route，会触发入PE形成S-PMSI AD Route并通告到出PE，出PE在收到S-PMSI AD Route时将通告标签模块构建S-PMSI隧道，入PE一定时延后将流量切换到S-PMSI上进行转发。

图 7-38 标签方式 MVPN 组网示意图



配置思路

1.组网示意中各网元配置规划参见下表。

设备名称	接口/实例名称	配置说明	其它
CE1	loopback1	配置接口地址，与PE1建立EBGP邻居	在BGP中通告该接口地址
	gei-0/1	配置接口地址	—
PE1	loopback1	配置接口地址	指定loopback1为LDP的router-id
	gei-1/3	配置接口地址	配置LDP和MLDP
	gei-1/2	配置接口地址	将gei-1/2绑定在vrf test1实例中

设备名称	接口/实例名称	配置说明	其它
	vrf test1	配置组播路由导入RT	—
P	loopback1	配置接口地址	指定loopback1为LDP的router-id
	gei-1/4	配置接口地址	配置LDP
	gei-1/5	配置接口地址	配置LDP
PE2	loopback1	配置接口地址	指定loopback1为LDP的router-id
	gei-1/6	配置接口地址	配置LDP
	gei-1/7.10	配置接口地址	将gei-1/7.10绑定在vrf test1实例中
	vrf test1	配置组播路由导入RT	—
CE2	loopback1	配置接口地址	指定loopback1为LDP的router-id
	gei-1/8.10	配置接口地址	—

2.PE1上配置OSPF协议并通告10.0.0.0/8网段，与PE2间配置MPBGP邻居并启用VPNv4和MCAST功能，与CE1建立EBGP邻居。

3.P上配置OSPF并通告10.0.0.0/8网段。

4.PE2上配置OSPF并通告10.0.0.0/8网段，与PE1间配置MPBGP邻居并启用VPNv4功能，与CE2建立OSPF邻居。

5.CE2上配置OSPF并通告10.10.10.2和loopback 200.1.1.1。

6.开启全局和VRF下的IP组播和PIM-SM协议以及provider-tunnel功能。

配置过程

CE1上的配置如下：

```
CE1(config)#interface loopback1
CE1(config-if-loopback1)#ip address 100.1.1.1 255.255.255.0
CE1(config-if-loopback1)#exit
CE1(config)#interface gei-0/1
CE1(config-if-gei-0/1)#no shutdown
CE1(config-if-gei-0/1)#ip address 10.1.1.2 255.255.255.0
CE1(config-if-gei-0/1)#exit
CE1(config)#interface gei-0/2
CE1(config-if-gei-0/2)#no shutdown
CE1(config-if-gei-0/2)#ip address 20.0.0.1 255.255.255.0
CE1(config-if-gei-0/2)#exit
CE1(config)#router bgp 200
CE1(config-bgp)#network 100.1.1.0 255.255.255.0
CE1(config-bgp)#network 20.0.0.0  255.255.255.0
CE1(config-bgp)#neighbor 10.1.1.1 remote-as 100
CE1(config-bgp)#exit
```

PE1上的配置如下：

```
PE1(config)#ip vrf test1
PE1(config-vrf-test1)#rd 100:1
PE1(config-vrf-test1)#address-family ipv4
PE1(config-vrf-test1-af-ipv4)#route-target import 100:1
PE1(config-vrf-test1-af-ipv4)#route-target export 100:1
PE1(config-vrf-test1-af-ipv4)#import multicast-route 10.10.1.1:100
/*配置组播路由导入RT，冒号之前必须是本机建立BGP邻居的地址*/
PE1(config-vrf-test1-af-ipv4)#exit
PE1(config-vrf-test1)#exit
PE1(config)#interface loopback1     /*用于公网建立MP-IBGP*/
PE1(config-if-loopback1)#ip address 10.10.1.1 255.255.255.255
PE1(config-if-loopback1)#exit
PE1(config)#interface gei-1/3
PE1(config-if-gei-1/3)#no shutdown
PE1(config-if-gei-1/3)#ip address 10.10.12.1 255.255.255.0
PE1(config-if-gei-1/3)#exit
PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#route-id loopback1
PE1(config-ldp-1)#interface gei-1/3
PE1(config-ldp-1-if-gei-1/3)#exit
PE1(config-ldp-1)#mldp            /*配置MLDP*/
PE1(config-ldp-1-mldp)#exit
PE1(config-ldp-1)#exit
PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#ip vrf forwarding test1
PE1(config-if-gei-1/2)#ip address 10.1.1.1 255.255.255.0
PE1(config-if-gei-1/2)#exit
PE1(config)#router ospf 1
PE1(config-ospf-1)#router-id 10.10.1.1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 10.0.0.0 0.255.255.255
PE1(config-ospf-1-area-0)#exit
PE1(config-ospf-1)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 10.10.3.3 remote-as 200
PE1(config-bgp)#neighbor 10.10.3.3 update-source loopback1
PE1(config-bgp)#address-family ipv4 vrf test1
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#neighbor 10.1.1.2 remote-as 200
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 10.10.3.3 activate
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#address-family vpnv4 mcast
PE1(config-bgp-af-ipv4-mcast-vpn)#neighbor 10.10.3.3 activate
/*使能vpnv4 mcast下的邻居，用于传递组播路由*/
PE1(config-bgp)#exit
```

P上的配置如下：

```
P(config)#interface gei-1/4
P(config-if-gei-1/4)#no shutdown
P(config-if-gei-1/4)#ip address 10.10.12.2 255.255.255.0
P(config-if-gei-1/4)#exit
P(config)#interface gei-1/5
P(config-if-gei-1/5)#no shutdown
P(config-if-gei-1/5)#ip address 10.10.23.2 255.255.255.0
P(config-if-gei-1/5)#exit
P(config)#interface loopback1
P(config-if-loopback1)#ip address 10.10.2.2 255.255.255.255
P(config-if-loopback1)#exit
P(config)#mpls ldp instance 1
P(config-ldp-1)#router-id loopback1
P(config-ldp-1)#interface gei-1/4
P(config-ldp-1-if-gei-1/4)#exit
```

```
P(config-ldp-1)#interface gei-1/5
P(config-ldp-1-if-gei-1/5)#exit
P(config-ldp-1)#mldp          /*配置MLDP*/
P(config-ldp-1-mldp)#exit
P(config-ldp-1)#exit
P(config)#router ospf 1
P(config-ospf-1)#router-id 10.10.2.2
P(config-ospf-1)#area 0
P(config-ospf-1-area-0)#network 10.0.0.0 0.255.255.255
P(config-ospf-1-area-0)#exit
```

PE2上的配置如下（使用以太网子接口与CE2连接）：

```
PE2(config)#ip vrf test1
PE2(config-vrf-test1)#rd 100:1
PE2(config-vrf-test1)#address-family ipv4
PE2(config-vrf-test1-af-ipv4)#route-target import 100:1
PE2(config-vrf-test1-af-ipv4)#route-target export 100:1
PE2(config-vrf-test1-af-ipv4)#import multicast-route 10.10.3.3:100
/*配置组播路由导入RT，冒号之前必须是本机建立BGP邻居的地址*/
PE2(config-vrf-test1-af-ipv4)#exit
PE2(config-vrf-test1)#exit
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 10.10.3.3 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#interface loopback2
PE2(config-if-loopback2)#ip address 3.3.3.3  255.255.255.255
 /*PE2侧使用PE上私网loopback地址作为RP，推荐这种方式，注意私网RP必须在PE上*/
PE2(config-if-loopback2)#exit
PE2(config)#interface gei-1/6
PE2(config-if-gei-1/6)#no shutdown
PE2(config-if-gei-1/6)#ip address 10.10.23.3 255.255.255.0
PE2(config-if-gei-1/6)#exit
PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#interface gei-1/6
PE2(config-ldp-1-if-gei-1/6)#exit
PE2(config-ldp-1)#mldp            /*配置MLDP*/
PE2(config-ldp-1-mldp)#exit
PE2(config-ldp-1)#exit
PE2(config)#interface gei-1/7.10
PE2(config-if-gei-1/7.10)#exit
PE2(config)#vlan-configuration
PE2(config-vlan)#interface gei-1/7.10
PE2(config-vlan-if-gei-1/7.10)#encapsulation-dot1q 10
PE2(config-vlan-if-gei-1/7.10)#exit
PE2(config-vlan)#exit
PE2(config)#interface gei-1/7.10
PE2(config-if-gei-1/7.10)#ip vrf forwarding test1
PE2(config-if-gei-1/7.10)#ip address 10.10.10.1 255.255.255.0
PE2(config-if-gei-1/7.10)#exit
PE2(config)#router ospf 1
PE2(config-ospf-1)#router-id 10.10.3.3
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 10.0.0.0 0.255.255.255
PE2(config-ospf-1-area-0)#exit
PE2(config-ospf-1)#exit
PE2(config)#router ospf 2 vrf test1
PE2(config-ospf-2)#area 0.0.0.0
PE2(config-ospf-2-area-0)#network 10.10.10.1 0.0.0.255
PE2(config-ospf-2-area-0)#network 3.3.3.3 0.0.0.0  /*通告loopback2地址*/
PE2(config-ospf-2-area-0)#exit
PE2(config-ospf-2)#redistribute bgp-int
PE2(config-ospf-2)#exit
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 10.10.1.1 remote-as 100
```

```
PE2(config-bgp)#neighbor 10.10.1.1 update-source loopback1
PE2(config-bgp)#address-family ipv4 vrf test1
PE2(config-bgp-af-ipv4-vrf)#redistribute ospf-int 2
PE2(config-bgp-af-ipv4-vrf)#redistribute connected
PE2(config-bgp-af-ipv4-vrf)#exit
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 10.10.1.1 activate
PE2(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#address-family vpnv4 mcast
PE1(config-bgp-af-ipv4-mcast-vpn)# neighbor 10.10.1.1 activate
/*使能vpnv4 mcast下的邻居，用于传递组播路由*/
PE2(config-bgp)#exit
```

CE2上的配置如下：

```
CE2(config)#interface loopback1
CE2(config-if-loopback1)#ip address 200.1.1.1 255.255.255.0
CE2(config-if-loopback1)#exit
CE2(config)#interface gei-1/8.10
CE2(config-if-gei-1/8.10)#exit
CE2(config)#vlan-configuration
CE2(config-vlan)#interface gei-1/8.10
CE2(config-vlan-if-gei-1/8.10)#encapsulation-dot1q 10
CE2(config-vlan-if-gei-1/8.10)#exit
CE2(config-vlan)#exit
CE2(config)#interface gei-1/8.10
CE2(config-if-gei-1/8.10)#ip address 10.10.10.2 255.255.255.0
CE2(config-if-gei-1/8.10)#exit
CE2(config)#interface gei-0/2
CE2(config-if-gei-0/2)#no shutdown
CE2(config-if-gei-0/2)#ip address 30.0.0.1 255.255.255.0
CE2(config-if-gei-0/2)#exit

CE2(config)#router ospf 1
CE2(config-ospf-1)#area 0
CE2(config-ospf-1-area-0)#network 10.10.10.2 0.0.0.255
CE2(config-ospf-1-area-0)#network 200.1.1.1 0.0.0.255
CE2(config-ospf-1-area-0)#network 30.0.0.1 0.0.0.255
CE2(config-ospf-1-area-0)#exit
```

配置组播功能：

```
/*配置CE1上的三层组播功能*/
CE1(config)#ip multicast-routing
CE1(config-mcast)#router pim
CE1(config-mcast-pim)#interface gei-0/1
CE1(config-mcast-pim-if-gei-0/1)#pimsm
CE1(config-mcast-pim-if-gei-0/1)#exit
CE1(config-mcast-pim)#interface gei-0/2
CE1(config-mcast-pim-if-gei-0/2)#pimsm
CE1(config-mcast-pim-if-gei-0/2)#exit
CE1(config-mcast-pim)#exit
CE1(config-mcast-pim)#static-rp 10.1.1.1
/*PE1上连接CE设备的接口地址，也可以使用私网侧loopback地址，见CE2上的配置*/
CE1(config-mcast-pim)#static-rp override
CE1(config-mcast-pim)#exit

/*配置PE1上的VRF组播功能*/
PE1(config)#ip multicast-routing
PE1(config-mcast)#vrf test1
PE1(config-mcast-vrf-test1)#provider-tunnel mldp-p2mp
/*配置私网组播业务使用MLDP LSP承载*/
PE1(config-mcast-vrf-test1)#router pim
PE1(config-mcast-vrf-test1-pim)#static-rp 10.1.1.1
/*配置私网vrf中的RP，该RP必须是本地PE私网的地址，不能是远端私网中的地址，此处举例配置静
```

```
态RP*/
PE1(config-mcast-vrf-test1-pim)#static-rp override   /*配置静态RP优先*/
PE1(config-mcast-vrf-wl-pim)#interface  gei-1/2
/*配置连接CE的私网侧接口地址开启PIM-SM*/
PE1(config-mcast-vrf-wl-pim-if-gei-1/2)#pimsm
PE1(config-mcast-vrf-wl-pim-if-gei-1/2)#exit

/*配置CE2上的三层组播功能*/
CE2(config)#ip multicast-routing
CE2(config-mcast)#router pim
CE2(config-mcast-pim)#interface gei-1/8.10
CE2(config-mcast-pim-if-gei-1/8.10)#pimsm
CE2(config-mcast-pim-if-gei-1/8.10)#exit
CE2(config-mcast-pim)#interface gei-0/2
CE2(config-mcast-pim-if-gei-0/2)#pimsm
CE2(config-mcast-pim-if-gei-0/2)#exit
CE2(config-mcast-pim)#exit
CE2(config-mcast-pim)#static-rp 3.3.3.3   /*PE2上配置的私网loopback2地址作为
RP*/
CE2(config-mcast-pim)#static-rp override
CE2(config-mcast-pim)#exit

/*配置PE2上的VRF组播功能*/
PE2(config)#ip multicast-routing
PE2(config-mcast)#vrf test1
PE2(config-mcast-vrf-test1)#provider-tunnel mldp-p2mp
/*配置私网组播业务使用MLDP LSP承载*/
PE2(config-mcast-vrf-test1)#router pim
PE2(config-mcast-vrf-test1-pim)#static-rp 10.10.10.1
/*配置私网vrf中的RP，该RP必须是本地CE侧的地址，不能是远端私网中的地址，此处举例配置静态
RP*/
PE2(config-mcast-vrf-test1-pim)#static-rp override   /*配置静态RP优先*/
PE2(config-mcast-vrf-wl-pim)#interface gei-1/7.10
/*配置连接CE的私网侧接口地址开启pimsm*/
PE2(config-mcast-vrf-wl-pim-if-gei-1/7.10)#pimsm
PE2(config-mcast-vrf-wl-pim-if-gei-1/7.10)#exit
```

配置验证

查看CE1与PE1建立EBGP连接：

```
inspur#show bgp vpnv4 unicast vrf-summary test1
Neighbor Ver As  MsgRcvd MsgSend Up/Down  State/PfxRcd
10.1.1.1 4   100 0       12      00:00:09 0
```

查看CE1的路由表如下，其中的BGP路由就是CE1学习到的VPN路由 ：

```
inspur#show ip forwarding route
IPv4 Routing Table:
Dest        Gw       Interface    Owner   Pri Metric
10.1.1.0/24  10.1.1.2  gei-0/1      DIRECT  0   0
10.1.1.2/32  10.1.1.2  gei-0/1      ADDRESS 0   0
100.1.1.0/24 100.1.1.1 loopback1    DIRECT  0   0
100.1.1.1/32 100.1.1.1 loopback1    ADDRESS 0   0
200.1.1.1/32 10.1.1.1  gei-0/1      BGP     20  0
```

组播源发送组播流，源IP为20.0.0.2，组为225.0.0.1，分别在CE1和PE1，PE2上查看私网组播表，此时由于没有成员加入，只有（S,G）表项，且出接口为空。

CE1上的组播表：

```
CE1(config)#show ip mroute  vrf  test1
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(20.0.0.2, 225.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-0/1, flags:
  Outgoing interface list:
```

PE1上的私网组播表：

```
PE1(config)#show ip mroute  vrf test1
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(20.0.0.2, 225.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-1/2, flags:
  Outgoing interface list:
```

查看PE1上的BGP通告的组播路由信息：

```
PE1(config)#show ip mvpn ad-route vrf wl
Flags: L- Local,R- Remote,J- Join Ptnl,S- Start Ptnl,T0- No Ptnl
      T1- RSVP-TE,T2- mLDP-P2MP,T3- PIM-SSM,T4- PIM-SM,T5- PIM-Bidir
      T6- Ingrs Repl,T7- mLDP-MP2MP
NLRI                          P-tunl/Next Hop                 Flags
(Type:Key)                     (flags:type:label:id)/Next Hop
1:10.10.1.1                    (0:2:0:2:1001: 10.10.1.1)          L/T2
  /*PE1通告的I-PMSI ，所有的PE之间都要建立该通路*/
5:(34.3.0.2,225.0.0.1)           10.10.1.1                        L
/*5型AD-routes，Source Active A-D route，表示有组播源，next-hop为组播源PE的loopback
地址*/
1:10.10.3.3                   (0:2:0:2:1001:10.10.3.3)          R/J/T2
/*PE2通告的I-PMSI ，所有的PE之间都要建立该通路，由于还没有加入因此还没有生成S-PMSI*/
```

PE2上查看私网组播表信息：

```
PE2(config)#show ip mroute  vrf test1
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(20.0.0.2, 225.0.0.1)
 TYPE: DYNAMIC, FLAGS:
  Incoming interface: mvpn_tunnel1, flags: MT      /*在PE2上入端口为mtunnl*/
  Outgoing interface list:
```

接收组发送加入后，分别在CE1和PE1，PE2上查看私网组播路由表。

在CE1设备上查看私网组播表：

```
CE1(config)#show ip mroute  vrf  test1
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(20.0.0.2, 225.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-0/1, flags:
  Outgoing interface list:
gei-0/2, flags:F/S     /*在CE1上其实就是普通三层组播*/
```

在PE1设备上查看私网组播表：

```
PE1(config)#show ip mroute  vrf test1
```

```
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(20.0.0.2, 225.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-1/2, flags:
  Outgoing interface list:
mvpn_tunnel1, flags: MT/S
/*在PE1上私网组播路由条目的出接口为mtunnel，即通过MLDP建立的ldp lsp进行转发*/
```

在PE1上查看BGP AD-routes 信息：

```
PE1(config)#show ip mvpn ad-route vrf test1
Flags: L- Local,R- Remote,J- Join Ptnl,S- Start Ptnl,T0- No Ptnl
      T1- RSVP-TE,T2- mLDP-P2MP,T3- PIM-SSM,T4- PIM-SM,T5- PIM-Bidir
      T6- Ingrs Repl,T7- mLDP-MP2MP
NLRI                          P-tunl/Next Hop                  Flags
(Type:Key)                    (flags:type:label:id)/Next Hop
1:10.10.1.1                   (0:2:0:2:1001: 10.10.1.1)          L/T2
3:(20.0.0.2,225.0.0.1)          (0:2:0:2:1002: 10.10.1.1)          L/S/T2
/*3型AD-routes  S-PMSI A-D route  */
5:( 20.0.0.2,225.0.0.1)           10.10.1.1                        L
1:10.10.3.3                   (0:2:0:2:1001: 10.10.3.3)          R/J/T2
7:( 20.0.0.2,225.0.0.1)           10.10.3.3                        R
/*7型AD-routes Source Tree Join route ，由成员加入的PE设备发起*/
```

PE2上查看私网组播表信息：

```
PE2(config)#show ip mroute  vrf test1
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(20.0.0.2, 225.0.0.1)
 TYPE: DYNAMIC, FLAGS:
  Incoming interface: mvpn_tunnel1, flags: MT      /*在PE2上入端口为mtunnl*/
  Outgoing interface list:
gei-1/7.10
```

在PE1上查看组播标记交换路径，由于组播源在PE1设备上，所以该路径的root在PE1：

```
PE1(config)#show mpls multicast forwarding-table mldp 10.10.1.1
Opaque Value type codes : TI:  Tunnel Id,     RM:  Rosen Mdt
                      4S:  IPv4 Source,   6S:  IPv6 Source
                      4B:  IPv4 Bidir,    6B:  IPv6 Bidir
                      V4S: VPNv4 Source,  V6S: VPNv6 Source
                      V4B: VPNv4 Bidir,   V6B: VPNv6 Bidir
                      PR:  Pub Recursive, VR:  VPN Recursive
Root/Opaque Value       Local    Outgoing Out Interface       Next Hop
                      label    label    or Vpn Id
10.10.1.1/TI[1001]      ----     16398    gei-1/3        10.10.12.2
/*I-PMSI 建立的mldp lsp，[1001]这个参数见show ip mvpn ad-routes命令中显示，
该表项表示这个是头节点，出方向标签是16398*/
10.10.1.1/TI[1002]      ----     16400    gei-1/3        10.10.12.2
/*S -PMSI 建立的mldp lsp，[1002]这个参数见show ip mvpn ad-routes命令中显示*/
```

在P上查看组播标记交换路径：

```
P#show mpls multicast forwarding-table mldp 100.0.5.1
Opaque Value type codes : TI:  Tunnel Id,     RM:  Rosen Mdt
                      4S:  IPv4 Source,   6S:  IPv6 Source
                      4B:  IPv4 Bidir,    6B:  IPv6 Bidir
                      V4S: VPNv4 Source,  V6S: VPNv6 Source
                      V4B: VPNv4 Bidir,   V6B: VPNv6 Bidir
                      PR:  Pub Recursive, VR:  VPN Recursive
```

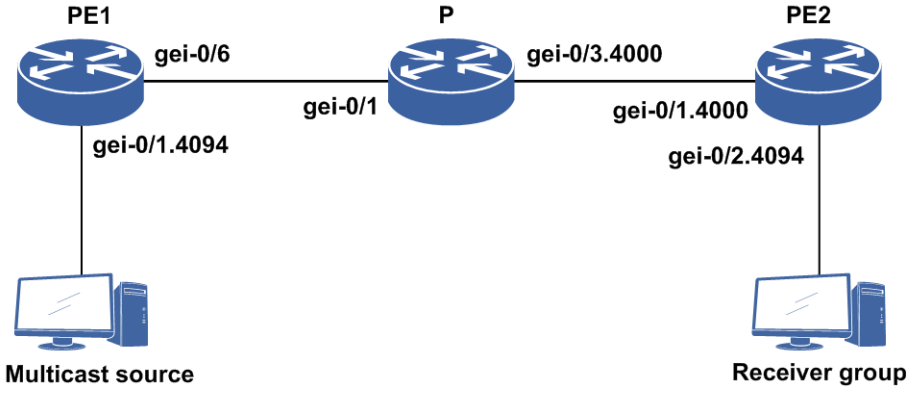
```
Root/Opaque Value      Local    Outgoing Out Interface       Next Hop
                     label    label    or Vpn Id
10.10.1.1/TI[1001]      16398    16388    gei-1/5      10.10.23.2
10.10.1.1/TI[1002]      16400    16392    gei-1/5      10.10.23.2
/*P设备上I-PMSI和S-PMSI都只做标签交换，无私网组播路由条目*/
```

7.4.4 MD 方式 MVPN 配置实例（GRE 方案）

配置说明

MD方式MVPN的典型组网示意如*图 7-39*所示，MD方案最大的优点是仅需要PE设备支持多实例，而无需升级CE和P设备，并且无需修改CE和P设备上原有的PIM配置。因此MD方案对于CE和P是透明的，CE和P无需改变。

图 7-39 MD 方式 MVPN 组网示意图



配置思路

1.接口模式下，配置路由设备接口地址。

2.打开组播模块的总开关**ip multicast—routing**。

3.进入PIM路由模式，再进入所要配置的接口。

4.接口模式下，开启PIM-SM协议。

5.PE设备组播模式下，进入VRF模式， 配置MDT方式VPN组播。

6.进入所要配置的接口开启PIM-SM。

配置过程

PE1的配置如下：

```
PE1(config)#ip vrf wl
PE1(config-vrf-wl)#rd 1:1
PE1(config-vrf-wl)#address-family ipv4
PE1(config-vrf-wl)#route-target import 1:1
```

```
PE1(config-vrf-wl)#route-target export 1:1
PE1(config-vrf-wl)#exit
PE1(config)#interface gei-0/1.4094   /*连接组播源设备的接口*/
PE1(config-if-gei-0/1.4094)#ip vrf forwarding wl
PE1(config-if-gei-0/1.4094)#ip address 34.3.0.1 255.255.255.0
PE1(config-if-gei-0/1.4094)#exit
PE1(config)#vlan-configuration
PE1(config-vlan)#interface gei-0/1.4094
PE1(config-vlan-if-gei-0/1.4094)#encapsulation-dot1q 4094
PE1(config-vlan-if-gei-0/1.4094)#!

PE1(config)#interface gei-0/6
PE1(config-if-gei-0/6)#ip address 33.2.0.1 255.255.255.252
PE1(config-if-gei-0/6)#no shutdown
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 100.0.5.1 255.255.255.255
PE1(config-if-loopback1)#exit

PE1(config)#router ospf 1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 100.0.5.1 0.0.0.0
PE1(config-ospf-1-area-0)#network 33.2.0.0 0.0.0.3
PE1(config-ospf-1-area-0)#!

PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 100.0.2.1 remote-as 100
PE1(config-bgp)#neighbor 100.0.2.1 activate
PE1(config-bgp)#neighbor 100.0.2.1 update-source loopback1
PE1(config-bgp)#address-family ipv4 vrf wl
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 100.0.2.1 activate
PE1(config-bgp-af-vpnv4)#!

PE1(config)#ip multicast-routing
PE1(config-mcast)#router pim
PE1(config-mcast-pim)#static-rp 100.0.5.1
PE1(config-mcast-pim)#static-rp override
PE1(config-mcast-pim)#interface  gei-0/6
PE1(config-mcast-pim-if-gei-0/6)#pimsm
PE1(config-mcast-pim-if-gei-0/6)#exit
PE1(config-mcast-pim)#interface loopback1
/*注意公网的loopback地址也要配置pimsm，用于建立公网的GRE隧道*/
PE1(config-mcast-pim-if-loopback1)#pimsm
PE1(config-mcast-pim-if-loopback1)#exit
PE1(config-mcast-pim)#exit
PE1(config-mcast)#vrf wl
PE1(config-mcast-vrf-wl)#mdt data 226.0.0.1 0.0.0.255
 /*配置MDT data组，可指定特定范围的组播组*/
PE1(config-mcast-vrf-wl)#mdt default 237.0.0.1
/*配置MDT default组，只能配置一个组播组地址*/
PE1(config-mcast-vrf-wl)#mtunnel loopback1
PE1(config-mcast-vrf-wl)#router pim
PE1(config-mcast-vrf-wl-pim)#static-rp 88.0.0.1
/*也可以配置动态RP，要求RP地址为私网路由可达，最好使用私网环回地址*/
PE1(config-mcast-vrf-wl-pim)#static-rp override
PE1(config-mcast-vrf-wl-pim)#interface gei-0/1.4094
PE1(config-mcast-vrf-wl-pim)#interface  gei-0/1.4094
PE1(config-mcast-vrf-wl-pim-if-gei-0/1.4094)#pimsm
PE1(config-mcast-vrf-wl-pim-if-gei-0/1.4094)#!

PE1(config)#mpls ldp instance 1
/*开启LDP，用于配置L3VPN单播路由*/
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#interface  gei-0/6
PE1(config-ldp-1-if-gei-0/6)#!
```

P设备上的配置：

```
P(config)#interface gei-0/1
P(config-if-gei-0/1)#ip address 33.2.0.2 255.255.255.252
P(config-if-gei-0/1)#no shutdown
P(config-if-gei-0/1)#exit
P(config)#interface gei-0/3.4000
P(config-if-gei-0/3.4000)#ip address 33.5.0.2 255.255.255.252
P(config-if-gei-0/3.4000)#exit
P(config)#vlan-configuration
P(config-vlan)#interface gei-0/3.4000
P(config-vlan-if-gei-0/3.4000)#encapsulation-dot1q 4000
P(config-vlan-if-gei-0/3.4000)#exit
P(config)#interface loopback1
P(config-if-loopback1)#ip address 100.1.53.1 255.255.255.255
P(config-if-loopback1)#exit

P(config)#router ospf 1
P(config-ospf-1)#area 0
P(config-ospf-1-area-0)#network 100.0.5.3 0.0.0.0
P(config-ospf-1-area-0)#network 33.2.0.0 0.0.0.3
P(config-ospf-1-area-0)#network 33.5.0.0 0.0.0.3
P(config-ospf-1-area-0)#exit
P(config-ospf-1)#exit

P(config)#ip multicast-routing    /*配置P设备上的公网组播*/
P(config-mcast)#router pim
P(config-mcast-pim)#static-rp 100.0.5.1
P(config-mcast-pim)#static-rp override
P(config-mcast-pim)#interface gei-0/1
P(config-mcast-pim-if-gei-0/1)#pimsm
P(config-mcast-pim-if-gei-0/1)# exit
P(config-mcast-pim)#interface  gei-0/3.4000
P(config-mcast-pim-if-gei-0/3.4000)#pimsm
P(config-mcast-pim-if-gei-0/3.4000)#exit
P(config-mcast-pim)#exit
P(config-mcast)#exit

P(config)#mpls ldp instance 1
P(config-ldp-1)#interface  gei-0/1
P(config-ldp-1-if-gei-0/1)#exit
P(config-ldp-1)#interface gei-0/3.4000
P(config-ldp-1-if-gei-0/3.4000)#exit
P(config-ldp-1)#exit
```

PE2上的配置：

```
PE2(config)#ip vrf wl
PE2(config-vrf-wl)#rd 1:1
PE2(config-vrf-wl)#address-family ipv4
PE2(config-vrf-wl)#route-target import 1:1
PE2(config-vrf-wl)#route-target export 1:1
PE2(config-vrf-wl)#exit
PE2(config)#interface gei-0/2.4094    /*连接组播成员设备的接口*/
PE2(config-if-gei-0/2.4094)#ip vrf forwarding wl
PE2(config-if-gei-0/2.4094)#ip address 44.1.0.1 255.255.255.0
PE2(config-if-gei-0/2.4094)#exit
PE2(config)#vlan-configuration
PE2(config-vlan)#interface gei-0/2.4094
PE2(config-vlan-if-gei-0/2.4094)#encapsulation-dot1q 4094
PE2(config-vlan-if-gei-0/2.4094)#!
PE2(config)#interface gei-0/1.4000
PE2(config-if-gei-0/1.4000)#ip address 33.5.0.1 255.255.255.252
PE2(config-if-gei-0/1.4000)#no shutdown
PE2(config)#vlan-configuration
```

```
PE2(config-vlan)#interface gei-0/1.4000
PE2(config-vlan-if-gei-0/1.4000)#encapsulation-dot1q 4000
PE2(config-vlan-if-gei-0/1.4000)#!
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 100.0.2.1 255.255.255.255
PE2(config-if-loopback1)#exit

PE2(config)#router ospf 1
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 100.0.2.1 0.0.0.0
PE2(config-ospf-1-area-0)#network 33.5.0.0 0.0.0.3
PE2(config-ospf-1-area-0)#!

PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 100.0.5.1 remote-as 100
PE2(config-bgp)#neighbor 100.0.5.1 activate
PE2(config-bgp)#neighbor 100.0.5.1 update-source loopback1
PE2(config-bgp)#address-family ipv4 vrf wl
PE2(config-bgp-af-ipv4-vrf)#redistribute connected
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 100.0.5.1 activate
PE2(config-bgp-af-vpnv4)#!

PE2(config)#ip multicast-routing
PE2(config-mcast)#router pim
PE2(config-mcast-pim)#static-rp 100.0.5.1
PE2(config-mcast-pim)#static-rp override
PE2(config-mcast-pim)#interface  gei-0/1.4000
PE2(config-mcast-pim-if-gei-0/1.4000)#pimsm
PE2(config-mcast-pim-if-gei-0/1.4000)#exit
PE2(config-mcast-pim)#interface  loopback1
/*注意公网的loopback地址也要配置pimsm，用于建立公网的GRE隧道*/
PE2(config-mcast-pim-if-loopback1)#pimsm
PE2(config-mcast-pim-if-loopback1)#exit
PE2(config-mcast-pim)#exit
PE2(config-mcast)#vrf wl
PE2(config-mcast-vrf-wl)#mdt data 226.0.0.1 0.0.0.255
/*配置MDT data组，可指定特定范围的组播组*/
PE2(config-mcast-vrf-wl)#mdt default 237.0.0.1
/*配置MDT default组，只能配置一个组播组地址*/
PE2(config-mcast-vrf-wl)#mtunnel loopback1
PE2(config-mcast-vrf-wl)#router pim
PE2(config-mcast-vrf-wl-pim)#static-rp 88.0.0.1
/*也可以配置动态RP，要求RP地址为私网路由可达，最好使用私网环回地址*/
PE2(config-mcast-vrf-wl-pim)#static-rp override
PE2(config-mcast-vrf-wl-pim)#interface gei-0/2.4094
PE2(config-mcast-vrf-wl-pim)#interface  gei-0/2.4094
PE2(config-mcast-vrf-wl-pim-if-gei-0/2.4094)#pimsm
PE2(config-mcast-vrf-wl-pim-if-gei-0/2.4094)#!

PE2(config)#mpls ldp instance 1
/*开启LDP，用于配置L3VPN单播路由*/
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#interface  gei-0/1.4000
PE2(config-ldp-1-if-gei-0/1.4000)#!
```

配置验证

在没有组播源和组播加入的情况下，MDT default组播路由表在配置完成后就会形成，显示如下。

在PE1设备上：

```
PE1(config)#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(*, 237.0.0.1)
  TYPE: DYNAMIC, FLAGS: MT
  RP: 100.0.5.1
  Incoming interface: NULL, flags:
  Outgoing interface list:
    gei-0/6, flags: F/S
    loopback1, mvrf: wl, flags: MT/S
(100.0.2.1, 237.0.0.1)
/*MDT default路由由PE设备的loopback地址发起，形成SG，所有PE和P设备上的
MDT default路由都是一致的*/
  TYPE: DYNAMIC, FLAGS: MT
  Incoming interface: gei-0/6, flags:
  Outgoing interface list:
    loopback1, mvrf: wl, flags: MT/S
(100.0.5.1, 237.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: loopback1, flags:
  Outgoing interface list:
    gei-0/6, flags: F/S
```

在P设备上：

```
P(config)#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(*, 237.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  RP: 100.0.5.1
  Incoming interface: gei-0/1, flags:
  Outgoing interface list:
    gei-0/3.4000, flags: F/S
(100.0.2.1, 237.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-0/3.4000, flags:
  Outgoing interface list:
    gei-0/1, flags: F/S
(100.0.5.1, 237.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-0/1, flags:
  Outgoing interface list:
gei-0/3.4000, flags: F/S
```

在PE2设备上：

```
PE2(config)#show ip mroute group 237.0.0.1
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(*, 237.0.0.1)
  TYPE: DYNAMIC, FLAGS: NS/MT
  RP: 100.0.5.1
  Incoming interface: gei-0/1.4000, flags: NS
  Outgoing interface list:
    loopback1, mvrf: wl, flags: MT/S
(100.0.2.1, 237.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: loopback1, flags:
  Outgoing interface list:
    gei-0/1.4000, flags: F/S
(100.0.5.1, 237.0.0.1)
  TYPE: DYNAMIC, FLAGS: MT
```

```
  Incoming interface: gei-0/1.4000, flags:
  Outgoing interface list:
loopback1, mvrf: wl, flags: MT/S
```

发送组播源和组播加入后，查看PE1的私网组播路由：

```
PE1(config)#show ip mroute vrf wl
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(34.3.0.2, 225.0.0.1)
  TYPE: DYNAMIC, FLAGS: MT
  Incoming interface: gei-0/1.4000, flags:
  Outgoing interface list:
mvpn_tunnel1, flags: MT/S
```

在PE2上查看组播表：

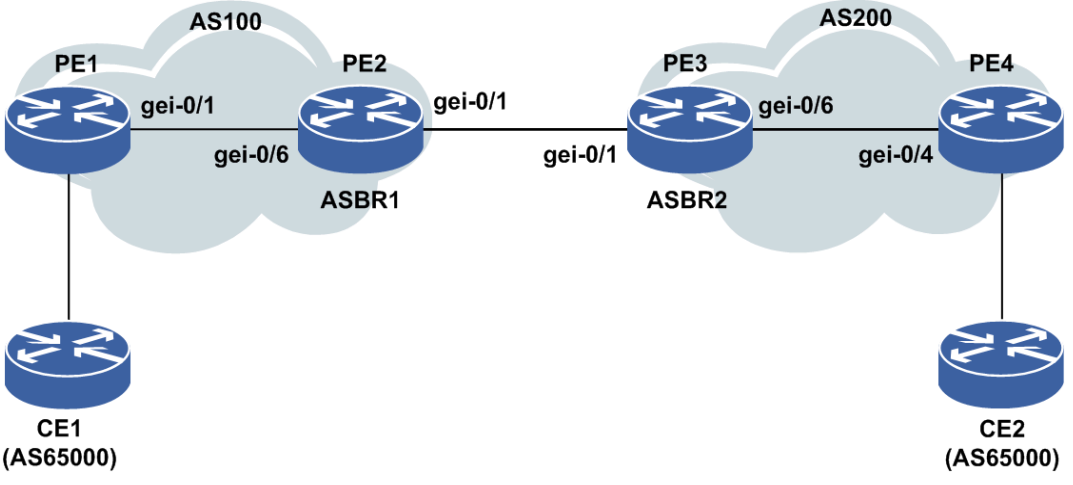
```
PE2(config)#show ip mroute vrf wl
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(*, 225.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  RP: 88.0.0.1
  Incoming interface: NULL, flags:
  Outgoing interface list:
    gei-0/2.4094, flags: F/S
(34.3.0.2, 225.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: mvpn_tunnel1, flags: MT
  Outgoing interface list:
    gei-0/2.4094, flags: F/S
```

7.4.5 MVPN 跨域配置实例

配置说明

如*图 7-40*所示，以跨域Option B方式为例说明跨域VPN组播的配置过程。

图 7-40 MVPN 跨域配置组网示意图



配置思路

1.接口地址规划参见下表。

设备	接口	规划地址	说明
PE1	gei-0/3	32.1.1.1/24	与CE1互连
	gei-0/1	37.64.1.1/24	与PE2互连
	loopback1	1.2.3.1/32	Router ID
PE2	gei-0/6	37.64.1.2/24	与PE1互连
	gei-0/1	109.65.1.1/24	与PE3互连
	loopback1	1.2.3.2/32	Router ID
PE3	gei-0/1	109.65.1.2/24	与PE2互连
	gei-0/6	63.44.1.1/24	与PE4互连
	loopback1	1.2.3.3/32	Router ID
PE4	gei-0/9	44.1.1.1/24	与CE2互连
	gei-0/4	63.44.1.2/24	与PE3互连
	loopback1	1.2.3.4/32	Router ID

2.PE1、PE2、PE3和PE4皆有VPN1，设置其RD和RT均为1:10。

3.PE1与PE2之间、PE3和PE4之间建立LDP、IGP和MP-IBGP邻居关系，Loopback地址采用IGP协议通告。

4.PE2与PE3之间建立MP-EBGP。

5.PE1为组播源，PE4为组播加入，需要配置VRF组播，PE2和PE3上没有组播成员和组播源，因此可以不配置VRF组播，但是要配置全局组播。

配置过程

PE1的配置如下：

```
PE1(config)#ip vrf vpn1
PE1(config-vrf-vpn1)#rd 1:10
PE1(config-vrf-vpn1)#route-target both 1:10
PE1(config-vrf-vpn1)#address-family ipv4
PE1(config-vrf-vpn1-af-ipv4)#exit
PE1(config-vrf-vpn1)#exit
PE1(config)#interface gei-0/3
PE1(config-if-gei-0/3)#no shutdown
PE1(config-if-gei-0/3)#ip vrf forwarding vpn1
PE1(config-if-gei-0/3)#ip address 32.1.1.1 255.255.255.0
PE1(config-if-gei-0/3)#exit
PE1(config)#interface gei-0/1
PE1(config-if-gei-0/1)#no shutdown
```

```
PE1(config-if-gei-0/1)#ip address 37.64.1.1 255.255.255.0
PE1(config-if-gei-0/1)#exit
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 1.2.3.1 255.255.255.255
PE1(config-if-loopback1)#exit

/*配置OSPF*/
PE1(config)#router ospf 1
PE1(config-ospf-1)#router-id 1.2.3.1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 37.64.1.0 0.0.0.255
PE1(config-ospf-1-area-0)#network 1.2.3.1 0.0.0.0
PE1(config-ospf-1-area-0)#!
/*配置LDP*/
PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#interface gei-0/1
PE1(config-ldp-1-if-gei-0/1)#exit
PE1(config-ldp-1)#exit
/*PE1与PE2建立MP-IBGP*/
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 1.2.3.2 remote-as 100
PE1(config-bgp)#redistribute connected  /*BGP通告直连网段*/
PE1(config-bgp)#neighbor 1.2.3.2 update-source loopback1
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 1.2.3.2 activate
PE1(config-bgp-af-vpnv4)#neighbor 1.2.3.2 send-connector
/*bgp通告connect属性，让远端私网路由下一跳指向PE而不是ASBR*/
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#address-family ipv4 vrf vpn1
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#address-family ipv4 mdt
PE1(config-bgp-af-ipv4-mdt)#neighbor 1.2.3.2 activate
PE1(config-bgp-af-ipv4-mdt)#exit
PE1(config-bgp)#exit

/*配置组播*/
PE1(config)#ip multicast-routing
PE1(config-mcast)#rpf-proxy-vector    /*开启PIM的vector属性*/
PE1(config-mcast)#router pim
PE1(config-mcast-pim)#ssm enable
PE1(config-mcast-pim)#ssm range group-list mcast
PE1(config-mcast-pim)#interface gei-0/1
PE1(config-mcast-pim-if-gei-0/1)#pimsm
PE1(config-mcast-pim-if-gei-0/1)#exit
PE1(config-mcast-pim)#interface loopback1
PE1(config-mcast-pim-if-loopback1)#pimsm
PE1(config-mcast-pim-if-loopback1)#exit
PE1(config-mcast-pim)#exit

PE1(config-mcast)#vrf vpn1
PE1(config-mcast-vrf-vpn1)#mdt data 236.0.0.1 0.0.0.0
PE1(config-mcast-vrf-vpn1)#mdt default 237.0.0.1
PE1(config-mcast-vrf-vpn1)#mtunnel loopback1
PE1(config-mcast-vrf-vpn1)#exit
PE1(config-mcast)#router pim
PE1(config-mcast-pim)#static-rp 44.1.1.1
PE1(config-mcast-pim)#static-rp override
PE1(config-mcast-pim)#interface gei-0/3
PE1(config-mcast-pim-if-gei-0/3)#pimsm
PE1(config-mcast-pim-if-gei-0/3)#exit
PE1(config-mcast-pim)#exit

/*配置SSM组的ACL列表*/
PE1(config)#ipv4-access-list mcast
```

```
PE1(config-ipv4-acl)#rule 1 permit 237.0.0.1 0.0.0.0
PE1(config-ipv4-acl)#rule 2 permit 236.0.0.1 0.0.0.0
```

PE2的配置如下：

```
/*PE2与PE1之间配置OSPF*/
PE2(config)#interface gei-0/6
PE2(config-if-gei-0/6)#no shutdown
PE2(config-if-gei-0/6)#ip address 37.64.1.2 255.255.255.0
PE2(config-if-gei-0/6)#exit
PE2(config)#interface gei-0/1
PE2(config-if-gei-0/1)#no shutdown
PE2(config-if-gei-0/1)#ip address 109.65.1.1 255.255.255.0
PE2(config-if-gei-0/1)#exit
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 1.2.3.2 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#router ospf 1
PE2(config-ospf-1)#router-id 1.2.3.2
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 37.64.1.0 0.0.0.255
PE2(config-ospf-1-area-0)#network 1.2.3.2 0.0.0.0
PE2(config-ospf-1-area-0)#!

/*配置LDP*/
PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#interface gei-0/6
PE2(config-ldp-1-if-gei-0/6)#exit
PE2(config-ldp-1)#exit

/*PE2与PE1之间配置MP-IBGP*/
PE2(config)#router bgp 100
PE2(config-bgp)#redistribute connected
PE2(config-bgp)#neighbor 1.2.3.1 remote-as 100
PE2(config-bgp)#neighbor 1.2.3.1 update-source loopback1
PE2(config-bgp)#no synchronization /*关闭BGP同步*/
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 1.2.3.1 activate
PE2(config-bgp-af-vpnv4)#neighbor 1.2.3.1 next-hop-self /*将下一跳设为自己*/
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#address-family ipv4 mdt
PE2(config-bgp-af-mdt)#neighbor 109.65.1.2 activate
PE2(config-bgp-af-mdt)#neighbor 1.2.3.1 activate
PE2(config-bgp-af-mdt)#exit
PE2(config-bgp)#no bgp default route-target filter
PE2(config-bgp)#exit

/*在两ASBR之间用直连接口建立MP-EBGP*/
PE2(config-bgp)#neighbor 109.65.1.2 remote-as 200
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 109.65.1.2 activate
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#exit


/*配置组播*/
PE2(config)#ip multicast-routing
PE2(config-mcast)#rpf-proxy-vector     /*开启PIM的vector属性*/
PE2(config-mcast)#router pim
PE2(config-mcast-pim)#ssm enable
PE2(config-mcast-pim)#ssm range group-list mcast
PE2(config-mcast-pim)#interface gei-0/6
PE2(config-mcast-pim-if-gei-0/6)#pimsm
PE2(config-mcast-pim-if-gei-0/6)#exit
PE2(config-mcast-pim)#interface gei-0/1
```

```
PE2(config-mcast-pim-if-gei-0/1)#pimsm
PE2(config-mcast-pim-if-gei-0/1)#exit
PE2(config-mcast-pim)#exit

/*配置SSM组的ACL列表*/
PE2(config)#ipv4-access-list mcast
PE2(config-ipv4-acl)#rule 1 permit 237.0.0.1 0.0.0.0
PE2(config-ipv4-acl)#rule 2 permit 236.0.0.1 0.0.0.0
```

PE3的配置如下：

```
/*配置OSPF*/
PE3(config)#interface gei-0/1
PE3(config-if-gei-0/1)#no shutdown
PE3(config-if-gei-0/1)#ip address ip address 109.65.1.2 255.255.255.0
PE3(config-if-gei-0/1)#exit
PE3(config)#interface gei-0/6
PE3(config-if-gei-0/6)#no shutdown
PE3(config-if-gei-0/6)#ip address 63.44.1.1 255.255.255.0
PE3(config-if-gei-0/6)#exit
PE3(config)#interface loopback1
PE3(config-if-loopback1)#ip address 1.2.3.3 255.255.255.255
PE3(config-if-loopback1)#exit
PE3(config)#router ospf 1
PE3(config-ospf-1)#router-id 1.2.3.3
PE3(config-ospf-1)#area 0
PE3(config-ospf-1-area-0)#network 63.44.1.0 0.0.0.255
PE3(config-ospf-1-area-0)#network 1.2.3.3 0.0.0.0
PE3(config-ospf-1-area-0)#exit

/*PE3与PE4之间配置LDP*/
PE3(config)#mpls ldp instance 1
PE3(config-ldp-1)#router-id loopback1
PE3(config-ldp-1)#interface gei-0/6
PE3(config-ldp-1-if-gei-0/6)#exit
PE3(config-ldp-1)#exit

/*PE3与PE4之间配置MP-IBGP*/
PE3(config)#router bgp 200
PE3(config-bgp)#neighbor 1.2.3.4 remote-as 200
PE3(config-bgp)#no neighbor 1.2.3.4 activate
PE3(config-bgp)#neighbor 1.2.3.4 update-source loopback1
PE3(config-bgp)#no synchronization
PE3(config-bgp)#address-family vpnv4
PE3(config-bgp-af-vpnv4)#neighbor 1.2.3.4 activate
PE3(config-bgp-af-vpnv4)#neighbor 1.2.3.4 next-hop-self
PE3(config-bgp-af-vpnv4)#exit
PE3(config-bgp)#address-family mdt
PE3(config-bgp-af-mdt)#neighbor 1.2.3.4 activate
PE3(config-bgp-af-mdt)#neighbor 109.65.1.1 activate
PE3(config-bgp-af-mdt)#exit
PE3(config-bgp)#no bgp default route-target filter
PE3(config-bgp)#exit

/*在两ASBR之间用直连接口建立MP-EBGP*/
PE3(config-bgp)#neighbor 109.65.1.1 remote-as 100
PE3(config-bgp)#address-family vpnv4
PE3(config-bgp-af-vpnv4)#neighbor 109.65.1.1 activate
PE3(config-bgp-af-vpnv4)#exit
PE3(config-bgp)#exit

/*配置组播*/
PE3(config)#ip multicast-routing
PE3(config-mcast)#rpf-proxy-vector     /*开启PIM的vector属性*/
PE3(config-mcast)#router pim
PE3(config-mcast-pim)#ssm enable
```

```
PE3(config-mcast-pim)#ssm range group-list mcast
PE3(config-mcast-pim)#interface gei-0/1
PE3(config-mcast-pim-if-gei-0/1)#pimsm
PE3(config-mcast-pim-if-gei-0/1)#exit
PE3(config-mcast-pim)#interface gei-0/6
PE3(config-mcast-pim-if-gei-0/6)#pimsm
PE3(config-mcast-pim-if-gei-0/6)#exit
PE3(config-mcast-pim)#interface loopback1
PE3(config-mcast-pim-if-loopback1)#pimsm
PE3(config-mcast-pim-if-loopback1)#exit
PE3(config-mcast-pim)#exit

/*配置SSM组的ACL列表*/
PE3(config)#ipv4-access-list mcast
PE3(config-ipv4-acl)#rule 1 permit 237.0.0.1 0.0.0.0
PE3(config-ipv4-acl)#rule 2 permit 236.0.0.1 0.0.0.0
```

PE4的配置如下：

```
PE4(config)#ip vrf vpn1
PE4(config-vrf-vpn1)#rd 1:10
PE4(config-vrf-vpn1)#route-target both 1:10
PE4(config-vrf-vpn1)#address-family ipv4
PE4(config-vrf-vpn1-af-ipv4)#exit
PE4(config-vrf-vpn1)#exit
PE4(config)#interface gei-0/9
PE4(config-if-gei-0/9)#no shutdown
PE4(config-if-gei-0/9)#ip vrf forwarding vpn1
PE4(config-if-gei-0/9)#ip address 44.1.1.1 255.255.255.0
PE4(config-if-gei-0/9)#exit
PE4(config)#interface gei-0/4
PE4(config-if-gei-0/4)#no shutdown
PE4(config-if-gei-0/4)#ip address 63.44. 1.2 255.255.255.0
PE4(config-if-gei-0/4)#exit
PE4(config)#interface loopback1
PE4(config-if-loopack1)#ip address 1.2.3.4 255.255.255.255
PE4(config-if-loopback1)#exit
 /*配置OSPF并通告路由*/
PE4(config)#router ospf 1
PE4(config-ospf-1)#router-id 1.2.3.4
PE4(config-ospf-1)#area 0
PE4(config-ospf-1-area-0)#network 63.44.1.0 0.0.0.255
PE4(config-ospf-1-area-0)#network 1.2.3.4 0.0.0.0
PE4(config-ospf-1-area-0)#!
/*接口配置LDP协议*/
PE4(config)#mpls ldp instance 1
PE4(config-ldp-1)#router-id loopback1
PE4(config-ldp-1)#interface gei-0/4
PE4(config-ldp-1-if-gei-0/4)#exit
PE4(config-ldp-1)#exit
/*配置BGP协议*/
PE4(config)#router bgp 200
PE4(config)#redistribute connected
PE4(config-bgp)#neighbor 1.2.3.3 remote-as 200
PE4(config-bgp)#no neighbor 1.2.3.3 activate
PE4(config-bgp)#neighbor 1.2.3.3 update-source loopback1
PE4(config-bgp)#address-family vpnv4 /*开启MP-BGP*/
PE4(config-bgp-af-vpnv4)#neighbor 1.2.3.3 activate
PE4(config-bgp-af-vpnv4)#neighbor 1.2.3.3 send-connector
PE4(config-bgp-af-vpnv4)#exit
PE4(config-bgp)#address-family ipv4 vrf vpn1
PE4(config-bgp-af-ipv4-vrf)#redistribute connected
/*重分发直连，如果PE与CE之间是通过动态路由协议，也需要重分发该动态路由协议*/
PE4(config-bgp-af-ipv4-vrf)#exit
PE4(config-bgp)#address-family ipv4 mdt
PE4(config-bgp-af-mdt)# neighbor 1.2.3.3 activate
```

```
PE4(config-bgp-af-mdt)#exit
PE4(config-bgp)#exit

/*配置组播*/
PE4(config)#ip multicast-routing
PE4(config-mcast)#rpf-proxy-vector     /*开启PIM的vector属性*/
PE4(config-mcast)#router pim
PE4(config-mcast-pim)#ssm enable
PE4(config-mcast-pim)#ssm range group-list mcast
PE4(config-mcast-pim)#interface gei-0/4
PE4(config-mcast-pim-if-gei-0/4)#pimsm
PE4(config-mcast-pim-if-gei-0/4)#exit
PE4(config-mcast-pim)#interface loopback1
PE4(config-mcast-pim-if-loopback1)#pimsm
PE4(config-mcast-pim-if-loopback1)#exit
PE4(config-mcast-pim)#exit

PE4(config-mcast)#vrf vpn1
PE4(config-mcast-vrf-vpn1)#mdt data 236.0.0.1 0.0.0.0
PE4(config-mcast-vrf-vpn1)#mdt default 237.0.0.1
PE4(config-mcast-vrf-vpn1)#mtunnel loopback1
PE4(config-mcast-vrf-vpn1)#exit
PE4(config-mcast)#router pim
PE4(config-mcast-pim)#static-rp 44.1.1.1
PE4(config-mcast-pim)#static-rp override
PE4(config-mcast-pim)#interface gei-0/9
PE4(config-mcast-pim-if-gei-0/9)#pimsm
PE4(config-mcast-pim-if-gei-0/9)#exit
PE4(config-mcast-pim)#exit

/*配置SSM组的ACL列表*/
PE4(config)#ipv4-access-list mcast
PE4(config-ipv4-acl)#rule 1 permit 237.0.0.1 0.0.0.0
PE4(config-ipv4-acl)#rule 2 permit 236.0.0.1 0.0.0.0
```

配置验证

在PE1和PE4上可以查询到VRF私网的PIM邻居，为远端的PE设备：

```
PE1(config)#show ip pim neighbor vrf vpn1
Neighbor Address: 1.2.3.4
  Interface: mvpn_tunnel1    /*接口为mtunnel接口*/
  Uptime: 07:14:45
  Expire: 00:01:35
  DR Pri: 1
  Attr: N/A
```

所有的PE设备上都会default组信息，如果有组播源和组播接口，则有data组路由信息。以PE1为例，没有私网组播源和组播成员加入时：

```
PE1(config)#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(1.2.3.1, 237.0.0.1)              /*本地default组*/
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: loopback1, flags:
  Outgoing interface list:
    gei-0/1, flags: F/S
(1.2.3.4, 237.0.0.1)              /*远端PE4通告的default组*/
  TYPE: DYNAMIC, FLAGS: MT
  Incoming interface: gei-0/1, flags:
```

```
  Outgoing interface list:
loopback1, mvrf: wl, flags: MT/S
```

PE2设备上：

```
PE2(config)#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(1.2.3.1, 237.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-0/6, flags:
  Outgoing interface list:
    gei-0/1, flags: F/S
(1.2.3.4, 237.0.0.1)
  TYPE: DYNAMIC, FLAGS: MT
  Incoming interface: gei-0/1, flags:
  Outgoing interface list:
gei-0/6, flags: F/S
```

发送组播的加入和组播流后，源在PE1，加入在PE4：

```
PE1(config)#show ip mroute
IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(1.2.3.1, 236.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: loopback1, flags:
  Outgoing interface list:
    gei-0/1, flags: F/S
(1.2.3.1, 237.0.0.1)          /*本地default组*/
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: loopback1, flags:
  Outgoing interface list:
    gei-0/1, flags: F/S
(1.2.3.4, 237.0.0.1)          /*远端PE4通告的default组*/
  TYPE: DYNAMIC, FLAGS: MT
  Incoming interface: gei-0/1, flags:
  Outgoing interface list:
loopback1, mvrf: wl, flags: MT/S

PE2(config)#show ip mroute

IP Multicast Routing Table
Flags:NS:SPT upsend, RT:Reg upsend, MT:Tunnel, F:Forward, S:Syn mrt,
NTP:NTP join, FLT:Flt add, FD:Flt del, DPU:Damping enable, DPD:Damping del,
(1.2.3.1, 236.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-0/6, flags:
  Outgoing interface list:
    gei-0/1, flags: F/S
(1.2.3.1, 237.0.0.1)
  TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-0/6, flags:
  Outgoing interface list:
    gei-0/1, flags: F/S
(1.2.3.4, 237.0.0.1)
  TYPE: DYNAMIC, FLAGS: MT
  Incoming interface: gei-0/1, flags:
  Outgoing interface list:
gei-0/6, flags: F/S
```

7.5 GRE 隧道

GRE是一种应用较为广泛的封装技术，经常被用来构造隧道穿越各种三层网络。GRE提供了将一种协议报文在另一种协议组成的网络中传输的能力，对某些网络层协议（如IP和IPX）的数据报进行封装，使这些被封装的数据报能够在另一个网络层协议（如IP）中传输。

GRE隧道可以划分为GRE over IPv4和GRE over IPv6两种，这两种隧道源和目的地址，都是通过GRE隧道的配置获取。

7.5.1 配置 GRE over IPv4 隧道

本节介绍GRE over IPv4隧道的配置步骤和命令。

1.创建GRE隧道接口。

步骤	命令	功能
1	inspur(config)#**interface gre_tunnel**<*tunnel-id*>	创建GRE隧道接口
2	inspur(config-if-gre_tunnelid)#**ip address** <*ip-address*><*net-mask*>	配置GRE隧道接口IP地址和掩码

2.配置GRE隧道。

步骤	命令	功能
1	inspur(config)#**gre-config**	进入GRE隧道配置模式
2	inspur(config-gre)#**interface gre_tunnel**<*tunnel-id*>	进入GRE隧道接口配置模式
3	inspur(config-gre-if-gre_tunnelid)#**tunnel mode ip**	配置当前隧道模式为GRE over IPv4
4	inspur(config-gre-if-gre_tunnelid)#**tunnel source ipv4** <*src-addr*>	配置隧道源地址
	inspur(config-gre-if-gre_tunnelid)#**tunnel source interface** <*interface-name*>	配置隧道的源IP为接口上的地址
5	inspur(config-gre-if-gre_tunnelid)#**tunnel destination ipv4** <*dst-addr*>	配置隧道目的地址

3.配置GRE隧道其他选项。

步骤	命令	功能
1	inspur(config-gre-if-gre_tunnelid)#**tu**	配置隧道KEY选项

步骤	命令	功能
	nnel key <*key-value*>	
2	inspur(config-gre-if-gre_tunnelid)#**tunnel checksum**	启用隧道校验和功能
3	inspur(config-gre-if-gre_tunnelid)#**tunnel vrf** <*vrf-name*>	配置隧道封装后跨越的VRF实例名称
4	inspur(config-gre-if-gre_tunnelid)#**tunnel clear-dont-fragment-bit**	清除报文不分片标志位
5	inspur(config-gre-if-gre_tunnelid)#**tunnel keepalive** [<*period*><*retry*>]	启用隧道保活功能
6	inspur(config-gre-if-gre_tunnelid)#**tunnel bfd**	开启隧道的BFD功能

<*period*>：保活报文发送周期，范围1~32767，单位：秒。

<*retry*>：保活报文发送的最大尝试次数，范围3~255。

<*key-value*>：用于隧道安全性的KEY值，KEY值为0~4294967295。

4.验证配置结果。

命令	功能
inspur#**show running-config-interface gre_tunnel**<*tunnel-number*>	查看指定GRE隧道的配置信息
inspur#**show ip interface gre_tunnel**<*tunnel-number*>	查看指定GRE隧道的状态信息

5.维护GRE over IPv4隧道。

命令	功能
inspur#**debug gre-tunnel**	打开GRE隧道debug开关，查看封装及解封装相关信息
inspur#**show debug gre-tunnel**	查看GRE隧道debug开关是否打开

7.5.2 配置 GRE over IPv6 隧道

本节介绍GRE over IPv6隧道的配置步骤和命令。

1.创建GRE隧道接口。

步骤	命令	功能

步骤	命令	功能
1	inspur(config)#**interface gre_tunnel**<*tunnel-id*>	创建GRE隧道接口
2	inspur(config-if-gre_tunnelid)#**ip address** <*ip-address*><*net-mask*>	配置GRE隧道接口IP地址和掩码

2.配置GRE隧道。

步骤	命令	功能
1	inspur(config)#**gre-config**	进入GRE隧道配置模式
2	inspur(config-gre)#**interface gre_tunnel**<*tunnel-id*>	进入GRE隧道接口配置模式
3	inspur(config-gre-if-gre_tunnelid)#**tunnel mode ipv6**	配置当前隧道模式为GRE over IPv6
4	inspur(config-gre-if-gre_tunnelid)#**tunnel source ipv6** <*src-addr*>	配置隧道源地址
	inspur(config-gre-if-gre_tunnelid)#**tunnel source interface** <*interface-name*>	配置隧道的源IP为接口上的地址
5	inspur(config-gre-if-gre_tunnelid)#**tunnel destination ipv6** <*dst-addr*>	配置隧道目的地址

3.配置GRE隧道其他选项。

步骤	命令	功能
1	inspur(config-gre-if-gre_tunnelid)#**tunnel key** <*key-value*>	配置隧道KEY选项
2	inspur(config-gre-if-gre_tunnelid)#**tunnel checksum**	启用隧道校验和功能
3	inspur(config-gre-if-gre_tunnelid)#**tunnel vrf** <*vrf-name*>	配置隧道封装后跨越的VRF实例名称
4	inspur(config-gre-if-gre_tunnelid)#**tunnel clear-dont-fragment-bit**	清除报文不分片标志位
5	inspur(config-gre-if-gre_tunnelid)#**tunnel keepalive** [<*period*><*retry*>]	启用隧道保活功能 GRE隧道发送保活报文周期为10秒，最大尝试次数为3次
6	inspur(config-gre-if-gre_tunnelid)#**tunnel bfd**	开启隧道的BFD功能

<*period*>：保活报文发送周期，范围1-32767，单位：秒。

<*retry*>：保活报文发送的最大尝试次数，范围3-255。

<*key-value*>：用于隧道安全性的KEY值，KEY值为0~4294967295。

4.验证配置结果。

命令	功能
inspur#**show running-config-interface gre_tunnel**<*tunnel-number*>	查看指定GRE隧道的配置信息
inspur#**show ip interface gre_tunnel**<*tunnel-number*>	查看指定GRE隧道的状态信息

5.维护GRE over IPv6隧道。

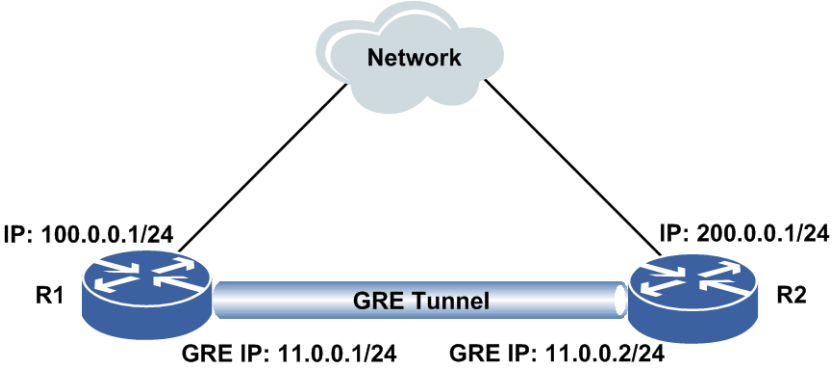
命令	功能
inspur#**debug gre-tunnel**	打开GRE隧道debug开关，查看封装及解封装相关信息
inspur#**show debug gre-tunnel**	查看GRE隧道debug开关是否打开

7.5.3 IPv4 GRE 配置实例

配置说明

如*图 7-41*所示，R1和R2之间配置GRE隧道。R1的接口地址100.0.0.1/24，GRE接口的地址11.0.0.1/24。R2的接口地址200.0.0.1/24，GRE接口的地址11.0.0.2/24。

图 7-41 IPv4 GRE 配置实例拓扑图



配置思路

1.配置R1、R2上的接口IP地址，并存在路由，使其可通。

2.全局模式下创建gre_tunnel接口，为其分配相应的IP地址。

3.全局模式下进入GRE配置模式，再进入所要配置GRE接口。

4.分别为R1、R2进行GRE配置，设定GRE工作模式，设定绑定的源和目的接口地址。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ip adderss 100.0.0.1 255.255.255.0
R1(config-if-gei-1/1)#exit
R1(config)#interface gre_tunnel1
R1(config-if-gre_tunnel1)#ip address 11.0.0.1 255.255.255.0
R1(config-if-gre_tunnel1)#exit

R1(config)#gre-config
R1(config-gre)#interface gre_tunnel1
R1(config-gre-if-gre_tunnel1)#tunnel mode ip
R1(config-gre-if-gre_tunnel1)#tunnel source ipv4 100.0.0.1
R1(config-gre-if-gre_tunnel1)#tunnel destination ipv4 200.0.0.1
R1(config-gre-if-gre_tunnel1)#exit
R1(config-gre)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-2/1
R2(config-if-gei-2/1)#no shutdown
R2(config-if-gei-2/1)#ip address 200.0.0.1 255.255.255.0
R2(config-if-gei-2/1)#exit
R2(config)#interface gre_tunnel1
R2(config-if-gre_tunnel1)#ip address 11.0.0.2 255.255.255.0
R2(config-if-gre_tunnel1)#exit

R2(config)#gre-config
R2(config-gre)#interface gre_tunnel1
R2(config-gre-if-gre_tunnel1)#tunnel mode ip
R2(config-gre-if-gre_tunnel1)#tunnel source ipv4 200.0.0.1
R2(config-gre-if-gre_tunnel1)#tunnel destination ipv4 100.0.0.1
R2(config-gre-if-gre_tunnel1)#exit
R2(config-gre)#exit
```

配置验证

查看R1，R2上的GRE配置和生效情况：

```
R1(config)#show running-config-interface gre_tunnel1
!<if-intf>
interface gre_tunnel1
  ip address 11.0.0.1 255.255.255.0
$
!</if-intf>
!<gre-tunnel>
gre-config
  interface gre_tunnel1
    tunnel mode ip
    tunnel source ipv4 100.0.0.1
    tunnel destination ipv4 200.0.0.1
  $
$
!</gre-tunnel>

R1(config)#show ip interface gre_tunnel1
 gre_tunnel1 AdminStatus is up, PhyStatus is up, line protocol is up
```

```
 Internet address is 11.0.0.1/24          /*全为UP, Tunnel生效*/
 Broadcast address is 255.255.255.255
 IP MTU is 1468 bytes

R2(config)#show running-config-interface gre_tunnel1
!<if-intf>
interface gre_tunnel1
  ip address 11.0.0.2 255.255.255.0
$
!</if-intf>
!<gre-tunnel>
gre-config
  interface gre_tunnel1
    tunnel mode ip
    tunnel source ipv4 200.0.0.1
    tunnel destination ipv4 100.0.0.1
  $
$
!</gre-tunnel>

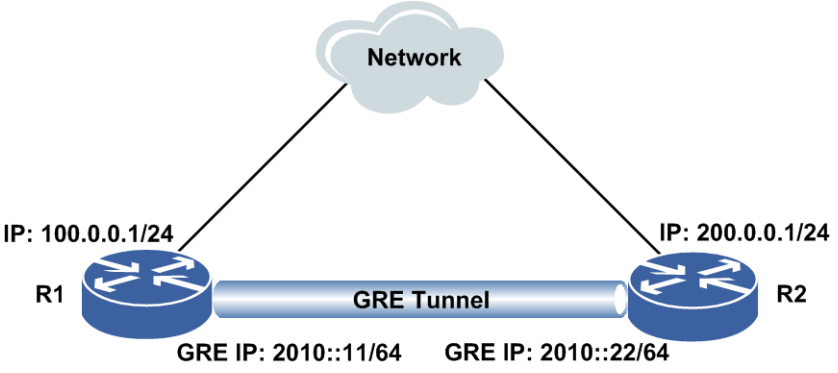
R2(config)#show ip interface gre_tunnel1
 gre_tunnel1 AdminStatus is up, PhyStatus is up, line protocol is up
 Internet address is 11.0.0.2/24          /*全为up, tunnel生效 */
 Broadcast address is 255.255.255.255
 IP MTU is 1468 bytes
```

7.5.4 GRE 6over4 配置实例

配置说明

如*图 7-42*所示，R1和R2之间配置GRE隧道。R1的接口地址100.0.0.1/24，GRE接口的地址2010::11/64。R2的接口地址200.0.0.1/24，GRE接口的地址2010::22/64。

图 7-42 GRE 6in4 配置实例拓扑图



配置思路

1.配置R1、R2上的接口IP地址，并存在路由，使其可通。

2.全局模式下创建gre_tunnel接口，为其分配相应的IPv6地址。

3.全局模式下进入GRE配置模式，再进入所要配置GRE接口。

4.分别为R1、R2进行GRE配置，设定GRE工作模式，设定绑定的源和目的接口地址。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ip adderss 100.0.0.1 255.255.255.0
R1(config-if-gei-1/1)#exit
R1(config)#interface gre_tunnel1
R1(config-if-gre_tunnel1)#ipv6 enable
R1(config-if-gre_tunnel1)#ipv6 address 2010::11/64
R1(config-if-gre_tunnel1)#exit

R1(config)#gre-config
R1(config-gre)#interface gre_tunnel1
R1(config-gre-if-gre_tunnel1)#tunnel mode ip
R1(config-gre-if-gre_tunnel1)#tunnel source ipv4 100.0.0.1
R1(config-gre-if-gre_tunnel1)#tunnel destination ipv4 200.0.0.1
R1(config-gre-if-gre_tunnel1)#tunnel key 1
R1(config-gre-if-gre_tunnel1)#exit
R1(config-gre)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-2/1
R2(config-if-gei-2/1)#no shutdown
R2(config-if-gei-2/1)#ip address 200.0.0.1 255.255.255.0
R2(config-if-gei-2/1)#exit
R2(config)#interface gre_tunnel1
R2(config-if-gre_tunnel1)#ipv6 enable
R2(config-if-gre_tunnel1)#ipv6 address 2010::22/64
R2(config-if-gre_tunnel1)#exit

R2(config)#gre-config
R2(config-gre)#interface gre_tunnel1
R2(config-gre-if-gre_tunnel1)#tunnel mode ip
R2(config-gre-if-gre_tunnel1)#tunnel source ipv4 200.0.0.1
R2(config-gre-if-gre_tunnel1)#tunnel destination ipv4 100.0.0.1
R2(config-gre-if-gre_tunnel1)#tunnel key 1
R2(config-gre-if-gre_tunnel1)#exit
R2(config-gre)#exit
```

配置验证

查看R1，R2上的GRE配置和生效情况：

```
R1(config)#show running-config-interface gre_tunnel1
!<if-intf>
interface gre_tunnel1
  ipv6 enable
  ipv6 address 2010::11/64
$
!</if-intf>
!<gre-tunnel>
gre-config
  interface gre_tunnel1
    tunnel mode ip
    tunnel source ipv4 100.0.0.1
    tunnel destination ipv4 200.0.0.1
    tunnel key 1
```

```
  $
$
!</gre-tunnel>

R1(config)#show ipv6 interface gre_tunnel1
Interface gre_tunnel1 is up, line protocol is up
  IPv6 is enable,  Hardware is Gre Tunnel
  index 17
  Bandwidth 100000 Kbits
  IPv6 MTU is 1472 bytes
  inet6 fe80::2d0:12ff:fe34:561f/10
  inet6 2010::11/64          /*如不生效会有[tentative]*/
  ND DAD is enable,number of DAD attemps:3
  ND reachable time is 30000 milliseconds

R2(config)#show running-config-interface gre_tunnel1
!<if-intf>
interface gre_tunnel1
  ipv6 enable
  ipv6 address 2010::22/64
$
!</if-intf>
!<gre-tunnel>
gre-config
  interface gre_tunnel1
    tunnel mode ip
    tunnel source ipv4 200.0.0.1
    tunnel destination ipv4 100.0.0.1
    tunnel key 1
  $
$
!<gre-tunnel>

R2(config)#show ipv6 interface gre_tunnel1
Interface gre_tunnel1 is up, line protocol is up
  IPv6 is enable,  Hardware is Gre Tunnel

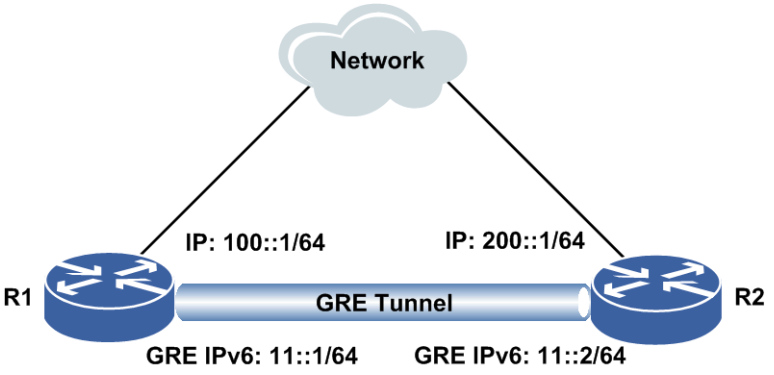
  index 17
  Bandwidth 100000 Kbits
  IPv6 MTU is 1472 bytes
  inet6 fe80::277:abff:fe13:3300/10
  inet6 2010::22/64       /*如不生效会有[tentative]*/
  ND DAD is enable,number of DAD attemps:3
  ND reachable time is 30000 milliseconds
```

7.5.5 IPv6 GRE 配置实例

配置说明

如*图 7-43*所示，R1和R2之间配置GRE隧道。R1的接口地址100::1/64，GRE接口的地址11::1/64。R2的接口地址200::1/64，GRE接口的地址11::2/64。

图 7-43 IPv6 GRE 配置实例拓扑图



配置思路

1.配置R1、R2上的接口IPv6地址，并存在路由，使其可通。

2.全局模式下创建gre_tunnel接口，为其分配相应的IPv6地址。

3.全局模式下进入GRE配置模式，再进入所要配置GRE接口。

4.分别为R1、R2进行GRE配置，设定GRE工作模式，设定绑定的源和目的接口地址。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ipv6 enable
R1(config-if-gei-1/1)#ipv6 address 100::1/64
R1(config-if-gei-1/1)#exit
R1(config)#interface gre_tunnel1
R1(config-if-gre_tunnel1)#ipv6 enable
R1(config-if-gre_tunnel1)#ipv6 address 11::1/64
R1(config-if-gre_tunnel1)#exit

R1(config)#gre-config
R1(config-gre)#interface gre_tunnel1
R1(config-gre-if-gre_tunnel1)#tunnel mode ipv6
R1(config-gre-if-gre_tunnel1)#tunnel source ipv6 100::1
R1(config-gre-if-gre_tunnel1)#tunnel destination ipv6 200::1
R1(config-gre-if-gre_tunnel1)#exit
R1(config-gre)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-2/1
R2(config-if-gei-2/1)#no shutdown
R2(config-if-gei-2/1)#ipv6 enable
R2(config-if-gei-2/1)#ipv6 address 200::1/64
R2(config-if-gei-2/1)#exit
R2(config)#interface gre_tunnel1
R2(config-if-gre_tunnel1)#ipv6 enable
R2(config-if-gre_tunnel1)#ipv6 address 11::2/64
R2(config-if-gre_tunnel1)#exit

R2(config)#gre-config
```

```
R2(config-gre)#interface gre_tunnel1
R2(config-gre-if-gre_tunnel1)#tunnel mode ipv6
R2(config-gre-if-gre_tunnel1)#tunnel source ipv6 200::1
R2(config-gre-if-gre_tunnel1)#tunnel destination ipv6 100::1
R2(config-gre-if-gre_tunnel1)#exit
R2(config-gre)#exit
```

配置验证

查看R1，R2上的GRE配置和生效情况：

```
R1(config)#show running-config-interface gre_tunnel1
!<if-intf>
interface gre_tunnel1
  ipv6 enable
  ipv6 address 11::1/64
$
!</if-intf>
!<gre-tunnel>
gre-config
  interface gre_tunnel1
    tunnel mode ipv6
    tunnel source ipv6 100::1
    tunnel destination ipv6 200::1
  $
$
!</gre-tunnel>
R1(config)#sho ipv6 interface gre_tunnel1
Interface gre_tunnel1 is up, line protocol is up    /*全为up, tunnel生效 */
  IPv6 is enabled,  Hardware is Gre Tunnel
  index 17288
  Bandwidth 100000 Kbits
  IPv6 MTU is 1456 bytes
  inet6 fe80::2d0:12ff:fe34:561f/10
  inet6 11::1/64
  ND DAD is enable,number of DAD attemps:3
  ND reachable time is 30000 millisecon

R2(config)#show running-config-interface gre_tunnel1
!<if-intf>
interface gre_tunnel1
  ipv6 enable
  ipv6 address 11::2/64
$
!</if-intf>
!<gre-tunnel>
gre-config
  interface gre_tunnel1
    tunnel mode ipv6
    tunnel source ipv6 200::1
    tunnel destination ipv6 100::1
  $
$
!</gre-tunnel>

R2(config)#show ip interface gre_tunnel1
 Interface gre_tunnel10 is up, line protocol is up   /*全为up, tunnel生效 */
  IPv6 is enabled,  Hardware is Gre Tunnel
  index 17225
  Bandwidth 100000 Kbits
  IPv6 MTU is 1456 bytes
  inet6 fe80::201:12ff:feac:121a/10
  inet6 11::2/64
  ND DAD is enable,number of DAD attemps:3
  ND reachable time is 30000 milliseconds
```

7.6 IPSec VPN

功能概述

IPSec VPN是一种在公有网络上提供安全可靠的私有通信的服务。企业的分支办公室和移动办公用户在公有Internet上使用IPSec VPN技术与企业总部建立连接。IPSec VPN与传统的使用专线或帧中继连接的网络相比，其最大的好处就是降低了成本，增强了灵活性。

IPSev VPN大致上可以分为两种应用模式：

·远程访问IPSec VPN

·站点到站点IPSec VPN

7.6.1 配置感兴趣流

配置IPsec感兴趣流，即通过访问控制列表来配置IPSec ACL，参见*《配置指导（策略模板）》*中的"ACL配置"。

7.6.2 配置 IKE 阶段 1

本节介绍IKE阶段1的配置步骤和命令。

1.配置全局ISAKMP基本功能。

步骤	命令	功能
1	`inspur(config)#`**isakmp enable**	开启IKE协商功能
2	`inspur(config)#`**isakmp identity** {**address**|**hostname**}	配置IKE协商的身份类型，默认为address
3	`inspur(config)#`**isakmp aggressive** {**disable**|**enable**}	允许/禁止对端使用野蛮模式，默认为允许
	`inspur(config)#`**isakmp phase1 aggressive crypto** { **enable**|**disable**}	对野蛮模式协商的第三条报文，开启或关闭加密功能
4	`inspur(config)#`**isakmp pre-shared key** {**ipv4-address** *<peer-ipv4-address>* **netmask** *<peer-ipv4-netmask>*[**vrf-name** *<ipv4-vrf-name>*]|**fqdn** *<hostname>*[**vrf-name** *<fqdn-vrf-name>*]}	进入IKE协商的预共享密钥
5	`inspur(config-isakmp-pre-shared-key)#`**key** *<key>*	配置IKE协商的预共享密钥

步骤	命令	功能
6	inspur(config)#**isakmp exchange-mode** {**main**|**aggressive**}{**ipv4-address** <*peer-ipv4-address*> **netmask** <*peer-ipv4-netmask*>[**vrf-name** <*ipv4-vrf-name*>]	配置IKE协商的交换类型，默认为main模式
7	inspur(config)#**nat-transparency keepalive** <*second*>	设置NAT穿越情况下NAT设备保活时间
8	inspur(config)#**nat-transparency udp-encapsulation**	开启设备支持NAT穿越功能

2.配置ISAKMP协商策略。

步骤	命令	功能
1	inspur(config)#**isakmp policy** <*policy-priority*>	创建IKE协商策略
2	inspur(config-isakmp-policy-priority)#**authentication** <*pre-share* | **rsa-sig**>	IKE策略的认证方式为预共享
3	inspur(config-isakmp-policy-priority)#**encryption** <*encryption-algorithm*>	指定IKE策略的加密算法，默认为3des
4	inspur(config-isakmp-policy-priority)#**group** {**1**|**2**|**5**}	指定IKE策略的DH交换群，默认为1
5	inspur(config-isakmp-policy-priority)#**hash** {**md5**|**sha1**}	指定IKE策略的hash算法，默认为sha1
6	inspur(config-isakmp-policy-priority)#**lifetime** <*lifetime*>	指定ISAKMPSA的生命期，默认为86400
7	inspur(config)#**isakmp peer** {**ipv4-address** <*peer-ipv4-address*>[**vrf-name** <*ipv4-vrf-name*>]} **policy** <*policy-priority*>	针对peer地址与VRF配置第一阶段policy

3.配置DPD功能。

步骤	命令	功能
1	inspur(config)#**isakmp global-keepalive** <*dpd-interval*> **retry** <*dpd-pkt-interval*>	设定全局DPD检测机制中DPD间隔和重传间隔
2	inspur(config)#**isakmp keepalive** <*dpd-interval*> **retry** <*dpd-pkt-interval*>{**ipv4-address** <*peer-ipv4-address*> **netmask** <*peer-ipv4-netmask*>[**vrf-name** <*ipv4-vrf-name*>]|**fqdn** <*hostname*>[**vrf-name** <*fqdn-vrf-name*>]}	为某个ISAKMP协商对端设定DPD检测机制中DPD间隔和重传间隔

步骤	命令	功能
3	inspur(config)#**isakmp resend-count** <*resend-count*>	指定重传次数

4.配置局部ISAKMP描述。

步骤	命令	功能
1	inspur(config)#**isakmp key-set** <*key-set-name*>	创建局部预共享密钥集
2	inspur(config-isakmp-key-set)#**pre-shared key** {**ipv4-address** <*peer-ipv4-address*> **netmask** <*peer-ipv4-netmask*>[**vrf-name** <*ipv4-vrf-name*>]|**fqdn** <*hostname*>[**vrf-name** <*fqdn-vrf-name*>]}	进入局部预共享密钥
3	inspur(config-isakmp-key-set-pre-shared-key)#**key** <*key*>	配置局部预共享密钥
4	inspur(config)#**isakmp profile** <*isakmp-profile-tag*>	创建局部ISAKMP描述
5	inspur(config-isakmp-profile)#**exchange-mode** {**main** | **aggressive**}{**ipv4-address** <*peer-ipv4-address*> **netmask** <*peer-ipv4-netmask*>[**vrf-name** <*ipv4-vrf-name*>]	配置局部协商的交换类型
6	inspur(config-isakmp-profile)#**keepalive** <*dpd-interval*> **retry** <*dpd-pkt-interval*>	配置局部DPD功能
7	inspur(config-isakmp-profile)#**key-set** <*key-set-name*>	描述中绑定预共享密钥集
8	inspur(config-isakmp-profile)#**default-key** <*key*>	配置ISAKMP profile的默认预共享密钥，协商过程中，优先匹配描述中**key-set**下的密钥，**default-key**作为最后的匹配方式
9	inspur(config-isakmp-profile)#**match identity** {**ipv4-address** <*peer-ipv4-address*>|**fqdn** <*hostname*>}	匹配对端协商信息
10	inspur(config-isakmp-profile)#**match any-identity enable**	配置ISAKMP profile允许所有的对方ID身份
11	inspur(config-isakmp-profile)#**nat-transparency udp-encapsulatio**	配置局部NAT穿越功能
12	inspur(config-isakmp-profile)#**nat-transparency keepalive** <*keepalive-time*>	局部NAT穿越情况下NAT设备保活时间信息
13	inspur(config-isakmp-profile)#**policy** <*policy-priority*>	描述中绑定IKE1协商策略

步骤	命令	功能
14	inspur(config-isakmp-profile)#**self-identity** {**address** | **hostname**}	配置本端标识局部协商方式
15	inspur(config-isakmp-profile)#**initiator** {**ikev1**| **ikev2**}	配置协商发起方采用的版本，默认为**ikev1**
16	inspur(config-isakmp-profile)#**ikev2-authentication** {**pre-share**|**rsa-sig**}	IKEv2协商时采用的认证方式，分为预共享认证方式和RSA签名认证方式，默认为预共享密钥认证方式

7.6.3 配置 IKE 阶段 2

本节介绍IKE阶段2的配置步骤和命令。

1.配置全局commit位。

命令	功能
inspur(config)#**crypto ipsec commit**	配置全局commit位

2.配置转码集。

步骤	命令	功能
1	inspur(config)#**crypto ipsec transform-set** <*transform-set-tag*>	创建用于IPSec保护的转码集
2	inspur(config-crypto-trans)#**algorithm** {[{**ah-md5-hmac**|**ah-sha-hmac**}][{**esp-md5-hmac**|**esp-sha-hmac**}]	配置转码集的转码
3	inspur(config-crypto-trans)#**encapsulation-mode** {**transport**|**tunnel**}	在转码集存在的情况下，设置转码集的封装模式

3.配置静态描述。

步骤	命令	功能
1	inspur(config)#**crypto ipsec static-profile** <*crypto-profile-tag*>	创建IPSec静态描述
2	inspur(config-ipsec-static-profile)#**match acl** <*access-list-name*> **v4**	配置描述指定访问列表
3	inspur(config-ipsec-static-profile)#**set transform-set**	配置描述指定转码集

步骤	命令	功能
	<*proposal-tag*>[<*proposal-tag*>|[<*proposal-tag*>|[<*proposal-tag*>|[<*proposal-tag*>]]]]	
4	inspur(config-ipsec-static-profile)#**set anti-replay** {**disable**|**enable**|**window-size** <*set-replay-window-size*>|**max-sequence** <*set-repaly-maximum-sequence*>}	配置描述指定抗重放策略
5	inspur(config-ipsec-static-profile)#**set pfs** {**group1**|**group2**|**group5**}	配置描述指定PFS群
6	inspur(config-ipsec-static-profile)#**set pfslevel** {**key-identity**}	配置描述指定PFS保护类型
7	inspur(config-ipsec-static-profile)#**set sa lifetime** {**kilobytes** <*lifetime-in-kilobytes*>|**seconds** <*lifetime-in-seconds*>}	配置描述指定生命周期
8	inspur(config-ipsec-static-profile)#**responder-only**	指定IPSec隧道接口被动响应对方协商

4.配置手工描述。

步骤	命令	功能
1	inspur(config)#**crypto ipsec manual-profile** <*crypto-profile-tag*>	创建IPSec手工描述
2	inspur(config-ipsec-manual-profile)#**set transform-set** <*proposal-tag*>	配置手工描述转码集
3	inspur(config-ipsec-manual-profile)#**set session-key inbound** {**ah** <*ah-spi*>{**string** <*ah-key-string*>|**hex** <*ah-key-hex*>}|**esp** <*esp-spi*>{[**authenticator** {**string** <*esp-authentication-key-string*>|**hex** <*esp-authentication-key-hex*>}],[**cipher** {**string** <*esp-cipher-key-string*>|**hex** <*esp-cipher-key-hex*>}]}}	为手工类型的profile设置入向SPI和密钥
4	inspur(config-ipsec-manual-profile)#**set session-key outbound** {**ah** <*ah-spi*>{**string** <*ah-key-string*>|**hex** <*ah-key-hex*>}|**esp** <*esp-spi*>{[**authenticator** {**string** <*esp-authentication-key-string*>|**hex** <*esp-authentication-key-hex*>}],[**cipher** {**string** <*esp-cipher-key-string*>|**hex** <*esp-cipher-key-hex*>}]}}	为手工类型的profile设置出向SPI和密钥

5.配置动态描述。

步骤	命令	功能
1	inspur(config)#**crypto ipsec dynamic-profile** <*crypto-profile-tag*>	创建IPSec动态描述
2	inspur(config-ipsec-dynamic-profile)#**set transform-set** <*proposal-tag*>	配置动态描述转码集

提示：

采用IKEv2版本自协商时只能使用局部ISAKMP描述进行协商。

7.6.4 配置隧道和传输模式

本节介绍配置隧道和传输模式的步骤和命令。

1.配置隧道模式。

步骤	命令	功能
1	inspur(config)#**ipsec-config**	进入IPSec隧道配置模式
2	inspur(config-ipsec)#**interface ipsec_tunnel**<*tunnel-id*>	进入IPSec隧道接口配置模式
3	inspur(config-ipsec-if-ipsec_tunnelid)#**tunnel mode ipv4**	指明IPSec隧道接口模式
4	inspur(config-ipsec-if-ipsec_tunnelid)#**tunnel local ipv4-address** <*local-ipv4-address*>| **tunnel local interface** <*interface-name*>	指明IPSec隧道接口的本地地址
5	inspur(config-ipsec-if-ipsec_tunnelid)#**tunnel remote ipv4-address** <*remote-ipv4-address*>	指明IPSec隧道接口的对端地址
6	inspur(config-ipsec-if-ipsec_tunnelid)#**tunnel vrf** <*vrf-name*>	为IPSec隧道接口配置外层VRF信息
7	inspur(config-ipsec-if-ipsec_tunnelid)#**ipsec-profile** <*profile-name*>	为IPSec隧道接口配置IPSecprofile
8	inspur(config-ipsec-if-ipsec_tunnelid)#**isakmp-profile** <*isakmp-profile-tag*>	（可选）使用局部ISAKMP描述协商
9	inspur(config-ipsec-if-ipsec_tunnelid)#**pre-fragmentation** {**enable**|**disable**}	开启或关闭预分片功能
10	inspur(config-ipsec-if-ipsec_tunnelid)#**df-bit inner** {**ignore**|**aware**}	配置根据原始IP报文的DF位进行处理的方式
11	inspur(config-ipsec-if-ipsec_tunnelid)#**df-bit outer** {**clear**|**copy**|**set**}	对IPSec隧道IP头的DF位进行设置

步骤	命令	功能
12	inspur(config-ipsec-if-ipsec_tunnelid)#**peer identity** {**(ipv4-address A.B.C.D)** | **(ipv6-address X:X::X:X)**|**(fqdn WORD)**}	配置IKEv2协商中发起方协商使用的对端ID，IKEv2协商必须配置
13	inspur(config-ipsec-if-ipsec_tunnelid)#**auth-pki-profile** <*pki-profile-name*>	采用证书认证时，绑定pki-profile
14	inspur(config-ipsec-if-ipsec_tunnelid)#**crypto-pki-profile** <*pki-profile-name*>	采用证书加解密时，绑定pki-profile

2.配置传输模式。

步骤	命令	功能
1	inspur(config)#**crypto ipsec-transport** <*index*>	创建传输模式
2	inspur(config-ipsec-transportindex)#**local ipv4-address** <*local-ipv4-address*>| **tunnel local interface** <*interface-name*>	指明IPSec传输模式的本地地址
3	inspur(config-ipsec-transportindex)#**remote ipv4-address** <*remote-ipv4-address*>	指明IPSec传输模式的目的地址
4	inspur(config-ipsec-transportindex)#**ipsec-profile** <*profile-name*>	为IPSec传输模式配置IPSec profile
5	inspur(config-ipsec-transportindex)#**bound-to** <*interface-name*>	为传输模式绑定出接口
6	inspur(config-ipsec-transportindex)#**vrf** <*vrf-name*>	为IPSec传输模式配置外层VRF信息
7	inspur(config-ipsec-transportindex)#**peer identity** {**(ipv4-address A.B.C.D)** |**(ipv6-address X:X::X:X)** |**(fqdn WORD)**}	配置IKEv2协商中发起方协商使用的对端id，IKEv2协商必须配置
8	inspur(config-ipsec-transportindex)#**auth-pki-profile** <*pki-profile-name*>	采用证书认证时，绑定pki-profile
9	inspur(config-ipsec-transportindex)#**crypto-pki-profile** <*pki-profile-name*>	采用证书加解密时，绑定pki-profile

7.6.5 验证和维护 IPSec

显示ISAKMP信息

命令	功能

命令	功能
inspur#**show isakmp exchange-mode**	显示IKE协商的交换模式设置
inspur#**show isakmp identity**	显示IKE协商的身份类型
inspur#**show isakmp key** {**ip**|**fqdn**}	显示IKE协商的预共享密钥设置
inspur#**show isakmp phase1**	显示野蛮模式加密标记信息
inspur#**show isakmp policy**	显示已配置的IKE协商策略
inspur#**show isakmp policy-of-peer**	显示已经配置的policy-of-peer
inspur#**show isakmp sa** [{**peer** <*peer-ipv4-address*>}|[**vrf-name** <*ipv4-vrf-name*>]]	显示ISAKMP SA
inspur#**show running-config isakmp** |**all**	显示所有ISAKMP相关设置

查看ISAKMP调试信息

命令	功能
inspur#**debug isakmp all**	打开IKE协商的所有调试开关
inspur#**debug isakmp error** [{**peer** <*ipv4-destination-address*>}[{[**local** <*ipv4-local-address*>],[**vrf-name** <*vrf-name*>]}]]	打开IKE协商的错误打印开关
inspur#**debug isakmp event** [{**peer** <*ipv4-destination-address*>}[{[**local** <*ipv4-local-address*>],[**vrf-name** <*vrf-name*>]}]]	打开IKE协商的事件打印开关
inspur#**debug isakmp packet** [{**peer** <*ipv4-destination-address*>}[{[**local** <*ipv4-local-address*>],[**vrf-name** <*vrf-name*>]}]]	打开IKE协商的报文打印开关
inspur#**debug isakmp schedule** [{**peer** <*ipv4-destination-address*>}[{[**local** <*ipv4-local-address*>],[**vrf-name** <*vrf-name*>]}]]	打开IKE协商的调度打印开关
inspur#**debug isakmp state** [{**peer** <*ipv4-destination-address*>}[{[**local** <*ipv4-local-address*>],[**vrf-name** <*vrf-name*>]}]]	打开IKE协商的状态打印开关

删除ISAKMP相关命令

命令	功能
inspur#**clear isakmp policy**	删除配置的所有IKE协商策略和policy-of-peer
inspur#**clear isakmp sa** [**peer**	删除指定激活的ISAKMP SA

命令	功能
{<*peer-ipv4-address*>[<*ipv4-vrf-name*>]}]	

显示IPSec负荷分担信息

命令	功能
inspur#**show crypto ipsec load-balance**	显示所有已配置的IPSec隧道和传输符合分担
inspur#**show crypto ipsec load-balance interface** <*interface-name*>	按照隧道接口显示负荷分担信息
inspur#**show crypto ipsec load-balance ipsec-transport** <*transport-number*>	按照隧道接口显示负荷分担信息
inspur#**show crypto ipsec load-balance timer**	显示负荷分担定时器信息
inspur#**show crypto ipsec client**	显示远程登录用户信息

显示IPSec其它信息

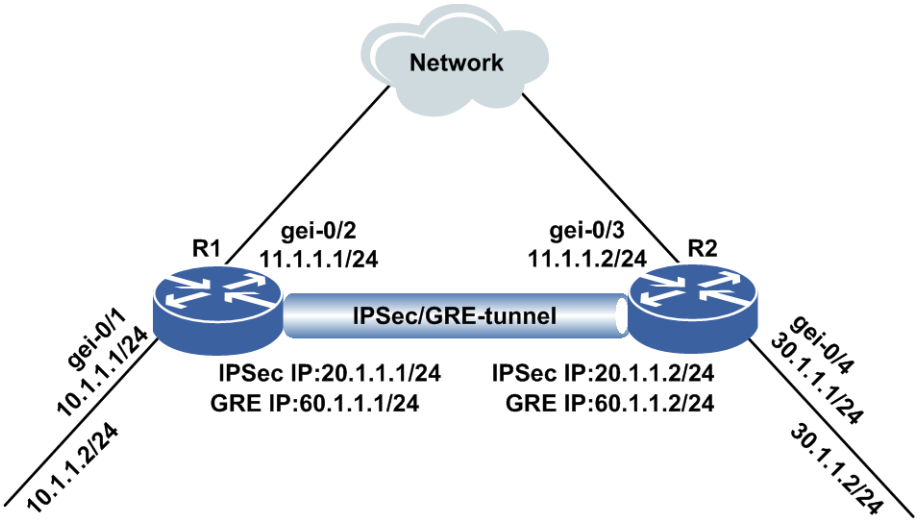
命令	功能
inspur#**show crypto ipsec profile** [<*profile-tag*>]	显示所有或特定的profile信息
inspur#**show crypto ipsec sa** {**manual**|**nego**}[**interface** <*interface-name*>| **ipsec-transport** <*transport-number*>]	显示IPSec SA
inspur#**show crypto ipsec transform-set** [<*transform-set-tag*>]	显示所有的或者特定的已配置转码集
inspur#**show running-config ipsec** |**all**	显示所有已配置IPSec命令

7.6.6 IPSec 基本组网配置实例

配置说明

要在如*图 7-44*所示的网络中配置IPSec功能。本节给出了基于*图 3-109*的接口地址、隧道地址的配置过程。

图 7-44 IPSec 基本组网图



配置过程

设备R1上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ip address 10.1.1.1/24
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit

inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip address 11.1.1.1/24
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit

inspur(config)#interface ipsec_tunnel1
inspur(config-if-ipsec_tunnel1)#ip address 20.1.1.1/24
inspur(config-if-ipsec_tunnel1)#exit

inspur(config)#interface gre_tunnel1
inspur(config-if-gre_tunnel1)#ip address 60.1.1.1/24
inspur(config-if-gre_tunnel1)#exit
```

设备R2上的配置如下：

```
inspur(config)#interface gei-0/3
inspur(config-if-gei-0/3)#ip address 11.1.1.2/24
inspur(config-if-gei-0/3)#no shutdown
inspur(config-if-gei-0/3)#exit

inspur(config)#interface gei-0/4
inspur(config-if-gei-0/4)#ip address 30.1.1.1/24
inspur(config-if-gei-0/4)#no shutdown
inspur(config-if-gei-0/4)#exit

inspur(config)#interface ipsec_tunnel1
inspur(config-if-ipsec_tunnel1)#ip address 20.1.1.2/24
inspur(config-if-ipsec_tunnel1)#exit

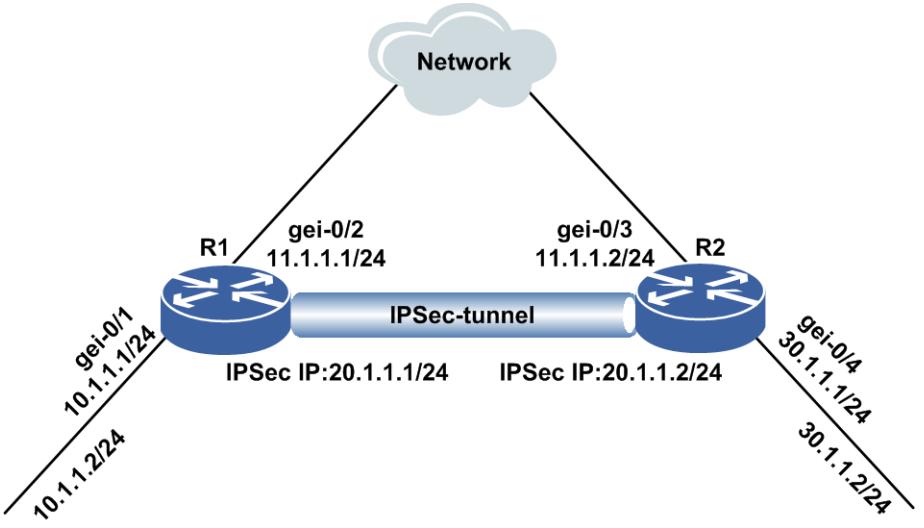
inspur(config)#interface gre_tunnel1
inspur(config-if-gre_tunnel1)#ip address 60.1.1.2/24
inspur(config-if-gre_tunnel1)#exit
```

7.6.7 IPSec 手工 SPI 站点到站点 VPN 配置实例

配置说明

手工配置SPI方式要求对等体双方都具有固定公网IP。该方式配置简单，但是可扩展性较差。在如*图 7-45*所示的网络中，配置IPSec手工SPI站点到站点VPN。

图 7-45 IPSec 手工 SPI 站点到站点 VPN 组网图



配置过程

接口地址的相关配置参见IPSec基本组网配置实例。

设备R1上的配置如下：

1.配置感兴趣流

```
inspur(config)#ipv4-access-list 1
inspur(config-ipv4-acl)#rule 1 permit ip 10.1.1.2 0.0.0.0 30.1.1.2 0.0.0.0
inspur(config-ipv4-acl)#exit
```

2.配置IPSec转码集

```
inspur(config)#crypto ipsec transform-set 1
inspur(config-crypto-trans)#algorithm ah-md5-hmac
inspur(config-crypto-trans)#exit
```

3.配置手工profile

```
inspur(config)#crypto ipsec manual-profile 1
inspur(config-ipsec-manual-profile)#set transform-set 1
inspur(config-ipsec-manual-profile)#match acl 1 v4
inspur(config-ipsec-manual-profile)#set session-key inbound ah 1000
string 1234567812345678
inspur(config-ipsec-manual-profile)# set session-key outbound ah 1001
string 8765432187654321
```

4.配置IPSec隧道模式

```
inspur(config)#ipsec-config
inspur(config-ipsec)#interface ipsec_tunnel1
```

```
inspur(config-ipsec-if-ipsec_tunnel1)#type manual
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel local ipv4-address 11.1.1.1
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel remote ipv4-address 11.1.1.2
inspur(config-ipsec-if-ipsec_tunnel1)#ipsec-profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#exit
inspur(config-ipsec)#exit
```

5.配置静态路由

```
inspur(config)#ip route 30.1.1.2 255.255.255.255 ipsec_tunnel1
```

设备R2上的配置如下：

1.配置感兴趣流

```
inspur(config)#ipv4-access-list 1
inspur(config-ipv4-acl)#rule 1 permit ip 30.1.1.2 0.0.0.0 10.1.1.2 0.0.0.0
inspur(config-ipv4-acl)#exit
```

2.配置IPSec转码集

```
inspur(config)#crypto ipsec transform-set 1
inspur(config-crypto-trans)#algorithm ah-md5-hmac
inspur(config-crypto-trans)#exit
```

3.配置手工profile

```
inspur(config)#crypto ipsec manual-profile 1
inspur(config-ipsec-static-profile)#set transform-set 1
inspur(config-ipsec-static-profile)#match acl 1 v4
inspur(config-ipsec-manual-profile)#set session-key outbound ah 1000
string 1234567812345678
inspur(config-ipsec-manual-profile)# set session-key inbound ah 1001
string 8765432187654321
```

4.配置IPSec隧道模式

```
inspur(config)#ipsec-config
inspur(config-ipsec)#interface ipsec_tunnel1
inspur(config-ipsec-if-ipsec_tunnel1)#type manual
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel local ipv4-address 11.1.1.2
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel remote ipv4-address 11.1.1.1
inspur(config-ipsec-if-ipsec_tunnel1)#ipsec-profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#exit
inspur(config-ipsec)#exit
```

5.配置静态路由

```
inspur(config)#ip route 10.1.1.2 255.255.255.255 ipsec_tunnel1
```

配置验证

通过**show crypto ipsec sa manual**命令查看手工隧道模式IPSec SA。

```
inspur(config)#show crypto ipsec sa manual
Interface: ipsec_tunnel1
 IKE version             : N/A
IPsec profile tag:1
 Local endpt:11.1.1.1      Current remote endpt: 11.1.1.2
 Access-list tag          : 1
 IPsec MTU               : 1448
 FVRF                    : not configure
 IVRF                    : not configure
 Pre-fragmentation        : enable
 Original IP header DF-bit : aware
 Tunnel IP header DF-bit   : clear
```

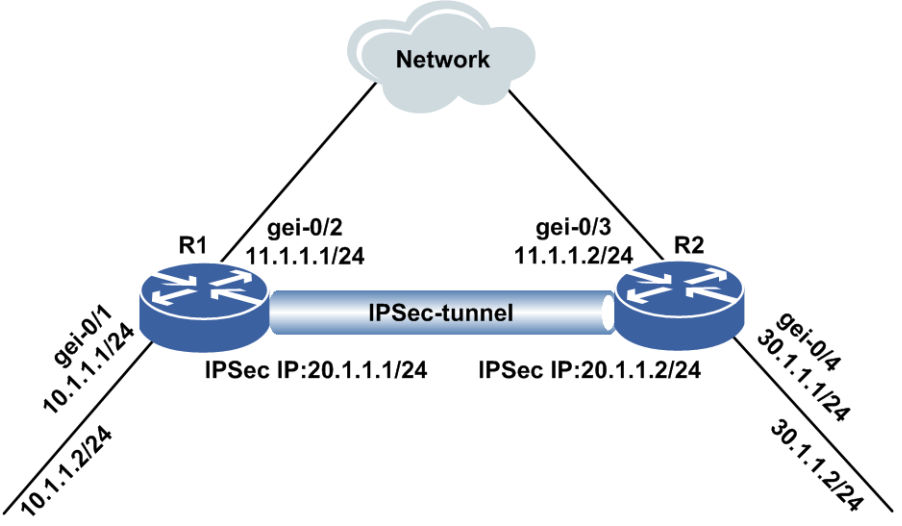
```
SA type                 : manual
Inbound ESP SA:
Inbound AH SA:
 SPI                    : 0x3e8
 Authentication algorithm : hmac-md5
 Encapsulation mode      : tunnel
 Throughput              : 0KB
Outbound ESP SA:
Outbound AH SA:
 SPI                    : 0x3e9
 Authentication algorithm : hmac-md5
 Encapsulation mode      : tunnel
 Throughput              : 0KB
```

7.6.8 IPSec IKE 协商站点到站点 VPN 配置实例

配置说明

使用IKEv1协商建立站点到站点IPSec VPN的可扩展性较强，该案例假设IPSec VPN对等体均具有固定公网IP。在如*图 7-46*所示的网络中配置IPSec IKE协商站点到站点VPN。

图 7-46 IPSec IKE 协商站点到站点 VPN 组网图



配置过程

接口地址的相关配置参见IPSec基本组网配置实例。

设备R1上的配置如下：

1.配置感兴趣流

```
inspur(config)#ipv4-access-list 1
inspur(config-ipv4-acl)#rule 1 permit ip 10.1.1.2 0.0.0.0 30.1.1.2 0.0.0.0
inspur(config-ipv4-acl)#exit
```

2.配置ISAKMP协商策略

```
inspur(config)#isakmp enable
```

```
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#authentication pre-share
inspur(config-isakmp-1)#encryption aes-128
inspur(config-isakmp-1)#group 2
inspur(config-isakmp-1)#hash md5
inspur(config-isakmp-1)#exit
```

3.配置ISAKMP KEY和交换类型

```
inspur(config)#isakmp pre-shared key ipv4-address 11.1.1.2 netmask
255.255.255.255
inspur(config-isakmp-pre-shared-key)#key ttt
inspur(config-isakmp-pre-shared-key)#exit
inspur(config)#isakmp exchange-mode main ipv4-address 11.1.1.2
netmask 255.255.255.255
```

4.配置IPSec转码集

```
inspur(config)#crypto ipsec transform-set 1
inspur(config-crypto-trans)#algorithm ah-md5-hmac
inspur(config-crypto-trans)#exit
```

5.配置静态profile

```
inspur(config)#crypto ipsec static-profile 1
inspur(config-ipsec-static-profile)#set transform-set 1
inspur(config-ipsec-static-profile)#match acl 1 v4
inspur(config-ipsec-static-profile)#exit
```

6.配置IPSec隧道模式

```
inspur(config)#ipsec-config
inspur(config-ipsec)#interface ipsec_tunnel1
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel local ipv4-address 11.1.1.1
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel remote ipv4-address 11.1.1.2
inspur(config-ipsec-if-ipsec_tunnel1)#ipsec-profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#exit
inspur(config-ipsec)#exit
```

7.配置静态路由

```
inspur(config)#ip route 30.1.1.2 255.255.255.255 ipsec_tunnel1
```

设备R2上的配置如下：

1.配置感兴趣流

```
inspur(config)#ipv4-access-list 1
inspur(config-ipv4-acl)#rule 1 permit ip 30.1.1.2 0.0.0.0 10.1.1.2 0.0.0.0
inspur(config-ipv4-acl)#exit
```

2.配置ISAKMP协商策略

```
inspur(config)#isakmp enable
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#authentication pre-share
inspur(config-isakmp-1)#encryption aes-128
inspur(config-isakmp-1)#group 2
inspur(config-isakmp-1)#hash md5
inspur(config-isakmp-1)#exit
```

3.配置ISAKMP KEY和交换类型

```
inspur(config)#isakmp pre-shared key ipv4-address 11.1.1.1 netmask
255.255.255.255
inspur(config-isakmp-pre-shared-key)#key ttt
inspur(config-isakmp-pre-shared-key)#exit
inspur(config)#isakmp exchange-mode main ipv4-address 11.1.1.1
netmask 255.255.255.255
```

4.配置IPSec转码集

```
inspur(config)#crypto ipsec transform-set 1
inspur(config-crypto-trans)#algorithm ah-md5-hmac
inspur(config-crypto-trans)#exit
```

5.配置静态profile

```
inspur(config)#crypto ipsec static-profile 1
inspur(config-ipsec-static-profile)#set transform-set 1
inspur(config-ipsec-static-profile)#match acl 1 v4
inspur(config-ipsec-static-profile)#exit
```

6.配置IPSec隧道模式

```
inspur(config)#ipsec-config
inspur(config-ipsec)#interface ipsec_tunnel1
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel local ipv4-address 11.1.1.2
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel remote ipv4-address 11.1.1.1
inspur(config-ipsec-if-ipsec_tunnel1)#ipsec-profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#exit
inspur(config-ipsec)#exit
```

7.配置静态路由

```
inspur(config)#ip route 10.1.1.2 255.255.255.255 ipsec_tunnel1
```

配置验证

隧道两端协商成功后，通过**show isakmp sa**查看IKE SA协商结果。

```
inspur#show isakmp sa
Codes: D - Dead Peer Detection
       N - NAT-Traversal
C-id Local         Port Remote        Port VRF     Ver Status Lifetime Cap
1    11.1.1.1      500  11.1.1.2      500          v1  active 86400
```

通过**show crypto ipsec sa nego**查看IPSec SA协商结果。

```
inspur#show isakmp sa peer 11.1.1.2
C-id:1
    Local:11.1.1.1          Port:500
    Peer :11.1.1.2          Port:500
    VRF:not config
    Ver:v1
    Side:INITIATOR
    Enc:AES-128     Hash:MD5    Group:2  Mode:MAIN      Auth:PSKEY
    Cki:c29199bc96db7839    Ckr:4ce7d15b7701f170    RemainTime:86144  Cap:
```

通过**show crypto ipsec sa nego**查看IPSec SA协商。

```
inspur#show crypto ipsec sa nego
Interface: ipsec_tunnel1
 IKE version             : v1
IPsec profile tag:1
 Local endpt:11.1.1.1      Current remote endpt: 11.1.1.2
 Local  ident(addr/mask/prot/port_min/port_max) :
  (10.1.1.2/255.255.255.255/0/Invalid/Invalid)
 Remote ident(addr/mask/prot/port_min/port_max) :
  (30.1.1.2/255.255.255.255/0/Invalid/Invalid)
 IPsec MTU               : 1448
 FVRF                    : not configure
 IVRF                    : not configure
 Pre-fragmentation         : enable
 Original IP header DF-bit : aware
 Tunnel IP header DF-bit   : clear
 SA type                 : negotiation
```

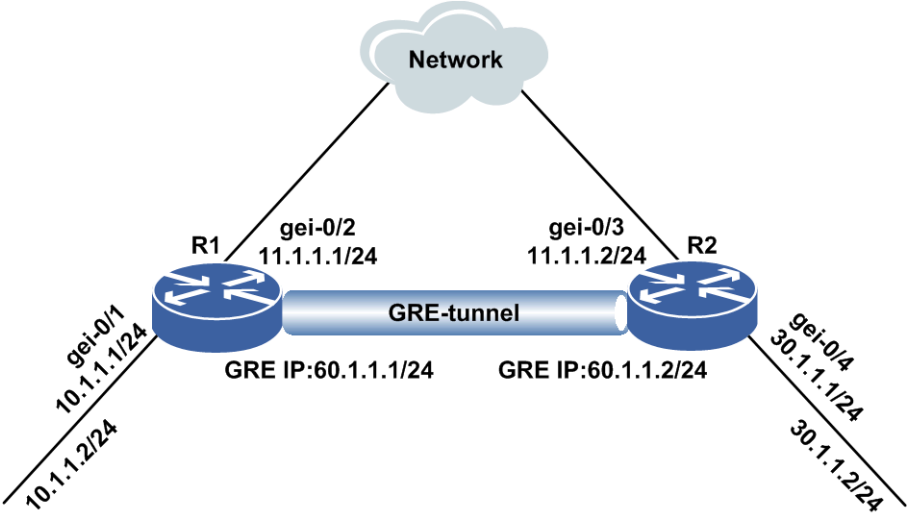
```
Inbound ESP SA:
Inbound AH SA:
 SPI                    : 0x100004a
 Authentication algorithm : hmac-md5
 Encapsulation mode       : tunnel
 Throughput             : 0KB
Outbound ESP SA:
Outbound AH SA:
 SPI                    : 0x1000065
 Authentication algorithm : hmac-md5
 Encapsulation mode       : tunnel
 Throughput             : 0KB
```

7.6.9 GRE OVER IPSec VPN 配置实例

配置说明

该方案将GRE隧道技术与IPSec加密技术相结合，可以解决普通的IPSec隧道不支持组播的问题。当需要利用VPN进行组播通信时，可以采用该方式进行配置，此处IPSec使用传输模式。在如*图 7-47*所示的网络中配置GRE OVER IPSec VPN。

图 7-47 GRE OVER IPSec VPN 组网图



配置过程

接口地址的相关配置参见IPSec基本组网配置实例。

设备R1上的配置如下：

1.配置感兴趣流

```
inspur(config)#ipv4-access-list 1
inspur(config-ipv4-acl)#rule 1 permit ip 11.1.1.1 0.0.0.0 11.1.1.2 0.0.0.0
inspur(config-ipv4-acl)#exit
```

2.配置ISAKMP协商策略

```
inspur(config)#isakmp enable
inspur(config)#isakmp policy 1
```

```
inspur(config-isakmp-1)#authentication pre-share
inspur(config-isakmp-1)#encryption aes-128
inspur(config-isakmp-1)#group 2
inspur(config-isakmp-1)#hash md5
inspur(config-isakmp-1)#exit
```

3.配置ISAKMP KEY和交换类型

```
inspur(config)#isakmp pre-shared key ipv4-address 11.1.1.2 netmask
255.255.255.255
inspur(config-isakmp-pre-shared-key)#key ttt
inspur(config-isakmp-pre-shared-key)#exit
inspur(config)#isakmp exchange-mode main ipv4-address 11.1.1.2
netmask 255.255.255.255
```

4.配置IPSec转码集

```
inspur(config)#crypto ipsec transform-set 1
inspur(config-crypto-trans)#algorithm ah-md5-hmac
inspur(config-crypto-trans)#encapsulation-mode transport
inspur(config-crypto-trans)#exit
```

5.配置静态profile

```
inspur(config)#crypto ipsec static-profile 1
inspur(config-ipsec-static-profile)#set transform-set 1
inspur(config-ipsec-static-profile)#match acl 1 v4
inspur(config-ipsec-static-profile)#exit
```

6.配置IPSec传输模式

```
inspur(config)#crypto ipsec-transport 1
inspur(config-ipsec-transport1)#local ipv4-address 11.1.1.1
inspur(config-ipsec-transport1)#remote ipv4-address 11.1.1.2
inspur(config-ipsec-transport1)#ipsec-profile 1
inspur(config-ipsec-transport1)#bound-to gei-0/2
```

7.配置GRE隧道模式

```
inspur(config)#gre-config
inspur(config-gre)#interface gre_tunnel1
inspur(config-gre-if-gre_tunnel1)#tunnel mode ip
inspur(config-gre-if-gre_tunnel1)#tunnel source ipv4 11.1.1.1
inspur(config-gre-if-gre_tunnel1)#tunnel destination ipv4 11.1.1.2
```

8.配置静态路由

```
inspur(config)#ip route 0.0.0.0 0.0.0.0 gre_tunnel1
```

设备R2上的配置如下：

1.配置感兴趣流

```
inspur(config)#ipv4-access-list 1
inspur(config-ipv4-acl)#rule 1 permit ip 11.1.1.2 0.0.0.0 11.1.1.1 0.0.0.0
inspur(config-ipv4-acl)#exit
```

2.配置ISAKMP协商策略

```
inspur(config)#isakmp enable
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#authentication pre-share
inspur(config-isakmp-1)#encryption aes-128
inspur(config-isakmp-1)#group 2
inspur(config-isakmp-1)#hash md5
inspur(config-isakmp-1)#exit
```

3.配置ISAKMP KEY和交换类型

```
inspur(config)#isakmp pre-shared key ipv4-address 11.1.1.1 netmask
255.255.255.255
```

```
inspur(config-isakmp-pre-shared-key)#key ttt
inspur(config-isakmp-pre-shared-key)#exit
inspur(config)#isakmp exchange-mode main ipv4-address 11.1.1.1
netmask 255.255.255.255
```

4.配置IPSec转码集

```
inspur(config)#crypto ipsec transform-set 1
inspur(config-crypto-trans)#algorithm ah-md5-hmac
inspur(config-crypto-trans)#encapsulation-mode transport
inspur(config-crypto-trans)#exit
```

5.配置静态profile

```
inspur(config)#crypto ipsec static-profile 1
inspur(config-ipsec-static-profile)#set transform-set 1
inspur(config-ipsec-static-profile)#match acl 1 v4
inspur(config-ipsec-static-profile)#exit
```

6.配置IPSec传输模式

```
inspur(config)#crypto ipsec-transport 1
inspur(config-ipsec-transport1)#local ipv4-address 11.1.1.2
inspur(config-ipsec-transport1)#remote ipv4-address 11.1.1.1
inspur(config-ipsec-transport1)#ipsec-profile 1
inspur(config-ipsec-transport1)#bound-to gei-0/3
```

7.配置GRE隧道模式

```
inspur(config)#gre-config
inspur(config-gre)#interface gre_tunnel1
inspur(config-gre-if-gre_tunnel1)#tunnel mode ip
inspur(config-gre-if-gre_tunnel1)#tunnel source ipv4 11.1.1.2
inspur(config-gre-if-gre_tunnel1)#tunnel destination ipv4 11.1.1.1
```

8.配置静态路由

```
inspur(config)#ip route 0.0.0.0 0.0.0.0 gre_tunnel1
```

配置验证

隧道两端协商成功后，通过**show isakmp sa**查看IKE SA协商结果。

```
inspur#show isakmp sa
Codes: D - Dead Peer Detection
      N - NAT-Traversal
C-id Local         Port Remote        Port VRF     Ver Status Lifetime Cap
1    11.1.1.1      500  11.1.1.2      500          v1  active 86400
```

通过**show crypto ipsec sa nego**查看IPSec SA协商。

```
inspur(config)#show crypto ipsec sa nego
Transport: ipsec_transport1
 IKE version             : v1
IPsec profile tag:1
 Local endpt:11.1.1.1      Current remote endpt: 11.1.1.2
 Local  ident(addr/mask/prot/port_min/port_max) :
  (11.1.1.1/255.255.255.255/0/Invalid/Invalid)
 Remote ident(addr/mask/prot/port_min/port_max) :
  (11.1.1.2/255.255.255.255/0/Invalid/Invalid)
 FVRF                   : not configure
 IVRF                   : not configure
 Pre-fragmentation        : disable
 Original IP header DF-bit : ignore
 SA type                 : negotiation
 Inbound ESP SA:
```

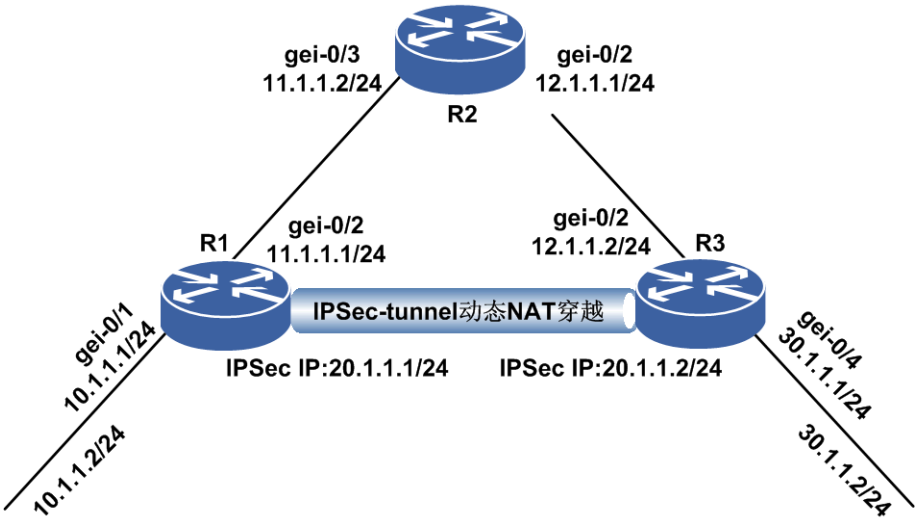
```
Inbound AH SA:
 SPI                    : 0x100004d
 Authentication algorithm : hmac-md5
 Encapsulation mode       : transport
 Throughput             : 0KB
Outbound ESP SA:
Outbound AH SA:
 SPI                    : 0x1000066
 Authentication algorithm : hmac-md5
 Encapsulation mode       : transport
 Throughput             : 0KB
```

7.6.10 IPSec 动态 NAT 穿越配置实例

配置说明

在如*图 7-48*所示的网络中配置IPSec动态NAT穿越，R2为NAT设备。

图 7-48 IPSec 动态 NAT 穿越组网图



配置过程

R1上主动发起端配置如下。

接口配置：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ip address 10.1.1.1/24
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit

inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip address 11.1.1.1/24
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit

inspur(config)#interface ipsec_tunnel1
inspur(config-if-ipsec_tunnel1)#ip address 20.1.1.1/24
inspur(config-if-ipsec_tunnel1)#exit
```

IPSec配置：

1.配置感兴趣流

```
inspur(config)#ipv4-access-list 1
inspur(config-ipv4-acl)#rule 1 permit ip 10.1.1.2 0.0.0.0 30.1.1.2 0.0.0.0
inspur(config-ipv4-acl)#exit
```

2.配置ISAKMP协商策略

```
inspur(config)#isakmp enable
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#authentication pre-share
inspur(config-isakmp-1)#encryption aes-128
inspur(config-isakmp-1)#group 2
inspur(config-isakmp-1)#hash md5
inspur(config-isakmp-1)#exit
```

3.配置ISAKMP描述

```
inspur(config)#isakmp key-set 1
inspur(config-isakmp-key-set)#pre-shared key fqdn inspur
inspur(config-isakmp-key-set-pre-shared-key)#key ipsec
inspur(config-isakmp-key-set-pre-shared-key)#!

inspur(config)#isakmp profile 1
inspur(config-isakmp-profile)#exchange-mode aggressive
inspur(config-isakmp-profile)#key-set 1
inspur(config-isakmp-profile)#match identity fqdn inspur
inspur(config-isakmp-profile)#nat-transparency udp-encapsulation
inspur(config-isakmp-profile)#policy 1
inspur(config-isakmp-profile)#self-identity hostname
```

4.配置IPSec转码集

```
inspur(config)#crypto ipsec transform-set 1
inspur(config-crypto-trans)#algorithm esp-md5-hmac esp-des
inspur(config-crypto-trans)#exit
```

5.配置静态profile

```
inspur(config)#crypto ipsec static-profile 1
inspur(config-ipsec-static-profile)#set transform-set 1
inspur(config-ipsec-static-profile)#match acl 1 v4
inspur(config-ipsec-static-profile)#exit
```

6.配置IPSec隧道模式

```
inspur(config)#ipsec-config
inspur(config-ipsec)#interface ipsec_tunnel1
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel local interface gei-0/2
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel remote ipv4-address 12.1.1.2
inspur(config-ipsec-if-ipsec_tunnel1)#ipsec-profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#isakmp-profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#exit
inspur(config-ipsec)#exit
```

7.配置静态路由

```
inspur(config)#ip route 30.1.1.2 255.255.255.255 ipsec_tunnel1
```

R2作为NAT设备配置如下。

接口配置：

```
inspur(config)#interface gei-0/3
inspur(config-if-gei-0/1)#ip address 11.1.1.2/24
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
```

```
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip address 12.1.1.1/24
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit
```

NAT配置：

```
inspur(config)#cgn
inspur(config-cgn)#cgn-pool n1 poolid 1 mode nat
inspur(config-cgn-natpool)#section 1 12.1.1.3
inspur(config-cgn-natpool)#exit

inspur(config-cgn)#domain 1 1 type sr ipv4-issued
inspur(config-cgn-domain)#dynamic source rule-id 1 ipv4-list patacl1 permit
pool n1
inspur(config-cgn-domain)#exit

inspur(config-cgn)#subscriber ipv4 public subscriber-id 1 nat-domain 1
inspur(config-cgn-sub)#interface gei-0/3
inspur(config-cgn-sub)#!

inspur(config)#ipv4-access-list patacl1
inspur(config-ipv4-acl)#rule 10 permit 11.1.1.1 0.0.0.0
```

R3被动端配置如下。

接口配置：

```
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/3)#ip address 12.1.1.2/24
inspur(config-if-gei-0/3)#no shutdown
inspur(config-if-gei-0/3)#exit

inspur(config)#interface gei-0/4
inspur(config-if-gei-0/4)#ip address 30.1.1.1/24
inspur(config-if-gei-0/4)#no shutdown
inspur(config-if-gei-0/4)#exit

inspur(config)#interface ipsec_tunnel1
inspur(config-if-ipsec_tunnel1)#ip address 20.1.1.2/24
inspur(config-if-ipsec_tunnel1)#exit
```

IPSec配置：

1.配置感兴趣流

动态隧道，不需要配置感兴趣流。

2.配置ISAKMP协商策略

```
inspur(config)#isakmp enable
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#authentication pre-share
inspur(config-isakmp-1)#encryption aes-128
inspur(config-isakmp-1)#group 2
inspur(config-isakmp-1)#hash md5
inspur(config-isakmp-1)#exit
```

3.配置ISAKMP描述

```
inspur(config)#isakmp key-set 1
inspur(config-isakmp-key-set)#pre-shared key fqdn inspur
inspur(config-isakmp-key-set-pre-shared-key)#key ipsec
inspur(config-isakmp-key-set-pre-shared-key)#!

inspur(config)#isakmp profile 1
inspur(config-isakmp-profile)#key-set 1
inspur(config-isakmp-profile)#match identity fqdn inspur
inspur(config-isakmp-profile)#nat-transparency udp-encapsulation
```

```
inspur(config-isakmp-profile)#policy 1
inspur(config-isakmp-profile)#self-identity hostname
```

4.配置IPSec转码集

```
inspur(config)#crypto ipsec transform-set 1
inspur(config-crypto-trans)#algorithm esp-md5-hmac esp-des
inspur(config-crypto-trans)#exit
```

5.配置静态profile

```
inspur(config)#crypto ipsec dynamic-profile 1
inspur(config-ipsec-static-profile)#set transform-set 1
inspur(config-ipsec-static-profile)#exit
```

6.配置IPSec隧道模式

```
inspur(config)#ipsec-config
inspur(config-ipsec)#interface ipsec_tunnel1
inspur(config-ipsec-if-ipsec_tunnel1)#type dynamic
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel local interface gei-0/2
inspur(config-ipsec-if-ipsec_tunnel1)#ipsec-profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#isakmp-profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#exit
inspur(config-ipsec)#exit
```

7.配置静态路由

```
inspur(config)#ip route 10.1.1.2 255.255.255.255 ipsec_tunnel1
```

配置验证

隧道两端协商成功后，通过**show isakmp sa**查看IKE SA协商结果。

```
inspur#show isakmp sa
Codes: D - Dead Peer Detection
       N - NAT-Traversal
C-id Local         Port Remote        Port VRF     Ver Status Lifetime Cap
1    11.1.1.1      4500  12.1.1.3      4500        v1  active 86400    N
```

通过**show crypto ipsec sa nego**查看IPSec SA协商。

```
inspur#show crypto ipsec sa nego
Interface: ipsec_tunnel1
 IKE version             : v1
IPsec profile tag:1
 Local endpt:11.1.1.1      Current remote endpt: 12.1.1.3
 Local  ident(addr/mask/prot/port_min/port_max) :
  (10.1.1.2/255.255.255.255/0/Invalid/Invalid)
 Remote ident(addr/mask/prot/port_min/port_max) :
  (30.1.1.2/255.255.255.255/0/Invalid/Invalid)
 IPsec MTU               : 1448
 FVRF                    : not configure
 IVRF                    : not configure
 Pre-fragmentation         : enable
 Original IP header DF-bit : aware
 Tunnel IP header DF-bit   : clear
 SA type                 : negotiation
 Inbound ESP SA:
 Inbound AH SA:
  SPI                    : 0x100004a
  Authentication algorithm : hmac-md5
  Encapsulation mode       : tunnel
  Throughput               : 0KB
 Outbound ESP SA:
 Outbound AH SA:
```

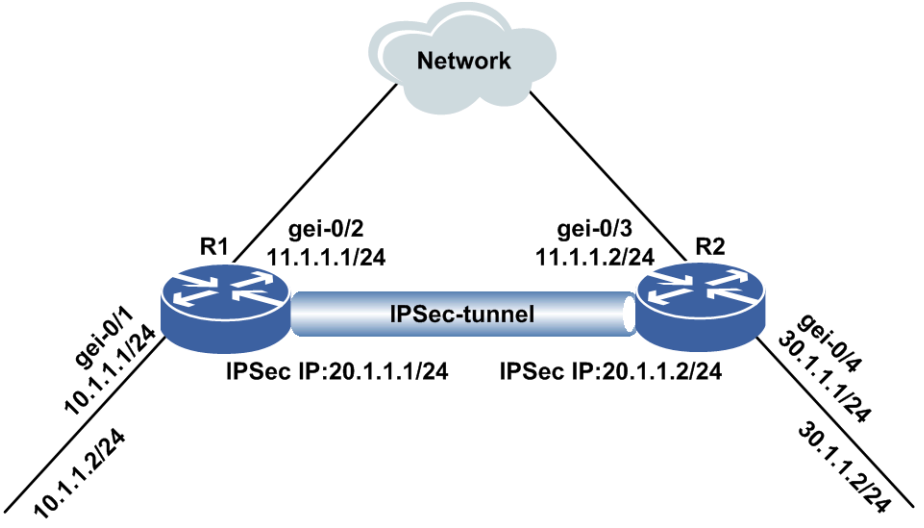
```
SPI                    : 0x1000065
Authentication algorithm : hmac-md5
Encapsulation mode       : tunnel
Throughput             : 0KB
```

7.6.11 IPSec 数字证书认证协商配置实例

配置说明

预共享密钥配置简单，但是扩展性很不好，仅使用于小型VPN网络。本节介绍采用证书方式协商站点到站点的VPN。场景如*图 7-49*所示。

图 7-49 IPSec 证书认证协商



配置过程

接口地址的相关配置参见IPSec基本组网配置实例。

设备R1上的配置如下：

1.离线方式导入证书

```
inspur(config)#pki
inspur(config-pki)#profile test1
inspur(config-pki)#import pkcs12 url disk /datadisk0/cert/test1.p12 test1
inspurR10
```

2.配置感兴趣流

```
inspur(config)#ipv4-access-list 1
inspur(config-ipv4-acl)#rule 1 permit ip 10.1.1.2 0.0.0.0 30.1.1.2 0.0.0.0
inspur(config-ipv4-acl)#exit
```

3.配置ISAKMP协商策略

```
inspur(config)#isakmp enable
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#authentication rsa-sig
```

```
inspur(config-isakmp-1)#encryption aes-128
inspur(config-isakmp-1)#group 2
inspur(config-isakmp-1)#hash md5
inspur(config-isakmp-1)#exit
```

4.配置ISAKMP Profile

```
inspur(config)#isakmp profile 1
inspur(config-isakmp-profile)#match identity ipv4-address 11.1.1.2
inspur(config-isakmp-profile)#policy 1
```

5.配置IPSec转码集

```
inspur(config)#crypto ipsec transform-set 1
inspur(config-crypto-trans)#algorithm ah-md5-hmac
inspur(config-crypto-trans)#exit
```

6.配置静态profile

```
inspur(config)#crypto ipsec static-profile 1
inspur(config-ipsec-static-profile)#set transform-set 1
inspur(config-ipsec-static-profile)#match acl 1 v4
inspur(config-ipsec-static-profile)#exit
```

7.配置IPSec隧道模式

```
inspur(config)#ipsec-config
inspur(config-ipsec)#interface ipsec_tunnel1
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel local ipv4-address 11.1.1.1
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel remote ipv4-address 11.1.1.2
inspur(config-ipsec-if-ipsec_tunnel1)#isakmp profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#ipsec-profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#auth-pki-profile test1
inspur(config-ipsec-if-ipsec_tunnel1)#exit
inspur(config-ipsec)#exit
```

8.配置静态路由

```
inspur(config)#ip route 30.1.1.2 255.255.255.255 ipsec_tunnel1
```

设备R2上的配置如下：

1.离线方式导入证书

```
inspur(config)#pki
inspur(config-pki)#profile test2
inspur(config-pki)#import pkcs12 url disk /datadisk0/cert/test2.p12 test2
```

2.配置感兴趣流

```
inspur(config)#ipv4-access-list 1
inspur(config-ipv4-acl)#rule 1 permit ip 30.1.1.2 0.0.0.0 10.1.1.2 0.0.0.0
inspur(config-ipv4-acl)#exit
```

3.配置ISAKMP协商策略

```
inspur(config)#isakmp enable
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#authentication rsa-sig
inspur(config-isakmp-1)#encryption aes-128
inspur(config-isakmp-1)#group 2
inspur(config-isakmp-1)#hash md5
inspur(config-isakmp-1)#exit
```

4.配置ISAKMP Profile

```
inspur(config)#isakmp profile 1
inspur(config-isakmp-profile)#match identity ipv4-address 11.1.1.1
inspur(config-isakmp-profile)#policy 1
```

5.配置IPSec转码集

```
inspur(config)#crypto ipsec transform-set 1
inspur(config-crypto-trans)#algorithm ah-md5-hmac
inspur(config-crypto-trans)#exit
```

6.配置静态profile

```
inspur(config)#crypto ipsec static-profile 1
inspur(config-ipsec-static-profile)#set transform-set 1
inspur(config-ipsec-static-profile)#match acl 1 v4
inspur(config-ipsec-static-profile)#exit
```

7.配置IPSec隧道模式

```
inspur(config)#ipsec-config
inspur(config-ipsec)#interface ipsec_tunnel1
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel local ipv4-address 11.1.1.2
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel remote ipv4-address 11.1.1.1
inspur(config-ipsec-if-ipsec_tunnel1)#isakmp profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#ipsec-profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#auth-pki-profile test2
inspur(config-ipsec-if-ipsec_tunnel1)#exit
inspur(config-ipsec)#exit
```

8.配置静态路由

```
inspur(config)#ip route 10.1.1.2 255.255.255.255 ipsec_tunnel1
```

配置验证

证书导入后，通过**show pki certificate local carol**查看证书导入情况。

```
inspur#show pki certificate local test1
----------------------------------------
Version: 3 (0x2)
Serial Number: 34:8d:1f:09:05:17:d5:4e
Signature Algorithm: sha1WithRSAEncryption
Issuer:
   C=CH
   O=Linux strongSwan
   CN=strongSwan Root CA
Validity:
   Not Before: Sep  1 08:09:18 2014 GMT
   Not After : Aug 31 08:09:18 2017 GMT
Subject:
   C=CH
   O=strongSwan
   CN=carol@strongswan.org
Subject Public Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key (2048 bit)
X509v3 extensions:
   X509v3 Basic Constraints:
      <EMPTY>
   X509v3 Key Usage:
      <EMPTY>
   X509v3 Subject Key Identifier:
      <EMPTY>
   X509v3 Authority Key Identifier:
      keyid:5D:A7:DD:70:06:51:32:7E:E7:B6:6D:B3:B5:E5:E0:60:EA:2E:4D:EF
```

隧道两端协商成功后，通过**show isakmp sa**查看IKE SA协商结果。

```
inspur#show isakmp sa
Codes: D - Dead Peer Detection
```

```
      N - NAT-Traversal
C-id Local         Port Remote        Port VRF     Ver Status Lifetime Cap
1    11.1.1.1      500  11.1.1.2      500          v1  active 86400
```

通过**show isakmp sa peer**查看ISA SA协商结果。

```
inspur#show isakmp sa peer 11.1.1.1
C-id:1
    Local:11.1.1.2          Port:500
    Peer :11.1.1.1          Port:500
    VRF:not config
    Ver:v1
    Side:RESPONDER
    Enc:AES-128     Hash:MD5    Group:2  Mode:MAIN      Auth:RSA-SIG
    Cki:b1ece20efe30f54b    Ckr:11e7fc838d062647    RemainTime:86323  Cap:
```

通过用**show crypto ipsec sa nego**查看IPSec SA协商。

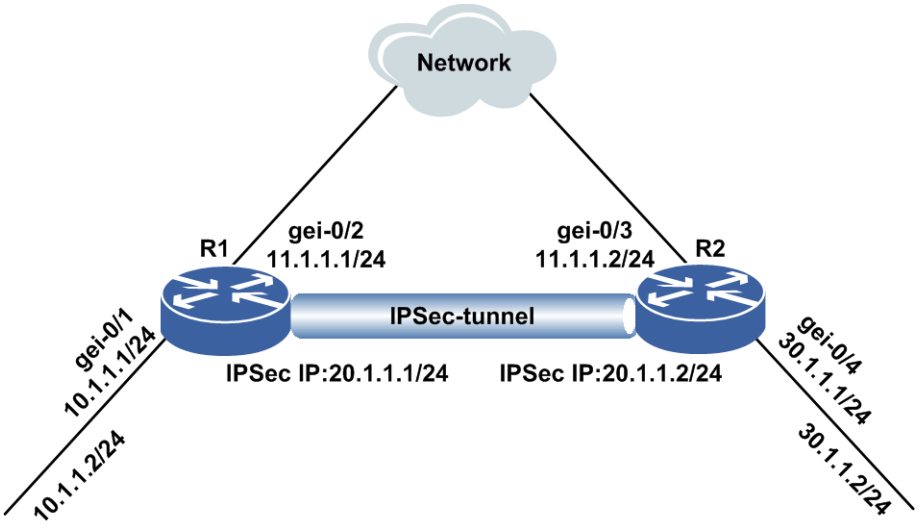
```
inspur#show crypto ipsec sa nego
Interface: ipsec_tunnel3
 IKE version             : v1
IPsec profile tag:ddd1
 Local endpt:11.1.1.2      Current remote endpt: 11.1.1.1
 Local  ident(addr/mask/prot/port_min/port_max) :
  (21.1.1.2/255.255.255.255/0/Invalid/Invalid)
 Remote ident(addr/mask/prot/port_min/port_max) :
  (21.2.1.2/255.255.255.255/0/Invalid/Invalid)
 IPsec MTU               : 1448
 FVRF                    : not configure
 IVRF                    : not configure
 Pre-fragmentation        : enable
 Original IP header DF-bit : aware
 Tunnel IP header DF-bit   : clear
 SA type                 : negotiation
 Inbound ESP SA:
 Inbound AH SA:
  SPI                    : 0x1000244
  Authentication algorithm : hmac-md5
  Encapsulation mode      : tunnel
  Throughput              : 0KB
 Outbound ESP SA:
 Outbound AH SA:
  SPI                    : 0x1000202
  Authentication algorithm : hmac-md5
  Encapsulation mode      : tunnel
  Throughput              : 0KB
```

7.6.12 IKEv2 配置实例

配置说明

在如*图 7-50*所示的网络，本节仅给出IPSec IKEv2静态隧道协商案例。IKEv2配置仅支持局部ISAKMP profile配置方式。

图 7-50 IKEv2 配置实例



配置过程

接口地址的相关配置参见IPSec基本组网配置实例。

设备R1上的配置如下：

1.配置感兴趣流

```
inspur(config)#ipv4-access-list 1
inspur(config-ipv4-acl)#rule 1 permit ip 10.1.1.2 0.0.0.0 30.1.1.2 0.0.0.0
inspur(config-ipv4-acl)#exit
```

2.配置ISAKMP协商策略

```
inspur(config)#isakmp enable
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#authentication pre-share
inspur(config-isakmp-1)#encryption aes-128
inspur(config-isakmp-1)#group 2
inspur(config-isakmp-1)#hash md5
inspur(config-isakmp-1)#prf sha1
inspur(config-isakmp-1)#exit
```

3.配置key-set

```
inspur(config)#isakmp key-set 1
inspur(config-isakmp-key-set)#pre-shared key inspur ipv4-address 11.1.1.2
netmask
255.255.255.255
inspur(config-isakmp-key-set-pre-shared-key)#key inspur
inspur(config-isakmp-key-set-pre-shared-key)#exit
```

4.配置ISAKMP profile

```
inspur(config)#isakmp profile 1
inspur(config-isakmp-profile)#initiator ikev2
inspur(config-isakmp-profile)#match identity ipv4-address 11.1.1.2
inspur(config-isakmp-profile)#policy 1
inspur(config-isakmp-profile)#key-set 1
inspur(config-isakmp-profile)#exit
```

5.配置IPSec转码集

```
inspur(config)#crypto ipsec transform-set 1
```

```
inspur(config-crypto-trans)#algorithm esp-sha-hmac esp-aes-192
inspur(config-crypto-trans)#exit
```

6.配置静态profile

```
inspur(config)#crypto ipsec static-profile 1
inspur(config-ipsec-static-profile)#set transform-set 1
inspur(config-ipsec-static-profile)#match acl 1 v4
inspur(config-ipsec-static-profile)#exit
```

7.配置IPSec隧道模式

```
inspur(config)#ipsec-config
inspur(config-ipsec)#interface ipsec_tunnel1
inspur(config-ipsec-if-ipsec_tunnel1)#peer identity ipv4-address 11.1.1.2
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel local ipv4-address 11.1.1.1
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel remote ipv4-address 11.1.1.2
inspur(config-ipsec-if-ipsec_tunnel1)#isakmp profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#ipsec-profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#exit
inspur(config-ipsec)#exit
```

8.配置静态路由

```
inspur(config)#ip route 30.1.1.2 255.255.255.255 ipsec_tunnel1
```

设备R2上的配置如下：

1.配置感兴趣流

```
inspur(config)#ipv4-access-list 1
inspur(config-ipv4-acl)#rule 1 permit ip 30.1.1.2 0.0.0.0 10.1.1.2 0.0.0.0
inspur(config-ipv4-acl)#exit
```

2.配置ISAKMP协商策略

```
inspur(config)#isakmp enable
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#authentication pre-share
inspur(config-isakmp-1)#encryption aes-128
inspur(config-isakmp-1)#group 2
inspur(config-isakmp-1)#hash md5
inspur(config-isakmp-1)#exit
```

3.配置key-set

```
inspur(config)#isakmp key-set 1
inspur(config-isakmp-key-set)#pre-shared key inspur ipv4-address 11.1.1.1
netmask
255.255.255.255
inspur(config-isakmp-key-set-pre-shared-key)#key inspur
inspur(config-isakmp-key-set-pre-shared-key)#exit
```

4.配置ISAKMP profile

```
inspur(config)#isakmp profile 1
inspur(config-isakmp-profile)#initiator ikev2
inspur(config-isakmp-profile)#match identity ipv4-address 11.1.1.2
inspur(config-isakmp-profile)#policy 1
inspur(config-isakmp-profile)#key-set 1
inspur(config-isakmp-profile)#exit
```

5.配置IPSec转码集

```
inspur(config)#crypto ipsec transform-set 1
inspur(config-crypto-trans)#algorithm esp-sha-hmac esp-aes-192
inspur(config-crypto-trans)#exit
```

6.配置静态profile

```
inspur(config)#crypto ipsec static-profile 1
```

```
inspur(config-ipsec-static-profile)#set transform-set 1
inspur(config-ipsec-static-profile)#match acl 1 v4
inspur(config-ipsec-static-profile)#exit
```

7.配置IPSec隧道模式

```
inspur(config)#ipsec-config
inspur(config-ipsec)#interface ipsec_tunnel1
inspur(config-ipsec-if-ipsec_tunnel1)#peer identity ipv4-address 11.1.1.1
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel local ipv4-address 11.1.1.2
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel remote ipv4-address 11.1.1.1
inspur(config-ipsec-if-ipsec_tunnel1)#isakmp profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#ipsec-profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#exit
inspur(config-ipsec)#exit
```

8.配置静态路由

```
inspur(config)#ip route 10.1.1.2 255.255.255.255 ipsec_tunnel1
```

配置验证

隧道两端协商成功后，通过**show isakmp sa**查看IKE SA协商结果。

```
inspur#show isakmp sa
Codes: D - Dead Peer Detection
       N - NAT-Traversal
C-id Local         Port Remote        Port VRF     Ver Status Lifetime Cap
1    11.1.1.1      500  11.1.1.2      500          v2  active 86400
```

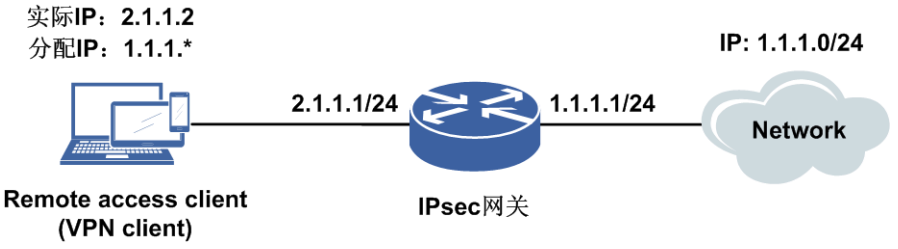
通过**show crypto ipsec sa nego**查看IPSec SA协商。

```
inspur (config)#show crypto ipsec sa nego
Interface: ipsec_tunnel11
 IKE version             : v2
IPsec profile tag:1
 Local endpt:11.1.1.1      Current remote endpt: 11.1.1.2
 Local  ident(addr/mask/prot/port_min/port_max) :
  (10.1.1.2/255.255.255.255/0/Invalid/Invalid)
 Remote ident(addr/mask/prot/port_min/port_max) :
  (30.8.1.2/255.255.255.255/0/Invalid/Invalid)
 IPsec MTU               : 1420
 FVRF                    : not configure
 IVRF                    : not configure
 Pre-fragmentation       : enable
 Original IP header DF-bit : aware
 Tunnel IP header DF-bit   : clear
 SA type                 : negotiation
 Inbound ESP SA:
  SPI                    : 0x1000012
  Authentication algorithm : hmac-sha1
  Encryption algorithm     : aes-192
  Encapsulation mode       : tunnel
  Throughput               : 0KB
 Inbound AH SA:
 Outbound ESP SA:
  SPI                    : 0x10000ed
  Authentication algorithm : hmac-sha1
  Encryption algorithm     : aes-192
  Encapsulation mode       : tunnel
  Throughput               : 0KB
 Outbound AH SA:
```

7.7 IPSec VPN 远程接入

IPSec远程接入的应用场景如*图 7-51*所示。出于安全原因方面的考虑，大部分的系统，网络安全管理员都要配置系统服务器，使得对这些系统的访问权限仅限于有内部网络IP地址的主机。例如：对于通过远程拨号访问组织网络的情况，远程访问服务器可以为远程拨号客户端分配内部网络IP地址。这样尽管拨号客户端物理上同组织内部网隔离，但仍被认为是内部设备。IPsec远程接入应用于此场景。

图 7-51 IPSec VPN 远程接入场景示意图



IPSec VPN远程接入的配置过程分为以下五步：

1.配置IPSec-Pool

2.配置远程用户组

3.配置IKE阶段1

4.配置KE阶段2

5.配置隧道

7.7.1 配置 IPSec Pool

本节介绍IPSec Pool的配置步骤和命令。

1.创建IPsec Pool。

命令	功能
`inspur(config)#`**ipsec-pool** *<ipsec-pool-tag>*	创建IPsec Pool，并进入Psec Pool配置模式

2.配置IPsec Pool。

命令	功能
`inspur(config-ipsec-pool)#`**wins first** *<first-wins>*[**second** *<second-wins>*]	配置WINS地址
`inspur(config-ipsec-pool)#`**dns first** *<first-wins>*[**second** *<second-wins>*]	配置DNS地址
`inspur(config-ipsec-pool)#`**ip-pool** *<ip-pool>*	绑定**ip-pool**地址池

7.7.2 配置远程用户组

本节介绍远程用户组的配置步骤和命令。

1.创建远程用户组。

命令	功能
inspur(config)#**isakmp user-group**<*WORD*>	创建远程用户组，并进入远程用户组配置模式

2.配置远程用户组。

命令	功能
inspur(config-isakmp-usergroup)#**ipsec-pool** <*WORD*>	用户组下绑定ipsec-pool
inspur(config-isakmp-usergroup)#**max-users** <*1-256*>	配置用户组的最大接入用户数量
inspur(config-isakmp-usergroup)#**identity ipv4 address** <*local-ipv4-address*>	配置IPv4 地址类型的用户身份
inspur(config-isakmp-usergroup)#**identity key-id** <*key-id*>	配置 key类型的用户身份
inspur(config-isakmp-usergroup)#**identity user** <*user-name*> **fqdn** <*fqdn-name*>	配置 User FQDN类型的用户身份
inspur(config-isakmp-usergroup)#**identity fqdn** <*fqdn-name*>	配置 FQDN类型的用户身份
inspur(config-isakmp-usergroup)#**user-name** <*user-name*> **password** {**encrypted** <*encrypted-password*>|<*password*>}	配置用户的用户名和密码
inspur(config-isakmp-usergroup)#**xauth** {**enable** | **disable**}	开启IPsec 扩展认证过程
inspur(config-isakmp-usergroup)#**authentication-template** <*template-number*>	绑定AAA认证模板
inspur(config-isakmp-usergroup)#**authorization-template** <*template-number*>	绑定AAA 授权模板
inspur(config-isakmp-usergroup)#**accounting-template** <*template-number*>	绑定AAA计费模板

7.7.3 配置远程接入隧道

IKE阶段1和IKE阶段2的配置，参见"配置IKE阶段1"和"配置IKE阶段2"。远程接入使用动态隧道，动态隧道具体配置参见"配置隧道和传输模式"。远程接入功能需在动态隧道下绑定用户组。

配置远程接入隧道。

命令	功能
inspur(config-ipsec-if-ipsec_tunnelid)#**reverse-route**	用户上线时分配IP地址，为分配的IP地址添加路由。
inspur(config-ipsec-if-ipsec_tunnelid)#**user-group** <*user-group-name*>	在动态隧道下绑定用户组

7.7.4 验证和维护远程接入

显示IPSec-Pool信息

命令	功能
inspur#**show ipsec-pool** <*pool-name*>	显示**ipsec-pool**配置信息

显示ISAKMP信息

命令	功能
inspur#**show isakmp user-group** <*group-name*>	显示用户组配置信息

IKE阶段1和IKE阶段2的验证和维护命令，参见"验证和维护IPSec"。

显示IPSec用户信息

命令	功能
inspur#**show crypto ipsec client** {**group** <*group-name*>| **interface** <*interface-name*>|**user-ip** <*ipv4-address*>}	显示远程登录的用户信息

显示反向路由生成信息

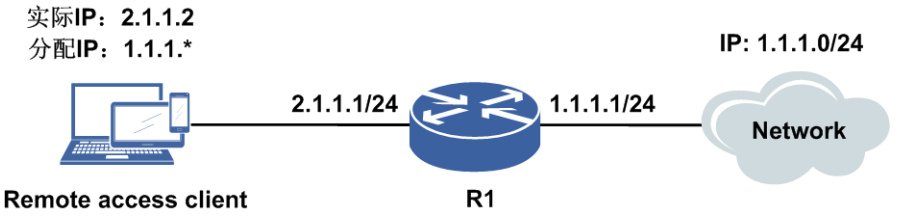
命令	功能
inspur#**show ip forwarding route** | **include IPsec**	显示路由IPSCE远程用户反向路由信息

7.7.5 IPSec VPN 远程接入配置实例

配置说明

如*图 7-52*所示， 为用户远程接入IPSec网关访问内网的场景。R1为IPsec网关，配置采用客户端FQDN和网关IP地址协商，使用野蛮模式。同时开启XAUTH，通过本地授权和本地认证进行客户端验证。

图 7-52 IPSec VPN 远程接入配置实例拓扑图



配置过程

设备R1上的配置如下：

1.配置接口IP地址，创建IPSec虚接口

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ip address 2.1.1.1 255.255.255.0
inspur(config-if-gei-0/1)#no shut
inspur(config-if-gei-0/1)#exit
inspur(config)#interface ipsec_tunnel1
inspur(config-if-ipsec_tunnel1)#ip address 100.1.1.1 255.255.255.0
inspur(config-if-ipsec_tunnel1)#exit
```

2.配置IPSec-pool

```
inspur(config)#ip pool inspur
inspur(config-ip-pool)#range 158.1.1.20 158.1.1.100 255.255.255.0
inspur(config-ip-pool)#exit
inspur(config)#ipsec-pool inspur
inspur(config-ipsec-pool)#ip-pool inspur
inspur(config-ipsec-pool)#wins first 1.1.2.2 second 2.2.3.3
inspur(config-ipsec-pool)#dns first 3.3.4.4 second 5.5.6.6
```

3.配置ISAKMP user-group

```
inspur(config)#isakmp user-group grp1
inspur(config-isakmp-usergroup)#ipsec-pool inspur
inspur(config-isakmp-usergroup)#identity fqdn hello
inspur(config-isakmp-usergroup)#xauth enable
```

```
inspur(config-isakmp-usergroup)#user-name inspur password inspur
```

4.配置ISAKMP协商策略

```
inspur(config)#isakmp enable
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#authentication pre-share
inspur(config-isakmp-1)#encryption aes-128
inspur(config-isakmp-1)#group 2
inspur(config-isakmp-1)#hash md5
inspur(config-isakmp-1)#exit
```

5.配置key-set

```
inspur(config)#isakmp key-set 1
inspur(config-isakmp-key-set)#pre-shared key fqdn hello
inspur(config-isakmp-key-set-pre-shared-key)#key inspur
inspur(config-isakmp-key-set-pre-shared-key)#exit
```

6.配置ISAKMP profile

```
inspur(config)#isakmp profile 1
inspur(config-isakmp-profile)#exchange-mode aggressive
inspur(config-isakmp-profile)#key-set 1
inspur(config-isakmp-profile)#policy 1
inspur(config-isakmp-profile)#match identity fqdn hello
```

7.配置IPSec转码集

```
inspur(config)#crypto ipsec transform-set 1
inspur(config-crypto-trans)#algorithm esp-md5-hmac esp-des
inspur(config-crypto-trans)#exit
```

8.配置静态profile

```
inspur(config)#crypto ipsec dynamic-profile 1
inspur(config-ipsec-static-profile)#set transform-set 1
inspur(config-ipsec-static-profile)#exit
```

9.配置IPSec隧道配置模式

```
inspur(config)#ipsec-config
inspur(config-ipsec)#interface ipsec_tunnel1
inspur(config-ipsec-if-ipsec_tunnel1)#type dynamic
inspur(config-ipsec-if-ipsec_tunnel1)#reverse-route
inspur(config-ipsec-if-ipsec_tunnel1)#tunnel local ipv4-address 2.1.1.1
inspur(config-ipsec-if-ipsec_tunnel1)#reverse-route
inspur(config-ipsec-if-ipsec_tunnel1)#user-group grp1
inspur(config-ipsec-if-ipsec_tunnel1)#isakmp-profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#ipsec-profile 1
inspur(config-ipsec-if-ipsec_tunnel1)#exit
inspur(config-ipsec)#exit
```

配置验证

用户上线后，通过下面几个项目检查配置。

查看用户节点是否生成：

```
inspur(config)#show crypto ipse client interface ipsec_tunnel1
Index Tunnel          Internal-IP    User-group     Remote-IP
1    ipsec_tunnel1    158.1.1.20     inspur1          2.1.1.2
```

查看IP pool是否成功分配地址：

```
inspur(config)#show ip local pool used-ip inspur
PoolName        Used-ip         Conflict:(*)
```

```
inspur            158.1.1.20
Total: 1
```

查看反向路由注入功能是否生效：

```
inspur(config)#show ip forwarding route | include IPsec
*> 158.1.1.20/32     2.1.1.2       ipsec_tunnel1      IPsec      0
```

查看IKE SA：

```
inspur#show isakmp sa
Codes: D - Dead Peer Detection
      N - NAT-Traversal
C-id Local      Port Remote        Port VRF     Ver Status Lifetime Cap
1    2.1.1.1     500  2.1.1.2      500         v1  active 86400
```

查看IPSec SA：

```
inspur#show crypto ipsec sa nego
Interface: ipsec_tunnel1
 IKE version             : v1
IPsec profile tag:1
 Local endpt: 2.1.1.1      Current remote endpt: 2.1.1.2
 Local  ident(addr/mask/prot/port_min/port_max) :
  (0.0.0.0/0.0.0.0/0/Invalid/Invalid)
 Remote ident(addr/mask/prot/port_min/port_max) :
  (158.1.1.20/255.255.255.255/0/Invalid/Invalid)
 IPsec MTU               : 1500
 FVRF                    : not configure
 IVRF                    : not configure
 Pre-fragmentation       : enable
 Original IP header DF-bit : aware
 Tunnel IP header DF-bit   : clear
 SA type                 : negotiation
 Inbound ESP SA:
  SPI                    : 0x1000062
  Authentication algorithm : hmac-md5
  Encryption algorithm    : des
  Encapsulation mode      : tunnel
  Throughput              : 739014KB
 Inbound AH SA:
 Outbound ESP SA:
  SPI                    : 0x4e4bbd14
  Authentication algorithm : hmac-md5
  Encryption algorithm    : des
  Encapsulation mode      : tunnel
  Throughput              : 10300896KB
 Outbound AH SA:
```

7.8 DVMPN

DMVPN（Dynamic Multipoint VPN，动态多点VPN），是为了解决传统IPSec VPN星形和网状拓扑存在高扩展性问题。当分支站点较多时，星形拓扑存在中心站点配置量大、分支站点间流量延时较大、分支站点间流量占用中心带宽等问题，而网状拓扑存在中心与分支站点配置量大、分支站点需要维护过多IPSec SA、每一个分支站点需要固定IP地址等问题。

DMVPN是MGRE、NHRP、IPSec结合产生的一种技术。其为具有点多面广分支机构特点的企业和公司，提供了一种以Internet为基础的低成本安全互联方案。

7.8.1 配置 MGRE

与MGRE相对的是普通的Point-to-Point GRE。MGRE也是GRE接口，只是不需要目的地址，基本配置继承自GRE，参见"VPN"中的"GRE隧道"。

配置MGRE。

步骤	命令	功能
1	inspur(config)#**gre-config**	进入GRE隧道配置模式
2	inspur(config-gre)#**interface gre_tunnel**<*tunnel-id*>	进入GRE隧道接口配置模式
3	inspur(config-gre-if-gre_tunnelid)#**tunnel mode multipoint**	配置当前隧道模式为MGRE

7.8.2 配置 NHRP

本节介绍NHRP的配置步骤和命令。

配置NHRP。

步骤	命令	功能
1	inspur(config)#**nhrp**	进入NHRP配置模式
2	inspur(config-nhrp)#**interface gre_tunnel**<*tunnel-id*>	进入对应的MGRE接口
3	inspur(config-nhrp-if-gre_tunnel1)#**ip nhrp authentication** <*authstring*>	配置NHRP认证密码，范围1~8个字符
4	inspur(config-nhrp-if-gre_tunnel1)#**ip nhrp holdtime** <*senconds*>	配置NHRP映射条目的老化时间，范围60~65535，默认7200
5	inspur(config-nhrp-if-gre_tunnel1)#**ip nhrp map** {**A.B.C.D A.B.C.D**| **multicast** {**A.B.C.D**|**dynamic**}}	配置单播和组播的NHRP地址到NBMA地址的映射条目，dynamic表示从Hub上动态学习spoke注册的条目
6	inspur(config-nhrp-if-gre_tunnel1)#**ip nhrp network-id** <*id*>	配置NBMA网络ID，范围1~4294967295
7	inspur(config-nhrp-if-gre_tunnel1)#**ip nhrp nhs** <*A.B.C.D*>	配置Hub的MGRE地址

7.8.3 配置 IPSec

IPSec配置为动态传输模式，参见"VPN"中的"IPSec VPN"。

配置传输模式。

步骤	命令	功能
1	inspur(config)#**crypto ipsec-transport** <*index*>	创建传输模式
2	inspur(config-ipsec-transport1)#**set sa-level per-host**	为每一个单独的流创建一个IPSec SA
3	inspur(config-ipsec-transport1)#**bound-to gre_tunnel**<*tunnel-id*>	IPSec传输模式绑定GRE接口
4	inspur(config-ipsec-transport1)#**tunnel protect gre_tunnel**<*tunnel-id*>	配置为GRE over IPSec

7.8.4 验证和维护 DMVPN

显示NHRP信息

命令	功能
inspur#**show ip nhrp map** [**gre_tunnel**<*tunnel-id*>]	显示NHRP映射信息
inspur#**show ip nhrp packet gre_tunnel**<*tunnel-id*>	显示MGRE接口的NHRP协议报文计数

删除NHRP动态条目

命令	功能
inspur#**clear ip nhrp gre_tunnel**<*tunnel-id*>	删除NHRP的动态条目

查看NHRP调试信息

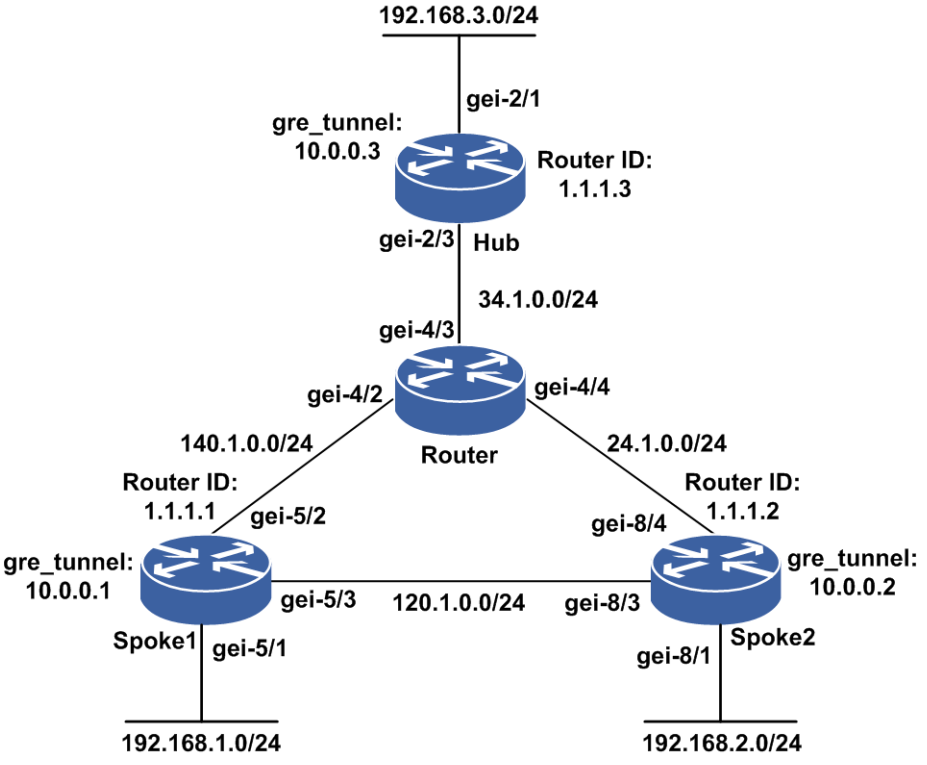
命令	功能
inspur#**debug nhrp all**	打开NHRP debug开关

7.8.5 DMVPN 配置实例

配置说明

如*图 7-53*所示，DMVPN的组网为NBMA组网，或者说是一种逻辑上的全连接，spoke到Hub上有逻辑连接，spoke之间也有逻辑连接，Hub为中心设备，spoke为站点设备。spoke到Hub的IPSec为长连接，spoke到spoke的IPSec连接流量触发。

图 7-53 DMVPN 配置实例组网图



配置思路

1.配置接口相关配置，包括物理接口和GRE接口。

2.配置MGRE。

3.配置NHRP，包括Hub和spoke。

4.配置IPSec。

5.配置静态或动态路由协议。

配置过程

Hub上配置如下：

1.接口配置。

```
inspur(config)#inter gei-2/3
inspur(config-if-gei-2/3)#ip addr 34.1.0.3/24
inspur(config-if-gei-2/3)#no shut
inspur(config-if-gei-2/3)#exit
inspur(config)#inter gei-2/1
inspur(config-if-gei-2/1)#ip addr 192.168.3.1/24
inspur(config-if-gei-2/1)#no shut
inspur(config-if-gei-2/1)#exit
inspur(config)#inter gre_tunnel1
inspur(config-if-gre_tunnel1)#ip addr 10.0.0.3/24
inspur(config-if-gre_tunnel1)#exit
inspur(config)#inter loopback1
inspur(config-if-loopback1)#ip addr 1.1.1.3/32
inspur(config-if-loopback1)#!
inspur(config)#
```

2.GRE配置。

```
inspur(config)#gre-config
inspur(config-gre)#interface gre_tunnel1
inspur(config-gre-if-gre_tunnel1)#tunnel mode multipoint
inspur(config-gre-if-gre_tunnel1)#tunnel source interface loopback1
inspur(config-gre-if-gre_tunnel1)#!
```

3.NHRP配置。

```
inspur(config)#nhrp
inspur(config-nhrp)#interface gre_tunnel1
inspur(config-nhrp-if-gre_tunnel1)#ip nhrp holdtime 60
inspur(config-nhrp-if-gre_tunnel1)#ip nhrp map multicast dynamic
inspur(config-nhrp-if-gre_tunnel1)#ip nhrp network-id 1
inspur(config-nhrp-if-gre_tunnel1)#!
```

4.ACL配置。

```
inspur(config)#ipv4-access-list ipsec
inspur(config-ipv4-acl)#rule 1 permit any
inspur(config-ipv4-acl)#!
```

5.IPSec配置。

```
inspur(config)#isakmp enable
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#lifetime 3600
inspur(config-isakmp-1)#exit
inspur(config)#isakmp key-set inspur
inspur(config-isakmp-key-set)#pre-shared key ipv4-address 1.1.1.0 netmask
255.255.255.0
inspur(config-iskamp-key-set-pre-shared-key)#key inspur
inspur(config-iskamp-key-set-pre-shared-key)#exit
inspur(config-iskamp-key-set)#exit
inspur(config)#isakmp profile wd
inspur(config-isakmp-profile)#policy 1
inspur(config-isakmp-profile)#match any-identity enable
inspur(config-isakmp-profile)#key-set inspur
inspur(config-isakmp-profile)#exit
inspur(config)#crypto ipsec transform-set wd
inspur(config-crypto-trans)#algorithm esp-md5-hmac esp-des
inspur(config-crypto-trans)#encapsulation-mode transport
inspur(config-crypto-trans)#exit
inspur(config)#crypto ipsec dynamic-profile wd
inspur(config-ipsec-dynamic-profile)#match acl ipsec v4
inspur(config-ipsec-dynamic-profile)#set transform-set wd
inspur(config-ipsec-dynamic-profile)#exit
```

```
inspur(config)#crypto ipsec-transport 1
inspur(config-ipsec-transport1)#set type dynamic
inspur(config-ipsec-transport1)#isakmp-profile wd
inspur(config-ipsec-transport1)#ipsec-profile wd
inspur(config-ipsec-transport1)#bound-to gre_tunnel1
inspur(config-ipsec-transport1)#tunnel protect gre_tunnel1
inspur(config-ipsec-transport1)#set sa-level per-host
inspur(config-ipsec-transport1)#exit
```

6.路由协议配置。

```
inspur(config)#router ospf 1
inspur(config-ospf-1)#area 0
inspur(config-ospf-1-area-0)#network 34.1.0.3 0.0.0.0
inspur(config-ospf-1-area-0)#network 1.1.1.3 0.0.0.0
inspur(config-ospf-1-area-0)#!
inspur(config)#router ospf 2
inspur(config-ospf-2)#area 0
inspur(config-ospf-2-area-0)#network 10.0.0.3 0.0.0.0
inspur(config-ospf-2-area-0)#network 192.168.3.1 0.0.0.0
inspur(config-ospf-2-area-0)#$
inspur(config-ospf-2)#inter gre_tunnel1
inspur(config-ospf-2-if-gre_tunnel1)#network broadcast
inspur(config-ospf-2-if-gre_tunnel1)#!
inspur(config)#
```

Spoke1上配置如下：

1.接口配置。

```
inspur(config)#inter gei-5/3
inspur(config-if-gei-5/3)#ip addr 120.1.0.1/24
inspur(config-if-gei-5/3)#no shut
inspur(config-if-gei-5/3)#exit
inspur(config)#inter gei-5/2
inspur(config-if-gei-5/2)#ip addr 140.1.0.1/24
inspur(config-if-gei-5/2)#$
inspur(config)#
inspur(config)#inter gei-5/1
inspur(config-if-gei-5/1)#ip addr 192.168.1.1/24
inspur(config-if-gei-5/1)#no shut
inspur(config-if-gei-5/1)#exit
inspur(config)#inter gre_tunnel1
inspur(config-if-gre_tunnel1)#ip addr 10.0.0.1/24
inspur(config-if-gre_tunnel1)#exit
inspur(config)#inter loopback1
inspur(config-if-loopback1)#ip addr 1.1.1.1/32
inspur(config-if-loopback1)#!
inspur(config)#
```

2.GRE配置。

```
inspur(config)#gre-config
inspur(config-gre)#interface gre_tunnel1
inspur(config-gre-if-gre_tunnel1)#tunnel mode multipoint
inspur(config-gre-if-gre_tunnel1)#tunnel source interface loopback1
inspur(config-gre-if-gre_tunnel1)#!
```

3.NHRP配置。

```
inspur(config)#nhrp
inspur(config-nhrp)#interface gre_tunnel1
inspur(config-nhrp-if-gre_tunnel1)#ip nhrp map 10.0.0.3 1.1.1.3
inspur(config-nhrp-if-gre_tunnel1)#ip nhrp map multicast 1.1.1.3
inspur(config-nhrp-if-gre_tunnel1)#ip nhrp nhs 10.0.0.3
```

```
inspur(config-nhrp-if-gre_tunnel1)#ip nhrp holdtime 60
inspur(config-nhrp-if-gre_tunnel1)#ip nhrp network-id 1
inspur(config-nhrp-if-gre_tunnel1)#!
```

4.ACL配置。

```
inspur(config)#ipv4-access-list ipsec
inspur(config-ipv4-acl)#rule 1 permit any
inspur(config-ipv4-acl)#!
```

5.IPSec配置。

```
inspur(config)#isakmp enable
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#lifetime 3600
inspur(config-isakmp-1)#exit
inspur(config)#isakmp key-set inspur
inspur(config-isakmp-key-set)#pre-shared key ipv4-address 1.1.1.0 netmask
255.255.255.0
inspur(config-iskamp-key-set-pre-shared-key)#key inspur
inspur(config-iskamp-key-set-pre-shared-key)#exit
inspur(config-iskamp-key-set)#exit
inspur(config)#isakmp profile wd
inspur(config-isakmp-profile)#policy 1
inspur(config-isakmp-profile)#match any-identity
inspur(config-isakmp-profile)#key-set inspur
inspur(config-isakmp-profile)#exit
inspur(config)#crypto ipsec transform-set wd
inspur(config-crypto-trans)#algorithm esp-md5-hmac esp-des
inspur(config-crypto-trans)#encapsulation-mode transport
inspur(config-crypto-trans)#exit
inspur(config)#crypto ipsec dynamic-profile wd
inspur(config-ipsec-dynamic-profile)#match acl ipsec v4
inspur(config-ipsec-dynamic-profile)#set transform-set wd
inspur(config-ipsec-dynamic-profile)#exit
inspur(config)#crypto ipsec-transport 1
inspur(config-ipsec-transport1)#set type dynamic
inspur(config-ipsec-transport1)#isakmp-profile wd
inspur(config-ipsec-transport1)#ipsec-profile wd
inspur(config-ipsec-transport1)#bound-to gre_tunnel1
inspur(config-ipsec-transport1)#tunnel protect gre_tunnel1
inspur(config-ipsec-transport1)#set sa-level per-host
inspur(config-ipsec-transport1)#exit
```

6.路由协议配置。

```
inspur(config)#router ospf 1
inspur(config-ospf-1)#area 0
inspur(config-ospf-1-area-0)#network 120.1.0.1 0.0.0.0
inspur(config-ospf-1-area-0)#network 140.1.0.1 0.0.0.0
inspur(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
inspur(config-ospf-1-area-0)#!
inspur(config)#router ospf 2
inspur(config-ospf-2)#area 0
inspur(config-ospf-2-area-0)#network 10.0.0.1 0.0.0.0
inspur(config-ospf-2-area-0)#network 192.168.1.1 0.0.0.0
inspur(config-ospf-2-area-0)#$
inspur(config-ospf-2)#inter gre_tunnel1
inspur(config-ospf-2-if-gre_tunnel1)#network broadcast
inspur(config-ospf-2-if-gre_tunnel1)#priority 0
inspur(config-ospf-2-if-gre_tunnel1)#!
inspur(config)#
```

Spoke2上配置如下：

1.接口配置。

```
inspur(config)#inter gei-8/3
inspur(config-if-gei-8/3)#ip addr 120.1.0.2/24
inspur(config-if-gei-8/3)#no shut
inspur(config-if-gei-8/3)#exit
inspur(config)#inter gei-8/4
inspur(config-if-gei-8/4)#ip addr 24.1.0.2/24
inspur(config-if-gei-8/4)#$
inspur(config)#
inspur(config)#inter gei-8/1
inspur(config-if-gei-8/1)#ip addr 192.168.2.1/24
inspur(config-if-gei-8/1)#no shut
inspur(config-if-gei-8/1)#exit
inspur(config)#inter gre_tunnel1
inspur(config-if-gre_tunnel1)#ip addr 10.0.0.2/24
inspur(config-if-gre_tunnel1)#exit
inspur(config)#inter loopback1
inspur(config-if-loopback1)#ip addr 1.1.1.2/32
inspur(config-if-loopback1)#!
inspur(config)#
```

2.GRE配置。

```
inspur(config)#gre-config
inspur(config-gre)#interface gre_tunnel1
inspur(config-gre-if-gre_tunnel1)#tunnel mode multipoint
inspur(config-gre-if-gre_tunnel1)#tunnel source interface loopback1
inspur(config-gre-if-gre_tunnel1)#!
```

3.NHRP配置。

```
inspur(config)#nhrp
inspur(config-nhrp)#interface gre_tunnel1
inspur(config-nhrp-if-gre_tunnel1)#ip nhrp map 10.0.0.3 1.1.1.3
inspur(config-nhrp-if-gre_tunnel1)#ip nhrp map multicast 1.1.1.3
inspur(config-nhrp-if-gre_tunnel1)#ip nhrp nhs 10.0.0.3
inspur(config-nhrp-if-gre_tunnel1)#ip nhrp holdtime 60
inspur(config-nhrp-if-gre_tunnel1)#ip nhrp network-id 1
inspur(config-nhrp-if-gre_tunnel1)#!
```

4.ACL配置。

```
inspur(config)#ipv4-access-list ipsec
inspur(config-ipv4-acl)#rule 1 permit any
inspur(config-ipv4-acl)#!
```

5.IPSec配置。

```
inspur(config)#isakmp enable
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#lifetime 3600
inspur(config-isakmp-1)#exit
inspur(config)#isakmp key-set inspur
inspur(config-isakmp-key-set)#pre-shared key ipv4-address 1.1.1.0 netmask
255.255.255.0
inspur(config-iskamp-key-set-pre-shared-key)#key inspur
inspur(config-iskamp-key-set-pre-shared-key)#exit
inspur(config-iskamp-key-set)#exit
inspur(config)#isakmp profile wd
inspur(config-isakmp-profile)#policy 1
inspur(config-isakmp-profile)#match any-identity enable
inspur(config-isakmp-profile)#key-set inspur
inspur(config-isakmp-profile)#exit
inspur(config)#crypto ipsec transform-set wd
inspur(config-crypto-trans)#algorithm esp-md5-hmac esp-des
```

```
inspur(config-crypto-trans)#encapsulation-mode transport
inspur(config-crypto-trans)#exit
inspur(config)#crypto ipsec dynamic-profile wd
inspur(config-ipsec-dynamic-profile)#match acl ipsec v4
inspur(config-ipsec-dynamic-profile)#set transform-set wd
inspur(config-ipsec-dynamic-profile)#exit
inspur(config)#crypto ipsec-transport 1
inspur(config-ipsec-transport1)#set type dynamic
inspur(config-ipsec-transport1)#isakmp-profile wd
inspur(config-ipsec-transport1)#ipsec-profile wd
inspur(config-ipsec-transport1)#bound-to gre_tunnel1
inspur(config-ipsec-transport1)#tunnel protect gre_tunnel1
inspur(config-ipsec-transport1)#set sa-level per-host
inspur(config-ipsec-transport1)#exit
```

6.路由协议配置。

```
inspur(config)#router ospf 1
inspur(config-ospf-1)#area 0
inspur(config-ospf-1-area-0)#network 120.1.0.2 0.0.0.0
inspur(config-ospf-1-area-0)#network 24.1.0.2 0.0.0.0
inspur(config-ospf-1-area-0)#network 1.1.1.2 0.0.0.0
inspur(config-ospf-1-area-0)#!
inspur(config)#router ospf 2
inspur(config-ospf-2)#area 0
inspur(config-ospf-2-area-0)#network 10.0.0.2 0.0.0.0
inspur(config-ospf-2-area-0)#network 192.168.2.1 0.0.0.0
inspur(config-ospf-2-area-0)#$
inspur(config-ospf-2)#inter gre_tunnel1
inspur(config-ospf-2-if-gre_tunnel1)#network broadcast
inspur(config-ospf-2-if-gre_tunnel1)#priority 0
inspur(config-ospf-2-if-gre_tunnel1)#!
inspur(config)#
```

设备Router的配置如下：

1.接口配置。

```
inspur(config)#inter gei-4/3
inspur(config-if-gei-4/3)#ip addr 34.1.0.4/24
inspur(config-if-gei-4/3)#no shut
inspur(config-if-gei-4/3)#exit
inspur(config)#inter gei-4/2
inspur(config-if-gei-4/2)#ip addr 140.1.0.4/24
inspur(config-if-gei-4/2)#$
inspur(config)#
inspur(config)#inter gei-4/4
inspur(config-if-gei-4/4)#ip addr 24.1.0.4/24
inspur(config-if-gei-4/4)#no shut
inspur(config-if-gei-4/4)#exit
```

2.路由协议配置。

```
inspur(config)#router ospf 1
inspur(config-ospf-1)#area 0
inspur(config-ospf-1-area-0)#network 24.1.0.4 0.0.0.0
inspur(config-ospf-1-area-0)#network 140.1.0.4 0.0.0.0
inspur(config-ospf-1-area-0)#network 34.1.0.4 0.0.0.0
inspur(config-ospf-1-area-0)#!
```

配置验证

在Spoke1上查看配置结果：

```
inspur(config)#ping 10.0.0.3
sending 5,100-byte ICMP echo(es) to 10.0.0.3,timeout is 2 second(s).
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/6/30 ms.
[finish]

inspur#ping 10.0.0.2
sending 5,100-byte ICMP echo(es) to 10.0.0.2,timeout is 2 second(s).
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 1/1/1 ms.
[finish]

inspur#show ip nhrp map
Target address   NBMA address     Mode       Interface
10.0.0.3         1.1.1.3         static     gre_tunnel1
10.0.0.2         1.1.1.2         dynamic    gre_tunnel1

inspur(config)#show crypto ipsec sa nego
Transport: ipsec_transport1
 IKE version             : v1
 IPsec profile tag        : p1
 Local endpt:1.1.1.1      Current remote endpt: 1.1.1.3
 Local  ident(addr/mask/prot/port_min/port_max) :
  (1.1.1.1/255.255.255.255/0/Invalid/Invalid)
 Remote ident(addr/mask/prot/port_min/port_max) :
  (1.1.1.3/255.255.255.255/0/Invalid/Invalid)
 FVRF                    : not configure
 IVRF                    : not configure
 Pre-fragmentation        : disable
 Original IP header DF-bit : ignore
 SA type                  : negotiation
 Remain inbound throughput : 1842609987(KB)
 Remain outbound throughput: 1842885412(KB)
 Inbound ESP SA:
  SPI                    : 0x1000047
  Authentication algorithm : hmac-md5
  Encryption algorithm     : des
  Encapsulation mode       : transport
  Throughput              : 590013KB
  Remain lifetime          : 8268(s)
 Inbound AH SA:
 Outbound ESP SA:
  SPI                    : 0x100001c
  Authentication algorithm : hmac-md5
  Encryption algorithm     : des
  Encapsulation mode       : transport
  Throughput              : 314588KB
  Remain lifetime          : 8268(s)
 Outbound AH SA:


Transport: ipsec_transport1
 IKE version             : v1
 IPsec profile tag        : p1
 Local endpt:1.1.1.1      Current remote endpt: 1.1.1.2
 Local  ident(addr/mask/prot/port_min/port_max) :
  (1.1.1.1/255.255.255.255/0/Invalid/Invalid)
 Remote ident(addr/mask/prot/port_min/port_max) :
  (1.1.1.2/255.255.255.255/0/Invalid/Invalid)
 FVRF                    : not configure
 IVRF                    : not configure
 Pre-fragmentation        : disable
```

```
Original IP header DF-bit : ignore
SA type                 : negotiation
Remain inbound throughput : 1843048346(KB)
Remain outbound throughput: 1843200000(KB)
Inbound ESP SA:
 SPI                   : 0x1000049
 Authentication algorithm : hmac-md5
 Encryption algorithm     : des
 Encapsulation mode       : transport
 Throughput              : 151654KB
 Remain lifetime          : 28681(s)
Inbound AH SA:
Outbound ESP SA:
 SPI                   : 0x1000060
 Authentication algorithm : hmac-md5
 Encryption algorithm     : des
 Encapsulation mode       : transport
 Throughput              : 0KB
 Remain lifetime          : 28681(s)
Outbound AH SA:
```

7.9 VPDN

VPDN是指利用公共网络（如ISDN或PSTN）的拨号功能接入公共网络，实现虚拟专用网，从而为企业、小型ISP、移动办公人员等提供接入服务。VPDN为远端用户与私有企业网之间提供了一种经济而有效的点到点连接方式。

VPDN采用专用的网络通信协议，在公共网络上为企业建立安全的虚拟专网。企业驻外机构和出差人员可从远程经由公共网络，通过虚拟隧道实现和企业总部之间的网络连接，而公共网络上其它用户则无法穿过虚拟隧道访问企业网内部的资源。

VPDN有以下两种实现方式：

•接入服务器发起VPDN连接。

•用户发起VPDN连接。

VPDN网关一般使用路由器或VPN专用服务器。

7.9.1 配置 VPDN

配置VPDN功能，用于在公共网络上为企业建立安全的虚拟专网。

1.配置VPDN基本功能。

步骤	命令	功能
1	inspur(config)#**vpdn**	进入VPDN配置模式
2	inspur(config-vpdn)#**enable**	开启L2TP功能
3	inspur(config-vpdn)#**check-hostname-avp**	配置隧道协商中是否强制检查hostname avp，默认配置开启

步骤	命令	功能
4	inspur(config-vpdn)#**default vpdn-group** <*group-name*>	配置默认的VPDN组，当不能匹配到VPDN组时，用户从该VPDN组上线
5	inspur(config)#**vpdn-group** <*group-name*>	创建VPDN组，进入VPDN组配置模式，VPDN组的名称长度1~31字符

2.配置L2TP隧道的基本属性。

步骤	命令	功能
1	inspur(config-vpdn-group)#**local name** <*local-name*>	配置隧道本地名字，长度范围为1~31字符。当未配置时，取设备的local name
2	inspur(config-vpdn-group)#**l2tp hidden**	配置隧道隐藏功能
	inspur(config-vpdn-group)#**l2tp tunnel authentication**	配置隧道协商时是否认证对方
	inspur(config-vpdn-group)#**l2tp tunnel password** {<*tunnel-password*>| **encrypted** <*tunnel-password*>}	配置隧道密码： 配置明文密码，取值范围为1~31字符 配置密文密码，取值为64字符
3	inspur(config-vpdn-group)#**l2tp tunnel hello** <*hello-time*>	配置隧道hello报文间隔，单位：秒，取值范围为1~3600，缺省60秒
	inspur(config-vpdn-group)#**l2tp tunnel receive-window** <*receive-window-number*>	隧道控制包接收窗口可以接收的包数，取值范围为4~10，缺省为4
	inspur(config-vpdn-group)#**l2tp tunnel retransmit retries** <*retry-count*>	配置隧道协商报文重传次数，取值范围为1~10，缺省为5
	inspur(config-vpdn-group)#**l2tp tunnel retransmit timeout** <*timeout-interval*>	配置隧道协商报文重传间隔，单位：秒，取值范围为1~8，缺省为8秒
	inspur(config-vpdn-group)#**l2tp tunnel timeout setup** <*timeout-time*>	配置隧道老化时间，单位：秒，取值范围5~60，缺省为10秒
	inspur(config-vpdn-group)#**l2tp tunnel timeout no-session** <*no-session-timeout* >	配置隧道空闲老化时间，单位：秒，取值范围1~65535，缺省为15秒

3.配置LNS。

步骤	命令	功能

步骤	命令	功能
1	inspur(config-vpdn-group)#**service-type** {**lns**}	配置VPDN组的服务类型为LNS
2	inspur(config-vpdn-group)#**virtual-template** <*virtual-template-number*>	配置vpdn-group绑定虚模板号
3	inspur(config-vpdn-group)#**force-local-chap**	配置对用户进行强制CHAP认证
4	inspur(config-vpdn-group)#**lcp renegotiation** {**disable** | **always** | **on-mismatch**}	配置LCP重协商方式 **always**：忽略代理认证结果，强制重协商 **disable**：关闭LCP重协商功能 **on-mismatch**：代理认证失败时再进行重协商
5	inspur(config-vpdn-group)#**terminate-from hostname** <*hostname*>	配置终结的LAC设备名，LNS根据该配置选择VPDN组
6	inspur(config-vpdn-group)#**lns-send-sli**	配置是否发送SLI报文，默认配置为**no lns-send-sli**不发送SLI报文
7	inspur(config-vpdn-group)#**vrf** <*vrf-name*>	配置该命令后，LNS根据接入接口的VRF来匹配VPDN组
8	inspur(config-vpdn-group)#**bind sal** <*sal-name*>	LNS上绑定默认域的值
9	inspur(config-vpdn-group)#**initiate-to-ip-addr** <*ip-address*>[**priority** <*priority*>]	配置隧道的对端地址
10	inspur(config-vpdn-group)#**source-ip-addr** <*ip-address*>	配置VPDN组源IP地址
11	inspur(config-vpdn-group)#**ip tcp adjust-mss** <*max-segment-size*>	设置TCP中数据包每次能传输的最大数据分段的大小
12	inspur(config)#**ppp**	进入PPP配置模式
13	inspur(config-ppp)#**interface virtual_template**<*num*>	PPP模式下进入虚模板
14	inspur(config-ppp-if-virtual_template-num)#**keepalive** [**disable** |<*times*>]	配置PPP保活时间，默认10秒
15	inspur(config-ppp-if-virtual_template-num)#**ppp authentication** {**chap** | **pap**}	配置PPP的认证方式
16	inspur(config-ppp-if-virtual_template-num)#**bind-ip-pool** <*pool-name*>	虚模板下绑定平台地址池

4.配置域。

步骤	命令	功能
1	inspur(config)#**subscriber-manage**	进入用户管理配置模式
2	inspur(config-submanage)#**authentication-template** <*authen-template-name*>	进入认证模板配置模式
3	inspur(config-submanage-authen-template)#**authentication-type** {**none** | **local** | **radius** | **local-radius** | **radius-local** | **radius-none**}	配置认证类型
4	inspur(config-submanage)#**authorization-template** <*author-template-name*>	进入授权模板配置模式
5	inspur(config-submanage-author-template)#**authorization-type** {**none** | **mix-radius** | **radius**}	配置授权方式
6	inspur(config-submanage)#**accounting-template** <*acct-template-name*>	进入计费模板配置模式
7	inspur(config-submanage-accounting-template)#**accounting-type** {**none** | **radius**}	配置计费方式
8	inspur(config-submanage)#**domain** <*domain-name*>	进入domain配置模式
9	inspur(config-submanage-domain)#**bind** <*template*>	绑定模板，包括：计费模板、认证模板、授权模板
10	inspur(config-submanage-domain)#**tunnel-domain** {**enable**|**disable**}	开启管理域的隧道接入功能，该域上的用户皆为VPDN用户
11	inspur(config-submanage)#**local-subscriber** <*sub-name*> **domain-name** <*domain-name*> **password** <*password*>	配置本地用户编号，并进入LOCALSUB配置模式

5.配置服务接入控制列表SAL。

步骤	命令	功能
1	inspur(config)#**subscriber-manage**	进入用户管理配置模式
2	inspur(config-submanage)#**sal** < *sal-name*>	进入SAL配置模式
3	inspur(config-submanage-sal)#**default domain** <*domain-name*>	配置缺省域功能
4	inspur(config-submanage-sal)#**permit**{**any** | **domain** < *domain-name* >}	设置允许接入的域
5	inspur(config-submanage-sal)#**deny**{**any** | **domain** < *domain-name* >}	设置禁止接入的域
6	inspur(config-submanage-sal)#**translate** {**any** | **src-domain** < *domain-name* >} **des-domain** < *domain-name* >	配置域名映射功能

步骤	命令	功能
7	inspur(config-submanage-sal)#**none domain** < *domain-name* >[**keep**]	配置漫游域功能
8	inspur(config-submanage-sal)#**change-domain** <*change-domain*> **local-domain** <*local-domain*>	将用户的change域名转换为一个本地域名，用change域名进行认证，用本地域进行管理

6.验证配置结果。

命令	功能
inspur#**show vpdn session** [**local-tunnel-id** <*local-tunnel-id*>]	显示VPDN会话信息
inspur#**show vpdn tunnel** {**brief** | **local-tunnel-id** <*tunnel-id*>| **remote-name** <*remote-name*>|**summary** | **statistic** }	显示VPDN隧道信息
inspur#**show vpdn failure**	显示VPDN用户下线原因

7.维护VPDN。

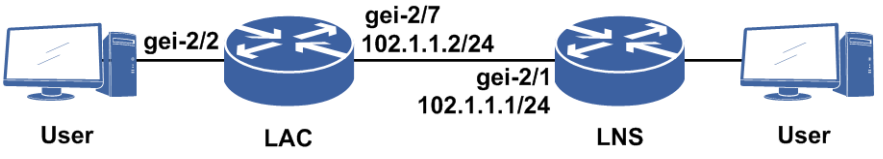
命令	功能
inspur#**debug l2tp** {**all** | **data** | **error** | **event** | **packet**}	开启L2TP的debug开关
inspur#**show debug l2tp**	显示VPDN的debug开关

7.9.2 LAC 配置实例

配置说明

在如*图 7-54*所示的网络中配置LAC的接入方式。

图 7-54 LAC 配置实例组网图



配置思路

1.进入到subscriber-manage配置模式下，配置认证模板（authentication-template），在认证模板下配置本地认证，退出到subscriber-manage配置模式下

2.创建并进入域（domain）配置模式，在域下绑定认证模板，打开tunnel-domain开关，退出到subscriber-manage配置模式下

3.配置本地认证用户（local-subscriber），配置用户名和密码，退出到subscriber-manage配置模式下

4.创建PPP模板，退出到subscriber-manage配置模式下

5.进入用户侧接口，执行no shutdown，并退出到全局配置模式

6.进入VCC配置模式，进入用户侧接口，这边是接口interface gei-2/2，配置封装模式为PPPoE，并绑定PPP模板，退出到全局配置模式

7.进入与LNS连接接口，配置IP地址，退出到全局配置模式

8.进入VPDN组配置模式，配置vpdn-group，这里的vpdn-group名字为inspur，配置隧道目的IP地址，源IP地址，本端名字，对端名字，关闭隧道认证，绑定域

9.进入VPDN配置模式，开启VPDN

配置过程

LAC设备上的配置如下：

```
inspur(config)#subscriber-manage
inspur(config-submanage)#authentication-template inspur
inspur(config-submanage-authen-template)#authentication-type local
inspur(config-submanage-authen-template)#exit
inspur(config-submanage)#domain l2tp
inspur(config-submanage-domain)#bind authentication-template inspur
inspur(config-submanage-domain)#tunnel-domain enable
inspur(config-submanage-domain)#exit

/*配置本地接入用户：lac1@l2tp 密码：123*/
inspur(config-submanage)#local-subscriber lac1 domain-name l2tp
 password 123
inspur(config-submanage-local-sub)#exit

/*配置pppox模板*/
inspur(config-submanage)#pppox-cfg 1
inspur(config-submanage-pppox)#exit
inspur(config-submanage)#exit

inspur(config)#interface gei-2/2
inspur(config-if-gei-2/2)#no shutdown
inspur(config-if-gei-2/2)#exit

/*配置vcc*/
inspur(config)#vcc-configuration
inspur(config-vcc)#interface gei-2/2
inspur(config-vcc-if)#encapsulation ppp-over-ethernet
inspur(config-vcc-if)#pppox template 1
inspur(config-vcc-if)#exit
inspur(config-vcc)#exit

inspur(config)#interface gei-2/7
inspur(config-if-gei-2/7)#no shutdown
inspur(config-if-gei-2/7)#ip address 102.1.1.2 255.255.255.0
inspur(config-if-gei-2/7)#exit

/*配置LAC vpdn组*/
inspur(config)#vpdn-group inspur
```

```
inspur(config-vpdn-group)#domain l2tp  /*绑定域*/
inspur(config-vpdn-group)#initiate-to-ip-addr 102.1.1.1  /*LNS上的接口IP*/
inspur(config-vpdn-group)#source-ip-addr 102.1.1.2   /*LAC上与LNS相连的接口的
IP*/
inspur(config-vpdn-group)#local name inspurlac
inspur(config-vpdn-group)#terminate-from hostname inspurlns
inspur(config-vpdn-group)#exit

/*全局配置，开启vpdn*/
inspur(config)#vpdn
inspur(config-vpdn)#enable
inspur(config-vpdn)#exit
```

配置验证

通过命令**show running-config vpdn all**查看VPDN配置情况：

```
inspur(config)#show running-config vpdn all
!  <VPDN>
vpdn-group inspur
  #service-type lac
  #ip tcp adjust-mss 1400
  #calling-number-format none
  domain l2tp
  local name inspurlac
  terminate-from hostname inspurlns
  #no force-local-chap
  #no l2tp hidden
  #no l2tp tunnel authentication
  #l2tp tunnel hello 60
  #l2tp tunnel receive-window 4
  #l2tp tunnel retransmit retries 5
  #l2tp tunnel retransmit timeout 8
  #l2tp tunnel timeout no-session 15
  #l2tp tunnel timeout setup 10
  #lcp renegotiation always
  #no lns-send-sli
  #max-session 16000
  #max-session-per-tunnel 16000
  source-ip-addr 102.1.1.2
  #set-dscp-outer 48
  initiate-to-ip-addr 102.1.1.1 priority 50
$
vpdn
  #vpdn-mode centralization
  #calling-number-avp disable
  #calling-number-format class1
  #check-hostname-avp
  enable
  #invalid-peerip-timeout 300
  #tid-alloc-mode first
  #no multihop
  #tunnel-num-per-spu 1000
$
! </VPDN>
```

其中参数**all**表示显示默认配置，可以看到全局模式下VPDN使能，和默认组等配置信息。

通过命令**show vpdn tunnel brief**查看隧道是否建立：

```
inspur(config)#show vpdn tunnel brief
```

```
LTID  RTID  RemoteName     State        RemoteAddr      RemotePort   Sessions
26566 59221 inspurlns        Established   102.1.1.1       1701         1
```

其中“state”一项如果是“Established”则代表隧道已经建立成功。

通过命令**show subscriber vpdn lac**查看是否用户已经上线：

```
inspur(config)#show subscriber vpdn lac
************************************************************************
*****
                        Subscriber     Information
------------------------------------------------------------------------
-----
                            Basic Information
------------------------------------------------------------------------
-----
subscriber-access-type :IPv4
user-identify         :20
user-name            :lac1
domain-name          :l2tp
local-domain-name     :l2tp
authorize-domain-name  :l2tp
mac-address          :0010.9434.0a01
session-id           :14
access-interface      :gei-2/2
internal-vlan         :0
external-vlan         :0
authentication-mode    :LOCAL
authentication-status  :ACCEPT
record-status         :CREATED
eap-type             :FALSE
sibprofileid          :0
hot-bak-status        :NONE
authentication-time    :2011/04/05  13:58:56
create-time          :2011/04/05  13:58:56
online-time          :207
limited-status        :UNLIMITED
restTimeType          :ABSOLUTE
vpdnAcctClass         :L2TP
route-map-name        :
------------------------------------------------------------------------
-----
                            IPv4 Information
------------------------------------------------------------------------
-----
subscriber-type       :VPDN
local-sessionid       :1
local-tunnelid        :26566
remote-sessionid      :123
remote-tunnelid       :59221
ipv4-address          :
vrf-name             :
vpn-id               :0
tunnel-vrf-name       :
tunnel-vpn-id         :0
lac-ipv4-address      :102.1.1.2
lns-ipv4-address      :102.1.1.1
record-status         :CREATED
************************************************************************
*****

------------------------------------------------------------------------
-----
session:         total     up        down
   IPv4          1         1         0
   IPv6          0         0         0
------------------------------------------------------------------------
```

```
-----
[Notes:hot-bak-status: master,slave,init; other-status: none]
subscriber:      total     none      master     slave      init
   ipv4-stack:   1         1         0          0          0
   ipv6-stack:   0         0         0          0          0
   dual-stack:   0         0         0          0          0
   all-stack:    1         1         0          0          0
------------------------------------------------------------------------------
-----
```

上面的输出表示该用户已经上线。

7.9.3 LNS 配置实例

配置说明

如*图 7-55*所示，R1作为LNS，用户PC通过VPN接入访问公司内网，VPN接入方式为L2TP。

图 7-55 LNS 配置实例组网图



配置思路

1.配置给用户分配地址的地址池。

2.全局模式下创建并进入虚模板，配置模式为PPP，并绑定接口。

3.在PPP模式下进入虚模板，配置用户认证方式为PAP，并绑定地址池。

4.退到全局配置模式下，再进入VPDN配置模式，配置vpdn-group；需要配置vpdn-group的服务类型、隧道本地名字、绑定虚接口

5.配置默认的VPDN组。

6.配置domain，本地用户等信息。

配置过程

```
R1(config)#interface gei-2/1
R1(config-if-gei-2/1)#no shutdown
R1(config-if-gei-2/1)#ip address 169.1.106.201 255.255.0.0
R1(config-if-gei-2/1)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 10.10.10.1 255.255.255.255
R1(config-if-loopback1)#exit
```

```
/*配置IP pool*/
R1(config)#ip pool vpn
R1(config-ip-pool)#range 10.10.10.2 10.10.10.200 255.255.255.0
R1(config-ip-pool)#exit

/*配置虚模板*/
R1(config)#interface virtual_template1
R1(config-if-virtual_template1)#mode ppp
R1(config-if-virtual_template1)#ip unnumbered loopback1
R1(config-if-virtual_template1)#exit

/*配置PPP*/
R1(config)#ppp
R1(config-ppp)#interface virtual_template1
R1(config-ppp-if-virtual_template1)#keepalive 20
R1(config-ppp-if-virtual_template1)#ppp authentication pap
R1(config-ppp-if-virtual_template1)#bind-ip-pool vpn
R1(config-ppp-if-virtual_template1)#exit
R1(config-ppp)#exit

/*配置LNS VPDN组*/
R1(config)#vpdn
R1(config-vpdn)#enable   /*启用VPDN*/
R1(config-vpdn)#exit
R1(config)#vpdn-group inspur
R1(config-vpdn-group)#service-type lns    /*配置服务类型为LNS*/
R1(config-vpdn-group)#local name inspurlns
R1(config-vpdn-group)#virtual-template 1
R1(config-vpdn-group)#bind sal inspur   /*配置服务接入控制列表SAL*/
R1(config-vpdn-group)#exit
R1(config)#vpdn
R1(config-vpdn)#default vpdn-group inspur /*配置默认接入vpdn-group inspur*/
R1(config-vpdn)#exit

/*配置用户认证模板*/
R1(config)#subscriber-manage
R1(config-submanage)#authentication-template inspur
R1(config-submanage-authen-template)#authentication-type local
R1(config-submanage-authen-template)#exit
R1(config-submanage)#domain l2tp
R1(config-submanage-domain)#bind authentication-template inspur
R1(config-submanage-domain)#tunnel-domain enable
R1(config-submanage-domain)#exit

/*配置本地接入用户：lac1@l2tp 密码：123*/
R1(config-submanage)#local-subscriber lac1 domain-name l2tp password 123
R1(config-submanage-local-sub)#exit

/*配置SAL*/
R1(config-submanage)#sal inspur
R1(config-submanage-sal)#default domain l2tp

/*PC拨号配置略*/
```

配置验证

通过命令**show vpdn tunnel brief**可以看到隧道已经建立。

```
R1#show vpdn tunnel brief
LTID  RTID  RemoteName     State         RemoteAddr      RemotePort  Sessions
26757 104   0001100535-1   Established   169.1.106.10    1701        1
R1#
```

通过命令**show ip local pool**可以查看地址池配置信息。

```
inspur(config)#show ip local pool
PoolName        Begin          End            Mask   Free      Used
vpn            10.10.10.2     10.10.10.200    24     198       1
TotalPool: 1
```

通过命令**show vpdn session**可以查看VPDN的会话信息

```
R1#show vpdn session
Session status:
  LocSID          :17           RemSID          :1
  LocTID          :2667         RemTID          :101
  State           :Established   OnlineTime      :527(s)
  Ident           :LNS          SesIntface      :N/A
  Username        :lac1@l2tp
  Call serial number is 17
```

通过命令**show subscriber user-type vpdn verbose**查看是否用户已经上线。

```
R1#show subscriber user-type vpdn verbose
********************************************************************************
*****
                     Subscriber   Verbose   Information
--------------------------------------------------------------------------------
-----
                            Basic Information
--------------------------------------------------------------------------------
-----
subscriber-access-type : IPv4
subscriber-author-type : IPv4
user-identify          : 14
user-group-identify    : 0
user-name             : lac1
domain-name           : l2tp
local-domain-name      : l2tp
authorize-domain-name  : l2tp
mac-address           : 0000.0000.0000
session-id            : 0
authentication-mode    : LOCAL
authentication-status  : ACCEPT
record-status         : CREATED
eap-type              : FALSE
proxy-flag            :
sibprofileid          : 0
domain-priority        : 0
domain-queue-share     : DISABLE
hot-bak-status         : NONE
access-interface       : virtual_template1
internal-vlan          : 0
external-vlan          : 0
create-time           : 2016/07/26  15:47:55
authentication-time    : 2016/07/26  15:47:55
online-time           : 10
remain-time           :
limited-status         : UNLIMITED
restTimeType          : ABSOLUTE
dpi-policy            : 0
user-priority-input    :
user-priority-output   :
vpdnAcctClass          : L2TP
calling-station-id     :

ani-location
```

```
    ------------------------------------------------------------------------
    Identifier:
    rack:0     frame:0     slot:0     sub-slot:0     port:0
    XpiEnable:Disable      xpi:0       xci:0
    ------------------------------------------------------------------------

onu-location
    ------------------------------------------------------------------------
    Identifier:
    slot:0     sub-slot:0     port:0     port-type:
    xpi:0       xci:0       AccessMethod:
    ------------------------------------------------------------------------

accounting information
    ------------------------------------------------------------------------
    restTime(s)     : unlimited       restFlow(KB)   : unlimited
    absTimeout(s)   : unlimited       idleTimeout(s) : 0
    idleTraffic(KB) : 0              acctInterval(s): 0
    sessionLimitType:                acctSession    :

------------------------------------------------------------------------
-----
                            IPv4 Information
------------------------------------------------------------------------
-----
subscriber-type       : IPv4 L2TP LNS
local-sessionid       : 20
local-tunnelid        : 26757
remote-sessionid      : 1
remote-tunnelid       : 104
ipv4-address          : 10.10.10.101
vrf-name              :
vpn-id                : 0
primary-dns           :
second-dns            :
tunnel-vrf-name       :
tunnel-vpn-id         : 0
lac-ipv4-address      : 169.1.106.10
lns-ipv4-address      : 169.1.106.201
record-status         : CREATED
nat-type              : NONE
nat-service           :
nat-static-flag       : DISABLE
nat-multi-flag        : DISABLE
nat-default-flag      : DISABLE
nat-inst-id           :
nat-domain-name       :
nat-block-id          :
nat-pool-name         :
nat-ipv4-address      :
nat-port-range        : 0~0
nat-session           :
route-map-name        :

framed-route
    ------------------------------------------------------------------------
    count  : 0
    ------------------------------------------------------------------------

user-acl
    ------------------------------------------------------------------------
    webAclName:
    aclInName :
    aclOutName:
    ispAclInName :
    ispAclOutName:
    specialAclName:
    ------------------------------------------------------------------------
```

```
QOS information
    ------------------------------------------------------------------------
    profileNameUp  :                              mode :together
    profileNameDown:                              mode :together
    subCarInfoUp-cir  : 0            subCarInfoUp-pir  : 0
    subCarInfoUp-cbs  : 0            subCarInfoUp-pbs  : 0
    subCarInfoDown-cir: 0            subCarInfoDown-pir: 0
    subCarInfoDown-cbs: 0            subCarInfoDown-pbs: 0
    ------------------------------------------------------------------------

float-accounting information
    ------------------------------------------------------------------------
    upDropPackets(Packets)  : 0         upDropCycles      : 0
    downDropPackets(Packets): 0         downDropCycles    : 0
    ispUpBytes(Bytes)       : 0         ispUpCycleCount   : 0
    ispDownBytes(Bytes)     : 0         ispDownCycleCount : 0
    upBytes(Bytes)          : 0         upCycleCount      : 0
    downBytes(Bytes)        : 0         downCycleCount    : 0
    upIspChargePackets      : 0         upIspChargeCycleCount     : 0
    downIspChargePackets    : 0         downIspChargeCycleCount   : 0
    upIspNoChargePackets    : 0         upIspNoChargeCycleCount   : 0
    downIspNoChargePackets  : 0         downIspNoChargeCycleCount : 0
    upPackets(Packets)      : 0         upPacketCycleCount        : 0
    downPackets(Packets)    : 0         downPacketCycleCount      : 0
************************************************************************
*****
------------------------------------------------------------------------
-----
session:         total      up        down
   IPv4          1          1         0
   IPv6          0          0         0
------------------------------------------------------------------------
-----
[Notes:hot-bak-status: master,slave,init; other-status: none]
subscriber:      total      none      master    slave     init
    ipv4-stack:   1          1         0         0         0
    ipv6-stack:   0          0         0         0         0
    dual-stack:   0          0         0         0         0
    all-stack :   1          1         0         0         0
------------------------------------------------------------------------
-----

R1#
```

上面的输出表示该用户已经上线。

7.10 GET VPN

GET VPN是一种基于IETF标准（RFC 3547 RFC 6407）的无隧道VPN技术。该技术为网 络基础设施提供了端到端的数据加密，同时能保持站点间的任意点到任意点通信。可以 将其部署在各种广域网核心传输网络中，如IP或多协议标签交换（MPLS）网络等。GET VPN可充分利用群组解释域（GDOI）协议，在网络设备之间建立一个安全的通信域。

GET VPN场景存在两种设备角色：组成员（group member，简称GM）在密钥服务器（KS）上注册，以获取对流经设备的数据流进行加密和解密所需的加密密钥，对匹配的数据流量进行加密和解密，同时还负责在安全与不安全的域之间执行路由及参与网络中已建立的组播通信；密钥服务器（Key Server，简称KS）是GET VPN的中枢系统，负责对GM做身份认证。KS还负责管理安全策略，决定应该对哪些流量进行加密。

KS通过GDOI协议将用于流量加密的会话密钥和安全策略分发给GM。

KS发给GM的密钥有两种：密钥加密密钥（KEK）及流量加密密钥（TEK）。KS利用KEK 来保护KS与GM之间的通信。GM利用TEK对GM之间传输的流量进行批量数据加密。KS 将按照需要发出密钥重置信息，其中包含了旧的IPSec安全关联（SA）到期以后应该使用 的新加密策略和加密密钥。密钥重置信息将在SA到期之前发出，以便确保所有GM都能获得新密钥。

KS是GET VPN部署中的一个重要组件。如果KS不可用，新的GM将无法注册和参与安全通信，而且现有的GM在当前的安全关联到期时也将收不到新的密钥和安全策略。为确保GET VPN网络的高可用性和永续性，冗余的KS以协作模式运行。协作密钥服务器（COOP KS）将共同管理群组的GDOI注册工作，共担GM注册负载。COOP KS在启动 时会进入一个选择流程，优先级最高的KS将成为主用设备，其它KS将作为备用设备。主 用KS负责创建并向GM重新发送安全策略和密钥，同时与备用KS进行同步。

7.10.1 配置 GDOI 组

本节介绍GDOI组的配置步骤和命令。

1.配置注册组信息。

步骤	命令	功能
1	inspur(config)#**crypto ipsec gdoi-group**<*group-name*>	设定GDOI注册使用的组信息
2	inspur(config-ipsec-gdoi-group)#**identity** {ipv4-address< *group-address*>| number < *group-id*> }	设定组号
3	inspur(config-ipsec-gdoi-group)#**server ipv4-address** <ks-address >	配置密钥服务器的地址
4	inspur(config-ipsec-gdoi-group)#**multicast -interface loopback** <1-64 >	配置组播接口

group-address：用于标识GDOI组的IP地址，可以为任意合法的IPv4地址。

group-id：GDOI组的编号，取值范围为0～2147483647。

2.配置GDOI profile。

步骤	命令	功能
1	inspur(config)#**crypto ipsec gdoi-profile** <profile-name >	设定GDOI profile
2	inspur(config-ipsec-gdoi-profile)#**match acl** <acl-name>{**v4**	**v6**}	配置本地兴趣流

3.传输模式配置GDOI

步骤	命令	功能
1	inspur(config)#**crypto ipsec-transport** <1-512>	进入传输模式配置
2	inspur(config-ipsec-transport)#**set type gdoi**	设置传输类型为GDOI
3	inspur(config-ipsec-transport)#**set gdoi-group** <*group-name*>	指明transport中绑定的GDOI组

4.验证和维护GDOI

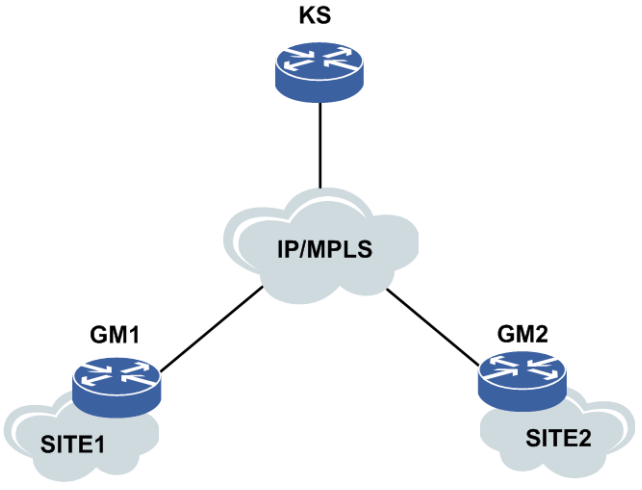
步骤	命令	功能
1	inspur(config)#**show crypto ipsec sa nego**	查看SA会话
2	inspur(config)#**show crypto ipsec gdoi gm** <*group-name*>	查看组信息

7.10.2 GET VPN 配置实例

配置说明

如*图 7-56*所示，GETVPN组网为总分组网，分支站点的GM在总部的KS上进行注册，通 过GDOI协议完成加密策略和秘钥的分发和更新，分支GM不再需要单独配置安全策略。

图 7-56 GETVPN 配置实例组网图



配置思路

由于KS和GM之间的交互决定了GETVPN的应用前提是全网可路由，因此配置思路为：

1.配置接口相关配置，全网路由可达。

2.配置IPSEC传输模式，GM注册组信息。

配置过程

GM1配置如下：

1.接口配置

```
inspur(config)#interface  gei-5/2
inspur(config-if-gei-5/2)#ip address 20.1.0.2 255.255.255.0
```

```
inspur(config-if-gei-5/2)#no shutdown
inspur(config-if-gei-5/2)#exit
inspur(config)#interface  gei-5/4
inspur(config-if-gei-5/2)#ip address 192.168.127.12 255.255.255.0
inspur(config-if-gei-5/2)#no shutdown
inspur(config-if-gei-5/2)#exit
inspur(config)#interface  gei-5/1
inspur(config-if-gei-5/2)#ip address 10.0.1.1 255.255.255.0
inspur(config-if-gei-5/2)#no shutdown
inspur(config-if-gei-5/2)#exit
```

2.配置IPSEC第一阶段

```
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#exit
inspur(config)#isakmp enable
inspur(config)#isakmp key-set s1
inspur(config-isakmp-key-set)#pre-shared  key  ipv4-address  192.168.127.72
netmask 255.255.255.255
inspur(config-isakmp-key-set-pre-shared-key)#key zte
inspur(config-isakmp-key-set-pre-shared-key)#exit
inspur(config-isakmp-key-set)#exit
inspur(config)#isakmp profile p1
inspur(config-isakmp-profile)#key-set s1
inspur(config-isakmp-profile)#match identity ipv4-address 192.168.127.72
inspur(config-isakmp-profile)#policy 1
inspur(config-isakmp-profile)#exit
```

3.配置IPSEC第二阶段

```
inspur(config)#crypto ipsec gdoi-group g1
inspur(config-ipsec-gdoi-group)#identity ipv4-address 1.1.1.1
inspur(config-ipsec-gdoi-group)#server ipv4-address 192.168.127.72
inspur(config-ipsec-gdoi-group)#exit
inspur(config)#crypto ipsec-transport 1
inspur(config-ipsec-transport1)#set type gdoi
inspur(config-ipsec-transport1)#set gdoi-group g1
inspur(config-ipsec-transport1)#isakmp-profile p1
inspur(config-ipsec-transport1)#local ipv4-address 192.168.127.12
inspur(config-ipsec-transport1)#bound-to gei-5/2
inspur(config-ipsec-transport1)#exit
```

GM2配置如下：

1.接口配置

```
inspur(config)#interface gei-5/2
inspur(config-if-gei-5/2)#ip address 20.1.0.1 255.255.255.0
inspur(config-if-gei-5/2)#no shutdown
inspur(config-if-gei-5/2)#exit
inspur(config)#interface gei-5/4
inspur(config-if-gei-5/2)#ip address 192.168.127.13 255.255.255.0
inspur(config-if-gei-5/2)#no shutdown
inspur(config-if-gei-5/2)#exit
inspur(config)#interface gei-5/1
inspur(config-if-gei-5/2)#ip address 10.0.2.1 255.255.255.0
inspur(config-if-gei-5/2)#no shutdown
inspur(config-if-gei-5/2)#exit
```

2.配置IPSEC第一阶段

```
inspur(config)#isakmp policy 1
inspur(config-isakmp-1)#exit
inspur(config)#isakmp enable
inspur(config)#isakmp key-set s1
```

```
inspur(config-isakmp-key-set)#pre-shared  key  ipv4-address  192.168.127.72
netmask 255.255.255.255
inspur(config-isakmp-key-set-pre-shared-key)#key zte
inspur(config-isakmp-key-set-pre-shared-key)#exit
inspur(config-isakmp-key-set)#exit inspur(config)#isakmp profile p1
inspur(config-isakmp-profile)#key-set s1
inspur(config-isakmp-profile)#match identity ipv4-address 192.168.127.72
inspur(config-isakmp-profile)#policy 1
inspur(config-isakmp-profile)#exit
```

3.配置IPSEC第二阶段

```
inspur(config)#crypto ipsec gdoi-group g1
inspur(config-ipsec-gdoi-group)#identity ipv4-address 1.1.1.1
inspur(config-ipsec-gdoi-group)#server ipv4-address 192.168.127.72
inspur(config-ipsec-gdoi-group)#exit
inspur(config)#crypto ipsec-transport 1
inspur(config-ipsec-transport1)#set type gdoi
inspur(config-ipsec-transport1)#set gdoi-group g1
inspur(config-ipsec-transport1)#isakmp-profile p1
inspur(config-ipsec-transport1)#local ipv4-address 192.168.127.12
inspur(config-ipsec-transport1)#bound-to gei-5/2
inspur(config-ipsec-transport1)#exit
```

配置验证

通过命令**show crypto ipsec sa nego** 查看GM1 SA显示情况：

```
inspur(config)#show crypto ipsec sa nego
Transport: ipsec_transport1
IKE version: v1
IPsec profile tag: not configure
Local endpt:192.168.127.12Current        remote        endpt:        Local
ident(addr/mask/prot/port_min/port_max) :
(10.0.0.0/255.0.0.0/0/Invalid/Invalid)
Remote ident(addr/mask/prot/port_min/port_max) :
(10.0.0.0/255.0.0.0/0/Invalid/Invalid) Local access-list tag: not configure
FVRF: not configure IVRF: not configure Pre-fragmentation: disable Original
IP header DF-bit : ignore
SA type: negotiation by GDOI Inbound ESP SA:
SPI: 0x37580486
Authentication algorithm : Encryption algorithm: aes-128
Encapsulation mode: transport
Throughput: 0KB Remain lifetime: 66(s) Inbound AH SA:
Outbound ESP SA:
SPI: 0x37580486
Authentication algorithm : Encryption algorithm: aes-128
Encapsulation mode: transport
Throughput: 0KB Remain lifetime: 66(s) Outbound AH SA:
```

通过命令**show crypto ipsec sa nego** 查看GM2 SA显示情况：

```
inspur(config)#show crypto ipsec sa nego
Transport: ipsec_transport1
IKE version: v1
IPsec profile tag: not configure
Local endpt:192.168.127.13Current remote endpt: Local
ident(addr/mask/prot/port_min/port_max) :
(10.0.0.0/255.0.0.0/0/Invalid/Invalid)
Remote ident(addr/mask/prot/port_min/port_max) :
(10.0.0.0/255.0.0.0/0/Invalid/Invalid) Local access-list tag: not configure
FVRF: not configure IVRF: not configure Pre-fragmentation: disable Original
IP header DF-bit : ignore
SA type: negotiation by GDOI Inbound ESP SA:
SPI: 0x37580486
```

```
Authentication algorithm : Encryption algorithm: aes-128
Encapsulation mode: transport
Throughput: 0KB Remain lifetime: 57(s) Inbound AH SA:
Outbound ESP SA:
SPI: 0x37580486
Authentication algorithm : Encryption algorithm: aes-128
Encapsulation mode: transport
Throughput: 0KB Remain lifetime: 57(s) Outbound AH SA:
```

8 QoS

8.1 QoS 简介

在传统的IP网络中，所有的报文都被无区别地对待，每个路由设备对所有的报文均采用先进先出（FIFO）的策略进行处理，尽最大的努力（best-effort）将报文送到目的地，但对报文传送的可靠性、传送延迟等性能不提供任何保证。

QoS即服务质量，旨在针对各种应用的不同需求，提供不同的服务质量，如提供专用带宽、降低报文丢失率、减少报文传送时延及时延抖动等。为实现上述目的，QoS提供了下列功能：

•报文分类

•报文标记

•流量监管和流量整形

•拥塞避免

•拥塞管理

8.2 CAR

流量在报文满足一定的条件时，如某个连接的报文流量过大，流量监管就可以对该报文采取不同的处理动作，例如丢弃报文，或重新设置报文的优先级等。CAR（Committed Access Rate，约定访问速率）不仅可以进行流量控制，还可以对报文进行标记和重标记。

要实现流量的监管，必须有一种机制可以对通过设备的流量进行度量，也就是粒度控制。令牌桶是目前最常采用的一种流量测量方法，在CAR及流量整形技术中都使用该方法进行流量速率的控制。

令牌桶可以看作是一个存放令牌的容器，预先设定一定的容量。系统按用户设定的速度向桶中放置令牌，当桶中令牌满时，多余的令牌溢出，且令牌的量不再增加。令牌桶对流量的测量又分为单令牌桶测量和双令牌桶测量。

流量监管采用约定访问速率CAR来对流量进行控制。先根据预先设置的匹配规则来对报文进行分类，后依据不同的评估结果，实施预先设定好的监管动作。这些动作可以是：

•转发（transmit）：对测量结果为“符合”的报文继续正常转发的处理，也可以为Diff-Serv（差分服务）提供带有标记DSCP的服务再转发。

•丢弃（drop）：对测量结果为“不符合”的报文进行丢弃。

•重标记并转发（set）：对测量结果为“不符合”的报文，重新设置IP Precedence、DSCP或EXP值再进行转发。

8.2.1 配置 CAR

在IR12000智能路由器上配置CAR的相关功能，用来对网络中的流量进行控制达到流量监管的目的。

1.配置CAR。

步骤	命令	功能
1	`inspur(config)#`**qos**	进入QoS配置模式
2	`inspur(config-qos)#`**interface** <*interface-name*>	进入QoS接口配置模式
3	`inspur(config-qos-if-interface-name)#`**rate-limit** {**input** | **output**}{**unicast** | **broadcast** | **unknown** | **ipv4-access-list** <*acl-name*>| **ipv6-access-list** <*acl-name*>| **localport** | **dscp** <*dscp-value*>| **mpls-exp** <*mpls-exp-value*>| **precedence** <*prec-value*>| **inner-8021p** <*in8021p-value*>[**outer-8021p** <*out8021p-value*>]| **outer-8021p** <*out8021p-value*>| **inner-vlan** <*inVlan-value*>[**outer-vlan** <*outVlan-value*>]| **outer-vlan** <*outVlan-value*>} **cir** <*cir-value*> **cbs** <*cbs-value*> **pir** <*pir-value*> **pbs** <*pbs-value*> **conform-action** <*action*> **exceed-action** <*action*> **violate-action** <*action*>	在接口下应用CAR，设置接口输入或输出的流量监管策略（不指定IP类型进行配置）
	`inspur(config-qos-if)#`**rate-limit** {**input** | **output**}{**ipv4** | **ipv6**}{**dscp** <*dscp-value*>| **precedence** <*prec-value*>} **cir** <*cir-value*> **cbs** <*cbs-value*> **pir** <*pir-value*> **pbs** <*pbs-value*> **conform-action** <*action*> **exceed-action** <*action*> **violate-action** <*action*>	在接口下应用CAR，设置接口输入或输出的流量监管策略（指定IP类型进行配置）

broadcast：L2VPN广播流。

unicast：L2VPN单播流。

unknown：L2VPN未知流。

dscp <*dscp-value*>：DSCP值，取值范围0~63。

mpls-exp <*mpls-exp-value*>：MPLS-EXP值，取值范围0~7。

precedence <*prec-value*>：IP优先级值，取值范围0~7。

outer-8021p <*outer-8021p-value*>：outer-802.1p值，参数范围0~7。

inner-8021p <*inner-8021p-value*>：inner-802.1p值，参数范围0~7。

outer-vlan <*outer-vlan-value*>：outer-vlan值，参数范围1~4094。

inner-vlan <*inner-vlan-value*>：inner-vlan值，参数范围1~4094。

cir <*cir-value*>：CIR值，取值范围8~16777215。

cbs <*cbs-value*>：CBS值，取值范围2000-5120000。

pir <*pir-value*>：PIR值，取值范围8~16777215。

pbs <*pbs-value*>：PBS值，取值范围2000-5120000。

<*action*>：对符合指定速率的数据包采取的动作行为，取值为以下关键字之一。

- **drop**：丢弃数据包
- **transmit**：发送数据包
- **set-dscp-transmit**：设置DSCP值（0~63）并发送数据包
- **set-prec-transmit**：设置IP优先级值（0~7）并发送数据包
- **set-exp-transmit**：设置MPLS优先级值（0~7）并发送数据包
- **set-8021p-transmit**：设置8021p优先级值（0~7）并发送数据包

2.验证配置结果。

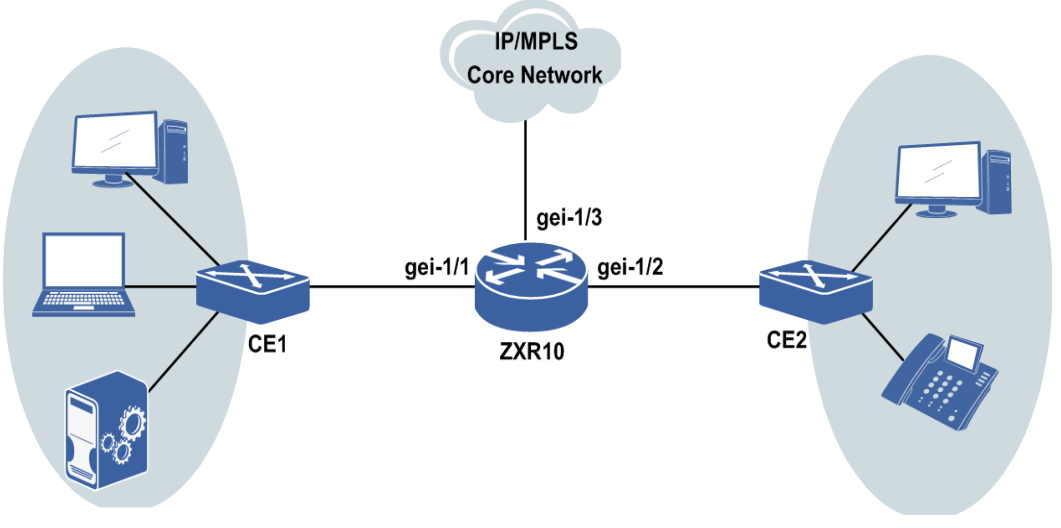
命令	功能
inspur#**show running-config car**	查看接口配置的CAR

8.2.2 CAR 配置实例

配置说明

如*图 8-1*所示，user1、user2分别从gei-1/1和gei-1/2接入，precedence分别为1和2，从gei-1/3出去。要求从gei-1/3出去的两个用户的precedence值为7，保证带宽为100M，最大带宽150M。

图 8-1 CAR 配置实例拓扑图



配置思路

在gei-1/3下行配置两个CAR，分别匹配precedence值1和2，并将通过的流量的precedence设为7。

配置过程

1.进入CAR配置模式：

```
inspur(config)#qos
inspur(config-qos)#
```

2.进入接口配置模式：

```
inspur(config-qos)#interface gei-1/3
inspur(config-qos-if-gei-1/3)#
```

3.配置CAR命令：

```
inspur(config-qos-if-gei-1/3)#rate-limit output precedence 1 cir 100000
cbs 200000 pir 150000 pbs 300000 conform-action set-prec-transmit 7
exceed-action set-prec-transmit 7 violate-action drop
inspur(config-qos-if-gei-1/3)#rate-limit output precedence 2 cir 100000
cbs 200000 pir 150000 pbs 300000 conform-action set-prec-transmit 7
exceed-action set-prec-transmit 7 violate-action drop
```

配置验证

通过**show running-config carset**命令查看接口配置的CAR：

```
inspur(config)#show running-config car
!<car>
qos
  interface gei-1/3
    rate-limit output precedence 1 cir 100000 cbs 200000 pir 150000 pbs 300000
conform-action set-prec-transmit 7 exceed-action set-prec-transmit 7 violate-
action drop
    rate-limit output precedence 2 cir 100000 cbs 200000 pir 150000 pbs 300000
conform-action set-prec-transmit 7 exceed-action set-prec-transmit 7 violate-
action drop
  $
$
!</car>
```

8.3 流分类

业务（服务）在网络中就是数据报文流，在提供业务的端对端的QoS前，需要对进入网络中的报文流进行分类和“标记”或“颜色”，以保证特殊的数据包能够得到区别的对待和处理。

8.3.1 配置流分类

对网络中的数据流进行流分类配置，分类后即可以使用QoS技术对流量进行控制与处理。

1.配置流分类。

步骤	命令	功能
1	inspur(config)#**class-map**<*class-map-name*>{**match-all** | **match-any**}	创建class-map名字并进入类映射配置模式，同时需要指定类映射的匹配方式
2	inspur(config-cmap)#**match** [**ipv4** | **ipv6**] **dscp** <*dscp-value*>[**,**<*dscp-min*>**-**<*dscp-max*>]	根据IP DSCP值来建立class-map数据流，取值范围0~63
	inspur(config-cmap)#**match** [**ipv4** | **ipv6**] **precedence** <*precedence*>[**,**<*precedence-min*>**-**<*precedence-max*>]	根据IP优先级字段来建立class-map数据流，取值范围0~7
	inspur(config-cmap)#**match mpls-exp** <*mpls-exp-value*>[**,**<*mpls-exp-min*>**-**<*mpls-exp -max*>]	根据MPLS标签包的EXP字段来建立class-map数据流，取值范围0~7
	inspur(config-cmap)#**match in-vlan** <*invlan-value*>[**,**<*invlan-min*>**-**<*invlan-max*>]	根据内层VLAN-ID来建立class-map数据流，取值范围1~4094
	inspur(config-cmap)#**match out-vlan** <*exvlan-value*>[**,**<*exvlan-min*>**-**<*exvlan-max*>]	根据外层VLAN-ID来建立class-map数据流，取值范围1~4094
	inspur(config-cmap)#**match in-8021p**<*in8021p-value*>[**,**<*in8021p-min*>**-**<*in8021p-max*>]	根据内层802.1p来建立class-map数据流，取值范围0~7
	inspur(config-cmap)#**match out-8021p**<*ex8021p-value*>[**,**<*ex8021p-min*>**-**<*ex8021p-max*>]	根据外层802.1p来建立class-map数据流，取值范围0~7
	inspur(config-cmap)#**match qos-group**<*qos-id*>	根据QoS ID值来建立class-map数据流
	inspur(config-cmap)#**match vrf-name**<*vrf-name*>	根据vrf-name来建立class-map数据流
	inspur(config-cmap)#**match uni-cast**	根据单播规则来建立class-map数据流
	inspur(config-cmap)#**match multi-cast**	根据组播规则来建立class-map数据流
	inspur(config-cmap)#**match mac-address**<*mac-address*>	根据mac-address值来建立class-map数据流
	inspur(config-cmap)#**match ipv4-access-list**<*acl4-name*>	根据ipv4-access-list来建立class-map数据流
	inspur(config-cmap)#**match ipv6-access-list** <*acl6-name*>	根据ipv6-access-list来建立class-map数据流
	inspur(config-cmap)#**match child**	标识匹配项为空的class-map数据流

配置流分类需要注意以下事项：

- 在Match-all模式下，**match dscp**与**match precedence**是冲突的；**match uni-cast**与**match multi-cast**是冲突的；**match child**与其它所有匹配规则是冲突的。
- Class map在创建时必须先指定match模式。
- 配置为**match all**，一个class-map下的多个match项之间是**match all**的关系，但是一个match项的多个match数值之间是**match any**的关系。

2.验证配置结果。

命令	功能
inspur#**show class-map** [<*class-map-name*>]	显示所有类映射及其所有匹配规则设置

8.3.2 空规则的流分类配置实例

配置说明

1.配置流分类时，match child与其它所有匹配规则冲突。如果配置了match条件是match child，则不能再配置任何其他的match条件，反之亦然。

2.在IR12000智能路由器设备上，流分类是在policy-map（基于流分类的流策略）当中使用的，也就是说每个策略生效的对象是某个类别的流量，而这个类别由class-map来定义。因为流策略可以多层嵌套使用，所以根据class-map所在的层级不同，match child的含义有如下区别：

- 如果以match child作为分类标准的流分类使用在单层流策略，则表示本策略中策略生效的对象（即class-map）的匹配规则为空，所有报文都归入本类。
- 如果以match child作为分类标准的流分类使用在多层流策略的非底层策略中，则表示凡是能进入本层级的流量都能归入本类，以下各层已经匹配过的流量在当前层次上不再进行区分，在本层汇聚为一类class-map。
- 一般match child的流分类不用于多层策略的底层。

配置思路

1.创建流分类，创建时指定名称为ipv4-all，指定匹配方式为match all，指定协议栈是IPv4。

2.给上述创建的流分类添加match条件，指定**match child**作为分类条件。

配置过程

IR12000智能路由器上配置如下：

```
inspur(config)#class-map ipv4-all match-all
inspur(config-cmap)#match child
inspur(config-cmap)#exit
```

配置验证

查看设备上所有的流分类：

```
inspur(config)#show class-map
class-map ipv4-all match-all
  match child
inspur(config)#
```

查看指定的流分类（指定查看ipv4-all流分类的class-map）：

```
inspur(config)#show class-map ipv4-all
class-map ipv4-all match-all
  match child
inspur(config)#
```

8.3.3 基于 EXP 的流分类配置实例

配置说明

1.指定mpls-exp的值可以有3种不同的方法：指定单一值，指定多个值，指定区间值。这三种方法可以任选其一。

2.和大部分match条件一样，不能在一个class-map当中配置多个以mpls-exp为分类标准的match语句。如有这样的配置，将报错提示用户。

3.match mpls-exp与match child互斥。

配置思路

1.创建流分类，创建时指定名称，指定匹配方式为**match all**，缺省协议栈配置，默认为同时支持IPv4/IPv6。

2.给这个流分类添加match条件，指定分类条件是match指定的mpls-exp。

配置过程

·match mpls-exp单一值：配置名为exp，匹配方式为match all，缺省协议栈配置，默认为同时支持IPv4/IPv6的流分类，分类条件是match 单一mpls-exp值。

```
inspur(config)#class-map exp match-all
inspur(config-cmap)#match mpls-exp 1
inspur(config-cmap)#exit
```

·match mpls-exp范围区间：配置名为exp1，匹配方式为match all，缺省协议栈配置，默认为同时支持IPv4/IPv6的流分类，分类条件是对于一个指定的mpls-exp范围区间，报文的相关字段match其一即可。

```
inspur(config)#class-map exp1 match-all
inspur(config-cmap)#match mpls-exp 0-4
inspur(config-cmap)#exit
```

·match mpls-exp多个值：在一个match mpls-exp语句中支持指定多个值，这个值可以是单一值，也可以是区间值（连续的单值会自动合并为一个区间）。本例分别示范配

置4个单一值，以及混合配置单一值与区间值。

配置名为exp2，匹配方式为match all，缺省协议栈配置，默认为同时支持IPv4/IPv6的流分类，分类条件是match 4个单一mpls-exp值。

```
inspur(config)#class-map exp2 match-all
inspur(config-cmap)#match mpls-exp 0,2,4,7
inspur(config-cmap)#exit
```

配置名为exp3，匹配方式为match all，缺省协议栈配置，默认为同时支持IPv4/IPv6的流分类，match 2个单一mpls-exp值和1个mpls-exp区间。

```
inspur(config)#class-map exp3 match-all
inspur(config-cmap)#match mpls-exp 0,2-5,7
inspur(config-cmap)#exit
```

配置验证

•验证match mpls-exp单一值：

```
inspur(config)#show class-map
class-map exp match-all
  match mpls-exp 1
inspur(config)#
```

•验证match mpls-exp范围区间：

```
inspur(config)#show class-map exp1
class-map exp1 match-all
  match mpls-exp 0-4
/*如果指定的mpls-exp是一个范围，则表示报文的mpls-exp的值符合其中之一，就可以划分为该类别*/
```

•验证match mpls-exp多个值：

验证配置class-map exp2：

```
inspur(config)#show class-map exp2
class-map exp2 match-all
  match mpls-exp 0,2,4,7
```

验证配置class-map exp3：

```
inspur(config)#show class-map exp3
class-map exp3 match-all
  match mpls-exp 0,2-5,7
```

8.3.4 基于 MAC 地址的流分类配置实例

配置说明

1.L2VPN环境下，进行基于MAC地址的流分类配置

2.L2VPN以太私网报文有源MAC和目的MAC，对于发送方来说，可以对目的MAC进行流分类，对于接收方来说，可以对源MAC进行流分类。

3.在配置流分类中基于mac_address的分类准则时并不指定是对源MAC分类还是对目的MAC分类。class-map被policy-map调用后，根据这个policy-map绑定在interface的input/output方向决定是对源MAC匹配还是对目的MAC匹配。绑定在input方向，则class-map当中的match mac_address条件对源MAC分类，绑定在output方向则对目的

MAC分类。

4.match mac_address与match child互斥。

配置思路

1.创建流分类，创建时指定名称为mac_address，指定匹配方式为match all，缺省协议栈配置，默认为同时支持IPv4/IPv6。

2.给这个流分类添加match条件，指定分类条件是match指定的MAC地址。

配置过程

1.创建名为mac_address的流分类：

```
PE1(config)#class-map mac_address match-all
/*创建class-map时，对协议族参数缺省配置，表示同时支持IPv4和IPv6*/
```

2.配置match条件如下：

```
PE1(config-cmap)#match mac-address 0010.9400.0002
/*MAC地址用点分16进制书写*/
PE1(config-cmap)#exit
```

配置验证

验证配置的基于MAC地址的分类：

```
PE1(config)#show class-map mac_address
class-map mac_address match-all
  match mac-address 0010.9400.0002
PE1(config)#
```

8.3.5 基于 IPv4 ACL 的流分类配置实例

配置说明

1.在同一个class-map中如果有相同类型的匹配项时，不允许再进行同种类型的匹配项配置，除非先将原来的匹配项删掉才能重新配置。但是匹配ACL除外，同一个class-map中最多可以match 64个ipv4-acl。

2.如果在一个class-map中配置匹配多个ACL列表，则匹配任意一个ACL即可划入当前的class-map。

3.match ipv4-access-list与match child互斥。

配置思路

1.创建流分类，创建时指定名称为v4_sip，指定匹配方式为match all，指定协议栈是

IPv4。

2.给这个流分类添加match条件，指定分类条件是match名为v4_sip的ipv4-access-list。

3.配置名为v4_sip的ipv4-access-list，在这个IPv4的ACL列表当中指定permit源地址为100.1.1.128的流量。

配置过程

创建名为v4_sip的class-map并配置match条件如下：

```
inspur(config)#class-map v4_sip match-all
inspur(config-cmap)#match ipv4-access-list v4_sip
inspur(config-cmap)#exit
inspur(config)#
```

创建名为v4_sip的ipv4-access-list并指定流量：

```
inspur(config)#ipv4-access-list v4_sip
inspur(config-ipv4-acl)#rule permit 100.1.1.128
inspur(config-ipv4-acl)#exit
```

配置验证

1.查看指定名称的ipv4-access-list：

```
inspur(config)#show ipv4-access-lists name v4_sip
ipv4-access-list v4_sip
 1/1 (showed/total)
   10 permit 100.1.1.128 0.0.0.0
inspur (config)#
```

2.查看指定名称的class-map

```
inspur(config)#show class-map v4_sip
class-map v4_sip match-all
  match ipv4-access-list v4_sip
inspur(config)#
```

8.3.6 匹配方式为 match-any 的流分类配置实例

配置说明

1.如果创建流分类时选择的匹配方式为match-any，那么流量只要和这个class-map当中的任意一个条件匹配，就可以划分到此类别当中。

2.Match-any方式的class-map内，match child和其他匹配项互斥。

3.Match-any方式的class-map当中同类型的匹配项只能配置一个（ACL除外）。

配置思路

1.创建一个名为anyone，匹配方式为match any，对IPv4/IPv6报文生效的流分类。分类标准当中配置多个匹配条件，效果为匹配其中之一即可划分为此类。

2.添加匹配条件a：匹配名为v4_sip的ipv4-access-list，在此IPv4的ACL列表当中指定permit源地址为100.1.1.128的流量。

3.添加匹配条件b：匹配mac_address，指定MAC为0010.9400.0002。

配置过程

IR12000智能路由器上配置如下：

```
inspur(config)#class-map anyone match-any
inspur(config-cmap)#match ipv4-access-list v4_sip
inspur(config-cmap)#match mac-address 0010.9400.0002
inspur(config-cmap)#exit
```

其中match的名为v4_sip的ipv4-access-list配置如下：

创建名为v4_sip的ipv4-access-list并指定流量。

```
inspur(config)#ipv4-access-list v4_sip
inspur(config-ipv4-acl)#rule permit 100.1.1.128
inspur(config-ipv4-acl)#exit
```

配置验证

查看指定名称的ipv4-access-list：

```
inspur(config)#show ipv4-access-lists name v4_sip
ipv4-access-list v4_sip
 1/1 (showed/total)
   10 permit 100.1.1.128 0.0.0.0
inspur(config)#
```

查看指定名称的class-map：

```
inspur(config)#show class-map anyone
class-map anyone match-any
  match ipv4-access-list v4_sip
  match mac-address 0010.9400.0002
```

8.4 流行为

流行为包括了报文标记、流量监管和流量整形、拥塞避免和拥塞管理。

8.4.1 配置流行为

对网络中的流量报文进行流行为配置，用来针对不同的应用需求提供不同的服务质量。

1.配置流行为。

步骤	命令	功能

步骤	命令	功能
1	inspur(config)#**policy-map** <*policy-map-name*>	创建policy-map名字并进入策略映射配置模式
2	inspur(config-pmap)#**class** <*class-map-name*>	关联class-map名字并进入策略类配置模式
3	inspur(config-pmap-c)#**bandwidth percent** <*percentage*>	配置策略类的最小可用带宽（百分比），取值范围1~100
	inspur(config-pmap-c)#**priority-level** <*pq-level*>	配置策略类的PQ优先级，取值范围1~4
	inspur(config-pmap-c)#**priority-llq**	配置策略类的LLQ优先
	inspur(config-pmap-c)#**police cir** <*cir-value*> **cbs** <*cbs-value*>[**pir** <*pir-value*> **pbs** <*pbs-value*>] **conform-action** <*action*> **exceed-action** <*action*> **violate-action** <*action*>	配置策略类的流量监管 <*cir*>取值范围8~20000000，单位kbit/s <*cbs*>取值范围2-250000000，单位kbytes <*pir*>取值范围8~20000000，单位kbit/s <*pbs*>取值范围2-250000000，单位kbytes
	inspur(config-pmap-c)#**set dscp** {<*dscp-value*>| **inherit-from** {**dscp**	**precedence**	**8021p**	**mpls-exp**}}	设置策略类使用指定值标记报文的DSCP字段
	inspur(config-pmap-c)#**set precedence** {<*ipp-value*>| **inherit-from** { **dscp**| **precedence**	**8021p**	**mpls-exp**}}	设置策略类使用指定值标记报文的IP优先级字段
	inspur(config-pmap-c)#**set 8021p** {<*8021p-value*>| **inherit-from** {**dscp**| **precedence**	**8021p**	**mpls-exp**}}	设置策略类使用指定值标记报文的802.1p字段
	inspur(config-pmap-c)#**set mpls-exp** {<*exp-value*>| **inherit-from** {**dscp**| **precedence**	**8021p**	**mpls-exp**}}	设置策略类使用指定值标记报文的MPLS-EXP字段
	inspur(config-pmap-c)#**random-detect enable**	设置策略类的WRED使能动作
	inspur(config-pmap-c)#**random-detect weight** <*weight-len*>	配置策略类的WRED的平均队列长度
	inspur(config-pmap-c)#**random-detect precedence** <*precedence*><*min-threshold*><*max-threshold*><*probability*>	配置策略类的WRED的基于IP Precedence的WRED参数 <*min-threshold*>，WRED的下限，取值范围1~1024000，单位是Kilo bytes <*max-threshold*>，WRED的上限，取值范围1~1024000，单位是Kilo bytes <*probability*>，WRED的丢弃概率，取值范围1~100
	inspur(config-pmap-c)#**service-policy**	配置策略类的层次化策略

步骤	命令	功能
	<*policy-map-name*>	
4	inspur(config)#**service-policy** <*interface-name*>{**input** | **output**}<*policy-map-name*>	在接口上绑定策略映射

配置流行为时需要注意以下一些事项：

- Set dscp与set precedence是冲突的。
- Bandwidth与priority-level动作在一个policy-map下是互斥的，默认队列除外。
- 当配置priority的调度关系时，一共可以指定4个优先级（不包括默认优先级）。该端口上的不匹配QoS策略的报文会进入默认队列。
- 当配置bandwidth的调度关系时，用户可以显式指定一个默认Class并配置权重。当用户不显式配置时，该端口上的不匹配QoS策略的报文会进入一个默认的Class，该Class与已配置的其他Class一样参与WFQ调度。
- 当配置police时，必须要带后面的动作，包括conform-action，exceed-action和violate-action。

2.配置流量整形。

命令	功能
inspur(config)#**traffic-shape** <*interface-name*> **rate** <*rate*><*cbs*><*ebs*>	配置接口的流量整形 <*rate-value*>取值范围8~10000000，单位kbit/s <*cbs*>取值范围2-250000000，单位kbytes <*ebs*>取值范围2-250000000，单位kbytes

3.验证配置结果。

命令	功能
inspur#**show class-map** [<*class-map-name*>]	显示所有类映射及其所有匹配规则设置
inspur#**show policy-map** [<*policy-map-name*>[**class** <*class-name*>]]	显示所有策略映射及其所有策略类的配置
inspur#**show service-policy** [<*interface-name*>]	显示所有接口下的策略绑定

8.4.2 报文标记配置实例

配置说明

1.标记功能支持对报文的如下字段进行标记：

- set 802.1p，对2层头部的802.1p字段进行标记
- set precedence/set dscp，对3层头部的precedence(0-7)/ dscp(0-63)字段
- set mpls-exp，对标签报文的mpls-exp字段标记

2.其中set dscp和set precedence互斥，其它项可以同时配置。

3.一个策略类中配置有多种set项时，其中set mpls-exp对匹配到的标签流生效，set precedence或set dscp对匹配到的普通v4流量生效，set 802.1p对匹配到的所有流量生效。

4.本例示范配置set 8021p 、set mpls-exp、set precedence。

配置思路

1.创建策略（policy-map），命名为mark。

2.对该policy-map指定一个流分类（为保证这个流分类有可能同时匹配到标签报文和普通报文，这个流分类可以选择以match mac-address/match child为分类条件的class-map）后，在策略类配置模式下配置set mpls-exp和set precedence的策略。

配置过程

1.配置基于match child的流分类：

```
inspur(config)#class-map child match-all
inspur(config-cmp)#match child
inspur(config-cmap)#exit
```

2.配置策略：

```
inspur(config)#policy-map mark
inspur(config-pmap)#class child
inspur(config-pmap-c)#set 8021p 5
inspur(config-pmap-c)#set mpls-exp 7
inspur(config-pmap-c)#set precedence 2
inspur(config-pmap-c)#set dscp 0
%Error 5553: The set dscp is incompatible with the set precedence in the
 same policy class, please check!
inspur(config-pmap-c)#exit
```

配置验证

验证配置的报文标记：

```
inspur(config)#show policy-map mark
policy-map mark
  class child
    set 8021p 5
    set mpls-exp 7
    set precedence 2
inspur(config)#
```

8.4.3 流量监管配置实例

配置说明

1.流量监管（Police）支持配置两种速率：承诺速率（cir）和峰值速率（pir），以及速率各自的突发尺寸（CBS和PBS）。

2.CIR和PIR以每秒钟的IP数据包所包含字节数来度量，单位是Kilo bits per second，PIR的值必须大于等于CIR的。

3.突发尺寸PBS和CBS是指在瞬间流量未达到指定速率的时候，余量可以用于处理这个时刻前后收到的其它流量。

4.PBS和CBS以每秒钟的IP数据包所包含字节数来度量，单位是Kilo bytes。在设置时，应注意将PBS和CBS的值设置为大于等于可能通过的IP数据包的最大字节数。

配置思路

1.创建策略（policy-map），命名为police。

2.对该policy-map指定一个流分类后，在策略类配置模式下配置police限速。

配置过程

IR12000智能路由器上配置流量监管：

```
inspur(config)#policy-map police
inspur(config-pmap)#class exp3
inspur(config-pmap-c)#police cir 100000 cbs 10 pir 120000 pbs 10
conform-action transmit exceed-action transmit violate-action drop
/*对匹配到class exp3的流量进行流量监管，保证100000Kb(100M)速率，
最大峰值速率120000Kb(120M)，令牌桶的尺寸都为10Kbytes*/
inspur(config-pmap-c)#exit
inspur(config-pmap)#exit
```

配置验证

验证配置的流量监管：

```
inspur(config)#show policy-map police
policy-map police
  class exp3
    police cir 100000 cbs 10 pir 120000 pbs 10
conform-action transmit exceed-action transmit violate-action drop
inspur(config)#
```

8.4.4 PQ 队列调度配置实例

配置说明

1.队列调度种类有多种：先进先出FIFO、PQ、WFQ、CBWFQ等，调度技术从根本上说是为了实现拥塞管理，当流量不超过带宽时调度对流量没有任何影响。

2.IR12000智能路由器支持的各种队列调度当中，除了默认的FIFO（先进先出）队列，其他的队列都是基于分类报文进行调度的。在配置policy-map时，在配置策略类（class-map）后可以设置对当前类别的流量指定优先级。

3.PQ调度也叫做优先级调度，有4种优先级，每个类别的报文对应一个优先级。总是最高优先级的报文优先得到发送，等到高优先级队列当中的报文发送完毕，才进行下一个优先级报文的发送。

4.由于PQ总是保证高优先级的报文得到优先转发，所以当高优先级的流量过多时，可能会造成低优先级的流量没有转发机会，所以使用PQ调度时应该合理规划各个优先级的流量，适当限制高优先级的流量，使低优先级的流量也获得发送机会。

5.PQ和Bandwith percent是互斥的配置，即一个policy-map当中基于优先级的调度和基于带宽的调度只能选用一种。

配置思路

1.本例示范的是配置基于PQ优先级的队列调度（priority-level）。

2.根据配置说明，对各种优先级的报文配置了由高到低的不同限速（police），既保证高优先级的报文能够得到优先发送，又能保证低优先级的报文获得一定的发送机会。

3.这个配置实例适合应用在MPLS转发环境，根据标签的mpls-exp字段的不同值进行分类和优先级设置，可达到如下效果：

- mpls-exp为1的报文优先级最高，且限速100 M。
- mpls-exp为2的报文优先级次之，且限速50 M。
- mpls-exp为3的报文优先级最低，限速30 M。
- 除此以外的报文不受影响，正常转发。

配置过程

1.配置流分类，备用于policy-map当中的策略类指定：

```
inspur(config)#class-map exp1 match-all
inspur(config-cmap)#match mpls-exp 1
inspur(config-cmap)#exit
inspur(config)#class-map exp2 match-all
inspur(config-cmap)#match mpls-exp 2
inspur(config-cmap)#exit
inspur(config)#class-map exp4 match-all
inspur(config-cmap)#match mpls-exp 3
inspur(config-cmap)#exit
```

2.配置policy-map，指定名称为pq，将上一步骤配置的流分类指定为此处的策略类，配置具体的PQ和police：

```
inspur(config)#policy-map pq
inspur(config-pmap)#class exp1
inspur(config-pmap-c)#priority-level 1
inspur(config-pmap-c)#police cir 100000 cbs 100
conform-action transmit exceed-action drop violate-action drop
inspur(config-pmap-c)#exit
inspur(config-pmap)#class exp2
inspur(config-pmap-c)#priority-level 2
inspur(config-pmap-c)#police cir 50000 cbs 50
conform-action transmit exceed-action drop violate-action drop
inspur(config-pmap-c)#exit
inspur(config-pmap)#class exp4
inspur(config-pmap-c)#priority-level 3
inspur(config-pmap-c)#police cir 30000 cbs 30
conform-action transmit exceed-action drop violate-action drop
inspur(config-pmap-c)#exit
inspur(config-pmap)#exit
```

配置验证

验证配置的PQ队列调度：

```
inspur(config)#show class-map
class-map exp1 match-all
  match mpls-exp 1
class-map exp2 match-all
  match mpls-exp 2
class-map exp4 match-all
  match mpls-exp 3

inspur(config)#show policy-map pq
policy-map pq
  class exp1
    police cir 100000 cbs 100
conform-action transmit exceed-action drop violate-action drop
    priority-level 1
  class exp2
    police cir 50000 cbs 50
conform-action transmit exceed-action drop violate-action drop
    priority-level 2
  class exp4
    police cir 30000 cbs 30
conform-action transmit exceed-action drop violate-action drop
    priority-level 3
```

8.4.5 WFQ 调度配置实例

配置说明

1.WFQ调度也是基于流分类的调度。每个流分类对应一个WFQ队列，各个队列之间是平等的关系，没有优先级的区分，出队列是按照特定的权值进行调度。队列的权值通过一定的算法实现，这样在公平的基础上对不同优先级的业务实现了区别对待。

2.一个policy-map下的所有策略类当中，设置的bandwith percent总和不能超过100。

3.Bandwith percent和PQ是互斥的配置，即一个policy-map当中基于带宽的调度和基于优先级的调度只能选用一种。

4.配置WFQ队列后，接口流量在不拥塞的情况下正常转发通过。出现拥塞时，按照配置的加权值对带宽进行分配，未匹配的流量可以占用剩余带宽权值。

配置思路

1.根据报文的IPP（ip precedence）字段将报文分为4类。

2.配置名为WFQ的policy-map，指定：

- ipp为1的报文，bandwidth为30。
- ipp为2的报文，bandwidth为30。
- ipp为3的报文，bandwidth为20。
- ipp为4的报文，bandwidth为20。

3.这样配置后，这四种报文预定了100的bandwith资源，未匹配的的流量不能够被转发。

配置过程

1.配置class分类：

```
inspur(config)#class-map pre1 match-all
inspur(config-cmap)#match precedence 1
inspur(config-cmap)#exit
inspur(config)#class-map pre2 match-all
inspur(config-cmap)#match precedence 2
inspur(config-cmap)#exit
inspur(config)#class-map pre3 match-all
inspur(config-cmap)#match precedence 3
inspur(config-cmap)#exit
inspur(config)#class-map pre4 match-all
inspur(config-cmap)#match precedence 4
inspur(config-cmap)#exit
```

2.配置policy-map，指定的名称为WFQ：

```
inspur(config)#policy-map WFQ
inspur(config-pmap)#class pre1
inspur(config-pmap-c)#bandwidth percent 30
inspur(config-pmap-c)#exit
inspur(config-pmap)#class pre2
inspur(config-pmap-c)#bandwidth percent 30
inspur(config-pmap-c)#exit
inspur(config-pmap)#class pre3
inspur(config-pmap-c)#bandwidth percent 20
inspur(config-pmap-c)#exit
inspur(config-pmap)#class pre4
inspur(config-pmap-c)#bandwidth percent 20
inspur(config-pmap-c)#exit
inspur(config-pmap)#exit
```

配置验证

用**show class-map**命令验证class-map配置是否正确：

```
inspur(config)#show class-map
```

```
class-map pre1 match-all
  match precedence 1
class-map pre2 match-all
  match precedence 2
class-map pre3 match-all
  match precedence 3
class-map pre4 match-all
  match precedence 4
```

用**show policy-map**命令验证策略配置是否正确：

```
inspur(config)#show policy-map WFQ
policy-map WFQ
  class pre1
    bandwidth percent 30
  class pre2
    bandwidth percent 30
  class pre3
    bandwidth percent 20
  class pre4
    bandwidth percent 20
```

8.4.6 CBWFQ 调度配置实例

配置说明

1.CBWFQ也是基于流分类的队列调度技术。每个流量对应一个队列。通常配置一个队列为LLQ队列（优先带宽保证队列），其他队列为WFQ队列。

2.CBWFQ中为LLQ队列指定的带宽通常是指在带宽拥塞时为该队列所保证的带宽。剩下的带宽，调度器按照权值分配给每个WFQ队列。

3.这样，在端口不发生拥塞的情况下，可以使各个流量类别的报文能完全转发，在端口拥塞的情况下，又可以保证属于优先队列的报文不会占用超出规定的带宽，保护其他报文得到相应的带宽。

配置思路

1.假设有四个用户的流量，不同用户的ip precedence字段值不相同，分别为1、2 、3和4，对此特征可以配置四个class进行分类

2.配置policy-map，可以命名为CBWFQ，其中：

- User1为LLQ队列，并限速500 M。
- User2为WFQ队列，bandwidth为30。
- User3为WFQ队列，bandwidth为20。
- User4为WFQ队列，bandwidth为10。

配置过程

1.配置class分类：

```
inspur(config)#class-map pre1 match-all
```

```
inspur(config-cmap)#match precedence 1
inspur(config-cmap)#exit
inspur(config)#class-map pre2 match-all
inspur(config-cmap)#match precedence 2
inspur(config-cmap)#exit
inspur(config)#class-map pre3 match-all
inspur(config-cmap)#match precedence 3
inspur(config-cmap)#exit
inspur(config)#class-map pre4 match-all
inspur(config-cmap)#match precedence 4
inspur(config-cmap)#exit
```

2.配置policy-map，指定名称为CBWFQ，对不同客户的流分类配置CBWFQ调度：

```
inspur(config)#policy-map CBWFQ
inspur(config-pmap)#class pre1
inspur(config-pmap-c)#priority-llq
inspur(config-pmap-c)#police cir 500000 cbs 500
conform-action transmit exceed-action drop violate-action drop
inspur(config-pmap-c)#exit
inspur(config-pmap)#class pre2
inspur(config-pmap-c)#bandwidth percent 30
inspur(config-pmap-c)#exit
inspur(config-pmap)#class pre3
inspur(config-pmap-c)#bandwidth percent 20
inspur(config-pmap-c)#exit
inspur(config-pmap)#class pre4
inspur(config-pmap-c)#bandwidth percent 10
inspur(config-pmap)#exit
```

配置验证

用**show class-map**命令验证class-map配置是否正确：

```
inspur(config)#show class-map
class-map pre1 match-all
  match precedence 1
class-map pre2 match-all
  match precedence 2
class-map pre3 match-all
  match precedence 3
class-map pre4 match-all
  match precedence 4
```

用**show policy-map**命令验证策略配置是否正确：

```
inspur(config)#show policy-map CBWFQ
policy-map CBWFQ
  class pre1
    priority-llq
    police cir 500000 cbs 500
conform-action transmit exceed-action drop violate-action drop
  class pre2
    bandwidth percent 30
  class pre3
    bandwidth percent 20
  class pre4
    bandwidth percent 10
```

8.4.7 WRED 配置实例

配置说明

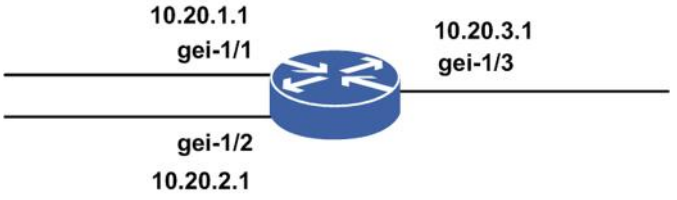
如*图 8-2*所示，在接口的上行配置WRED策略，使得不同的优先级报文在发生拥塞时有不同的丢弃策略。其中：

1.优先级为0的队列最低丢弃门限为30 kb，最高丢弃门限为100 kb，丢弃概率为90%，平均队列长度的指数为8。

2.优先级为1的队列最低丢弃门限为120 kb，最高丢弃门限为200 kb，丢弃概率为80%，平均队列长度的指数为8。

3.优先级为2的队列最低丢弃门限为220 kb，最高丢弃门限为300 kb，丢弃概率为70%，平均队列长度的指数为8。

图 8-2 WRED 配置实例拓扑图



配置思路

1.建立一个新的class-map，匹配precedence 0-2。

2.建立一个新的policy-map，在策略中加入新建的匹配precedence 0-2的class类，在类中对不同的优先级队列加入WRED。

3.将第2步中的policy-map策略绑在接口的出方向。

配置过程

1.配置class分类。

```
inspur(config)#class-map pr0-2 match-all
inspur(config-cmap)#match precedence 0-2
inspur(config-cmap)#exit
```

2.创建policy-map，指定名称为WRED，配置PQ队列和随机检测。

```
inspur(config)#policy-map wred
inspur(config-pmap)#class pr0-2
inspur(config-pmap-c)#priority-level 1
inspur(config-pmap-c)#random-detect enable
inspur(config-pmap-c)#random-detect weight 8
inspur(config-pmap-c)#random-detect precedence 0 30 100 90
inspur(config-pmap-c)#random-detect precedence 1 120 200 80
inspur(config-pmap-c)#random-detect precedence 2 220 300 70
inspur(config-pmap-c)#exit
inspur(config-pmap)#exit
```

3.将策略绑定到接口。

```
inspur(config)#service-policy gei-1/3 output wred
```

配置验证

用**show class-map**命令验证class-map配置是否正确：

```
inspur(config)#show class-map
class-map pr0-2 match-all
  match precedence 0-2
```

用**show policy-map**命令验证策略配置是否正确：

```
inspur(config)#show policy-map
policy-map wred
  class pr0-2
    random-detect enable
    random-detect weight 8
    random-detect precedence 0 30 100 90
    random-detect precedence 1 120 200 80
    random-detect precedence 2 220 300 70
 priority-level 1
```

用**show service-policy**验证绑定接口是否正确：

```
inspur#show service-policy
service-policy gei-1/3 output wred
```

8.4.8 流量整形配置实例

配置说明

如*图 8-3*所示，在接口的下行配置流量整形，使得下行接口流量能够平缓发送出去。

图 8-3 流量整形配置实例拓扑图



配置思路

在下行接口配置流量整形，使得下行接口流量平缓发送。

配置过程

在下行接口绑定流量整形：

```
inspur(config)#traffic-shape gei-1/2 rate 10000 10 10
```

配置验证

用**show running-config hqos**命令验证配置是否正确：

```
inspur(config)#show  running-config hqos
!<hqos>
traffic-shape gei-1/2 rate 10000 10 10
!</hqos>
```

8.5 H-QoS

H-QoS（Hierarchy-QoS，层次化QoS）可以根据实际需要，设置调度器之间的层次关系。H-QoS通过多级逻辑调度器，由上级调度器控制一组下级调度器的总带宽，且上级调度器能够根据下级调度器的级别和权重合理分配下级调度器的承诺带宽（CIR）和峰值带宽（PIR）。

8.5.1 配置 H-QoS

用户可以根据需要在IR12000智能路由器上配置H-QoS的功能，对流量进行层次化调度。

1.配置H-QoS。

命令	功能
inspur(config)#**service-policy** <*interface-name*>{**input** | **output**}<*policy-map-name*>	在接口上绑定策略映射

2.验证配置结果。

命令	功能
inspur#**show class-map** [<*class-map-name*>]	显示所有类映射及其所有匹配规则设置
inspur#**show policy-map** [<*policy-map-name*>[**class** <*class-name*>]]	显示所有策略映射及其所有策略类的配置
inspur#**show service-policy** [<*interface-name*>]	显示所有接口下的策略绑定
inspur#**show running-config hqos**	显示配置的class-map、policy-map信息

提示：

H-QoS目前不支持队列调度，仅支持多级流量监管。

8.5.2 H-QoS 配置实例

配置说明

如*图 8-4*所示，gei-1/1接入两种流量voice和data，分别要求如下：

·voice和data的总带宽400k。

·voice保证速率150k，可以大于150k。

·data保证速率250k，可以大于250k。

图 8-4 H-QoS 配置实例拓扑图



配置思路

1.在gei-1/2下行配置H-QoS，这样可以保证每种流量的带宽。

2.两种流量的precedence分别为1和2，配置两个class进行分类。

3.总带宽限速为400k，并配置下一层policy进行限速。

4.在第二层policy中，voice流量的cir=150k，pir=400k；data流量的cir=250k，pir=400k。

配置过程

1.接口配置

```
inspur(config)#interface gei-1/1
inspur(config-if-gei-1/1)#ip address 10.20.1.1 255.255.255.0
inspur(config-if-gei-1/1)#exit
inspur(config)#interface gei-1/2
inspur(config-if-gei-1/2)#ip address 10.20.2.1 255.255.255.0
inspur(config-if-gei-1/2)#exit
```

2.配置class分类：

```
inspur(config)#class-map hqos match-all
inspur(config-cmp)#match child
inspur(config-cmp)#exit
inspur(config)#class-map voice match-all
inspur(config-cmp)#match precedence 1
inspur(config-cmp)#exit
inspur(config)#class-map data match-all
inspur(config-cmp)#match precedence 2
inspur(config-cmp)#exit
```

3.配置第二层的policy：

```
inspur(config)#policy-map car1
inspur(config-pmap)#class voice
inspur(config-pmap-c)#police cir 150 cbs 15 pir 400 pbs 40 conform-action
```

```
  transmit exceed-action transmit violate-action drop
  inspur(config-pmap-c)#exit
  inspur(config-pmap)#class data
  inspur(config-pmap-c)#police cir 250 cbs 25 pir 400 pbs 40 conform-action
  transmit exceed-action transmit violate-action drop
  inspur(config-pmap-c)#exit
  inspur(config-pmap)#exit
```

4.配置第一层的policy：

```
  inspur(config)#policy-map test
  inspur(config-pmap)#class hqos
  inspur(config-pmap-c)#police cir 400 cbs 40 conform-action
  transmit exceed-action drop violate-action drop
  inspur(config-pmap-c)#service-policy car1
  inspur(config-pmap-c)#exit
  inspur(config-pmap)#exit
```

5.将策略绑定到接口：

```
  inspur(config)#service-policy gei-1/2 output test
```

配置验证

用**show class-map**命令验证class-map配置是否正确：

```
inspur(config)#show class-map
class-map hqos match-all
match child
class-map voice match-all
match precedence 1
class-map data match-all
match precedence 2
```

用**show policy-map**命令验证策略配置是否正确：

```
inspur(config)#show policy-map
policy-map car1
 class voice
 police cir 150 cbs 15 pir 400 pbs 40 conform-action transmit exceed-action
transmit violate-action drop
 class data
 police cir 250 cbs 25 pir 400 pbs 40 conform-action transmit exceed-action
transmit violate-action drop
policy-map test
 class hqos
 police cir 400 cbs 40 conform-action transmit exceed-action drop
violate-action drop
 service-policy car1
```

用**show service-policy**验证绑定接口是否正确：

```
inspur#show service-policy
service-policy gei-1/2 output test
```

8.6 优先级继承

优先级继承是QoS模块的重要功能之一，IR12000智能路由器系列设备实现了各种类型数据包（普通IP包、VLAN包和MPLS包）之间的优先级继承，亦即实现了IP-Precedence、VLAN-802.1p和MPLS-EXP之间的相互转换。

优先级继承包括两大类：

·二层到三层的优先级字段的继承

·MPLS-EXP到IP优先级字段的映射

8.6.1 配置优先级继承

在IR12000智能路由器上配置优先级继承功能，实现各种类型数据包之间的优先级继承。

1.在接口上配置EXP-IPP优先级继承和802.1p继承。

步骤	命令	功能
1	inspur(config)#**mls-qos-mode** <*interface-name*>{**uniform** | **pipe** | **short-pipe**}	在指定的接口上配置优先级继承
2	inspur(config)#**qos-dot1p** <*interface-name*>[**cvlan-in**]	在指定的接口上配置802.1p继承
3	inspur(config)#**ttl-qos-mode** <*interface-name*>{**uniform** | **pipe**}	配置接口的TTL复制属性

2.在H-QoS中对匹配上流分类的数据报可以使用如下方法配置EXP-IPP优先级继承和802.1p继承。

i.参照“配置流分类”内容配置流分类。

ii.在策略中配置8021p 、mpls-exp和IPP之间的继承关系。

步骤	命令	功能
1	inspur(config)#**policy-map**<*policy-map-name*>	创建policy-map名字并进入策略映射配置模式
2	inspur(config-pmap)#**class** <*class-map-name*>	关联class-map名字并进入策略类配置模式
3	inspur(config-pmap-c)#**set** {**8021p** | **mpls-exp** | **precedence**| **dscp**} **inherit-from** {**8021p** | **mpls-exp** | **precedence**| **dscp**}	配置8021p、mpls-exp和IPP之间的继承关系

iii.参照“配置H-QoS”内容在接口上绑定策略映射。

3.在VRF接口上配置EXP-IPP优先级继承和TTL继承。

步骤	命令	功能
1	inspur(config)#**ip vrf** <*vrf-name*>	配置VRF实例，<*vrf-name*>为vrf实例名，1~32个字符
2	inspur(config-vrf-vrf-name)#**ds-mode** {**pipe**| **short-pipe**| **uniform** }	配置MPLS标签的优先级和IP报文中优先级字段的继承

步骤	命令	功能
3	inspur(config-vrf-vrf-name)#**ttl-mode** {**pipe** | **uniform**}	配置MPLS标签的优先级和IP报文中ttl值的继承

4.验证配置结果。

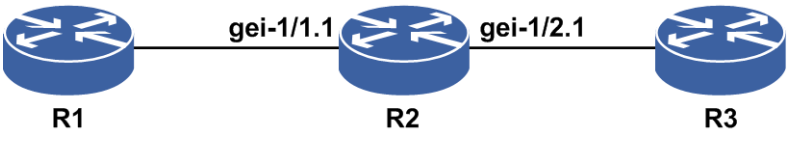
命令	功能
inspur#**show mls-qos-mode** [<*interface-name*>]	显示所有接口上配置的优先级继承
inspur#**show qos-dot1p** [<*interface-name*>]	显示所有接口上配置的802.1p继承
inspur#**show class-map** [<*class-map-name*>]	显示所有类映射及其所有匹配规则设置
inspur#**show policy-map** [<*policy-map-name*>[**class** <*class-name*>]]	显示所有策略映射及其所有策略类的配置
inspur#**show service-policy** [<*interface-name*>]	显示所有接口下的策略绑定
inspur#**show running-config hqos**	显示配置的H-QoS信息
inspur#**show running-config hqos-if**	显示优先级继承策略

8.6.2 802.1P 字段继承配置实例

配置说明

如*图 8-5*所示，要求R2上从VLAN子接口（gei-1/1.1）入的流转发出去时，实现入接口流的802.1P到出接口流的IPP的映射。

图 8-5 优先级继承配置实例拓扑图



配置思路

1.创建VLAN子接口。

2.配置VLAN ID。

3.配置VLAN子接口的IP地址。

4.配置802.1p继承策略。

配置过程

R2上的配置如下：

```
R2(config)#interface gei-1/1.1
R2(config-if-gei-1/1.1)#exit
R2(config)#interface gei-1/2.1
R2(config-if-gei-1/2.1)#exit
R2(config)#vlan-configuration
R2(config-vlan)#interface gei-1/1.1
R2(config-vlan-if-gei-1/1.1)#encapsulation-dot1q 100
R2(config-vlan-if-gei-1/1.1)#exit
R2(config-vlan)#interface gei-1/2.1
R2(config-vlan-if-gei-1/2.1)#encapsulation-dot1q 100
R2(config-vlan-if-gei-1/2.1)#exit
R2(config-vlan)#exit
R2(config)#interface gei-1/1.1
R2(config-if-gei-1/1.1)#ip address 23.22.21.1 255.255.255.0
R2(config-if-gei-1/1.1)#exit
R2(config)#interface gei-1/2.1
R2(config-if-gei-gei-1/2.1)#ip address 33.32.31.1 255.255.255.0
R2(config-if-gei-gei-1/2.1)#exit
R2(config)#class-map child match-all
R2(config-cmap)#match child
R2(config-cmap)#exit
R2(config)#policy-map 802.1p
R2(config-pmap)#class child
R2(config-pmap-c)#set precedence inherit-from 8021p
R2(config-pmap-c)#exit
R2(config-pmap)#exit
R2(config)#service-policy gei-1/1.1 input 802.1p
```

R1和R3只需要配置VLAN子接口和IP地址，具体配置省略。

配置验证

在R2上查看配置结果：

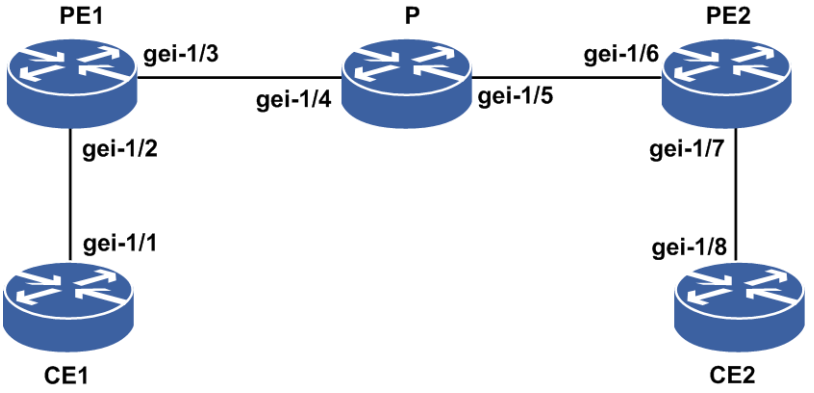
```
R2(config)#show running-config hqos
!<hqos>
class-map child match-all
  match child
$
policy-map 802.1p
  class child
    set precedence inherit-from 8021p
  $
$
service-policy gei-1/1.1 input 802.1p
$
!<hqos>
```

8.6.3 Pipe 模式配置实例

配置说明

如*图 8-6*所示，要求从PE到CE的接口做QoS时信任MPLS-EXP字段，即根据MPLS-EXP字段决定报文发送的优先级。

图 8-6 Pipe 模式配置拓扑图



上图中，CE1和CE2在同一个VPN中，CE1的loopback地址为100.1.1.1/32，CE2的loopback地址为200.1.1.1/32，要求进行适当的VPN配置，使得CE1和CE2能够互相学习到对端的loopback路由。

CE1与PE1之间运行BGP协议，CE2与PE2之间运行OSPF协议。

图中各个接口的地址规划如*表 8-1*所示。

表 8-1 MPLS VPN 基本配置地址规划表

设备	接口名	地址
CE1	gei-1/1	10.1.1.2/24
PE1	gei-1/2	10.1.1.1/24
	gei-1/3	10.10.12.1/24
P	gei-1/4	10.10.12.2/24
	gei-1/5	10.10.23.2/24
PE2	gei-1/6	10.10.23.3/24
	gei-1/7	10.10.10.1/24
CE2	gei-1/8	10.10.10.2/24

配置思路

1.配置三层VPN。

2.在PE1的vrf test1和PE2的vrf test1内的ds-mode分别配置为pipe模式。

配置过程

CE1的配置如下：

```
CE1(config)#interface loopback1
CE1(config-if-loopback1)#ip address 100.1.1.1 255.255.255.255
CE1(config-if-loopback1)#exit
CE1(config)#interface gei-1/1
```

```
CE1(config-if-gei-1/1)#ip address 10.1.1.2 255.255.255.0
CE1(config-if-gei-1/1)#exit
CE1(config)#router bgp 200
CE1(config-bgp)#network 100.1.1.1 255.255.255.255
CE1(config-bgp)#neighbor 10.1.1.1 remote-as 200
CE1(config-bgp)#exit
```

PE1的配置如下：

```
PE1(config)#ip vrf test1
PE1(config-vrf-test1)#rd 100:1
PE1(config-vrf-test1)#route-target import 100:1
PE1(config-vrf-test1)#route-target export 100:1
PE1(config-vrf-test1)#ds-mode pipe
PE1(config-vrf-test1)#address-family ipv4
PE1(config-vrf-test1-af-ipv4)#exit
PE1(config-vrf-test1)#exit
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 10.10.1.1 255.255.255.255
PE1(config-if-loopback1)#exit
PE1(config)#interface gei-1/3
PE1(config-if-gei-1/3)#ip address 10.10.12.1 255.255.255.0
PE1(config-if-gei-1/3)#no shutdown
PE1(config-if-gei-1/3)#exit
PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#interface gei-1/3
PE1(config-ldp-1-if-gei-1/3)#exit
PE1(config-ldp-1)#exit
PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#ip vrf forwarding test1
PE1(config-if-gei-1/2)#ip address 10.1.1.1 255.255.255.0
PE1(config-if-gei-1/2)#exit
PE1(config)#router ospf 1
PE1(config-ospf-1)#router-id 10.10.1.1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 10.0.0.0 0.255.255.255
PE1(config-ospf-1-area-0)#exit
PE1(config)#router bgp 200
PE1(config-bgp)#neighbor 10.10.3.3 remote-as 200
PE1(config-bgp)#neighbor 10.10.3.3 update-source loopback1
PE1(config-bgp)#address-family ipv4 vrf test1
PE1(config-bgp-af-ipv4-vrf)#redistribute connected
PE1(config-bgp-af-ipv4-vrf)#neighbor 10.1.1.2 remote-as 200
PE1(config-bgp-af-ipv4-vrf)#exit
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af-vpnv4)#neighbor 10.10.3.3 activate
PE1(config-bgp-af-vpnv4)#exit
PE1(config-bgp)#exit
PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#exit
```

P上的配置如下：

```
P(config)#interface gei-1/4
P(config-if-gei-1/4)#ip address 10.10.12.2 255.255.255.0
P(config-if-gei-1/4)#no shutdown
P(config-if-gei-1/4)#exit
P(config)#mpls ldp instance 1
P(config-ldp-1)#interface gei-1/4
P(config-ldp-1-if-gei-1/4)#exit
P(config-ldp-1)#exit
P(config)#interface gei-1/5
P(config-if-gei-1/5)#ip address 10.10.23.2 255.255.255.0
P(config-if-gei-1/5)#no shutdown
P(config-if-gei-1/5)#exit
P(config)#mpls ldp instance 1
P(config-ldp-1)#interface gei-1/5
P(config-ldp-1-if-gei-1/5)#exit
P(config-ldp-1)#exit
```

```
P(config)#interface loopback1
P(config-if-loopback1)#ip address 10.10.2.2 255.255.255.255
P(config-if-loopback1)#exit
P(config)#router ospf 1
P(config-ospf-1)#area 0
P(config-ospf-1-area-0)#network 10.0.0.0 0.0.0.255
P(config-ospf-1-area-0)#!
P(config)#mpls ldp instance 1
P(config-ldp-1)#router-id loopback1
P(config-ldp-1)#exit
```

PE2的配置如下：

```
PE2(config)#ip vrf test1
PE2(config-vrf-test1)#rd 100:1
PE2(config-vrf-test1)#route-target import 100:1
PE2(config-vrf-test1)#route-target export 100:1
PE2(config-vrf-test1)#ds-mode pipe
PE2(config-vrf-test1)#address-family ipv4
PE2(config-vrf-test1-af-ipv4)#exit
PE2(config-vrf-test1)#exit
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 10.10.3.3 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#interface gei-1/6
PE2(config-if-gei-1/6)#ip address 10.10.23.3 255.255.255.0
PE2(config-if-gei-1/6)#no shutdown
PE2(config-if-gei-1/6)#exit
PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#interface gei-1/6
PE2(config-ldp-1-if-gei-1/6)#exit
PE2(config-ldp-1)#exit
PE2(config)#interface gei-1/7
PE2(config-if-gei-1/7)#ip vrf forwarding test1
PE2(config-if-gei-1/7)#ip address 10.10.10.1 255.255.255.0
PE2(config-if-gei-1/7)#no shutdown
PE2(config-if-gei-1/7)#exit
PE2(config)#router ospf 1
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 10.0.0.0 0.255.255.255
PE2(config-ospf-1-area-0)#!
PE2(config)#router ospf 2 vrf test1
PE2(config-ospf-2)#redistribute bgp-int
PE2(config-ospf-2)#area 0
PE2(config-ospf-2-area-0)#network 10.10.10.1 0.0.0.0
PE2(config-ospf-2-area-0)#!
PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 10.10.1.1 remote-as 200
PE2(config-bgp)#neighbor 10.10.1.1 update-source loopback1
PE2(config-bgp)#address-family ipv4 vrf test1
PE2(config-bgp-af-ipv4-vrf)#redistribute ospf-int 1
PE2(config-bgp-af-ipv4-vrf)#redistribute connected
PE2(config-bgp-af-ipv4-vrf)#exit
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af-vpnv4)#neighbor 10.10.1.1 activate
PE2(config-bgp-af-vpnv4)#exit
PE2(config-bgp)#exit
PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#exit
```

CE2上的配置如下：

```
CE2(config)#interface loopback1
CE2(config-if-loopback1)#ip address 200.1.1.1 255.255.255.255
CE2(config-if-loopback1)#exit
CE2(config)#interface gei-1/8
CE2(config-if-gei-1/8)#ip address 10.10.10.2 255.255.255.0
CE2(config-if-gei-1/8)#no shutdown
CE2(config-if-gei-1/8)#exit
```

```
CE2(config)#router ospf 1
CE2(config-ospf-1)#area 0
CE2(config-ospf-1-area-0)#network 10.10.10.2 0.0.0.0
CE2(config-ospf-1-area-0)#network 200.1.1.1 0.0.0.0
CE2(config-ospf-1-area-0)#exit
```

配置验证

查看CE1与PE1建立了IBGP连接：

```
CE1#show ip bgp summary
Neighbor    Ver   As    MsgRcvd   MsgSend    Up/Down(s)    State/PfxRcd
10.1.1.1    4     200   0         12         00:00:09      0
```

在PE1上查看接口Pipe的配置：

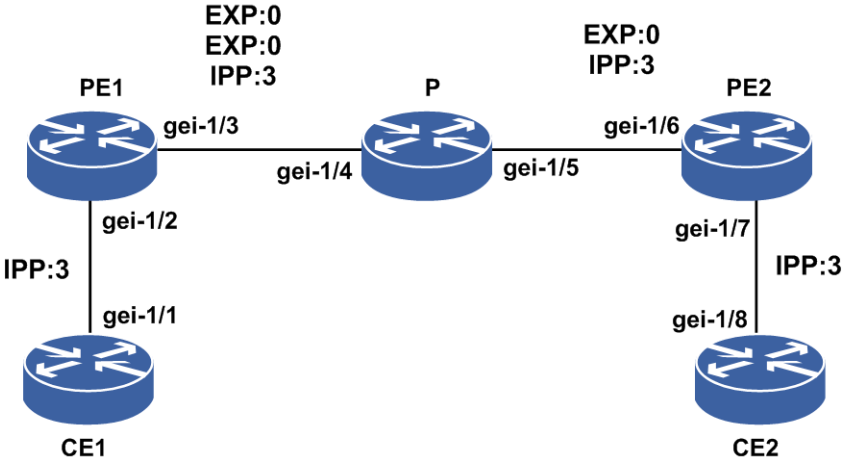
```
PE1(config)#show running-config vrf | begin ip vrf test1
ip vrf test1
  rd 100:1
  route-target import 100:1
  route-target export 100:1
  address-family ipv4
  $
$
!</vrf>
```

在PE2上查看接口Pipe的配置：

```
PE2(config)#show running-config vrf | begin ip vrf test1
ip vrf test1
  rd 100:1
  route-target import 100:1
  route-target export 100:1
  address-family ipv4
  $
$
!</vrf>
```

各优先级字段的变化如*图 8-7*所示。

图 8-7 Pipe 模式各优先级字段的变化拓扑图



8.7 QPPB

QPPB技术是一项通过BGP路由策略部署QoS的技术，通过基于BGP路由的团体列表、

AS paths list和Prefix list等属性进行路由分类，对不同的分类应用不同的QoS策略。

QPPB技术通过BGP路由发送者设置BGP属性预先对路由进行分类，可以简化路由接收者的策略修改。

8.7.1 配置 QPPB

在IR12000智能路由器上配置QPPB，实现通过BGP传播QoS策略的功能。

1.配置QPPB。

步骤	命令	功能
1	inspur(config)#**qos-policy** {**destination** | **source**}{**ip-precedence** | **qos-id**}<*interface-name*>	开启接口QPPB功能
2	inspur(config)#**interface** <*interface-name*>	进入接口配置模式
3	inspur(config-if-interface-name)#**qos-policy** {**destination** | **source**}{**ip-precedence** | **qos-id**}	在接口配置模式开启接口QPPB功能

2.验证配置结果。

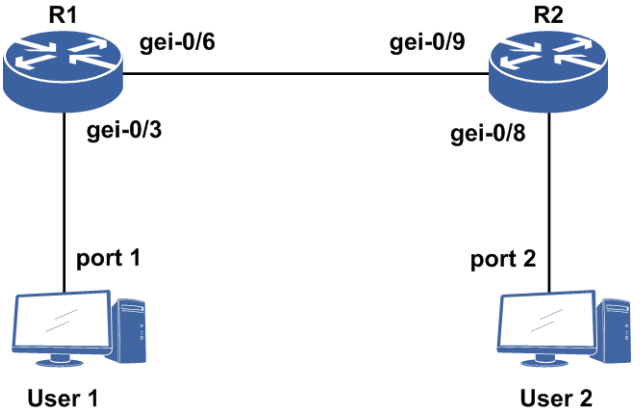
命令	功能
inspur(config)#**show qppb-groups**[[**by-direction** { **destination** | **source** }][**by-interface** <*interface-name*>]][**by-option** { **ip-precedence** | **qos-id** }]	显示QPPB配置信息（可设置选项进行显示）
inspur(config)#**show running-config qppb**	显示所有QPPB配置

8.7.2 QPPB 配置实例

配置说明

如*图 8-8*所示，两台IR12000智能路由器设备R1、R2作为PE，两端分别接用户的port1和port2，用户1、2模拟CE设备。

图 8-8 QPPB 配置实例拓扑图



配置目标如下：

·User 2的port2口通告一条带标记的BGP路由

·从User 1的port1口发一条目的地址为通告路由的流到User 2的port2

·IR12000智能路由器设备能够对目的地址为通告的这条路由的流进行QoS策略

配置思路

1.在IR12000智能路由器设备R1、R2上启用BGP协议

2.从User 2的port2口通告一条带团体属性100：200的BGP路由到R2

3.在R1上配置QPPB策略，使发往目的地址是带团体属性100：200的路由的流限速100 M

配置过程

1.接口配置

R1上的接口配置如下：

```
R1(config)#interface gei-0/3
R1(config-if-gei-0/3)#ip address 111.1.1.1 255.255.255.0
R1(config-if-gei-0/3)#no shutdown
R1(config-if-gei-0/3)#exit
R1(config)#interface gei-0/6
R1(config-if-gei-0/6)#ip address 130.1.1.28 255.255.255.0
R1(config-if-gei-0/6)#no shutdown
R1(config-if-gei-0/6)#exit
```

R2上的接口配置如下：

```
R2(config)#interface gei-0/9
R2(config-if-gei-0/9)#ip address 130.1.1.30 255.255.255.0
R2(config-if-gei-0/9)#no shutdown
R2(config-if-gei-0/9)#exit
R2(config)#interface gei-0/8
R2(config-if-gei-0/8)#ip address 112.1.1.1 255.255.255.0
R2(config-if-gei-0/8)#no shutdown
R2(config-if-gei-0/8)#exit
```

2.配置BGP协议

R1上的配置如下：

```
R1(config)#router bgp 300
R1(config-bgp)#neighbor 111.1.1.2 remote-as 200
R1(config-bgp)#neighbor 111.1.1.2 activate
R1(config-bgp)#neighbor 130.1.1.30 remote-as 100
R1(config-bgp)#neighbor 130.1.1.30 activate
R1(config-bgp)#exit
```

R2上的配置如下：

```
R2(config)#router bgp 100
R2(config-bgp)#neighbor 112.1.1.2 remote-as 200
R2(config-bgp)#neighbor 112.1.1.2 activate
R2(config-bgp)#neighbor 130.1.1.28 remote-as 300
R2(config-bgp)#neighbor 130.1.1.28 activate
R2(config-bgp)#exit
```

3.在R2上配置发送BGP的团体属性

```
R2(config)#router bgp 100
R2(config-bgp)#neighbor 130.1.1.28 send-community
R2(config-bgp)#exit
```

4.在R1的接口上配置QPPB

```
R1(config)#qos-policy destination qos-id gei-0/3
```

5.在R1上配置route-map策略，使匹配团体属性100：200的BGP路由

```
R1(config)#ip community-list 1 permit 100:200
R1(config)#route-map 1
R1(config-route-map)#match community-list 1
R1(config-route-map)#set qos-id 1
R1(config-route-map)#exit
R1(config)#exit
```

6.将route-map的信息在BGP中进行映射

```
R1(config)#router bgp 300
R1(config-bgp)#table-map 1
R1(config-bgp)#exit
```

7.在R1上建立QoS策略

```
R1(config)#class-map qppb match-all
R1(config-cmap)#match qos-group 1
R1(config-cmap)#exit
R1(config)#policy-map qppb
R1(config-pmap)#class qppb
R1(config-pmap-c)#police cir 100000 cbs 100 conform-action transmit
exceed-action drop violate-action drop
R1(config-pmap-c)#exit
R1(config-pmap)#exit
```

8.将QoS策略绑定到接口

```
R1(config)#service-policy gei-0/3 input qppb
```

配置验证

用命令**show service-policy**、**show policy-map**和**show class-map**来查看策略绑的接口及绑的方向：

```
R1#show service-policy
service-policy gei-0/3 input qppb

R1#show policy-map
policy-map qppb
  class qppb
    police cir 100000 cbs 100

R1#show class-map
class-map qppb match-all
  match qos-group 1
```

用命令**show qppb-groups**来查看接口配置的QPPB策略：

```
R1#show qppb-groups
Direction        Option       Interface name
-----------------------------------------------
destination      qos-id       gei-0/3
```

用**show running-config community-list**和**show route-map**查看ip community-list和route-map的配置信息：

```
R1#show running-config community-list
!<community-list>
ip community-list 1 permit  100:200
!</community-list>

R1#show route-map
[route-map 1]IP type: Not set
route-map 1 permit 10
  match community-list 1
  set qos-id 1
```

9 安全

9.1 控制平面安全

路由器常见的攻击主要包括两大类：

·路由协议等控制平面的流量冲击。

·来自外部的非法攻击。

路由协议等控制平面的流量冲击，是属于合法的流量，但是由于流量过大，或路由器控制平面处理负荷过重而导致CPU瘫痪，致使路由器不可用。

来自于外部的非法攻击，如ICMP攻击、IP分片攻击、TCP攻击、DoS攻击、DDoS攻击等。

控制平面安全通过先进的保护措施，防止路由器受到上述攻击，确保路由器稳定工作。控制平面安全主要由软件和硬件协同实现，依次完成如下功能：

1.报文简单分类调度。

2.协议报文分类并送入指定队列。

3.根据用户的需求提供灵活的预定义调度策略和在线修改限速策略。

4.下发驱动的协议报文分类表。

5.按优先级调度报文和协议上送时按多优先级收发报文。

9.1.1 配置接口上送限速

在设备上配置接口限速功能。

1.配置基于接口的上送速率限制。

接口级限速，针对某物理接口或子接口，作用于该接口的一个总的报文上送速率限制，并不针对某种特定类型报文，所有从该接口上送的报文均统计在内。

步骤	命令	功能
1	inspur(config)#**control-plane-security**	进入控制面安全配置模式
2	inspur(config-cps)#**interface** <*interface-name*>	进入控制面安全接口配置模式
3	inspur(config-cps-if-interface-name)#**port-limit untag** {**high** | **low**} **cir** <*0-200000*> **cbs** {<*16-20000*>| **default**}	在CPS接口模式下，配置基于接口的上送速率限制。
	inspur(config-cps-if-interface-name)#**port-limit** {**high** | **low**} **cir** <*0-200000*> **cbs** {<*16-20000*>| **default**}	在CPS子接口模式下，配置基于接口的上送速率限制。

步骤3中的参数描述如下：

参数	说明
high	高优先级桶，Flowtype调度优先级为0和1的进high

参数	说明
low	低优先级桶，Flowtype调度优先级为2-7的进low
cir <*0-200000*>	端口上送流速率值，范围0~200000，单位pps（包/每秒），高桶cir缺省值为255，低桶cir缺省值为745
cbs <*16-20000*>	端口允许突发上送的报文数，范围16~20000，单位KB，缺省值为0
default	cbs缺省配置

示例：

```
inspur(config-cps-if-gei-0/1)#port-limit untag high cir 200 cbs 20
inspur(config-cps-if-gei-0/1.1)#port-limit high cir 100 cbs 20

inspur(config)#show cps port-limit interface gei-0/1
High cir(pps)   High cbs(KB)     Low cir(pps)   Low cbs(KB)
200             20               745            0
```

2.配置基于VLAN的上送速率限制。

步骤	命令	功能
1	inspur(config)#**control-plane-security**	进入控制面安全配置模式
2	inspur(config-cps)#**interface** <*interface-name*>	进入控制面安全接口配置模式
3	inspur(config-cps-if-interface-name)#**vlan-limit** {**high** | **low**} **cir** <*0-200000*> **cbs** {<*16-20000*>| **default**}	在CPS子接口模式下，配置基于VLAN的上送速率限制。 针对vlan-range的情况，如果配置了vlan-linit，则每个vlan的上送速率是vlan-limit的值；如果vlan-limit和port-limit都配置了，vlan-limit优先；如果只配置port-limit，则每个vlan的上送速率在port-limit限速值范围内无限制。

步骤3中的参数描述如下：

参数	说明
cir <*0-200000*>	cir配置范围，单位：pps，高桶cir缺省值为255，低桶cir缺省值为745
cbs <*16-20000*>	cbs配置范围，单位：KB，缺省值为0
default	cbs缺省配置

示例：

```
inspur(config-cps)#interface gei-0/1.1
inspur(config-cps-if-gei-0/1.1)#vlan-limit high cir 100 cbs 20

inspur(config)#show cps vlan-limit interface gei-0/1.1
High cir(pps)   High cbs(KB)     Low cir(pps)   Low cbs(KB)
```

```
100             20              745             0
```

3.配置基于物理接口的特定类型流量的限速。

配置基于物理接口的特定类型流量的限速有两种实现方式：第一种是直接在CPS接口模式下配置限速，第二种是先配置flowtype限速策略，再将flowtype限速策略绑定到某指定接口上；两者同时配置时，第一种优先级高。

步骤	命令	功能
1	inspur(config)#**control-plane-security**	进入控制面安全配置模式
2	inspur(config-cps)#**interface** <*interface-name*>	进入控制面安全接口配置模式
3	inspur(config-cps-if-interface-name)#**flow limit** | **flowtype** <*flowtype*> **rate-limit** <*speed-value*> **quota-limit** <*speed-value*>	直接在CPS接口模式下配置限速
	inspur(config-cps)#**flow limit profile** <*profile-name*>	配置flowtype限速策略，再将flowtype限速策略绑定到某指定接口上
	inspur(config-cps-flow-limit-profile-profile-name)#**flow limit flowtype** <*flow-type*> **rate-limit** <*speed-value*> **quota-limit** <*speed-value*>	
	inspur(config-cps-if-interface-name)#**apply flow limit profile** <*profile-name*>	

步骤3中的参数描述如下：

参数	说明
flowtype <*flowtype*>	指定进行限速的flowtype流类型名。 设备定义了多种流类型，每种流类型都有默认的调度优先级和针对物理接口的上送速率，也可以手动修改针对物理接口的上送速率。另外，对于GE\XGE\40GE\100GE接口，由于本身速率较高，原有默认上送速率可能比较低，设备会根据不同接口下发不同的flowtype上送速率，以减少手动修改的麻烦。
rate-limit <*speed-value*>	指定flowtype上送速率，范围0~85000，单位pps
quota-limit <*speed-value*>	指定flowtype接收配额，用于反压，范围0~85000，单位pps
<*profile-name*>	flowtype限速的模板名，范围：1~16

示例：

直接在CPS接口模式下配置限速：

```
inspur(config-cps-if-gei-0/1)#flow limit flowtype nd
rate-limit 1 quota-limit 11
inspur(config-cps-if-gei-0/1)#flow limit flowtype gre
rate-limit 2 quota-limit 21
inspur(config-cps-if-gei-0/1)#flow limit flowtype dhcp
rate-limit 3 quota-limit 31

inspur(config-cps)#show cps flow limit interface gei-0/1
Interface      IfIndex   Flowtype          Rate(pps) Quota(pps)
gei-0/1        7         ah                10        10        (*)
gei-0/1        7         arp-default       100       100       (*)
gei-0/1        7         arp-suppress      100       100       (*)
gei-0/1        7         atm-oam           10        10        (*)
gei-0/1        7         bfd-default       20        20        (*)
```

配置flowtype限速策略，再将flowtype限速策略绑定到某指定接口上：

```
inspur(config-cps)#flow limit profile 10
inspur(config-cps-flow-limit-profile-10)#flow limit flowtype nd rate-limit
100
quota-limit 100
inspur(config-cps-flow-limit-profile-10)#flow limit flowtype gre rate-limit
2
quota-limit 21
inspur(config-cps-flow-limit-profile-10)#flow    limit    flowtype    dhcp
rate-limit 3
quota-limit 31
inspur(config-cps-flow-limit-profile-10)#flow    limit    flowtype    gvrp
rate-limit 4
quota-limit 41
inspur(config-cps-if-gei-0/1)#apply flow limit profile 5

inspur#show cps flow limit profile 10
Profile 10
      Flowtype          Rate(pps)  Quota(pps)
      dhcp               3          31
      nd                 1          11
      gre                2          21
      gvrp               4          41
```

4.配置单板或接口到CPU的限速。

步骤	命令	功能
1	inspur(config)#**control-plane-security**	进入控制面安全配置模式
2	inspur(config-cps)#**interface** <*interface-name*>	进入控制面安全接口配置模式
4	inspur(config-cps)#**ctm rate-limit destcpu** {**l-cpu** | **r-cpu**} **board** <*name*>**-**<*slot*>{**up-ctm** | **down-ctm**} **cir** <*speed-value*> **cbs** <*speed-value*> **eir** <*speed-value*>	从指定单板到指定CPU的上送限速 CPU可以是MPU（RP）或PFU（LP），对MPU，只有上行方向（微码上行方向）的上送速率限制，对PFU，还有下行方向（微码下行方向）的上送速率限制
5	inspur(config-cps)#**ctm queue-limit** {**high** | **middle** | **normal** | **low**} **destcpu** {**l-cpu** | **r-cpu**} **priority-queue** <*queue-id*> **interface** <*interface-name*>	从指定接口到指定CPU的队列深度配置

步骤4中的参数描述如下：

参数	说明
destcpu {**l-cpu** | **r-cpu**}	CPU名称，用于指定上送的目的CPU，l-cpu为线卡，r-cpu为主控板。
board <*name*>**-**<*slot*>	board名称-槽位号，指定上送报文的源单板
up-ctm	上行
down-ctm	下行

参数	说明
cir <*speed-value*>	约定信息速率，范围up-ctm是0~600000，down-ctm是0~2000000，单位kbps
cbs <*speed-value*>	约定突发尺寸，范围0~256，单位KByte
eir <*speed-value*>	额外信息速率，范围up-ctm是0~200000，down-ctm是0~2000000，单位kbps

步骤5中的参数描述如下：

参数	说明
high	高深度值，4M bytes
middle	中深度值，1M bytes
normal	正常深度值，512K bytes
low	低深度值，128K bytes，缺省为low
priority-queue <*queue-id*>	队列号，也就是优先级，范围：0~7（上行）和16~19（下行）
interface <*interface-name*>	队列深度作用的物理接口名称

示例：

```
inspur(config-cps)#ctm rate-limit destcpu l-cpu board PFU-8 up-ctm
cir 100 cbs 100 eir 100
inspur(config-cps)#ctm rate-limit destcpu l-cpu board PFU-8 down-ctm
cir 100 cbs 100 eir 100
inspur(config-cps)#ctm rate-limit destcpu r-cpu board PFU-8 up-ctm
cir 100 cbs 100 eir 100

inspur(config-cps)#show cps ctm-rate destcpu l-cpu board PFU-8
Cpu    Board    Location  Cir(kbps) Cbs(KByte) Eir(kbps)
l-cpu  PFU-8  down-ctm  100       100        100
l-cpu  PFU-8  up-ctm    100       100        100
```

在安全配置模式下，设置作用于接口gei-0/1，到主控CPU的队列2的队列深度为high级别：

```
inspur(config-cps)#ctm queue-limit high destcpu r-cpu priority-queue 2
interface gei-0/1

inspur#show  cps  ctm-queue  destcpu  R-CPU  priority-queue  2  interface
gei-0/1/0/5
Cpu      Interface          Priority     Level
r-cpu    gei-0/1            2            high
```

5.配置流量反压策略。

步骤	命令	功能
1	inspur(config-cps)#**flow back-press profile** <*profile-name*>	配置流量反压策略
2	inspur(config-cps-back-press-profile-pro	配置当接收流量的速率超过

步骤	命令	功能
	file-name)#**overshot** <*Exceed quota percent num(%)*> **decline** <*Decline the percent of rate limit num(%)*>	quota速率值并到达设置的百分比时，将上送速率在原先限速速率的基础上，降低的百分比
	inspur(config-cps-back-press-profile-profile-name)#**overshot** <*Exceed quota percent num(%)*> **restore**	配置当接收流量的速率超过quota速率值并到达设置的百分比时，将上送速率恢复到之前设定值
	inspur(config-cps-back-press-profile-profile-name)#**overshot** <*Exceed quota percent num(%)*>**suspend**	配置当接收流量的速率超过quota速率值并到达设置的百分比时，将上送速率降低为0
3	inspur(config-cps-if-interface-name)#**flow back-press flowtype** <*flow-type*> **profile** <*profile-name*>	配置将流量反压策略针对某指定类型报文绑定到某指定接口上
4	inspur(config-cps)#**flow statistics-interval** <*interval*>	配置CPS统计信息上报开关以及上送时间周期

步骤1中的参数描述如下：

参数	说明
<*profile-name*>	策略名称范围1~16，无缺省值

步骤2中的参数描述如下：

参数	说明
<*Exceed quota percent num(%)*>	超过quota值的百分比，范围1~100，无缺省值
<*Decline the percent of rate limit num(%)*>	在配置的限速值基础上降低的百分比，范围1~100，无缺省值
restore	恢复原速率，即decline 0
suspend	抑制上送速率，即decline

步骤4中的参数描述如下：

参数	说明
<*interval*>	▸取值为0：flowtype计数开关，表示停止统计。 ▸取值为5-120：统计的定时器时间间隔，单位：秒。 ▸取值为1-4是无效值。 缺省值为10秒。

示例：

```
inspur(config-cps)#flow back-press profile 2
inspur(config-cps-back-press-profile-2)#overshot 20 decline 10
/*超过配额值20% ，反压原速率10%*/
```

```
inspur(config-cps-if-gei-0/1)#flow back-press flowtype nd profile 2

inspur(config-cps)#show cps flow back-press profile 2
Profile2
exceed 20%          decline 10%
inspur(config-cps)#show cps flow back-press flowtype interface gei-0/1
Interface           Flowtype                      Profile
gei-0/1              nd                           2
```

6.配置业务口及管理口属性。

步骤	命令	功能
1	inspur(config-cps)#**management-service** {**deny** | **permit**}{**telnet** | **ssh** | **ftp** | **snmp**| **http**}[**interface** *<interface-name>*]	配置业务口管理协议收包的permit/deny策略，支持Telnet、SSH、FTP、SNMP和HTTP五种协议，缺省各业务口的管理协议均是**permit**。当参数**interface**不设置时，配置对全局接口生效，该配置对设备作为服务端与客户端同时生效
2	inspur(config-cps)#**mng-access peer-ip** {**permit** | **deny**}{*<ip-address><mask>*| **any**}	配置管理口收包时对报文源IP安全过滤策略，系统默认不对管理口收包的源IP进行过滤
3	inspur(config-cps)#**mng-access peer-ipv6** {**permit** | **deny**}{*<ipv6-address-mask>*| **any**}	配置管理口收包时对报文源IPv6安全过滤策略，系统默认不对管理口收包的源IPv6地址进行过滤
4	inspur(config-cps)#**mng-access peer-mac** {**permit** | **deny**}{*<mac-address>*| **any**}	配置管理口收包时对报文源MAC安全过滤策略，系统默认不对管理口收包的源MAC进行过滤
5	inspur(config-cps)#**mng-access protocol** {**deny**|**permit**}[**rate-limit** *<rate-limit-value>*]*<mng-access-protocol-name>*	配置管理口收包时对报文接入协议过滤策略
6	inspur(config-cps)#**mng-access port** {**deny** | **permit**}{**tcp** | **udp**}{**local** | **remote**}*<port>*	配置管理口收包时对报文接入端口过滤策略

步骤2中的参数描述如下：

参数	说明
<ip-address><mask>|**any**	远端IP地址和远端IP地址掩码或所有IP地址。 ▸如配置**any**参数，则对所有源IP生效 ▸如同时指定*<ip-address>*和**any**参数，则以细粒度的*<ip-address>*配置优先 ▸管理口配置的同时指定了**peer ip**地址过滤、**peer mac**地址过滤以及**protocol**过滤时，系统匹配顺序为：先匹配**peer mac**地址规则，再匹配**peer ip**地址规则，最后匹配**protocol**

步骤3中的参数描述如下：

参数	说明
<*ipv6-address-mask*>|**any**	远端IPv6地址前缀或所有IPv6地址。 ▸如配置**any**参数，则对所有源IPv6生效 ▸如同时指定<*ipv6-address-mask*>和**any**参数，则以细粒度的<*ipv6-address-mask*>配置优先 ▸管理口配置的同时指定了**peer ipv6**地址过滤、**peer mac**地址过滤以及**protocol**过滤时，系统匹配顺序为：先匹配**peer mac**地址规则，再匹配**peer ipv6**地址规则，最后匹配**protocol**

步骤4中的参数描述如下：

参数	说明
<*mac-address*>|**any**	远端接入的MAC地址或者所有MAC地址。 ▸如配置**any**参数，则对所有源MAC生效 ▸如同时指定<*mac-address*>和**any**参数，则以细粒度的<*mac-address*>配置优先 ▸管理口配置的同时指定了**peer ip**地址过滤、**peer mac**地址过滤以及**protocol**过滤时，系统匹配顺序为：先匹配**peer mac**地址规则，再匹配**peer ip**地址规则，最后匹配**protocol**

步骤5中的参数描述如下：

参数	说明
<*rate-limit-value*>|**any**	指定协议上送速率。单位：pps，取值1~10000
<*mng-access-protocol-name*>	描述管理口接入的协议

步骤6中的参数描述如下：

参数	说明
local	本端端口号
remote	远端端口号
<*port*>	端口号，取值1-65535

7.开启日志功能。

设备当受到攻击时，需要能提供有效的方法进行攻击溯源，便于发现追踪到攻击源；同时，当设备实施了控制面安全策略而选择性丢包时，也需要有手段记录这些丢包信息便于诊断定位，控制面安全日志实现了上述两个功能。

命令	功能
`inspur(config-cps)#`**cps-log on**	开启日志功能

示例：

```
inspur(config-cps)#cps-log on
三层IP报文格式：
"CPS discard packet: [flowtype:%s,src-ip:%s,dest-ip:%s,protocol:%u,ttl:%u]
reason[%s]"

TCP/UDP报文格式：
"CPS                              discard                              packet:
[flowtype:%s,src-ip:%s,dest-ip:%s,protocol:%u,ttl:%u,src-port:%d,
dest-port:%d] reason[%s]"

ICMP报文格式：
"CPS                              discard                              packet:
[flowtype:%s,src-ip:%s,dest-ip:%s,protocol:%u,ttl:%u,icmp-type:%u,
icmp-code:%u] reason[%s]"

以太二层报文格式：
"CPS discard packet: [flowtype:%s,src-mac:%s,dest-mac:%s,protocol-type:%d]
reason[%s]"

未知格式：
"CPS discard packet: [flowtype:%s,packet:%s] reason[%s]"
```

8.验证配置结果。

命令	功能
inspur#**show running-config cps** [**all**]	显示控制面安全的所有配置
inspur#**show running-config-interface** <*interface-name*>[**all**]	显示接口配置的限速值
inspur#**show cps port-limit interface** <*interface-name*>	显示接口CAR限速配置
inspur#**show cps vlan-limit interface** <*interface-name*>	显示接口基于VLAN的控制面安全属性
inspur#**show cps flow back-press profile** [<*profile-name*>]	查看用户配置的期望的流量反压策略
inspur#**show cps flow back-press flowtype interface** <*interface-name*>	显示某个接口下用户期望的反压策略与物理接口的FlowType进行绑定的信息
inspur#**show cps flow limit profile** [<*profile-name*>]	查看用户配置的flowtype限速策略
inspur#**show cps flow limit interface** <*interface-name*>	显示某个接口下的flowtype限速策略
inspur#**show cps management-service interface** <*interface-name*>	显示指定接口的管理协议的安全配置
inspur#**show cps gtsm statistics**	查看GTSM统计计数信息
inspur#**show cps flow statistics** [**flowtype** <*flowtype*>]{**interface** <*interface-name*>| **cpu** <*name*>**-**<*slot*>**/**<*cpu*>}	显示指定物理接口控制面流量指定flowtype的上送/丢弃计数 显示指定上送CPU控制面流量指定flowtype的入包计数

命令	功能
inspur#**show cps mng-access**	显示管理口生效的安全过滤规则

9.维护控制平面安全。

命令	功能
inspur#(config-cps)**clear cps gtsm statistics**	清除GTSM统计计数信息
inspur#(config-cps)**clear cps flow statictics**	清除上送控制面流量各flowtype的上送/丢弃计数

9.1.2 配置路由安全

在设备上开启GTSM功能。

1.配置OSPF GTSM。

步骤	命令	功能
1	inspur(config)#**router ospf** <*process-id*>[**vrf** <*vrf-name*>]	启动OSPF进程，运行OSPF协议，并进入OSPF协议配置模式
2	inspur(config-ospf-process-id)#**ttl-security all-interfaces hops** <*hops*>	配置OSPF实例所有接口的邻居跳数
3	inspur(config-ospf-process-id)#**interface** <*interface-name*>	进入OSPF接口
4	inspur(config-ospf-process-id-if-interface-name)#**ttl-security hops** <*hops*>	配置OSPF实例指定接口的邻居跳数

步骤2和步骤4的参数描述如下：

参数	说明
<*hops*>	允许的跳数，缺省不配置，范围：1~254，单位：跳 这里的跳数是两个邻居之间的距离，而不是TTL值。 若配置为n，只有当邻居数据包IP头中的TTL在范围<255-n+1，255>之内时，本地才接收该数据包。

示例：

```
inspur(config-ospf-1)#ttl-security all-interfaces hops 3
inspur(config-ospf-1)#interface gei-0/1
inspur(config-ospf-1-if-gei-0/1)#ttl-security hops 2
```

2.配置BGP GTSM。

步骤	命令	功能
1	inspur(config)#**router bgp** <*as-number*>	启动BGP进程并指定本路由器所在的AS号
2	inspur(config-bgp)#**neighbor** {<*ipv4-address*>|<*ipv6-address*>|<*peer-group-name*>} **ttl-security-hops** [<*hops*>]	配置到达EBGP邻居的最大跳数。该命令只适用于EBGP。
3	inspur(config-bgp)#**address-family ipv4 vrf** < *vrf-name*>	进入相应VRF的地址族配置模式
4	inspur(config-bgp-af-ipv4-vrf)#**neighbor** {<*ipv4-address*>|<*peer-group-name*>} **ttl-security-hops** [<*hops*>]	配置到达EBGP邻居的最大跳数。该命令只适用于EBGP。

步骤2的参数描述如下：

参数	说明
<*ipv4-address*>	邻居的IPv4地址，十进制点分形式
<*ipv6-address*>	邻居的IPv6地址，十六进制冒分形式
<*peer-group-name*>	Peer group名称，长度1~31个字符
<*hops*>	允许的跳数，缺省为1，范围：1~254，单位：跳

示例：

设置EBGP邻居1.1.1.1的最大跳数为200：

```
inspur(config-bgp)#neighbor 1.1.1.1 ttl-security-hops 200
inspur(config-bgp)#address-family ipv4 vrf inspur
inspur(config-bgp-af-ipv4-vrf)#neighbor 1.1.1.1 ttl-security-hops 200
```

3.配置LDP GTSM。

步骤	命令	功能
1	inspur(config-ldp-instance-id)#**gtsm target-neighbor** < *ip-address* > **hop-count** <*hop-num*>	配置设备检查对端发送来的LDP报文的跳数，该设置针对非直连会话
2	inspur(config-ldp-instance-id-if-ifname)#**gtsm**	配置设备检查对端发送来的LDP报文的跳数，该设置针对直连会话

缺省情况下，LDP不支持GTSM功能，需要配置触发。配置后需要对接收的该邻居的报文进行TTL范围校验，TTL必须大于或等于255 – n+1。

步骤1的参数描述如下：

参数	说明
< *ip-address* >	对端LSR地址

参数	说明
<*hop-num*>	跳数，取值为1~254

示例：

```
inspur(config)#mpls ldp instance 1
inspur(config-ldp-1)#gtsm target-neighbor 20.20.0.3 hop-count 2
inspur(config-ldp-1)#interface smartgroup1
inspur(config-ldp-1-if-smartgroup1)#gtsm
```

4.配置MSDP GTSM。

步骤	命令	功能
1	inspur(config-mcast)#**router msdp**	启用MSDP协议
2	inspur(config-mcast-msdp)#**peer** <*peer-address*>	配置MSDP邻居，参数为邻居地址
3	inspur(config-mcast-msdp-peer)#**ttl-security-hops** <*hops*>	配置本地接收邻居的跳数，范围1~254

步骤3的参数描述如下：

参数	说明
<*hops*>	跳数，取值为1~254 限制本地接收MSDP邻居数据包的ttl范围。若配置为n，只有当邻居数据包IP头中的TTL在范围<255-n+1，255>之内时，本地才接收该数据包

示例：

```
inspur(config)#ip multicast-routing
inspur(config-mcast)#router msdp
inspur(config-mcast-msdp)#peer 1.1.1.1
inspur(config-mcast-msdp-peer)#ttl-security-hops 8
```

9.1.3 配置 ARP 防攻击

在设备上配置ARP防攻击功能。

1.配置ARP抑制。

对接口收到的ARP报文速率进行限制，当收到的ARP报文速率达到抑制上限时，在ARP抑制时间内不进行ARP报文处理。

步骤	命令	功能
1	inspur(config)#**arp**	进入ARP配置模式

步骤	命令	功能
2	inspur(config-arp)#**port-speed** <*interface-name*><*speed*>	指定接口的抑制速率，即每秒钟允许上送报文的最大数，范围1~1000
3	inspur(config-arp)#**limit-time** <*interface-name*><*time*>	指定接口的抑制时间，范围0~1000，单位：秒，默认10秒
4	inspur(config-arp)#**interface** <*interface-name*>	进入ARP接口配置模式
5	inspur(config-arp-if-interface-name)#**port-speed** <*speed*>	配置该接口的抑制速率，即每秒钟允许上送报文的最大数，范围1~1000
6	inspur(config-arp-if-interface-name)#**limit-time** <*time*>	配置该接口的抑制时间，范围0~1000，单位：秒，默认10秒

2.配置ARP保护。

当ARP条目数达到指定值时，停止学习ARP。

步骤	命令	功能
1	inspur(config)#**arp**	进入ARP配置模式
2	inspur(config-arp)#**protect interface** <*interface-name*> **limit-num** <*protect-limit-number*>	对特定的接口设置ARP保护条目上限，范围为1~262144
3	inspur(config-arp)#**interface** <*interface-name*>	进入ARP接口配置模式
4	inspur(config-arp-if-interface-name)#**protect limit-num** <*protect-limit-number*>	配置该接口的ARP保护条目上限，范围为1~262144
5	inspur(config-arp)#**protect special-mac** <*mac-address*> **limit-num** <*protect-limit-number*>	对特定的MAC地址设置ARP保护条目上限，范围为1~262144
6	inspur(config-arp)#**protect common-mac limit-num** <*protect-limit-number*>	设置所有MAC地址的ARP保护条目上限，范围为1~262144
7	inspur(config-arp)#**protect whole limit-num** <*protect-limit-number*>	设置全局的ARP保护条目上限，范围为1~262144

3.配置ARP学习限制

非本设备请求的ARP应答报文属于无效报文，如果不区别处理，会浪费设备的CPU资源，如果收到大量这样的报文，也产生了攻击。接口配置了ARP学习限制之后，只要不是自己请求回来的响应报文都丢弃，不学习ARP。

步骤	命令	功能
1	inspur(config)#**arp**	进入ARP配置模式
2	inspur(config-arp)#**learn-limit**<*interface-name*>	配置指定接口的ARP学习限制功能，默认关闭
3	inspur(config-arp)#**interface** <*interface-name*>	进入ARP接口配置模式
4	inspur(config-arp-if-interface-name)#**learn-limit**	配置该接口的ARP学习限制功能，默认关闭

4.配置接口的控制平面安全可信任属性

当配置了接口为控制面安全的信任接口时，设备收到需要上送控制面的ARP请求/应答报文后会判断ARP报文目的地址是否为配置接口的主地址，如果是，则作为优先级高的信任报文进行安全保护上送控制面。

步骤	命令	功能
1	inspur(config-arp)#**interface** <*interface-name*>	进入ARP接口配置模式
2	inspur(config-arp-if-interface-name)#**cps-trust**	配置接口的控制平面安全可信任属性

5.配置ARP源过滤

当开启ARP源过滤功能时，路由器对于收到的ARP报文会根据报文源IP地址查找路由表，检查该ARP报文的出接口是否为收到该ARP报文的入接口。如果ARP报文的出接口是入接口，则学习该ARP；否则，丢弃该ARP报文。ARP源过滤能防止某些病毒产生的攻击，默认情况下，路由器的ARP源过滤功能是开启的。

步骤	命令	功能
1	inspur(config)#**arp**	进入ARP配置模式
2	inspur(config-arp)#**source-filtered** <*interface-name*> [**disable**]	配置指定接口的ARP源过滤功能
3	inspur(config-arp)#**interface** <*interface-name*>	进入ARP接口配置模式
4	inspur(config-arp-if-interface-name)#**source-filtered** [**disable**]	配置该接口的ARP源过滤功能

9.1.4 配置 IGMP 防攻击

在设备上配置IGMP防攻击。

1.配置IGMP报文抑制。

步骤	命令	功能
1	inspur(config-mcast)#**router igmp**	进入IGMP配置模式
2	inspur(config-mcast-igmp)#**shaping packets-number** <*number*>	在IGMP配置模式下，限制所有接口收到报文的总和，范围：1~4294967295
3	inspur(config-mcast-igmp)#**interface** <*interface-name*>	进入IGMP接口配置模式
4	inspur(config-mcast-igmp-if-interface-name)#**shaping-packets-number** <*number*>	在IGMP接口配置模式下，限制一个接口收到报文的数量，范围：1~4294967295

2.限制一个查询周期中IGMP接口允许的最大组加入数。

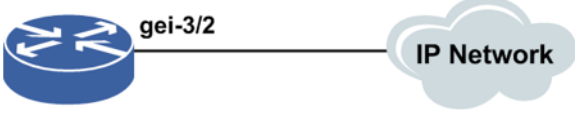
步骤	命令	功能
1	inspur(config-mcast)#**router igmp**	进入IGMP配置模式
2	inspur(config-mcast-igmp)#**interface** <*interface-name*>	进入IGMP接口配置模式
3	inspur(config-mcast-igmp-if-interface-name)#**maximum-joins** <*number*>	限制一个查询周期中IGMP接口允许的最大组加入数，范围：1~40000

9.1.5 控制平面安全基本功能配置实例

配置说明

如*图 9-1*所示，配置控制平面安全基本功能，减少设备受到网络中攻击的影响。

图 9-1 控制平面安全配置实例拓扑图



配置思路

1.在接口上配置限速。

2.配置CTM限速速率。

配置过程

IR12000智能路由器上的配置如下：

```
/*在control-plane-security配置模式下，对物理接口进行限速配置*/
inspur(config)#control-plane-security
inspur(config-cps)#interface gei-3/2
inspur(config-cps-if-gei-3/2)#port-limit untag high cir 360 cbs default
/*配置接口上送速率*/
inspur(config-cps-if-gei-3/2)#flow limit flowtype pim rate-limit 1000
quota-limit 1000
/*配置接口上送的flowtype速率*/
inspur(config-cps-if-gei-3/2)#exit
inspur(config-cps)#exit

/*在control-plane-security配置模式下，对上送的目的CPU和收包源单板速率进行配置*/
inspur(config)#control-plane-security
inspur(config-cps)#ctm rate-limit destcpu PIU-3/0 board PIU-3 up-ctm cir 1000
cbs 100 eir 1000
inspur(config-cps)#ctm rate-limit destcpu MPFU-5/0 board PIU-3 up-ctm cir 1000
cbs 100 eir 1000    /*上送目的CPU为R-CPU*/
inspur(config-cps)#exit
```

配置验证

查看配置信息：

```
inspur(config)#show running-config-interface gei-3/2
!<if-intf>
interface gei-3/2
$
control-plane-security
  interface gei-3/2
    port-limit untag high cir 360 cbs default
  $
$
!</if-intf>
!<cps>
control-plane-security
  interface gei-3/2
    flow limit flowtype pim rate-limit 1000 quota-limit 1000
  $
$
!</cps>

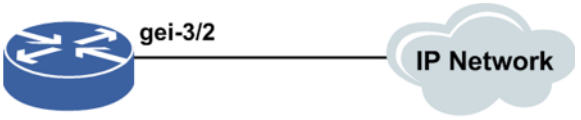
inspur(config)#show running-config cps
!<cps>
control-plane-security
  ctm rate-limit destcpu PIU-3/0 board PIU-3 up-ctm cir 1000 cbs 100 eir 1000
  ctm rate-limit destcpu MPFU-5/0 board PIU-3 up-ctm cir 1000 cbs 100 eir 1000
  interface gei-3/2
    flow limit flowtype pim rate-limit 1000 quota-limit 1000
  $
$
!</cps>
```

9.1.6 基于流的控制平面安全功能配置实例

配置说明

如*图9-2*所示，网络中的设备很容易成为各种报文攻击的目标，通过配置基于流的控制平面安全功能，可以有针对性的减少特定攻击对于网络设备的影响。

图 9-2 基于流控制平面安全配置实例拓扑图



配置思路

1.配置基于流的限速。

2.配置反压功能。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#control-plane-security
inspur(config-cps)#flow limit profile 1
inspur(config-cps-flow-limit-profile-1)#flow limit flowtype ttl1 rate-limit
100 quota-limit 100
inspur(config-cps-flow-limit-profile-1)#exit
inspur(config-cps)#interface gei-3/2
inspur(config-cps-if-gei-3/2)#apply flow limit profile 1
/*限制gei-3/2口ttl=1类型流量的上送速率为100 pps*/
inspur(config-cps-if-gei-3/2)#exit
inspur(config-cps)#flow back-press profile 1
inspur(config-cps-back-press-profile-1)#overshot 10 restore
inspur(config-cps-back-press-profile-1)#overshot 20 decline 20
inspur(config-cps-back-press-profile-1)#overshot 50 decline 50
inspur(config-cps-back-press-profile-1)#overshot 70 suspend
inspur(config-cps-back-press-profile-1)#exit
inspur(config-cps)#interface gei-3/2
inspur(config-cps-if-gei-3/2)#flow back-press flowtype ttl1 profile 1
/*配置对于ttl=1的上送流量进行反压*/
inspur(config-cps-if-gei-3/2)#exit
inspur(config-cps)#end
```

配置验证

查看配置信息：

```
inspur#show running-config cps
!<cps>
control-plane-security
  flow back-press profile 1
```

```
    overshot 20 decline 20
    overshot 50 decline 50
    overshot 70 suspend
    overshot 10 restore
  $
  flow limit profile 1
    flow limit flowtype ttl1 rate-limit 100 quota-limit 100
  $
  interface gei-3/2
    apply flow limit profile 1
    flow back-press flowtype ttl1 profile 1
  $
$
!</cps>
```

9.1.7 黑白名单功能配置实例

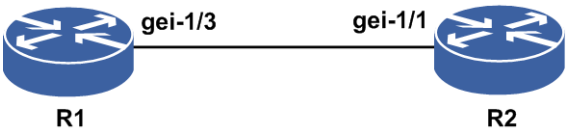
配置说明

为支持协议白名单功能，对于控制面流量使用flowtype进行区分，不同的flowtype其分配的缺省速率、调度优先级均不相同。对于面向连接的协议，可以分配不同级别的flowtype：default、config、known。

- Default的流是指：开启侦听，等待对端连接建链的协议报文，按黑名单处理，报文按BGP default的flowtype处理。
- Config的流是指：已配置了对端邻居，对端主动发起建链的协议报文，按灰名单处理，报文按BGP config的flowtype处理。
- Known的流是指：本端主动发起建链的协议报文或是对端主动发起建链，邻居建立成功的协议报文（这里的邻居建立成功是指协议认为连接建立成功），称按白名单处理，报文按BGP known的flowtype处理。

本配置实例以BGP协议建链为例进行说明，如*图 9-3*所示。

图 9-3 黑白名单功能配置实例拓扑图



配置思路

1.开启BGP侦听。

2.建立BGP邻居。

3.当存在大量BGP连接时，需要将bgp-known的限速放大。

配置过程

R1上的配置如下：

```
/*查看建链接口的flowtype默认限速值*/
R1#show cps flow limit interface gei-1/3
Interface IfIndex Flowtype Rate(pps) Quota(pps)
gei-1/3 21 default 1000 1000 (*)
gei-1/3 21 bgp-default 30 30 (*)
gei-1/3 21 bgp-config 50 50 (*)
gei-1/3 21 bgp-known 500 500 (*)
gei-1/3 21 ospf-default 100 100 (*)
……/*其他报文的显示省略*/

R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#ip address 131.4.1.1 255.255.255.0
R1(config-if-gei-1/3)#exit
R1(config)#router bgp 200  /*开启BGP侦听，协议报文按bgp-default的flowtype处理*/

/*开启BGP侦听后，R1上查看bgp-default流量，如下显示数据表示未超过限速值*/
R1#show cps flow statistics interface gei-1/3
Flowtype          In-packets     Upsend-packets  Drop-packets
default           0              0               0
bgp-default        4271           4271            0
bgp-config         0              0               0
bgp-known          0              0               0

R1(config-bgp)#neighbor 131.4.1.2 remote-as 200
/*配置邻居，协议报文按bgp-known的flowtype处理*/

/*当BGP建链时，R1上查看到bgp-known流量，如下显示数据表示，BGP建链报文丢包，
需要放大bgp-known的flowtype限速*/
R1#show cps flow statistics interface gei-1/3
Flowtype          In-packets     Upsend-packets  Drop-packets
default           0              0               0
bgp-default        4271           4271            0
bgp-config         0              0               0
bgp-known          221063         188102          32961

/*放开bgp-known的flowtype限速配置*/
R1(config)#control-plane-security
R1(config-cps)#interface gei-1/3
R1(config-cps-if-gei-1/3)#flow limit flowtype bgp-known rate-limit 10000
quota-limit 10000
R1(config-cps-if-gei-1/3)#exit
R1(config-cps)#end
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ip address 131.4.1.2 255.255.255.0
R2(config-if-gei-1/1)#exit
R2(config)#router bgp 200
R2(config-bgp)#neighbor 131.4.2.1 remote-as 200
R2(config-bgp)#exit
```

配置验证

R1上查看放开bgp-known的flowtype限速之后的配置信息：

```
inspur#show cps flow limit interface gei-1/3
Interface IfIndex Flowtype Rate(pps) Quota(pps)
gei-1/3 21 default 1000 1000 (*)
gei-1/3 21 bgp-default 30 30 (*)
gei-1/3 21 bgp-config 50 50 (*)
gei-1/3 21 bgp-known 10000 10000
gei-1/3 21 ospf-default 100 100 (*)
……/*其他报文的显示省略*/
```

当存在大量BGP连接时，协议报文不丢包，BGP邻居都能够建链成功。

9.2 URPF

URPF的主要功能是防止基于源地址欺骗的网络攻击行为。

URPF通过检查数据包中源IP地址以及根据接收到数据包的接口和路由表中是否存在源地址路由信息条目，来确定流量是否真实有效，并选择数据包是转发或丢弃。

URPF有以下三种工作模式：

·严格URPF

·松散URPF

·忽略缺省路由的URPF

9.2.1 配置 URPF

在IR12000智能路由器上配置URPF功能，用于防止基于源地址欺骗的网络攻击行为。

1.配置URPF。

步骤	命令	功能
1	inspur(config)#**ipv4 verify unicast source reachable-via** {**rx interface** <*interface-name*>[**acl-name** <*acl-name*>]| **any interface** <*interface-name*>[**acl-name** <*acl-name*>][**ignore-default-route**]}	开启接口IPv4 URPF功能 ▸**rx**，严格模式 ▸**any**，松散模式 ▸**ignore-default-route**，忽略缺省路由选项，仅适用于松散模式
2	inspur(config)#**interface** <*interface-name*>	进入接口配置模式
3	inspur(config-if-interface-name)#**ipv4 verify unicast source reachable-via** {**rx** [**acl-name** <*acl-name*>]| **any** [**acl-name** <*acl-name*>][**ignore-default-route**]}	接口配置模式下开启接口IPv4 URPF功能

2.验证配置结果。

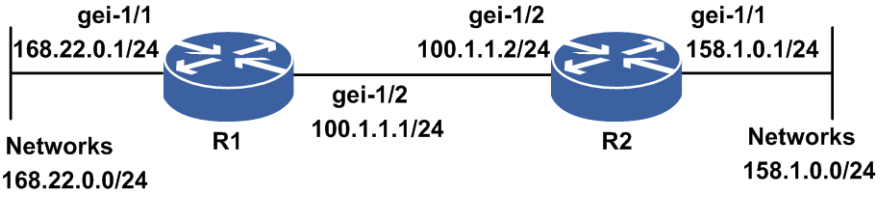
命令	功能
inspur#**show running-config urpf** [**all**]	查看所有URPF配置
inspur#**show running-config-interface** <*interface-name*>[**all**]	查看某个接口下的URPF配置

9.2.2 严格 URPF 配置实例

配置说明

如*图 9-4*所示，在路由器R1的gei-1/1接口上配置严格URPF，防止来自168.22.0.0/24前面的网络用户恶意攻击R1后面的网络，同时允许源地址是22.1.1.0/24网段的数据流通过URPF检查。

图 9-4 URPF 配置实例拓扑图



配置思路

1.为接口配置IP地址。

2.创建ACL，添加符合需求的ACL规则，如允许源地址为22.1.1.0/24网段的数据流通过。

3.接口绑定带有ACL列表的严格URPF。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 168.22.0.1 255.255.255.0
R1(config-if-gei-1/1)#exit
R1(config)#ipv4-access-list acl
R1(config-ipv4-acl)#rule 1 permit 22.1.1.0 0.0.0.255
R1(config-ipv4-acl)#exit
R1(config)#ipv4 verify unicast source reachable-via rx interface gei-1/1
acl-name acl
```

配置验证

查看配置结果：

```
R1(config)#show running-config urpf
!<urpf>
interface gei-1/1
  ipv4 verify unicast source reachable-via rx acl-name acl
$
!</urpf>

R1(config)#show running-config-interface gei-1/1
!<if-intf>
interface gei-1/1
```

```
  no shutdown
  ip address 168.22.0.1 255.255.255.0
$
!</if-intf>
!</urpf>
interface gei-1/1
  ipv4 verify unicast source reachable-via rx acl-name acl
$
!</urpf>

R1(config)#show ipv4-access-lists name acl
ipv4-access-list acl
 1/1 (showed/total)
  1 permit 22.1.1.0 0.0.0.255
```

9.2.3 松散 URPF 配置实例

配置说明

如*图 9-5*所示，在路由器R1的gei-2/1接口上配置松散URPF，允许来自源为88.1.1.8，目的地址为12.131.1.0网段的流量通过URPF检查。

图 9-5 松散 URPF 配置实例



配置思路

1.R1和R2之间增加一条子接口链路，配置各个接口地址。

2.R1和R2之间配置OSPF，使得单播互通。

3.R1的入口gei-2/1配置松散URPF和ACL。

4.发流源是88.1.1.8，从R1到R2。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/1
R2(config-if-gei-2/1)#no shutdown
R1(config-if-gei-2/1)#ip address 16.1.1.1 255.255.255.0
R1(config-if-gei-2/1)#exit
R1(config)#interface gei-2/2
R2(config-if-gei-2/2)#no shutdown
R1(config-if-gei-2/2)#ip address 17.1.1.1 255.255.255.0
R1(config-if-gei-2/2)#exit
R1(config)#interface gei-2/2.1
R1(config-if-gei-2/2.1)#exit

R1(config)#vlan-configuration
```

```
R1(config-vlan)#interface gei-2/2.1
R1(config-vlan-if-gei-2/2.1)#encapsulation-dot1q 100
/*配置子接口，建立另一条链路*/
R1(config-vlan-if-gei-2/2.1)#exit
R1(config-vlan)#exit
R1(config)#interface gei-2/2.1
R1(config-if-gei-2/2.1)#ip address 56.1.1.1 255.255.255.0
R1(config-if-gei-2/2.1)#exit

R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 17.1.1.0 0.0.0.255
R1(config-ospf-1-area-0)#network 12.131.1.0 0.0.0.255
R1(config-ospf-1-area-0)#exit

R1(config)#interface gei-2/1
R1(config-if-gei-2/1)#ipv4 verify unicast source reachable-via any acl-name
wd
/*接口绑定松散URPF*/
R1(config-if-gei-2/1)#exit

R1(config)#ipv4-access-list wd
R1(config-ipv4-acl)#rule permit 88.1.1.8
R1(config-ipv4-acl)#exit
R1(config)#ip route 88.1.1.8 255.255.255.255 56.1.1.2
/*配置静态路由指定到源的路由的出接口和流的入口是不相同的*/
```

R2上的配置如下：

```
R2(config)#interface gei-3/2
R2(config-if-gei-3/2)#no shutdown
R2(config-if-gei-3/2)#ip address 12.131.1.1 255.255.255.0
R2(config-if-gei-3/2)#exit
R2(config)#interface gei-3/1
R2(config-if-gei-3/1)#no shutdown
R2(config-if-gei-3/1)#ip address 17.1.1.2 255.255.255.0
R2(config-if-gei-3/1)#exit
R2(config)#interface gei-3/1.1
R2(config-if-gei-3/1.1)#exit

R2(config)#vlan-configuration
R2(config-vlan)#interface gei-3/1.1
R2(config-vlan-if-gei-3/1.1)#encapsulation-dot1q 100
/*配置子接口，建立另一条链路*/
R2(config-vlan-if-gei-3/1.1)#exit
R2(config-vlan)#exit
R2(config)#interface gei-3/1.1
R2(config-if-gei-3/1.1)#ip address 56.1.1.2 255.255.255.0
R2(config-if-gei-3/1.1)#exit

R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 17.1.1.0 0.0.0.255
R2(config-ospf-1-area-0)#network 12.131.1.0 0.0.0.255
R2(config-ospf-1-area-0)#exit
```

配置验证

满足URPF配置的流量可以正常转发。

9.3 RADIUS

RADIUS是一种在网络接入设备和认证服务器之间承载认证、授权、计费和配置信息的协议。RADIUS协议是在认证、授权、计费方面应用最为广泛的协议之一，具有以下特点：

•客户端/服务器结构

•采用共享密钥保证网络传输安全性

•良好的可扩展性

•认证机制灵活

9.3.1 配置 RADIUS

在IR12000智能路由器上配置RADIUS认证、计费的相关功能和属性，保障用户信息的安全。

1.配置RADIUS认证组的基本属性。

步骤	命令	功能
1	inspur(config)#**radius authentication-group** <*group-number*>	创建RADIUS认证组，并进入RADIUS认证组配置模式，认证组范围1~2000
2	inspur(config-authgrp-number)#**algorithm** {**first** | **round-robin**}	配置RADIUS服务器的选择算法，有以下两种： ▸**first**：总是选择当前有效的一个服务器作为新呼叫用户的认证服务器 ▸**round-robin**：总是选择下一个有效的服务器作为认证服务器。 缺省为**first**方式
3	inspur(config-authgrp-number)#**alias** <*alias-name*>	配置RADIUS服务器组的别名，一个唯一的ASCII字符串别名，别名可以是任何字母数字串，长度1~31个字符

2.配置RADIUS认证组的可选属性。

命令	功能
inspur(config-authgrp-number)#**calling-station-format** {**class1** | **class2** | **class3** | **user-defined** {**slot** | **port** | **sub-slot** | **vlan** | **second-vlan** | **mac1** | **mac2** | **mac3** | **mac4** | **mac5** | **mac6**} **text** <*string*>}	配置Calling-Station-Id字段格式定义，可设置为class1，class2，class3，class4，class5和user-defined，缺省为class3
inspur(config-authgrp-number)#**deadtime** <*time*>	设置认证服务器的无效时间 一个认证信息发送到认证服务器，没有收到正常响应，并重发一定次数后，

命令	功能
	IR12000智能路由器将认为该认证服务器在一个时间段内是无效的，这个时间段就是由该命令设定的。这个无效时间段过后，如果必要，IR12000智能路由器会尝试重新采用该认证服务器 单位：分钟，范围0~3600，缺省值为5分钟 如果认证组只配置一个认证服务器，建议配置为0；如果认证组配置多个认证服务器，建议使用缺省值
inspur(config-authgrp-number)#**ip vrf** {<*vrf-name*>| **mng**}	把RADIUS认证服务器组和一个VRF关联，VRF名称1~32字符 缺省RADIUS认证服务器组与全局路由表关联。RADIUS认证服务器组可以和一个VRF关联，关联后该RADIUS认证服务器组使用VRF定义的资源。没有和VRF关联的RADIUS认证服务器组属于全局路由域。 如果RADIUS认证服务器组使用管理口进行认证，需要配置**ip vrf mng**，默认不使用管理口认证
inspur(config-authgrp-number)#**max-retries** <*times*>	设置RADIUS认证服务器超时重发次数 在一个认证信息发送到认证服务器，但没有收到正常响应的情况下，IR12000智能路由器重发该认证信息的最大次数，范围1~255，缺省值为3
inspur(config-authgrp-number)#**nas-ip-address** <*ip-address*>	设置RADIUS服务器的NAS-IP，对应协议包的NAS-IP-Address字段和协议包的源IP地址
inspur(config-authgrp-number)#**server** <*server-number*><*ip-address*>[**master**] **key** {**encrypted** <*encrypted-password*>|<*password*>}[**port** <*port-number*>]	设置RADIUS服务器及其参数，包括： ▸服务器编号，范围1~4 ▸服务器IP地址 ▸服务器与NAS之间的共享密文密钥或明文密钥，明文密钥长度1~31字符，密文密钥长度64个字符 ▸服务器端口号，可选参数，范围1025~65535，认证服务器组的缺省值为1812 ▸**master**，可选参数，表示该服务器为主服务器，一个认证服务器组只能有一个主服务器 IP地址的类型需要与NAS-IP的配置一致
inspur(config-authgrp-number)#**timeout** <*time*>	设置RADIUS服务器认证超时时间，IR12000智能路由器向RADIUS Server发送认证信息，超过这个设置值没有收到正常响应之后，就重发认证信息，单位：秒，范围1~255，缺省值为3秒

命令	功能
inspur(config-authgrp-number)#**user-name-format** {**include-domain** | **strip-domain** | **only-domain**}	配置IR12000智能路由器向RADIUS Server发送的用户名字段的格式 配置**strip-domain**后，NAS向RADIUS Server发送的用户名字段不包含域名 举例说明：用户实际用户名为xxx@local： ▸如果设置**include-domain**，则发往认证服务器的用户名为xxx@local ▸如果设置了**strip-domain**，则发往认证服务器的用户名为xxx ▸如果设置**only-domain**，则发往认证服务器的用户名为local
inspur(config-authgrp-number)#**vendor** {**enable** | **disable**}	配置发送的RADIUS协议包中是否需要厂商自定义属性： ▸**enable**：发送厂商自定义属性 ▸**disable**：不发送厂商自定义属性 缺省为**enable**
inspur(config)#**radius server-port-check** {**on** | **off**}	设置是否检查RADIUS服务器发送的报文中的源端口号，默认值为**on**
inspur(config)#**radius attribute vendor-specific vendor-id** <*vendor-id*>	配置NAS向服务器发送的报文中的私有属性的vendor号，范围1~65535，默认值为3902
inspur(config)#**radius dev-backup** {**master** | **slave**}	配置NAS的RADIUS主备状态，默认是**master**

class1：表示用户接入的物理信息和MAC信息，格式为slot port vpi vci vlanid mac，ASCII字符，数值以16进制表示；各字段占字符长度为：2，2，2，4，4，12。

class2：表示用户接入的物理信息，格式为slot port vpi vci vlanid，ASCII字符，数值以16进制表示；各字段占字符长度为：2，2，2，4，1；vlanid只取实际值的低4位。

class3：仅保留MAC地址，格式为xx:xx:xx:xx:xx:xx。

user-defined {**slot** | **port** | **sub-slot** | **vlan** | **second-vlan**| **mac1** | **mac2** | **mac3** | **mac4** | **mac5** | **mac6** | **text** <*string*>}：支持Calling-Station-Id按照用户配置的字符串格式编码，slot、subslot、port、vlan、second-vlan、mac等可选择。参数组织格式由text输入的字符串决定，最大为88字符，格式串采用ANSIC标准C语言定义的格式化输入字符串，格式字符介绍如下。

▸**d**，以带符号的十进制形式输出整数（正数不输出符号）

▸**x, X**，以十六进制无符号形式输出整数（不输出前导符0x）， 用x则输出十六进制数的a~f时以小写形式输出。用X时，则以大写字母输出

▸**u**，以无符号十进制形式输出整数

▸**字母l**，用于长整型整数，可加在格式符d，x，X，u前面

▸**数字m**，加在以上格式字符组合前面，表示最小输出宽度，不满足最小宽度默认使用空格填充，超过最大按实际宽度输出

▸**数字n**，加在以上格式字符组合前面，表示不足宽度要求用来填充的数字

3.配置RADIUS计费组的基本属性。

步骤	命令	功能
1	inspur(config)#**radius accounting-group** <*group-number*>	创建RADIUS计费组，并进入RADIUS计费组配置模式，计费组范围1~2000
2	inspur(config-acctgrp-number)#**algorithm** {**first** | **round-robin**}	配置RADIUS服务器的选择算法，有以下两种： ▸**first**：总是选择当前有效的一个服务器作为新呼叫用户的计费服务器 ▸**round-robin**：总是选择下一个有效的服务器作为计费服务器。 缺省为**first**方式
3	inspur(config-acctgrp-number)#**alias** <*name-string*>	配置RADIUS服务器组的别名，一个唯一的ASCII字符串别名，别名可以是任何字母数字串，不可以包含空格，长度不要超过31

4.配置RADIUS计费组的可选属性。

命令	功能
inspur(config-acctgrp-number)#**calling-station-format** {**class1** | **class2** | **class3** | **class4** | **class5** | **user-defined** {**slot** | **port** | **sub-slot** | **vlan** | **second-vlan** | **mac1** | **mac2** | **mac3** | **mac4** | **mac5** | **mac6** | **text** <*string*>}}	配置Calling-Station-Id字段格式定义，可设置为class1，class2，class3，class4，class5s和user-defined，缺省为class3
inspur(config-acctgrp-number)#**deadtime** <*time*>	设置计费服务器的无效时间 一个计费信息发送到计费服务器，没有收到正常响应，并重发一定次数后，IR12000智能路由器将认为该计费服务器在一个时间段内是无效的，这个时间段就是由该命令设定的； 这个无效时间段后，如果必要，IR12000智能路由器会尝试重新采用该计费服务器，单位：分钟，范围0~3600，缺省值为5分钟 如果计费组只配置一个计费服务器，建议配置为0；如果计费组配置多个计费服务器，建议使用缺省值
inspur(config-acctgrp-number)#**ip vrf** {<*vrf-name*>| **mng**}	把RADIUS计费服务器组和一个VRF关联，VRF名称长度为1~32个字符 缺省RADIUS计费服务器组与全局路由表关联。RADIUS计费服务器组可以和一个VRF关联，关联后该RADIUS计费服务器组使用VRF定义的资源。

命令	功能
	没有和VRF关联的RADIUS计费服务器组属于全局路由域。 如果RADIUS认证服务器组使用管理口进行计费，需要配置**ip vrf mng**，默认不使用管理口计费
inspur(config-acctgrp-number)#**interim-packet-quota** <*quota*>	配置计费更新包占用计费发送队列的比例限额，限额是一个百分比值，配置限额越大表示计费更新包可以占用的比例越大，给计费开始包和计费结束包预留的队列空间越小，范围0~100，IR12000智能路由器默认为80
inspur(config-acctgrp-number)#**local-buffer** {**enable** | **disable**}	设置计费服务器组是否进行本地缓存： ▸**enable**：启用计费本地缓存 ▸**disable**：不进行计费本地缓存 默认是**disable**
inspur(config-acctgrp-number)#**life-time** <*time*>	计费开始和计费结束报文在缓存队列中的生命时间，范围2~1024，单位：小时，默认是2小时
inspur(config-acctgrp-number)#**max-retries** <*times*>	设置RADIUS计费服务器超时重发次数 在一个计费信息发送到计费服务器，但没有收到正常响应的情况下，IR12000智能路由器重发该计费信息的最大次数，范围1~255，缺省值为3
inspur(config-acctgrp-number)#**nas-ip-address** <*ip-address*>	设置RADIUS服务器的NAS-IP，对应协议包的NAS-IP-Address字段和协议包的源IP地址
inspur(config-acctgrp-number)#**server** <*server-number*><*ip-address*>[**master**] **key** {**encrypted** <*encrypted-password*>|<*password*>}[**port** <*port-number*>]	设置RADIUS服务器及其参数，包括： ▸服务器编号，范围1~4 ▸服务器IP地址 ▸服务器与NAS之间的共享密文密钥或者明文密钥，明文密钥长度为1~31字符，密文秘钥长度64个字符 ▸服务器端口号，可选参数，范围1025~65535，缺省值计费服务器组1813 ▸**master**，可选参数，表示该服务器为主服务器，一个计费服务器组只能有一个主服务器 IP地址的类型需要与NAS-IP的配置一致
inspur(config-acctgrp-number)#**timeout** <*time*>	设置RADIUS服务器计费超时时间，IR12000智能路由器向RADIUS Server发送计费信息，超过这个设置值没有

命令	功能
	收到正常响应之后，就重发计费信息，单位：秒，范围1~255，缺省值为3秒
inspur(config-acctgrp-number)#**user-name-format** {**include-domain** | **strip-domain** | **only-domain**}	配置IR12000智能路由器向RADIUS Server发送的用户名字段的格式 配置strip-domain后，NAS向RADIUS server发送的用户名字段不包含域名 举例说明：用户实际用户名为xxx@local： ▸如果设置**include-domain**，则发往计费服务器的用户名为xxx@local ▸如果设置了**strip-domain**，则发往计费服务器的用户名为xxx ▸如果设置**only-domain**，则发往计费服务器的用户名为local
inspur(config-acctgrp-number)#**vendor** {**enable** | **disable**}	配置发送的RADIUS协议包中是否需要厂商自定义属性： ▸**enable**：发送厂商自定义属性 ▸**disable**：不发送厂商自定义属性 缺省为**enable**

5.配置RADIUS手动发送accounting-off包。

命令	功能
inspur#**radius accounting-off** {**all** | **group** <*group-number*>[**server** <*server-number*>]}	手动发送accounting-off包，**all**表示手动发送所有RADIUS计费组accounting-off包

6.验证配置结果。

命令	功能
inspur#**show configuration radius all**	显示RADIUS的所有配置
inspur#**show configuration radius server-port-check**	显示RADIUS server-port-check的配置
inspur#**show configuration radius attribute**	显示RADIUS发送厂商属性的厂商号的配置
inspur#**show radius-server all**	显示RADIUS所有认证计费组服务器信息
inspur#**show configuration radius dev-backup**	显示RADIUS热备状态
inspur#**show radius-server authentication-group** <*group-number*>	显示RADIUS指定认证组服务器信息
inspur#**show radius-server accounting-group** <*group-number*>	显示RADIUS指定计费组服务器信息

命令	功能
inspur#**show accounting local-buffer all**	显示RADIUS所有本地缓存的计费报文
inspur#**show accounting local-buffer group** <*group-number*>[{**head** <*count*>| **tail** <*count*>| **index** <*index-num*>[<*count*>]}]	显示RADIUS 指定计费组本地缓存的计费报文 <*count*>是需要显示的缓存记录的条目数，范围1~3072 <*index-num*>是指定从哪一条缓存记录开始显示，范围是1~3072
inspur#**show accounting local-buffer name** <*alias-name*>	显示RADIUS指定计费组别名的本地缓存的计费报文
inspur#**show accounting local-buffer session** <*session-id*>	显示RADIUS指定计费session值的计费报文
inspur#**show accounting local-buffer sum**	显示RADIUS所有本地缓存的计费报文的个数统计
inspur#**show accounting local-buffer user** <*user-name*>[<*count*>]	显示RADIUS指定用户名的本地缓存的计费报文；RADIUS计费报文的用户名，如果有domain名需包含domain名

7.维护RADIUS。

命令	功能
inspur#**radius-ping authentication-group** <*group-number*><*username*><*password*>[**domain** <*domain-name*>]{**pap** | **chap**}[**detail**]	检测RADIUS认证组是否可达
inspur#**radius-ping accounting-group** <*group-number*> <*username*> [**domain** <*domain-name*>] [**detail**]	检测RADIUS计费组是否可达
inspur#**clear accounting local-buffer** {**all** | **group** <*group-name*>}	清除所有或者指定RADIUS本地缓存的计费报文
inspur#**debug radius all**	打开RADIUS所有的debug显示
inspur#**debug radius authentication data**	打开RADIUS认证组data信息显示
inspur#**debug radius authentication error**	打开RADIUS认证组错误信息显示
inspur#**debug radius authentication event**	打开RADIUS认证组event信息显示
inspur#**debug radius authentication packet** {<*group-number*>| **all**}	打开RADIUS某认证组或所有认证组的packet信息显示
inspur#**debug radius accounting data**	打开RADIUS计费组data信息显示
inspur#**debug radius accounting error**	打开RADIUS计费错误信息显示
inspur#**debug radius accounting event**	打开RADIUS计费组event信息显示
inspur#**debug radius accounting packet** {<*group-number*>| **all**}	打开RADIUS某计费组或所有计费组packet信息显示

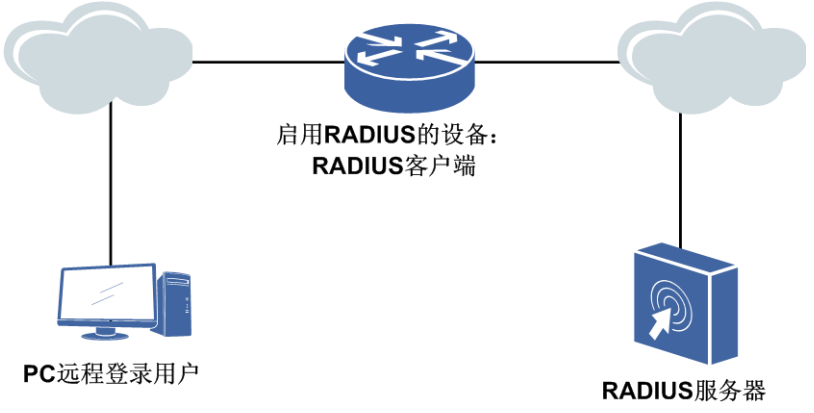
命令	功能
inspur#**debug radius exception**	打开RADIUS额外的信息打印显示
inspur#**debug radius user** *<username><domian-name>*	打开RADIUS指定用户的打印显示
inspur#**show debug radius**	显示RADIUS打开了哪些debug打印

9.3.2 RADIUS 配置实例

配置说明

如*图 9-6*所示，用户通过PC终端登录路由器，启用RADIUS认证服务的路由器将认证、授权信息和RADIUS服务器交互，通过服务器的认证和授权则用户可以登录，否则提示不能登录。

图 9-6 RADIUS 认证的常见组网拓扑图



配置思路

1.创建RADIUS认证组，并进入RADIUS认证组配置模式。

2.设置RADIUS认证组的服务器。

3.配置RADIUS服务器参数。

4.配置AAA认证模板；认证模板中配置认证方式为**radius**，认证组为已配置的RADIUS组。

5.配置AAA授权模板；授权模板中配置授权方式为**radius-local**。

6.配置用户管理模块认证模板和授权模板，用户管理模块模板再绑定AAA模板。

7.创建用户，将用户绑定到用户管理模块模板中。

配置过程

本实例中接口IP地址的配置过程省略，网络设备上认证和授权的配置如下：

```
inspur(config)#radius authentication-group 1
inspur(config-authgrp-1)#server 1 192.168.70.5 master key inspur port 1812
inspur(config-authgrp-1)#algorithm first
inspur(config-authgrp-1)#timeout 5
inspur(config-authgrp-1)#max-retries 10
inspur(config-authgrp-1)#deadtime 5
inspur(config-authgrp-1)#calling-station-format class1
inspur(config-authgrp-1)#nas-ip-address 192.168.70.1
inspur(config-authgrp-1)#user-name-format strip-domain
inspur(config-authgrp-1)#vendor disable
inspur(config-authgrp-1)#exit
inspur(config)#aaa-authentication-template 2001
inspur(config-aaa-authen-template)#aaa-authentication-type radius
inspur(config-aaa-authen-template)#authentication-radius-group 1
inspur(config-aaa-authen-template)#exit
inspur(config)#aaa-authorization-template 2001
inspur(config-aaa-author-template)#aaa-authorization-type radius-local
inspur(config-aaa-author-template)#exit
inspur(config)#system-user
inspur(config-system-user)#authentication-template 1
inspur(config-system-user-authen-temp)#bind     aaa-authentication-template
2001
inspur(config-system-user-authen-temp)#exit
inspur(config-system-user)#authorization-template 1
inspur(config-system-user-author-temp)#bind aaa-authorization-template 2001
inspur(config-system-user-author-temp)#exit
inspur(config-system-user)#user-name who
inspur(config-system-user-username)#bind authentication-template 1
inspur(config-system-user-username)#bind authorization-template 1
inspur(config-system-user-username)#password who
```

计费配置类同，如下：

```
inspur(config)#ip vrf vrf1      /*如果server在私网上，需要配置vrf*/
inspur(config-vrf-vrf1)#rd 1:1
inspur(config-vrf-vrf1)#address-family ipv4
inspur(config-vrf-vrf1-af-ipv4)#route-target 1:1
inspur(config-vrf-vrf1-af-ipv4)# exit
inspur(config-vrf-vrf1)#exit

inspur(config)#radius accounting-group 1
inspur(config-acctgrp-1)#alias acc_grp1
inspur(config-acctgrp-1)#ip vrf vrf1
inspur(config-acctgrp-1)#server 1 192.168.70.5 master key inspur port 1813
inspur(config-acctgrp-1)#algorithm first
inspur(config-acctgrp-1)#timeout 5
inspur(config-acctgrp-1)#max-retries 10
inspur(config-acctgrp-1)#deadtime 3
inspur(config-acctgrp-1)#calling-station-format class2
inspur(config-acctgrp-1)#nas-ip-address 192.168.70.2
inspur(config-acctgrp-1)#user-name-format include-domain
inspur(config-acctgrp-1)#vendor enable
inspur(config-acctgrp-1)#local-buffer enable
inspur(config-acctgrp-1)#exit
```

配置验证

用**show**命令验证配置结果：

```
inspur(config)#show configuration radius
!<radius>
radius authentication-group 1
```

```
  algorithm first
  calling-station-format class1
  deadtime 5
  max-retries 10
  nas-ip-address 192.168.70.1
  server 1 192.168.70.5 master key encrypted
33A8EC1030727EB3A9B61002E10BDBEDB5BEA986F5505AD19582826921F45FCB port 1812
  timeout 5
  user-name-format strip-domain
  vendor disable
$
radius accounting-group 1
  algorithm first
  alias acc_grp1
  calling-station-format class2
  deadtime 3
  ip vrf vrf1
  local-buffer enable
  max-retries 10
  nas-ip-address 192.168.70.1
  server 1 192.168.70.5 master key encrypted
33A8EC1030727EB3A9B61002E10BDBEDB5BEA986F5505AD19582826921F45FCB port 1813
  timeout 5
  user-name-format include-domain
  vendor enable
$
!</radius>
```

9.4 TACACS+

TACACS+协议通过一台或多台中心服务器为路由设备、网络接入服务设备和其他网络设备提供接入控制。

TACACS+通过分离验证、授权、计费功能对NAS和服务器之间的报文进行加密。

TACACS+的特点如下：

- 验证、授权、计费的功能分离是TACACS+的设计基础。将验证和授权分离的好处是授权可以是一个动态的处理过程而不必一定要在验证之后才可以进行授权的操作。
- TACACS+协议可以与PPP、ARAP等其他协议结合而具有更加灵活的特点。
- TACACS+的计费功能可以提供安全审计或服务计费。

9.4.1 配置 TACACS+

在IR12000智能路由器上配置TACACS+协议的相关功能和属性，保障用户信息的安全。

1.配置开启TACACS+功能及基本属性。

步骤	命令	功能
1	inspur(config)#**tacacs enable**	全局开启TACACS+功能 在配置TACACS+前，要先开启TACACS+

步骤	命令	功能
2	inspur(config)#**tacacs-server timeout** <*timeout*>	在全局配置模式下配置TACACS+全局超时时长，即配置TACACS+客户端和服务器连接的超时时长，单位：秒，有效值1~1000，默认5秒
3	inspur(config)#**tacacs-server key** {**encrypted** <*secret_key*>|<*password*>}	在全局配置模式下配置全局TACACS+协议密文密钥或者明文密钥，对所有未指定密钥的服务器有效 明文可以配置1~63字符（不包括空格），密文长度128个字符（不包括空格）
4	inspur(config)#**tacacs-server packet** <*length*>	配置TACACS+协议最大报文长度，范围1024~4096，单位：字节，默认1024字节
5	inspur(config)#**tacacs-client** <*client-ip-address*>[**port** <*port-number*>]	在全局配置模式下配置TACACS+客户端IP地址和端口，作为IR12000智能路由器和TACACS+服务器通信的IP地址，范围1025~65535

2.配置TACACS+服务器组。

创建服务器组并进入TACACS+的服务器组配置模式，在组中添加已经配置的服务器，一个组中最多添加4个服务器。

命令	功能
inspur(config)#**tacacs-server host** [**vrf** {<*vrf-name*>| **mng**}]<*server-ip-address*>[**port** <*port-number*>][**timeout** <*timeout*>][**key** {**encrypted** <*secret_key*>|<*password*>}]	在全局配置模式下配置TACACS+服务器
inspur(config)#**tacplus group-server** <*group-name*>	在全局配置模式下配置服务器组
inspur(config-sg)#**server** [**vrf** {<*vrf-name*>| **mng**}]<*server-ip-address*>[**port** <*port-number*>]	向组中添加服务器

port <*port-number*>：定义TACACS+服务器的端口号，范围1025~65535，默认49。

timeout <*timeout*>：连接超时时间，1~1000，单位：秒，此处配置将使全局配置无效。

key {**encrypted** <*secret_key*>|<*password*>}：设备和TACACS+服务器之间的密钥，明文密钥长度1~63个字符（不包括空格），密文密钥长度固定128个字符（不包括空格）。

group-server <*group-name*>：TACACS+服务器组名称，1~31个字符，在TACACS+中支持最多配置256个服务器组，每个组下最多配置4个服务器。

3.验证配置结果。

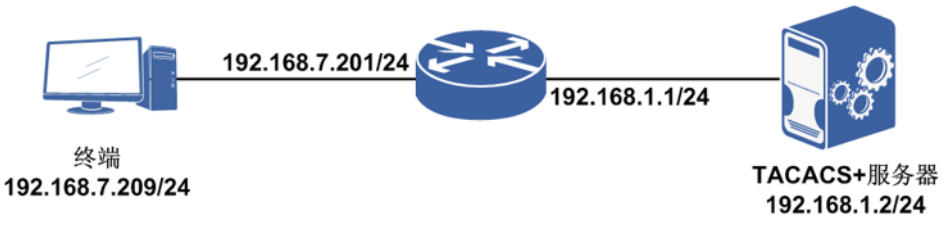
命令	功能
inspur#**show running-config tacplus**	显示当前TACACS+模块的所有配置
inspur#**show tacacs-server**	显示TACACS+服务器的配置信息
inspur#**show tacacs global-config**	显示TACACS+的全局配置信息
inspur#**show tacplus group-server** [<*group-name*>]	显示TACPLUS Group组的配置信息

9.4.2 TACACS+认证授权配置实例

配置说明

如*图 9-7*所示，假设IR12000上设置了TACACS+认证和授权的服务，192.168.7.209是登录IR12000的终端，192.168.1.2是IR12000指定的TACACS+认证和授权服务器。在终端登录设备时需要经过TACACS+认证和授权，通过则可以登录，不通过则提示不能登录。

图 9-7 TACACS+配置实例拓扑图



配置思路

1.开启TACACS+功能。

2.配置TACACS Server。

3.配置TACACS+服务器参数（可选配置）

4.创建TACACS+的TACPLUS group-server，并将之前配置的TACACS Server加入TACPLUS group-server中。

5.配置TACACS+客户端IP地址，作为IR12000路由器和TACACS+服务器通信的IP（可选配置）。

6.配置AAA认证模板；认证模板中配置认证方式为TACACS，认证组为已配置的TACACS组。

7.配置AAA授权模板；授权模板中配置授权方式为local-tacacs，授权组为已配置的TACACS组。

8.配置用户管理模块认证模板和授权模板，用户管理模块模板再绑定AAA模板。

9.创建用户，将用户绑定到用户管理模块模板中。

配置过程

IR12000设备上的配置如下：

```
inspur(config)#tacacs enable
inspur(config)#tacacs-client 192.168.1.1
inspur(config)#tacacs-server host 192.168.1.2 key inspur
inspur(config)#tacplus group-server inspur
inspur(config-sg)#server 192.168.1.2
inspur(config-sg)#exit

inspur(config)#aaa-authentication-template 2001
inspur(config-aaa-authen-template)#aaa-authentication-type tacacs
inspur(config-aaa-authen-template)#authentication-tacacs-group inspur
inspur(config-aaa-authen-template)#exit
inspur(config)#aaa-authorization-template 2001
inspur(config-aaa-author-template)#aaa-authorization-type local-tacacs
inspur(config-aaa-author-template)#authorization-tacacs-group inspur
inspur(config-aaa-author-template)#exit

inspur(config)#system-user
inspur(config-system-user)#authentication-template 1
inspur(config-system-user-authen-temp)#bind     aaa-authentication-template
2001
inspur(config-system-user-authen-temp)#exit
inspur(config-system-user)#authorization-template 1
inspur(config-system-user-author-temp)#bind aaa-authorization-template 2001
inspur(config-system-user-author-temp)#exit
inspur(config-system-user)#user-name who
inspur(config-system-user-username)#bind authentication-template 1
inspur(config-system-user-username)#bind authorization-template 1
inspur(config-system-user-username)#password who
```

配置验证

```
inspur(config)#show running-config tacplus
!<tacplus>
tacacs enable
tacacs-client 192.168.1.1
tacacs-server host 192.168.1.2 key encrypted

30FD73F50A27785F93622A84DDD81BD4908AC3F8B8592C89C1BFFA6FEC35A0D3CA5A47042B
891AE780450CAB513FA47FCEB551F82FC4D1741D58612D9FE71267
tacplus group-server inspur
  server 192.168.1.2
$
!</tacplus>
```

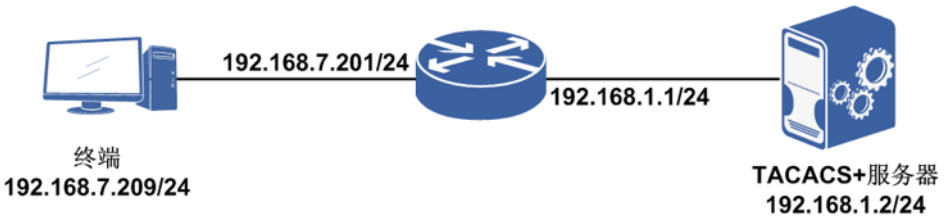
9.4.3 TACACS+记账配置实例

配置说明

如*图 9-8*所示，终端设备登录路由器，经过认证之后，输入命令等操作由路由器的记账功能送到第三方记账软件上，在第三方记账软件TACACS Server上可以看到相关的

记账数据。

图 9-8 TACACS+记账配置实例拓扑图



配置思路

1.路由器上配置TACACS Server group。

2.配置AAA模板并且绑定到记账模板。

3.连接路由器，进行操作，TACACS Server上查看。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#tacacs enable
inspur(config)#tacacs-server host 192.168.1.2
inspur(config)#tacplus group-server wd
inspur(config-sg)#server 192.168.1.2
inspur(config-sg)#exit
inspur(config)#aaa-accounting-template 2001
inspur(config-aaa-acct-template)#aaa-accounting-type tacacs
inspur(config-aaa-acct-template)#accounting-tacacs-group wd
inspur(config-aaa-acct-template)#exit
inspur(config)#system-user
inspur(config-system-user)#account-switch on accounting-template 2001
```

配置验证

在第三方TACACS Server上查看相应的数据库数据记录。

9.5 镜像

镜像功能可以把源端口的部分或全部流量拷贝到另一个专门指定的“镜像端口”或“目的端口”，在不严重影响源端口正常吞吐流量的情况下，通过镜像端口对网络的流量进行监控分析。

镜像的功能简单地说就是将被监控流量镜像到监控端口，以便对被监控流量进行故障定位、流量分析、流量备份等。被监控流量所在端口就称为源端口，监控端口也称为目的端口，目的端口直接与网络分析器等相连。

9.5.1 配置镜像

配置端口镜像功能，有效的提供了对端口的实时监控能力。

1.配置端口镜像。

步骤	命令	功能
1	inspur(config)#**monitor session** <*session-number*>	添加一个镜像会话条目，会话号取值范围1~64
2	inspur(config-monitor-session)#**rule** {**ipv4-access-list** | **ipv6-access-list**}<*acl-name*> **destination** {**interface** <*interface-name*>}	向会话条目添加带ACL的目的端口（带ACL的目的端口至多可配置四条）
3	inspur(config-monitor-session)#**default destination** {**interface** <*interface-name*>}	向会话条目添加默认目的端口（至多配置一条）
4	inspur(config)#**monitor apply session** <*session-number*> **source** {**interface** <*interface-name*>[**direction** {**both** | **rx** | **tx**}]	将指定会话绑定到源接口（每个会话至多可配置八条）

<*session-number*>：会话号，范围1~64。

direction：指定镜像方向，默认为**both**。

both：指定镜像的方向为入向和出向。

rx：指定镜像的方向为入向。

tx：指定镜像的方向为出向，VPWS类型时方向只能为入向。

2.验证配置结果。

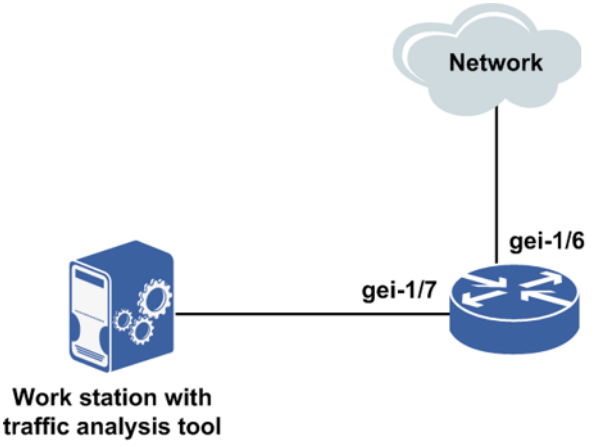
命令	功能
inspur#**show monitor session** {**all** |<*session-number*>}	显示全部或指定会话条目的内容
inspur#**show running-config monitor**	显示当前镜像模块的所有配置

9.5.2 本地端口镜像配置实例

配置说明

端口镜像的作用是分析指定端口的流量情况。如*图 9-9*所示，先对目标端口gei-1/6的RX方向流量进行镜像，再发送给目的端口gei-1/7。其中，目的端口连接的是具有流量分析功能的工作站。

图 9-9 端口镜像配置实例拓扑图



配置思路

1.将一台服务器连在路由器上的一个未使用的端口gei-1/7上。

2.配置端口镜像实例。

3.配置端口镜像的目的端口为gei-1/7。

4.配置端口镜像的源端口为待分析的指定端口gei-1/6的RX方向。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#monitor session 1
inspur(config-monitor-session)#default destination interface gei-1/7
inspur(config-monitor-session)#exit
inspur(config)#monitor apply session 1 source interface gei-1/6 direction rx
```

配置验证

配置完成后用**show**命令检验配置：

```
inspur(config)#show running-config monitor
!<monitor>
monitor session 1
  default destination interface gei-1/7
$
monitor apply session 1 source interface gei-1/6 direction rx
!</monitor>
```

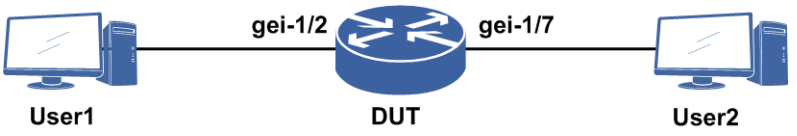
9.5.3 本地流镜像配置实例

配置说明

会话配置了ACL，则认为是流镜像，流镜像只采集经过ACL过滤后的数据包，举例本

地流镜像，组网如*图 9-10*所示。

图 9-10 本地流镜像配置实例拓扑图



配置思路

1.用户1与DUT的gei-1/2直连，用户1发送的数据流自发自收。

2.DUT上配置端口镜像业务，gei-1/2端口流量镜像到目的端口gei-1/7。

3.用户2与DUT设备的gei-1/7直连。

配置过程

DUT上配置如下：

```
inspur(config)#ipv4-access-list inspur
inspur(config-ipv4-acl)#rule permit any
inspur(config-ipv4-acl)#exit
inspur(config)#monitor session 1    /*带ACL的流镜像配置*/
inspur(config-monitor-session)#rule  ipv4-access-list  inspur  destination
interface gei-1/7
inspur(config-monitor-session)#exit
inspur(config)#monitor apply session 1 source interface gei-1/2 direction both
```

配置验证

配置完后用**show**命令查看配置：

```
inspur#show running-config monitor
!<monitor>
monitor session 1
  rule ipv4-access-list inspur destination interface gei-1/7
$
monitor apply session 1 source interface gei-1/2 direction both
!</monitor>
```

同时，用户2上可以监测到gei-1/2端口流量。

9.6 防火墙

IR12000智能路由器系列路由器支持防火墙功能，能对异常和攻击报文进行过滤和丢弃。IR12000智能路由器上的防火墙主要实现硬件防火墙功能，在报文正常转发前检查防火墙策略，并执行相应动作，因此无特殊组网要求。

IR12000智能路由器上的防火墙功能包括：

·IP源防攻击功能

·区域内策略

·区域间策略

9.6.1 配置 IP 源防攻击功能

本节介绍了配置IP+MAC绑定和配置IP Source Guard功能的过程和命令，用来实现IP源防攻击功能。

1.配置IP+MAC绑定功能，过滤非绑定的MAC的数据包。

步骤	命令	功能
1	inspur(config)#**arp**	进入ARP配置模式
2	inspur(config-arp)#**arp** <*interface-name*> **permanent** <*ip-address*><*mac-address*>	针对接口配置某IP地址的永久ARP

<*ip-addr-start*>：扫描起始网络地址的前缀，为十进制点分形式。

<*ip-addr-end*>：扫描结尾网络地址的前缀，为十进制点分形式。

2.配置ARP扫描及静态化功能，过滤非绑定的MAC的数据包。

步骤	命令	功能
1	inspur#**arp-scan** <*interface-name*><*ip-addr-start*><*ip-addr-end*>	在全局模式下进行ARP扫描，自动获得IP+MAC地址对进入IP Source Guard配置模式
2	inspur(config)#**arp**	进入ARP配置模式
3	inspur(config-arp)#**to-static**	批量将动态ARP变为静态ARP，从而实现MAC与IP的绑定

3.验证配置结果。

命令	功能
inspur#**show arp**	查看ARP条目的学习情况

9.6.2 配置防火墙区域内策略

本节介绍了黑/白名单功能、区域内防攻击功能的配置命令和过程。防火墙区域内策略是报文始发区域要执行的安全策略。

1.创建防火墙区域实例。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**zone security** <*zone-name*> **priority** <*priority of zone security*>	创建区域，并为区域命名，指定区域的优先级

<*priority of zone security*>：区域优先级，取值范围1~254。

2.配置黑名单功能。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**blacklist**	进入黑名单配置模式
3	inspur(config-fw-black)#**ip blacklist** <*ip-address*>[**vrf** <*vpn-name*>][**time-range** <*timerange-name*>]	配置黑名单列表
4	inspur(config-fw)#**zone security** <*zone-name*>	进入已创建区域的配置模式
5	inspur(config-fw-zone)#**blacklist enable**	在该区域内开启黑名单功能

3.配置白名单功能。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**whitelist**	进入白名单配置模式
3	inspur(config-fw-black)#**ip whitelist** <*ip-address*>[**vrf** <*vpn-name*>][**time-range** <*timerange-name*>]	配置白名单列表
4	inspur(config-fw)#**zone security** <*zone-name*>	进入已创建区域的配置模式
5	inspur(config-fw-zone)#**whitelist enable**	在该区域内开启白名单功能

4.配置区域内防攻击功能。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**zone security** <*zone-name*>	进入已创建区域的配置模式
3	inspur(config-fw-zone)#**ip defend all**	开启全部防攻击功能

步骤	命令	功能
4	inspur(config-fw-zone)#**ip defend fin-no-ack**	开启fin-no-ack防攻击功能
	inspur(config-fw-zone)#**ip defend fraggle**	开启fraggle防攻击功能
	inspur(config-fw-zone)#**ip defend icmp-fragment**	开启icmp-fragment防攻击功能
	inspur(config-fw-zone)#**ip defend icmp-redirect**	开启icmp-redirect防攻击功能
	inspur(config-fw-zone)#**ip defend icmp-unreachable**	开启icmp-unreachable防攻击功能
	inspur(config-fw-zone)#**ip defend ip-fragment**	开启ip-fragment防攻击功能
	inspur(config-fw-zone)#**ip defend ip-option-attact**	开启ip-option-attact防攻击功能
	inspur(config-fw-zone)#**ip defend land-attact**	开启land-attact防攻击功能
	inspur(config-fw-zone)#**ip defend malform-ip-option**	开启malform-ip-option防攻击功能
	inspur(config-fw-zone)#**ip defend ping-death**	开启ping-death防攻击功能
	inspur(config-fw-zone)#**ip defend smurf**	开启smurf防攻击功能
	inspur(config-fw-zone)#**ip defend tcp-no-flag**	开启tcp-no-flag防攻击功能
	inspur(config-fw-zone)#**ip defend tcp-syn-fin**	开启tcp-syn-fin防攻击功能
	inspur(config-fw-zone)#**ip defend tcp-syn-fragment**	开启tcp-syn-fragment防攻击功能
	inspur(config-fw-zone)#**ip defend teardrop**	开启teardrop防攻击功能
	inspur(config-fw-zone)#**ip defend tracert**	开启tracert防攻击功能
	inspur(config-fw-zone)#**ip defend**	开启unknown-protocol防攻击功能
	inspur(config-fw-zone)#**ip defend winnuke**	开启winnuke防攻击功能
	inspur(config-fw-zone)#**ip defend larg-ping** <*Max-ping-length*>	开启large-ping防攻击功能 <*Max-ping-length*>取值范围1~65507
	inspur(config-fw-zone)#**ip defend udp-flood** <*Committed packets per second*>	开启udp-flood反攻击功能 <*Committed packets per second*>取值范围10~10000000

步骤	命令	功能
	inspur(config-fw-zone)#**ip defend icmp-flood** <*Committed packets per second*>	开启icmp-flood防攻击功能 <*Committed packets per second*>取值范围10~10000000
	inspur(config-fw-zone)#**ip defend syn-flood** <*Committed packets per second*>	开启syn-flood防攻击功能 <*Committed packets per second*>取值范围10~10000000

如果不配置步骤3中的开启全部防攻击功能，则可以根据实际需要，按照步骤4中的配置，开启需要的防攻击功能。

5.配置区域内虚拟分片重组功能。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**zone security** <*zone-name*>	进入已创建区域的配置模式
3	inspur(config-fw-zone)#**ip virtual-reassembly**	开启虚拟分片重组功能

6.配置源目的会话数限制功能。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**zone security** <*zone-name*>	进入已创建区域的配置模式
3	inspur(config-fw-zone)#**session limit source-ip-based** <*session number threshold*>	配置源区域会话数限制功能
	inspur(config-fw-zone)#**session limit destination-ip-based** <*session number threshold*>	配置目的区域会话数限制功能

7.将接口与区域绑定。

步骤	命令	功能
1	inspur(config)#**interface** <*interface-name*>	进入接口配置模式
2	inspur(config-if)#**zone-member security** <*zone-name*>	将接口与指定区域绑定

8.验证配置结果。

命令	功能
inspur(config)#**show firewall blacklist**	查看配置的黑名单信息
inspur(config)#**show firewall whitelist**	查看配置的白名单信息
inspur(config)#**show firewall ip defend zone** <*zone-name*>	查看防攻击配置信息
inspur(config)#**show firewall ip virtual-reassembly zone** <*zone-name*>	查看虚拟分片重组配置

9.6.3 配置防火墙区域间策略

本节介绍了配置应用状态防火墙功能、配置WEB/IM/UDP字符串过滤功能的配置过程和命令。

1.创建区域间实例。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**zone-pair security** <*zone-pair-name*> **source** <*zone-name1*> **destination** <*zone-name2*>	创建区域间实例

2.配置区域间策略。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**zone-pair security** <*zone-pair-name*>	进入已创建的区间实例
3	inspur(config-fw-pair)#**ipv4-access-group** <*acl-name*>	配置区域间策略

3.配置应用状态防火墙FTP/SIP功能。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**zone-pair security** <*zone-pair-name*>	进入已创建区间的配置模式
3	inspur(config-fw-pair)#**stateful inspect**	配置应用状态防火墙

步骤	命令	功能
	{**ftp** | **sip** }	

4.配置WEB过滤列表。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**http url-filter-list**	进入URL过滤列表配置模式
3	inspur(config-fw-url)#**http** {[**host** <*host-name*>][**url** <*url-string*>][**mime** <*mime-type*>]}[**time-range** <*timerange-name*>]}	配置URL过滤列表

<*host-name*>：范围1~63个字符。

<*url-string*>：范围1~127个字符。

<*mime-type*>：范围1~63个字符。

<*timerage-name*>：范围1~31个字符。

5.配置应用状态防火墙WEB过滤功能。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**zone-pair security** <*zone-pair-name*>	进入区域间策略配置模式
3	inspur(config-fw-pair)#**stateful inspect http url-filter**	配置URL过滤功能
	inspur(config-fw-pair)#**stateful inspect http activex-block**	配置activex过滤功能
	inspur(config-fw-pair)#**stateful inspect http javaapplet-block**	配置javaapplet过滤功能

6.配置IM过滤列表。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**instant-msg svr-block-list**	进入IM过滤列表配置模式
3	inspur(config-fw-im)#**server** <*svr-name*><*ip-address*>[{**tcp** | **udp**}<*port*>][**time-range** <*timerange-name*>]	配置IM服务器列表

<*svr-name*>：范围1~31个字符。

<*port*>：范围1~65535个字符。

<*timerage-name*>：范围1~31个字符。

7.配置应用状态防火墙IM过滤功能。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**zone-pair security** <*zone-pair-name*>	进入区域间策略配置模式
3	inspur(config-fw-pair)#**stateful inspect instant-msg qq-block** [**time-range** <*timerange-name*>]	配置QQ过滤功能
	inspur(config-fw-pair)#**stateful inspect instant-msg msn-block** [**time-range** <*timerange-name*>]	配置MSN过滤功能
	inspur(config-fw-pair)#**stateful inspect instant-msg server-block**	配置自定义过滤功能

<*timerage-name*>：范围1~31个字符。

8.配置UDP过滤列表。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**udp data-filter-list**	进入UDP滤列表配置模式
3	inspur(config-fw-im)#**udp-data offset** <*offset-value*>{**include** | **match**}<*match-string*>[**time-range** <*timerange-name*>]	配置UDP过滤列表

<*offset-value*>：范围0~1472。

<*match-string*>：范围1~31个字符。

<*timerage-name*>：范围1~31个字符。

9.配置应用状态防火墙UDP过滤功能。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**zone-pair security** <*zone-pair-name*>	进入区域间策略配置模式

步骤	命令	功能
3	inspur(config-fw-pair)#**stateful inspect udp data-filter**	配置UDP过滤功能

10.配置应用状态防火墙股票证券过滤功能。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**zone-pair security** <*zone-pair-name*>	进入区域间策略配置模式
3	inspur(config-fw-pair)#**stateful inspect stock-trading-block** [**time-range** <*timerange-name*>]	配置股票证券过滤功能

<*timerage-name*>：范围1~31个字符。

11.验证配置结果。

命令	功能
inspur#**show firewall zone-pair security** <*pair-name*>	查看区域间策略配置

9.6.4 配置 TCP 拦截功能

本节介绍了TCP拦截功能的配置步骤和命令。

1.创建区域间实例。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**zone-pair security** <*zone-pair-name*> **source** <*zone-name1*> **destination** <*zone-name2*>	创建区域间实例

2.配置TCP拦截参数。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**ip tcp intercept drop-mode** {**oldest** | **random**}	配置老化方式

步骤	命令	功能
3	inspur(config-fw)#**ip tcp intercept finrst-timeout** <*time*>	配置接收到FIN/RST后的老化时间
4	inspur(config-fw)#**ip tcp intercept max-incomplete high** <*high-threshold*> **low** <*low-threshold*>	配置水线阈值上下限
5	inspur(config-fw)#**ip tcp intercept one-minute high** <*high-threshold*> **low** <*low-threshold*>	配置一分钟水线阈值上下限
6	inspur(config-fw)#**ip tcp intercept mode watch**	配置TCP拦截方式为监控方式
7	inspur(config-fw)#**ip tcp intercept watch-timeout** <*watch-time*>	配置监控半连接时间

<*time*>：范围1秒~10秒。

<*high-threshold*>：范围1~500000。

<*low-threshold*>：范围1~500000。

<*watch-time*>：范围1秒~60秒。

3.绑定TCP拦截过滤列表。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**zone-pair security** <*zone-pair-name*>	进入已创建区间的配置模式
3	inspur(config-fw-pair)#**ip tcp intercept list** <*tcp-acl*>	绑定TCP拦截过滤列表

<*tcp-acl*>：范围1~31个字符。

4.验证配置结果。

命令	功能
inspur#**show running-config firewall** [**all**]	显示防火墙配置信息

9.6.5 基于协议和端口号设置老化时间

本节介绍了基于协议和端口号的会话老化时间配置步骤和命令。

1.创建区域间实例。

步骤	命令	功能
1	inspur(config)#**firewall**	进入防火墙配置模式
2	inspur(config-fw)#**session timeout** {**ftp**|**http**|**icmp**|**sip**|**tcp**|**tcp-port** <*port-number*>|**udp**|**udp-port** <*port-number*>}<*time*>	配置老化时间

<*port-number*>：协议端口号，取值范围0~65535。

<*time*>：协议会话的老化时间，取值范围1~7200，单位秒。

2.验证配置结果。

命令	功能
inspur#**show running-config firewall** [**all**]	显示防火墙配置信息

9.6.6 IP 源防攻击配置实例

配置说明

配置IP+MAC绑定功能，实现IP与MAC绑定过滤。下面的配置思路1和2是两种并列的实现方式，分别是配置永久ARP和ARP扫描静态化。

配置思路

1.ARP配置模式下配置永久ARP条目实现MAC绑定IP

2.配置ARP扫描，在ARP模式下通过**to-static**命令批量将动态ARP变为静态ARP，从而实现MAC绑定IP

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#arp
inspur(config-arp)#arp gei-5/2 permanent 30.0.2.2 0001.0001.0001
 /*配置永久ARP绑定*/
inspur(config-arp)#exit

inspur#arp-scan gei-5/1.1 30.0.1.2 30.0.1.2     /*在接口下配置ARP扫描功能*/
inspur(config-arp)#to-static    /*将动态ARP变为静态ARP，实现MAC绑定IP*/
inspur(config-arp)#exit
```

配置验证

执行命令**show arp**查看MAC绑定IP的信息：

```
inspur(config-arp)#show arp
Arp protect whole is disabled
The count is 6
IP                  Hardware                Exter  Inter  Sub
Address       Age     Address       Interface    VlanID VlanID Interface
------------------------------------------------------------------------------
------
30.0.1.1      H       0a0b.0cd1.b4a1  gei-5/1.1      1    N/A    N/A
30.0.1.2      TS      0000.1e00.0101  gei-5/1.1      1    N/A    gei-5/1.1
30.0.2.1      H       0a0b.0cd1.b4a1  gei-5/2       N/A   N/A    N/A
30.0.2.2      P       0001.0001.0001  gei-5/2       N/A   N/A    N/A
```

9.6.7 黑名单配置实例

配置说明

本实例介绍配置黑名单，并开启黑名单过滤功能。

配置思路

1.进入防火墙配置模式。

2.配置黑名单列表。

3.配置区域。

4.区域配置模式下开启黑名单。

5.接口绑定区域。

配置过程

IR12000智能路由器上的配置过程如下：

```
inspur(config)#time-range enable
inspur(config)#time-range tr1
inspur(config-tr-tr1)#periodic daily 00:00:00 23:00:00
inspur(config-tr-tr1)#exit
inspur(config)#firewall
inspur(config-fw)#blacklist
inspur(config-fw-black)#ip blacklist 30.0.2.2 time-range tr1
/*配置黑名单列表*/
inspur(config-fw-black)#exit

inspur(config-fw)#zone security test1 priority 1
inspur(config-fw-zone)#(config-fw)#blacklist enable
/*在该区域内开启黑名单功能*/
inspur(config-fw-zone)#exit
inspur(config-fw)#exit

inspur(config)#interface gei-5/1
inspur(config-if-gei-5/1)#zone-member security test1
```

```
/*将接口与指定区域绑定*/
inspur(config-if-gei-5/1)#exit

inspur(config)#interface gei-5/2
inspur(config-if-gei-5/2)#zone-member security test1
/*将接口与指定区域绑定*/
inspur(config-if-gei-5/2)#exit
```

配置验证

执行命令**show firewall blacklist**查看黑名单配置：

```
inspur(config)#show firewall blacklist
Ip-Address      Vrf                  Hit-Count       Time-Range
30.0.2.2        N/A                  0               tr1
```

9.6.8 白名单配置实例

配置说明

本实例介绍了配置白名单并开启白名单功能。

配置思路

1.进入防火墙配置模式。

2.配置白名单列表。

3.配置区域。

4.区域配置模式下开启白名单。

5.接口绑定区域。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#firewall
inspur(config-fw)#whitelist
inspur(config-fw-black)#ip whitelist 30.0.1.2
/*配置白名单列表*/
inspur(config-fw-black)#exit

inspur(config-fw)#zone security test1 priority 1
inspur(config-fw-zone)#whitelist enable
/*在该区域内开启白名单功能*/
inspur(config-fw-zone)#exit
inspur(config-fw)#exit

inspur(config)#interface gei-5/1
inspur(config-if-gei-5/1)#zone-member security test1
/*将接口与指定区域绑定*/
inspur(config-if-gei-5/1)#exit
```

```
inspur(config)#interface gei-5/2
inspur(config-if-gei-5/2)#zone-member security test1
/*将接口与指定区域绑定*/
inspur(config-if-gei-5/2)#exit
```

配置验证

执行命令**show firewall whitelist**查看白名单配置：

```
inspur#show firewall whitelist
Ip-Address      Vrf                   Hit-Count       Time-Range
30.0.1.2        N/A                   0               N/A
```

9.6.9 防攻击配置实例

配置说明

本实例介绍了在区域内配置防攻击功能。

配置思路

1.进入防火墙配置模式。

2.配置区域。

3.区域配置模式下配置防攻击功能。

4.接口绑定区域。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#firewall
inspur(config-fw)#zone security test1 priority 1
/*创建防火墙区域实例*/
inspur(config-fw-zone)#ip defend smurf
/*开启smurf防攻击功能*/
inspur(config-fw-zone)#ip defend unknown-protocol
/*开启unknown-protocol防攻击功能*/
inspur(config-fw-zone)#ip defend land-attact
/*开启land-attact防攻击功能*/
inspur(config-fw-zone)#exit
inspur(config-fw)#exit

inspur(config)interface gei-5/1
inspur(config-if-gei-5/1)#zone-member security test1
/*将接口与指定区域绑定*/
inspur(config-if-gei-5/1)#exit
inspur(config)#interface gei-5/2
inspur(config-if-gei-5/2)#zone-member security test1
/*将接口与指定区域绑定*/
inspur(config-if-gei-5/2)#exit
```

配置验证

执行命令**show firewall ip defend zone**查看防攻击配置：

```
inspur(config)#show firewall ip defend zone test1
Ip-Defend          Admin       Hit-Count
land-attact         ON          0
smurf              ON          0
winnuke            ON          0
syn-flood           ON          0
udp-flood           ON          0
icmp-flood          ON          0
ping-death          ON          0
icmp-unreachable     ON          0
icmp-fragment       ON          0
teardrop           ON          0
tracert            ON          0
tcp-syn-fragment     OFF         0
ip-option-attact     OFF         0
tcp-syn-fin         ON          0
larg-ping          ON          0
icmp-redirect       ON          0
ip-fragment         ON          0
fraggle            ON          0
malform-ip-option    ON          0
unknown-protocol     OFF         0
tcp-no-flag         ON          0
fin-no-ack          ON          0
```

9.6.10 0 虚拟分片重组功能配置实例

配置说明

本实例介绍了配置虚拟分片重组功能。

配置思路

1.进入防火墙配置模式。

2.配置区域。

3.区域配置模式下开启虚拟分片重组功能。

4.接口绑定区域。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#firewall
inspur(config-fw)#zone security test1 priority 1
/*创建防火墙区域实例*/
inspur(config-fw-zone)#ip virtual-reassembly
/*开启区域内虚拟分片重组功能*/
inspur(config-fw-zone)#exit
inspur(config-fw)#exit
```

```
inspur(config)#interface gei-5/1
inspur(config-if-gei-5/1)#zone-member security test1
/*将接口与指定区域绑定*/
inspur(config-if-gei-5/1)#exit
inspur(config)#interface gei-5/2
inspur(config-if-gei-5/2)#zone-member security test1
/*将接口与指定区域绑定*/
inspur(config-if-gei-5/2)#exit
```

配置验证

执行命令**show firewall ip virtual-reassembly zone**查看虚拟分片重组配置：

```
inspur(config-fw-zone)#show firewall ip virtual-reassembly zone test1
ip virtual-reassembly: enable
```

9.6.11 区域间策略配置实例

配置说明

本实例介绍了配置区域间策略。

配置思路

1.配置ACL策略。

2.进入防火墙配置模式。

3.配置不同优先级的区域。

4.配置区域间实例。

5.区域间实例配置区域间策略。

6.接口绑定区域。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#ipv4-access-list acl
inspur(config-ipv4-acl)#rule 1 permit tcp any any eq www
inspur(config-ipv4-acl)#rule 2 permit tcp any any eq ftp
inspur(config-ipv4-acl)#rule 3 permit tcp any any eq pop3
inspur(config-ipv4-acl)#exit

inspur(config)#firewall
inspur(config-fw)#zone security test1 priority 1
inspur(config-fw-zone)#exit
inspur(config-fw)#zone security test2 priority 2
inspur(config-fw-zone)#exit
inspur(config-fw)#zone-pair security pair2 source test1 destination test2
```

```
inspur(config-fw-pair)#(config-fw)#ipv4-access-group acl
/*应用区域间策略,后面的区域间策略都基于此策略*/
inspur(config-fw-pair)#stateful inspect ftp
inspur(config-fw-pair)#stateful inspect sip
inspur(config-fw-pair)#stateful inspect http url-filter
inspur(config-fw-pair)#stateful inspect http activex-block
inspur(config-fw-pair)#stateful inspect http javaapplet-block
inspur(config-fw-pair)#stateful inspect instant-msg qq-block
inspur(config-fw-pair)#stateful inspect instant-msg msn-block
inspur(config-fw-pair)#stateful inspect instant-msg svr-block
inspur(config-fw-pair)#stateful inspect udp data-filter
inspur(config-fw-pair)#stateful inspect stock-trading-block
inspur(config-fw-pair)#!

inspur(config)#interface gei-5/1
inspur(config-if-gei-5/1)#zone-member security test1
/*将接口与指定区域绑定*/
inspur(config-if-gei-5/1)#exit
inspur(config)#interface gei-5/2
inspur(config-if-gei-5/2)#zone-member security test2
/*将接口与指定区域绑定*/
inspur(config-if-gei-5/2)#exit
```

配置验证

执行命令**show firewall zone-pair security**查看区域间策略配置：

```
inspur#show firewall zone-pair security pair2
source zone security: test1                    priority: 1
dest zone security  : test2                    priority: 2
ipv4-access-group: acl
stateful inspect:
  ftp      :ON  sip          :ON  udp-filter     :ON
  url-filter:ON  activex-block :ON  javaapplet-block:ON
  qq-block  :ON  msn-block     :ON  server-block    :ON
  stock-trading-block:ON
```

9.6.12 过滤列表配置实例

配置说明

配置过滤列表功能要与区域间的应用状态防火墙配合使用。本实例介绍了配置IM过滤列表、WEB过滤列表和UDP字符串过滤列表。

配置思路

1.进入防火墙配置模式。

2.配置IM过滤列表。

3.配置WEB过滤列表。

4.配置UDP过滤列表。

配置过程

IR12000智能路由器上的配置如下。

1.进入防火墙配置模式：

```
inspur(config)#firewall
```

2.配置instant-msg服务器列表：

```
inspur(config-fw)#instant-msg svr-block-list
inspur(config-fw-im)#server qq 119.147.45.223 tcp 80 time-range tr1
inspur(config-fw-im)#server qq 112.95.240.10 tcp 443
inspur(config-fw-im)#server qq 12.90.84.75 udp 8000
inspur(config-fw-im)#server msn 64.4.9.190 tcp 863
```

3.配置WEB过滤：

```
inspur(config-fw)#http url-filter-list
inspur(config-fw-url)#http host *.qq.com time-range tr1
inspur(config-fw-url)#http host *.bt.com url *.torrent
inspur(config-fw-url)#http host *.youku.com url *.swf
inspur(config-fw-url)#http mime application/x-shockwave-flash
```

4.配置UDP过滤：

```
inspur(config-fw)#udp data-filter-list
inspur(config-fw-udp)#udp-data offset 0 include a time-range tr1
inspur(config-fw-udp)#udp-data offset 0 include b
```

配置验证

执行命令**show firewall instant-msg svr-block-list**查看IM列表：

```
inspur#show firewall instant-msg svr-block-list
Svr-Name                    Ip-Addr        Tcp/Udp  Port  Time-Range
msn                         64.4.9.190      TCP     863
qq                          12.90.84.75     UDP     8000
qq                          112.95.240.10   TCP     443
qq                          119.147.45.223  TCP     80    tr1
```

执行命令**show firewall http url-filter-list**查看HTTP过滤列表：

```
inspur#show firewall http url-filter-list
http filter rule:
  host: *.youku.com
  url : *.swf
  time-range:

http filter rule:
  host: *.bt.com
  url : *.torrent
  time-range:

http filter rule:
  host: *.qq.com
  url : *
  time-range: tr1

http filter rule:
  mime-type: application/x-shockwave-flash
  time-range:
```

执行命令**show firewall udp data-filter-list**查看UDP过滤列表：

```
inspur#show firewall udp data-filter-list
Offset Mode    Keyword                      Time-Range
```

```
0     include  b
0     include  a                          tr1
```

9.6.13 TCP 拦截功能配置实例

配置说明

本实例介绍TCP拦截的使用和配置。

配置思路

1.配置TCP-ACL策略。

2.进入防火墙配置模式。

3.配置TCP拦截参数。

4.配置不同优先级的区域。

5.配置区域间实例。

6.区域间实例绑定拦截TCP-ACL。

7.接口绑定区域。

配置过程

IR12000智能路由器上的配置如下。

```
inspur(config)#ipv4-access-list tcp-acl
inspur(config-ipv4-acl)#rule 1 permit any
inspur(config-ipv4-acl)#exit

inspur(config)#firewall
inspur(config-fw)#ip tcp intercept drop-mode oldest
inspur(config-fw)#ip tcp intercept finrst-timeout 10
inspur(config-fw)#ip tcp intercept max-incomplete high 500000 low 500000
inspur(config-fw)#ip tcp intercept one-minute high 500000 low 500000
inspur(config-fw)#ip tcp intercept mode watch
inspur(config-fw)#ip tcp intercept watch-timeout 30
inspur(config-fw)#zone security test1 priority 1
inspur(config-fw-zone)#exit
inspur(config-fw)#zone security test2 priority 2
inspur(config-fw-zone)#exit
inspur(config-fw)#zone-pair security pair2 source test1 destination test2
inspur(config-fw-pair)#ip tcp intercept list tcp-acl
inspur(config-fw-pair)#!

inspur(config)#interface gei-5/1
inspur(config-if-gei-5/1)#zone-member security test1
/*将接口与指定区域绑定*/
inspur(config-if-gei-5/1)#exit
inspur(config)#interface gei-5/2
inspur(config-if-gei-5/2)#zone-member security test2
/*将接口与指定区域绑定*/
inspur(config-if-gei-5/2)#exit
```

配置验证

执行命令**show running-config firewall**查看TCP拦截策略配置：

```
inspur#show running-config firewall
!<firewall>
firewall
  zone security test1 priority 1
  $
  zone security test2 priority 2
  $
  ip tcp intercept finrst-timeout 10
  ip tcp intercept max-incomplete high 500000 low 500000
  ip tcp intercept mode watch
  ip tcp intercept one-minute high 500000 low 500000
  zone-pair security pair2 source test1 destination test2
    ip tcp intercept list tcp-acl
  $
$
interface gei-5/2
  zone-member security test2
$
interface gei-5/1
  zone-member security test1
$
!<firewall>
```

9.6.14 基于协议和端口号的会话老化时间配置实例

配置说明

本实例介绍基于协议和端口号的会话老化时间的配置。

配置思路

1.配置ACL

2.进入防火墙配置模式。

3.配置区域间实例并绑定状态ACL。

4.配置基于协议和端口的老化时间。

5.接口绑定区域。

配置过程

IR12000智能路由器上的配置如下。

```
inspur(config)#ipv4-access-list acl
inspur(config-ipv4-acl)#rule 1 permit any
inspur(config-ipv4-acl)#exit

inspur(config)#firewall
inspur(config-fw)#zone security test1 priority 1
inspur(config-fw-zone)#exit
inspur(config-fw)#zone security test2 priority 2
```

```
inspur(config-fw-zone)#exit
inspur(config-fw)#zone-pair security pair2 source test1 destination test2
inspur(config-fw-pair)#ipv4-access-group acl
inspur(config-fw-pair)#exit
inspur(config-fw)#session timeout tcp 7200
inspur(config-fw)#exit

inspur(config)#interface gei-5/1
inspur(config-if-gei-5/1)#zone-member security test1
/*将接口与指定区域绑定*/
inspur(config-if-gei-5/1)#exit
inspur(config)#interface gei-5/2
inspur(config-if-gei-5/2)#zone-member security test2
/*将接口与指定区域绑定*/
inspur(config-if-gei-5/2)#exit
```

配置验证

已建立的TCP会话的老化时间变为7200秒。

9.7 DPI

DPI（Deep Packet Inspection，深度包检测）是一种基于应用层的流量检测和控制技术。普通报文检测仅仅分析IP包的四层以下的内容，包括源地址、目的地址、源端口、目的端口以及协议类型，而DPI则在此基础上，增加了对应用层的分析，可识别出各种应用及其内容。

DPI将网络上的数据报文根据五元组分为一个个的应用流，并通过识别技术对应用流中的特定数据报文进行探测，从而确定应用流对应的应用或者用户的动作。针对不同的协议类型，识别技术可划分为以下三类：

·基于特征字的识别技术

·应用层网关识别技术

·行为模式识别技术

这三类识别技术分别适用于不同类型的协议，相互之间无法替代。综合运用这三种识别技术，可高效、灵活地识别出网络上的各种应用。

9.7.1 配置 DPI

在IR12000智能路由器上配置DPI的相关策略，深度检测、识别流量。

1.配置DPI策略。

步骤	命令	功能
1	`inspur(config)#`**dpi**	进入DPI配置模式
2	`inspur(config-dpi)#`**dpi-policy** *<policy-id>*	进入dpi-policy配置模式

步骤	命令	功能
3	inspur(config-dpi-policy-id)#**match protocol** <*category*><*protocol-name*>	配置需要识别的协议
4	inspur(config-dpi-policy-id-pid-id)#**drop**	设置动作为丢弃
	inspur(config-dpi-policy-id-pid-id)#**set** <*action*>	配置指定协议的动作
5	inspur(config-dpi)#**analyse interface** <*interface-name*>[**dpi-policy** <*policy-id*>]	配置接口绑定DPI策略

<*policy-id*>：DPI的策略号，取值范围1~128。

<*category*>：协议分类，有email/web/p2p/voip等。

<*protocol-name*>：协议名称。

set <*action*>包括下面几种：

- **set ip dscp** <*dscp-value*>：设置DSCP值，参数范围0~63。
- **set ip prec** <*prec-value*>：设置precedence值，参数范围0~7。
- **set ip tos** <*tos-value*>：设置ToS值，参数范围0~15。
- **set tcp fin**：强制TCP打上FIN标记。
- **set tcp reset**：强制TCP打上Reset标记。

2.配置QoS支持DPI流分类。

步骤	命令	功能
1	inspur(config)#**class-map** <*class-map-name*>{**match-all** | **match-any**}[**ipv4**]	创建class-map并进入类映射配置模式
2	inspur(config-cmap)#**match protocol** <*category*><*protocol-name*>	根据DPI识别的协议来建立class-map数据流

提示：

必须在流量经过的任一接口上开启DPI功能（analyse interface <*interface-name*>）才能使match protocol的流分类生效。

3.验证配置结果。

命令	功能
inspur#**show dpi protocol**	显示DPI协议名称及分类信息
inspur#**show dpi policy** [<*policy-id*>]	显示DPI策略的配置信息
inspur#**show running-config dpi**	显示DPI的所有配置信息

4.维护DPI。

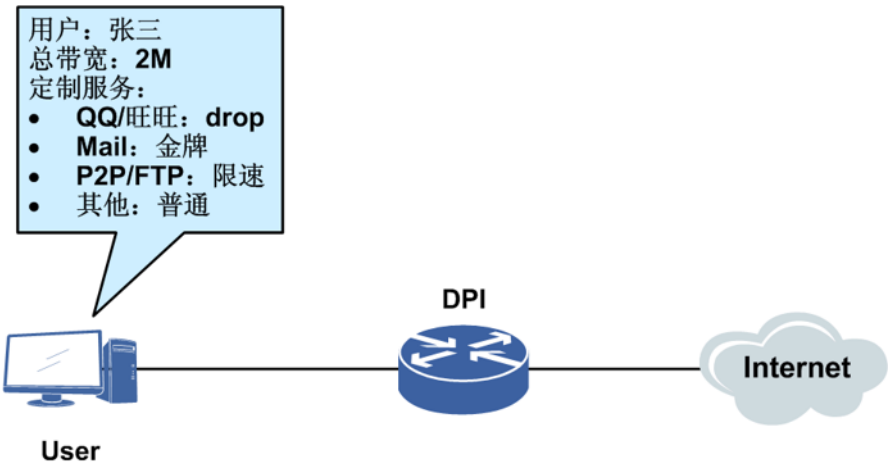
命令	功能
inspur#**show dpi statistic** [**drop**|<*category*><*protocol-name*>[**drop**]| **classified** <*category*>[**drop**]]	显示DPI全局统计信息
inspur#**clear dpi statistic** [<*category*><*protocol-name*>|**classified** <*category*>]	清除DPI统计信息

9.7.2 DPI 配置实例

配置说明

如*图 9-11*所示的网络中给出了一个DPI的配置实例，用户定制服务阻止QQ/ali-wangwang的协议通过，设置P2P/FTP协议的下载限速，并设置Mail协议为高优先级，其它协议为普通优先级。

图 9-11 DPI 配置实例组网图



配置思路

1.配置丢弃QQ/ali-wangwang协议的DPI策略，并在用户侧接口绑定此DPI策略

2.配置基于Mail协议和P2P/FTP协议的流分类

3.配置QoS策略，Mail流量进入PQ高优先级队列优先发送，对P2P/FTP的下载流量限速为1 M

4.在用户侧接口上绑定QoS策略

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#dpi
inspur(config-dpi)#dpi-policy 1
inspur(config-dpi-policy-1)#match protocol im qq   /*配置需要识别的协议是qq*/
inspur(config-dpi-policy-1-pid-107)#drop     /*丢弃qq协议*/
inspur(config-dpi-policy-1-pid-107)#exit
inspur(config-dpi-policy-1)#match protocol im ali-wangwang
/*配置需要识别的协议是ali-wangwang*/
inspur(config-dpi-policy-1-pid-21)#drop      /*丢弃ali-wangwang协议*/
inspur(config-dpi-policy-1-pid-21)#exit
inspur(config-dpi-policy-1)#exit
inspur(config-dpi)#analyse interface gei-0/1 dpi-policy 1
/*在接口gei-0/1上绑定DPI策略*/
inspur(config-dpi)#exit

inspur(config)#class-map email match-any      /*创建class-map，名为email*/
inspur(config-cmap)#match protocol email imap
inspur(config-cmap)#match protocol email imap-ssl
inspur(config-cmap)#match protocol email pop3
inspur(config-cmap)#match protocol email pop3-ssl
inspur(config-cmap)#match protocol email smtp
inspur(config-cmap)#match protocol email smtp-ssl
inspur(config-cmap)#exit
inspur(config)#class-map p2p&ftp match-any    /*创建class-map，名为p2p&ftp*/
inspur(config-cmap)#match protocol p2p thunder
inspur(config-cmap)#match protocol p2p qq-download
inspur(config-cmap)#match protocol p2p web-thunder
inspur(config-cmap)#match protocol p2p bt
inspur(config-cmap)#match protocol p2p dht
inspur(config-cmap)#match protocol p2p edk
inspur(config-cmap)#match protocol p2p kad
inspur(config-cmap)#match protocol filetrans ftp-control
inspur(config-cmap)#match protocol filetrans ftp-data
inspur(config-cmap)#exit

inspur(config)#policy-map test   /*创建名为test的策略映射*/
inspur(config-pmap)#class email
inspur(config-pmap-c)#priority-level 1
inspur(config-pmap-c)#exit
inspur(config-pmap)#class p2p&ftp
inspur(config-pmap-c)#police  cir  1024  cbs  10  conform-action  transmit
exceed-action
 drop violate-action drop /*配置限速策略*/
inspur(config-pmap-c)#exit
inspur(config-pmap)#exit
inspur(config)#service-policy gei-0/1 output test
/*在接口gei-0/1的出方向上应用test策略映射*/
```

配置验证

显示DPI策略的配置信息：

```
inspur(config)#show dpi policy
DPI POLICY ID: 1
MATCH RULE:
PID  PROTOCOL NAME                 ACTION
---- ------------------------------ -------------------------
21   im.ali-wangwang               drop
107  im.qq                        drop
```

显示流分类及其匹配选项：

```
inspur(config)#show class-map
class-map email match-any
  match protocol email imap
  match protocol email imap-ssl
  match protocol email pop3
```

```
  match protocol email pop3-ssl
  match protocol email smtp
  match protocol email smtp-ssl
class-map p2p&ftp match-any
  match protocol p2p thunder
  match protocol p2p qq-download
  match protocol p2p web-thunder
  match protocol p2p bt
  match protocol p2p dht
  match protocol p2p edk
  match protocol p2p kad
  match protocol filetrans ftp-control
  match protocol filetrans ftp-data
```

显示所有策略映射以及策略类和相关的动作：

```
inspur(config)#show policy-map
policy-map test
  class email
    priority-level 1
  class p2p&ftp
    police cir 1024 cbs 10 conform-action transmit exceed-action
      drop violate-action drop
```

9.8 SSL 和 PKI

SSL协议是一个安全协议。SSL协议是介于HTTP协议和TCP协议之间的一个可选协议，为端到端的通信提供的私密性和可靠性。在实际应用过程中，HTTP层将高级别应用层的用户消息翻译成HTTP请求后发送给SSL层，SSL协议利用密钥加密HTTP请求，再通过TCP层将加密的HTTP请求发送往对端。

PKI是通过使用公开密钥技术和数字证书来确保系统信息安全，并负责验证数字证书持有者身份的一种体系。

9.8.1 配置 SSL 和 PKI

本节介绍在IR12000智能路由器上配置SSL和PKI的步骤和命令。

1.配置Https Server。

步骤	命令	功能
1	inspur(config)#**web secure-server enable**	开启Https Server功能
2	inspur(config)#**web secure-server ssl-context** <*ssl-ctx-name*>[**pki-profile** <*pki-profile-name*>]	关联SSL的配置模板和PKI的配置模板

2.配置SSL模板。

步骤	命令	功能
1	inspur(config)#**ssl**	进入SSL配置模式

步骤	命令	功能
2	inspur(config-ssl)#**context** <*ssl-ctx-name*>	配置ssl-ctx模板
3	inspur(config-ssl)#**ciphersuite** {**3des-ede-cbc-sha**|**aes-128-cbc-sha**| **aes-256-cbc-sha**|**des-cbc-sha**| **rc4-128-md5**| **rc4-128-sha**}	配置SSL协商的加密算法
4	inspur(config-ssl-context-name)#**version** {**ssl2.0**| **ssl3.0**| **tls1.0**}	配置SSL协商版本
5	inspur(config-ssl-context-name)#**session timeout** <*time-value*>	配置SSL会话老化时间
6	inspur(config-ssl-context-name)#**verify** {**enable**|**disable**}	开启对端证书验证

<*ssl-ctx-name*>：证书名称，范围1~31个字符。

characters des-cbc-sha：支持DES块加密算法，SHA1摘要算法。

3des-ede-cbc-sha：支持3DES块加密算法，SHA1摘要算法 。

aes-128-cbc-sha：支持AES-128块加密算法，SHA1摘要算法。

aes-256-cbc-sha：支持AES-256块加密算法，SHA1摘要算法。

rc4-128-md5：支持RC4流加密算法，密钥长度128bit，MD5摘要算法。

rc4-128-sha：支持RC4流加密算法，密钥长度128bit，SHA1摘要算法。

<*time-value*>：超时时间，范围60~86400s。

3.配置PKI模板。

步骤	命令	功能
1	inspur(config)#**pki**	进入PKI配置模式
2	inspur(config-pki)#**profile** <*pki-profile-name*>	创建PKI模板
3	inspur(config-pki)#**import pem url** {**disk** <*disk-address/cert-filename*>| **ftp** <*ftp-path/cert-filename*>}<*pki-profile-name*> **ca**	导入CA证书
4	inspur(config-pki)#**import pem url** {**disk** <*disk-address/cert-filename*>| **ftp** <*ftp-path/cert-filename*>}<*pki-profile-name*> **local**	导入本地证书
5	inspur(config-pki)#**import pem url** {**disk** <*disk-address/cert-filename*>| **ftp** <*ftp-path/cert-filename*>}<*pki-profile-name*> **key** <*key-password*>	导入私钥
6	inspur(config-pki)#**import pkcs12 url** {**disk** <*disk-address/cert-filename*>| **ftp** <*ftp-path/cert-filename*>}<*pki-profile-name*><*password*>	导入指定PKI模板的PKCS12格式证书

步骤	命令	功能
7	inspur(config-pki)#**clear certificate** {**ca**|**ra**|**local**}{**all**|**name**< *pki-profile-name* >}	删除已导入的证书

<*pki-profile-name*>：PKI实体名，范围1~63个字符。

<*cert-filename*>：证书文件名，范围1~63个字符。

<*password*>：证书加密密码，范围1~31个字符。

4.验证配置结果。

命令	功能
inspur#**show ssl context**	显示SSL模板内容
inspur#**show pki certificate** {**all**|**ca** <*pki-profile-name*>|**local** <*pki-profile-name*>}	显示PKI证书
inspur#**show pki profile**	显示PKI实体

9.8.2 SSL 和 PKI 配置实例

配置说明

SSL和PKI配置实例，准备证书文件，导入后开启https并绑定SSL与PKI模板。

配置思路

1.将申请的证书通过FTP方式导入设备。

2.进入PKI配置模式，配置PKI实体，并导入证书文件。

3.进入SSL配置模式，配置SSL模板并绑定PKI实体。

4.开启https功能并绑定SSL、PKI模板。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#ftp-server enable
inspur(config)#ftp-server top-directory /datadisk0/cert/
将制作好的证书文件server1.pfx导入设备的cert目录下。
inspur(config)#pki
inspur(config-pki)#profile pki1
inspur(config-pki)#import pkcs12 url disk /datadisk0/cert/server1.pfx pki1
123456
inspur(config)#ssl
```

```
inspur(config-ssl)#context ssl
inspur(config-ssl-context-ssl)#pki-profile pki
inspur(config-ssl-context-ssl)#!
inspur(config)#web secure-server enable
inspur(config)#web secure-server ssl-context ssl pki-profile pki
```

配置验证

在设备上通过**show ssl context**查看SSL配置信息：

```
inspur(config)#show ssl context
ssl-context:ssl
  profile-name   :pki
  verify        :No
  retry times    :10
  session timeout:3600s
  ciphersuite             :DES_CBC_SHA    3DES_EDE_CBC_SHA    AES_128_CBC_SHA
AES_256_CBC_SHA R
C4_128_MD5 RC4_128_SHA
  version       :SSLv2.0 SSLv3.0 TLSv1.0
```

在设备上通过**show pki context**查看PKI配置信息：

```
inspur(config)#show pki profile
PKI profile name :pki
```

使用浏览器通过https访问设备的WEB可以成功。

10 可靠性

10.1 可靠性简介

目前广泛应用的NGN/3G/4G、IPTV流媒体、大客户专线和VPN互联等重要的电信级业务，对IP电信网的可靠性有着很高的要求，主要包括三个层面：设备可靠性、链路可靠性和网络可靠性。

承载网中的网络设备可用性要求达到99.999%，大致相当于设备在一年的连续运行中因各种可能原因造成停机维护的时间要少于5分钟。因此，高可靠性是电信级设备的基本要求，是电信运营商建设网络的基本出发点，并且作为业务承载主体的基础网络，其可靠性也因此成为日益关注的焦点。

在路由设备或者PTN设备中，主要的可靠性技术包括设备硬件冗余、网络可靠性等关键技术，这里所要描述的可靠性主要是指网络可靠性技术。

网络可靠性技术根据侧重点不同，主要包括网络故障检测技术和保护倒换技术。

10.2 业务可靠性管理

SAMGR即业务可靠性管理，用于业务与可靠性关系的管理，主要功能包括：

·Track对象管理

·Track组管理

·OAM绑定关系

·OAM Mapping管理

SAMGR能实现业务与检测技术之间的联动，保证在网络链路出现故障时，能够进行快速切换。

在实际的应用中，路由设备支持多种检测技术，同时也会存在多种保护倒换应用需要监视检测的实时结果，以实现不同组网环境下的可靠性需求。因此业务可靠性管理用来实现各种检测技术与业务之间的联动。

10.2.1 配置业务可靠性管理

本节介绍业务可靠性管理的配置步骤和命令。

1.配置track对象。

步骤	命令	功能
1	`inspur(config)#samgr`	进入samgr配置模式

步骤	命令	功能
2	inspur(config-samgr)#**track** <*name*> **efm interface** <*interface-name*>	配置检测类型为EFM的track对象
3	inspur(config-samgr)#**track** <*name*> **cfm md** <*1-65535*> **ma** <*1-65535*> **remote-mep** <*1-8191*>	配置检测类型为CFM的track对象
4	inspur(config-samgr)#**track** <*name*> **ping-detect group** <*1-100*>	配置检测类型为ping-detect的track对象，ping检测的组号范围为1~100
5	inspur(config-samgr)#**track** <*name*> **sqa instance** <*1-150*>	配置检测类型为SQA的track对象，SQA检测实例号范围为1~150
6	inspur(config-samgr)#**track** <*name*> **pw pw-name** <*pw-name*>	配置检测类型为PW的track对象
7	inspur(config-samgr)#**track** <*name*> **vrrp interface** <*interface-name*> **vrid** <*1-255*>	配置检测类型为VRRP的track对象
8	inspur(config-samgr)#**track** <*name*> **bfd session** <*bfd-session-name*>	配置检测类型为BFD的track对象，<*bfd-session-name*>表示BFD的名称（1~32字符）
9	inspur(config-samgr)#**track** <*name*> **interface**<*interface-name*>	配置检测类型为接口的track对象

2.配置track组。

步骤	命令	功能
1	inspur(config)#**samgr**	进入samgr配置模式
2	inspur(config-samgr)#**track-group** <*group-name*>	配置track组名称，并进入track组配置模式
3	inspur(config-samgr-group-track-group-name)#**track** <*track-name*>	配置将track对象加入track组
4	inspur(config-samgr-group-track-group-name)#**inactive-number** <*1-10*>	配置track组的策略，描述组中会导致track组down的track对象down的数目

3.配置绑定关系。

步骤	命令	功能
1	inspur(config)#**samgr**	进入samgr配置模式
2	inspur(config-samgr)#**sa-bind track** <*name*> **to** {**track** | **track-group**}<*name*>	配置track对象与track对象或track组之间的绑定关系

4.验证配置结果。

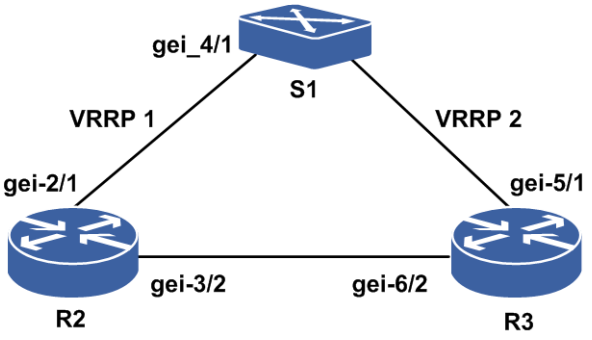
命令	功能
inspur#**show samgr brief**	简要显示配置的track对象的相关信息
inspur#**show samgr track** [<*trackname*>[**verbose**]]	详细显示track对象的信息，显示track对象状态变化信息
inspur#**show samgr track-group** [<*trackname*>[**verbose**]]	详细显示track组的信息，显示track组状态变化信息

10.2.2 EFM 联动 VRRP 配置实例

配置说明

如*图 10-1*所示，R2和R3之间运行VRRP协议。VRRP虚拟地址选用R2的接口地址10.0.0.1，R2将作为主用路由器。

图 10-1EFM 联动 VRRP



配置思路

1.S1、R2直连接口配置EFM连接。

2.R2的业务可靠性管理配置模式下，对直连接口配置检测类型为EFM的track对象。

3.R2，R3配置相同的VRRP组号及虚拟地址，为使R2作为主用路由器，R2的VRRP绑定EFM的track对象。

4.S1关闭EFM功能，R2的VRRP组变为Init状态，R3的VRRP变为Master状态；S1上开启EFM功能，R2的VRRP组变为Master状态，R3的VRRP变为Backup状态。

配置过程

S1上的配置如下：

```
S1(config)#set ethernet-oam enable
```

```
S1(config)#interface gei_4/1
S1(config-gei_4/1)#set ethernet-oam enable
```

R2上的配置如下：

```
R2(config)#interface gei-2/1
R2(config-if-gei-2/1)#no shutdown
R2(config-if-gei-2/1)#ip address 10.0.0.1 255.255.0.0
R2(config-if-gei-2/1)#exit
R2(config)#interface gei-3/2
R2(config-if-gei-3/2)#no shutdown
R2(config-if-gei-3/2)#ip address 192.168.0.1 255.255.0.0
R2(config-if-gei-3/2)#exit

R2(config)#efm
R2(config-efm)#set ethernet-oam function enable
R2(config-efm)#interface gei-2/1
R2(config-efm-if-gei-2/1)#set ethernet-oam function enable
R2(config-efm-if-gei-2/1)#set ethernet-oam link-monitor function enable
R2(config-efm-if-gei-2/1)#exit
R2(config-efm)#exit

R2(config)#samgr
R2(config-samgr)#track efm efm interface gei-2/1
R2(config-samgr)#exit

R2(config)#vrrp
R2(config-vrrp)#interface gei-2/1
R2(config-vrrp-if-gei-2/1)#vrrp 1 ipv4 10.0.0.1
R2(config-vrrp-if-gei-2/1)#vrrp 1 out-interface gei-3/2
R2(config-vrrp-if-gei-2/1)#vrrp 1 track object efm link-type
R2(config-vrrp-if-gei-2/1)#exit
```

R3上的配置如下：

```
R3(config)#interface gei-5/1
R3(config-if-gei-5/1)#
R3(config-if-gei-5/1)#ip address 10.0.0.2 255.255.0.0
R3(config-if-gei-5/1)#exit
R3(config)#interface gei-6/2
R3(config-if-gei-6/2)#no shutdown
R3(config-if-gei-6/2)#ip address 192.168.0.2 255.255.0.0
R3(config-if-gei-6/2)#exit

R3(config)#vrrp
R3(config-vrrp)#interface gei-5/1
R3(config-vrrp-if-gei-5/1)#vrrp 1 ipv4 10.0.0.1
R3(config-vrrp-if-gei-5/1)#vrrp 1 out-interface gei-6/2
R3(config-vrrp-if-gei-5/1)#end
```

配置验证

查看R2、R3的VRRP配置和生效情况，看到R2为Master，R3为Backup，R2上用命令**show samgr**看到EFM的track对象处于up状态。

```
R2#show vrrp  ipv4 brief
Interface        vrID Pri Time   A P L State  Master addr     VRouter addr
gei-2/1           1    255 1000   A P    Master 10.0.0.1       10.0.0.1

R2(config)#show samgr brief
The total of track at this Router is 3.
================================================================================
======
Track-name                    Detect-type     App-num   State     TransState
efm                          efm           1        up       T-ok

R3#show vrrp ipv4 brief
```

```
Interface        vrID Pri Time   A P L State  Master addr     VRouter addr
gei-5/1           1    100 1000     P   Backup 10.0.0.2       10.0.0.1
```

S1关闭EFM功能，R2的VRRP由 Master变为Init，R3变为Master，R2上用命令**show samgr**看到efm的track对象处于L-DOWN状态。

```
S1(config)#set ethernet-oam enable
S1(config-efm)#set ethernet-oam function disable
S1(config-efm)#exit

R2#show vrrp ipv4 brief
Interface      vrID Pri Time   A P L State  Master addr     VRouter addr
gei-2/1         1    100 1000     P   Init      0.0.0.0      10.0.0.1

R2#show samgr brief
The total of track at this Router is 1.
================================================================================
==
Track-name    Detect-type       App-num     State    TransState
efm          efm              1          L-down   T-ok

R3#show vrrp ipv4 brief
Interface        vrID Pri Time   A P L State  Master addr     VRouter addr
gei-5/1           1    100 1000     P    Master 10.0.0.2      10.0.0.1
```

S1开启EFM功能，R2的VRRP变为Master，R3变为Backup，R2上efm的track对象恢复up状态。

```
S1(config)#set ethernet-oam enable
S1(config-efm)#set ethernet-oam function enable
S1(config-efm)#exit

R2#show vrrp ipv4 brief
Interface        vrID Pri Time   A P L State  Master addr     VRouter addr
gei-2/1           1    100 1000     P   Master  10.0.0.1      10.0.0.1

R2#show samgr brief
The total of track at this Router is 1.
================================================================================
==
Track-name    Detect-type       App-num     State     TransState
efm             efm              1          up

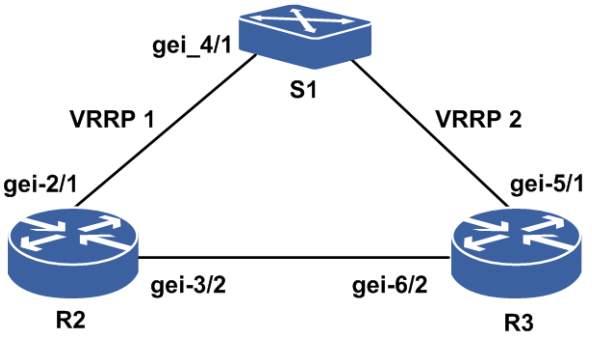
R3#show vrrp ipv4 brief
Interface        vrID Pri Time   A P L State   Master addr    VRouter addr
gei-5/1           1    100 1000     P   Backup  10.0.0.2      10.0.0.1
```

10.2.3 CFM 联动 VRRP 配置实例

配置说明

如*图 10-2*所示，R2和R3之间运行VRRP协议。VRRP虚拟地址选用R2的接口地址10.0.0.1，R2将作为主用路由器。

图 10-2 CFM 联动 VRRP



配置思路

1.S1、R2直连接口配置CFM连续性检测。

2.R2的业务可靠性管理配置模式下，对直连接口配置检测类型为cfm的track对象。

3.R2，R3配置相同的VRRP组号及虚拟地址。为使R2作为主用路由器，R2的VRRP绑定cfm的track对象。

4.S1上关闭CFM功能，R2的VRRP组变为Init状态，R3的VRRP变为Master状态；S1上开启CFM功能，R2的VRRP组变为Master状态，R3的VRRP变为Backup状态。

配置过程

S1上的配置如下：

```
S1(config)#cfm enable
S1(config)#cfm ccm-format 1
S1(config)#cfm create md session 1 name md2 level 7
S1(config-md)#ma create session 1 name a4
S1(config-md-ma)#create mep session 1 8 direction down
S1(config-md-ma)#create rmep session 1 16 remote-mac 00d0.d011.3377
S1(config-md-ma)#assign mep 8 to interface gei_4/1
S1(config-md-ma)#mep 8 state enable
S1(config-md-ma)#mep 8 ccm-send enable
S1(config-md-ma)#mep 16 state enable
```

R2上的配置如下：

```
R2(config)#interface gei-2/1
R2(config-if-gei-2/1)#no shutdown
R2(config-if-gei-2/1)#ip address 10.0.0.1 255.255.0.0
R2(config-if-gei-2/1)#exit
R2(config)#interface gei-3/2
R2(config-if-gei-3/2)#no shutdown
R2(config-if-gei-3/2)#ip address 192.168.0.1 255.255.0.0
R2(config-if-gei-3/2)#exit

R2(config)#cfm
R2(config-cfm)#set cfm enable
R2(config-cfm)#create md index 2 name-format 2 name md2 level 7
R2(config-cfm)#md index 2
R2(config-cfm-md-2)#create ma index 4 name-format 2 name a4
R2(config-cfm-md-2)#ma index 4
R2(config-cfm-md-2-ma-4)#create mep mepid 16 direction down interface gei-2/1
R2(config-cfm-md-2-ma-4)#create rmep mepid 8 remote-mac 00a1.1122.0011
R2(config-cfm-md-2-ma-4)#set mep 16 state enable
```

```
R2(config-cfm-md-2-ma-4)#set mep 16 ccm-send enable
R2(config-cfm-md-2-ma-4)#set mep 8 state enable
R2(config-cfm-md-2-ma-4)#exit
R2(config-cfm-md-2)#exit
R2(config-cfm)#exit

R2(config)#samgr
R2(config-samgr)#track cfm cfm md 2 ma 4 remote-mep 8
R2(config-samgr)#exit

R2(config)#vrrp
R2(config-vrrp)#interface gei-2/1
R2(config-vrrp-if-gei-2/1)#vrrp 1 ipv4 10.0.0.1
R2(config-vrrp-if-gei-2/1)#vrrp 1 out-interface gei-3/2
R2(config-vrrp-if-gei-2/1)#vrrp 1 track object cfm link-type
R2(config-vrrp-if-gei-2/1)#exit
```

R3上的配置如下：

```
R3(config)#interface gei-5/1
R3(config-if-gei-5/1)#no shutdown
R3(config-if-gei-5/1)#ip address 10.0.0.2 255.255.0.0
R3(config-if-gei-5/1)#exit
R3(config)#interface gei-6/2
R3(config-if-gei-6/2)#no shutdown
R3(config-if-gei-6/2)#ip address 192.168.0.2 255.255.0.0
R3(config-if-gei-6/2)#exit

R3(config)#vrrp
R3(config-vrrp)#interface gei-5/1
R3(config-vrrp-if-gei-5/1)#vrrp 1 ipv4 10.0.0.1
R3(config-vrrp-if-gei-5/1)#vrrp 1 out-interface gei-6/2
R3(config-vrrp-if-gei-5/1)#end
```

配置验证

查看R2、R3的VRRP配置和生效情况，看到R2为Master，R3为Backup，R2上用命令**show samgr**看到CFM的track对象处于up状态。

```
R2#show vrrp  ipv4 brief
Interface        vrID Pri Time   A P L State  Master addr     VRouter addr
gei-2/1           1    255 1000    A P   Master 10.0.0.1      10.0.0.1

R2(config)#show samgr brief
The total of track at this Router is 3.
================================================================================
======
Track-name                    Detect-type     App-num   State     TransState
cfm                             cfm            1        up       T-ok

R3#show vrrp ipv4 brief
Interface        vrID Pri Time   A P L State  Master addr    VRouter addr
gei-5/1           1    100 1000     P   Backup 10.0.0.2       10.0.0.1
```

S1关闭CFM功能，R2的VRRP由Master变为Init，R3变为Master，R2上cfm的track对象处于local down状态。

```
S1(config)#cfm disable
S1(config-cfm)#set cfm disable
S1(config-cfm)#exit

R2#show vrrp ipv4 brief
Interface        vrID Pri Time   A P L State  Master addr     VRouter addr
gei-2/1           1    100 1000     P   Init     0.0.0.0      10.0.0.1

R2#show samgr brief
The total of track at this Router is 3.
```

```
================================================================================
======
Track-name                      Detect-type     App-num   State     TransState
cfm                             cfm             1         L-down    T-ok

R3#show vrrp ipv4 brief
Interface        vrID Pri Time   A P L State   Master addr    VRouter addr
gei-5/1           1    100 1000     P   Master  10.0.0.2       10.0.0.1
```

S1开启CFM功能，R2的VRRP变为Master，R3变为Backup，R2上CFM的track对象恢复up状态。

```
S1(config)#cfm enable
S1(config-cfm)#set cfm enable
S1(config-cfm)#exit

R2#show vrrp ipv4 brief
Interface        vrID Pri Time   A P L State  Master addr     VRouter addr
gei-2/1           1    255 1000   A P    Master 10.0.0.1       10.0.0.1

R2#show samgr brief
The total of track at this Router is 3.
================================================================================
======
Track-name                       Detect-type     App-num   State     TransState
cfm                             cfm             1         up        T-ok

R3#show vrrp ipv4 brief
Interface        vrID Pri Time   A P L State    Master addr    VRouter addr
gei-5/1           1    100 1000     P    Backup   10.0.0.2       10.0.0.1
```

10.3 VRRP

VRRP是一种容错协议，通过物理设备和逻辑设备的分离，实现在多个出口网关之间选路。

在具有多播或广播能力的局域网（如以太网）中，VRRP提供逻辑网关确保高利用度的传输链路，不仅能够解决因某网关设备故障带来的业务中断，而且无需修改路由协议的配置。

为了增强网络安全性，VRRP在原有字符简单认证方式之外增加MD5认证方式。MD5是一种更加安全的信息完整性认证方式，包括明文认证和密文认证，明文长度1~8字符，密文长度24个字符。

10.3.1 配置 VRRP

本节介绍VRRP的配置步骤和命令。

1.配置VRRP。

步骤	命令	功能
1	inspur(config)#**vrrp**	进入VRRP配置模式
2	inspur(config-vrrp)#**interface** <*interface-name*>	进入VRRP接口配置模式

步骤	命令	功能
3	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*>**ipv4**<*ip-address*>[**secondary**]	配置VRRP协议的虚拟IPv4地址；<*vrid*>是虚拟路由器的ID，范围：1~255
4	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **priority** <*level*>	配置VRRP优先级，<*level*>取值范围为1~254，缺省优先级100
5	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **preempt** [**delay** <*seconds*>| **disable**]	配置VRRP组是否抢占，缺省为抢占模式，<*seconds*>为抢占延时，延时范围0~3600秒，默认为0
6	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **timers advertise** {<*1-40*>| **msec** <*50-40000*>}	配置发送VRRP通告的时间间隔，缺省VRRP通告时间间隔为1秒 参数<*1-40*>的单位为秒，<*50-40000*>的单位为毫秒，**msec**表示将时间间隔的单位从秒变为毫秒（可选）
7	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **timers learn**	配置VRRP是否从通告报文中学习发送时间间隔，缺省不学习
8	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **reload-delay** <*0-65535*>}	配置VRRP链路回切时的延迟时间，默认为0秒
9	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **track interface** <*interface-name*>[**priority-decrement** <*1-254*>| **rapid-down**]	配置VRRP跟踪接口，如不指定降低的优先级，则默认下降优先级10，缺省不跟踪任何链路状态
10	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **out-interface** <*interface-name*>	配置VRRP心跳线，在VRRP接口配置模式下配置指定VRRP报文出接口
11	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **text-authentication** <*string*>	配置VRRP认证字符串，字符串长度为1~8个字符（仅在VRRP的Version 2中有效，Version 3中该配置不生效）
12	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **authentication md5** {**simple** <*word*>| **encrypted** <*key-word*>}	配置VRRP MD5认证模式 **simple**为设置明文，字符串长度为1~8 **encrypted** 为设置密文，字符串长度必须固定为24
13	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **track** { **group**	**object**}<*string*>{ **link-type**	**peer-type**	**priority-decrement** <*1-254*>}	配置VRRP检测的事件组或检测对象及其策略类型
14	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **version** {**2**|**3**}	设置VRRP的版本号 v2版本支持IPv4配置，v3版本支持IPv4和IPv6配置

步骤	命令	功能
15	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **accept**	配置accept功能，默认开启
16	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **check-ttl**	配置check-ttl功能，默认开启
17	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **admin-group** { **owner** | **interface** <*interface-name*> **vrid** <*1-255*>}	配置VRRP管理组功能
18	inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **send-mode** {**all** | **rotation**}	VRRP的出接口（心跳线）发包方式配置 **all**：所有心跳线同时发包 **rotation**：轮询发包

<*vrid*>：虚拟路由器的ID，取值范围1~255。

secondary：表明该虚拟路由器支持的辅IP地址。

priority-decrement：降低指定跟踪链路的优先级值，默认优先级下降10。

rapid-down：优先级立即切换为1，如果是Master，发送0优先级报文使Backup快速切换。

priority-decrement <*1-254*>：指定降低优先级值。

owner：当前组为管理者，负责收发报文和状态管理。

2.配置VRRP关联LINK BFD或者PEER BFD。

命令	功能
inspur(config-samgr)#**track** <*track-object-name*> **bfd session** <*bfd-session-name*>	在SAMGR下面配置track对象
inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **track** {**group** | **object**}<*string*>{**link-type** | **peer-type** | **priority-decrement** <*1-254*>}	在VRRP接口配置模式下配置VRRP检测的事件组或检测对象及其策略类型

3.验证配置结果。

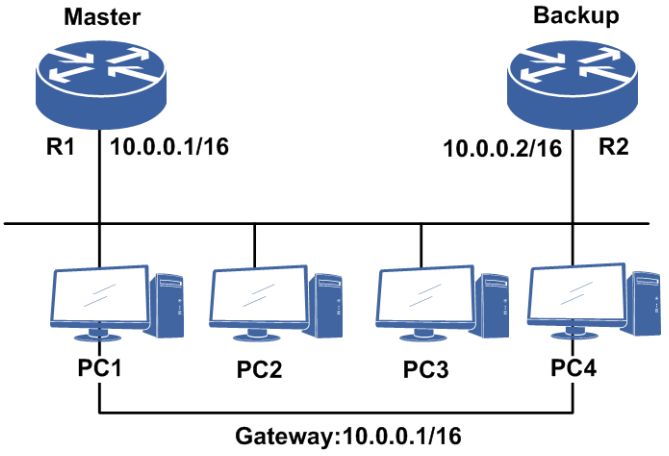
命令	功能
inspur#**show vrrp ipv4 brief**	查看路由器上所有IPv4 VRRP组简要信息
inspur#**show vrrp ipv4 brief interface** <*interface-name*>	简要查看路由器上指定接口下的所有IPv4 VRRP组信息
inspur#**show vrrp interface** <*interface-name*>[**vrid** <*1-255*>]	查看指定接口下的所有或指定VRRP组详细信息

10.3.2 基本 VRRP 配置实例

配置说明

如*图 10-3*所示，R1和R2之间运行VRRP协议。R1的接口地址配置为10.0.0.1，R2的接口地址配置为10.0.0.2，VRRP虚拟地址选用R1的接口地址10.0.0.1，此时R1被称为IP地址拥有者，拥有最高优先级255，R1将作为主用路由器。当然VRRP虚拟地址也可以配置其他的IP地址，R1上配置较高优先级，使其成为主用路由器。

图 10-3 基本 VRRP 配置实例拓扑图



配置思路

1.进入要配置VRRP的接口，为其配置网络IP地址。

2.全局模式下进入VRRP配置模式，再进入要配置VRRP的接口。

3.分别为R1，R2配置相同的VRRP组号及虚拟地址。为使R1作为主用路由器，要让R1设备具有较高的优先级，可以先在R1上按照以上配置步骤执行，因为相同优先级（默认100）情况下，先配置VRRP使其生效开始发布报文的路由器会作为组内的主用路由器。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-0/1
R1(config-if-gei-0/1)#no shutdown
R1(config-if-gei-0/1)#ip address 10.0.0.1 255.255.0.0
R1(config-if-gei-0/1)#exit
R1(config)#vrrp
R1(config-vrrp)#interface gei-0/1
R1(config-vrrp-if-gei-0/1)#vrrp 1 ipv4 10.0.0.1
R1(config-vrrp-if-gei-0/1)#end
```

R2的配置：

```
R2(config)#interface gei-0/1
R2(config-if-gei-0/1)#no shutdown
```

```
R2(config-if-gei-0/1)#ip address 10.0.0.2 255.255.0.0
R2(config-if-gei-0/1)#exit
R2(config)#vrrp
R2(config-vrrp)#interface gei-0/1
R2(config-vrrp-if-gei-0/1)#vrrp 1 ipv4 10.0.0.1
R2(config-vrrp-if-gei-0/1)#end
```

配置验证

查看R1的VRRP配置和生效情况：

```
R1#show vrrp ipv4 brief
Interface     vrID Pri Time A P L  State    Master addr    VRouter addr
gei-0/1         1  255 1000 A P    Master   10.0.0.1       10.0.0.1
/*A：是否Owner。P：是否抢占。L：是否自学习MASTER的VRRP报文发送时间间隔*/

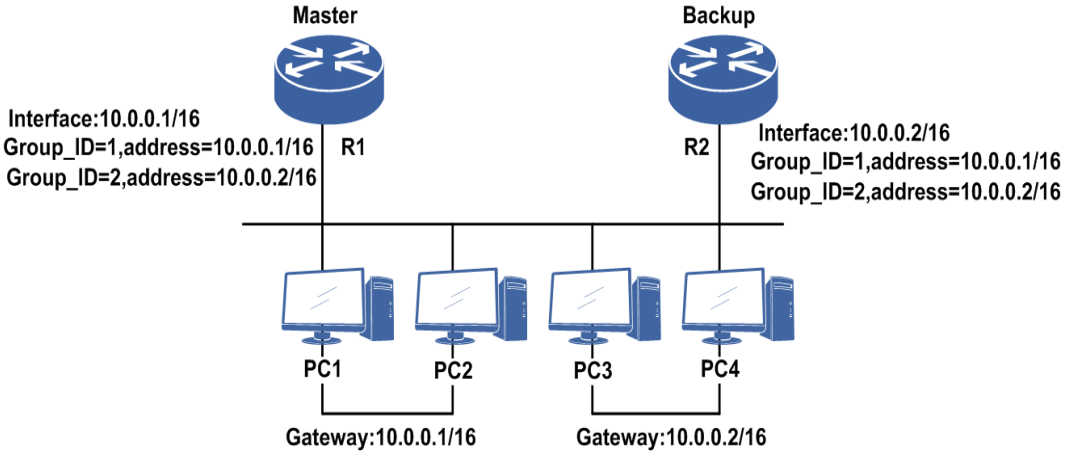
R1#show vrrp interface gei-0/1 vrid 1
gei-0/1 - vrID 1
  Vrrp configure info:                /*VRRP配置信息*/
    IP version 4, VRRP version 3
    Virtual IP address is 10.0.0.1
    Virtual MAC address is 0000.5e00.0101
    Advertise time is 1.000 (s)
    Configured priority is 100
    Preemption enable, delay 0 (s)
    Reload delay 0 (s)
    No authentication data
    Check ttl enable
    Vrrp accept mode enable
    Out-interface send-mode is all
    Tracked interface items: 0
       Interface                    State  Policy        Reduce-Priority
    Tracked detect items: 0
    Admin-group is None
  Vrrp run info:
/*VRRP在当前接口的运行信息*/
State is Master
/*VRRP运行状态*/
     1 state changes, last state change 07:57:25 7 day(s)
/*切换次数与上次切换时系统已经运行的时间，如果尚未发生过切换，这个时间为0*/
Current priority is 255
/*当前优先级，Owner状态优先级为最高255*/
    Master router is local
      Master router address is 10.0.0.1
      Master router priority is 255
      Master Advertisement interval is 1.000 (s)
      Master Down interval is 3.003 (s), no learn
```

10.3.3 对称 VRRP 配置实例

配置说明

如*图 10-4*所示，对称VRRP即为支持负载分担的组网应用，本例中启动了两个VRRP组，其中PC1和PC2使用组1的虚拟路由器作为默认网关，地址为10.0.0.1，而PC3和PC4则使用组2的虚拟路由器作为默认网关，地址为10.0.0.2。路由器R1和R2互为备份，只有当两个路由器全部失效时四台主机与外界的通信才会中断。

图 10-4 对称 VRRP 配置实例拓扑图



配置思路

1.进入要配置使能VRRP的接口，为其配置网络IP地址。

2.全局模式下进入VRRP配置模式，再进入要配置VRRP的接口。

3.在R1，R2上分别配置VRRP组1，组2及相应的虚拟地址，R1上的VRRP组1配置为较高优先级，R2上的VRRP组2配置为较高优先级，这样R1成为组1的主用路由器，同时成为组2的备用路由器；R2成为组2的主用路由器，同时成为组1的备用路由器，R1和R2互为备份。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-0/1
R1(config-if-gei-0/1)#no shutdown
R1(config-if-gei-0/1)#ip address 10.0.0.1 255.255.0.0
R1(config-if-gei-0/1)#exit
R1(config)#vrrp
R1(config-vrrp)#interface gei-0/1
R1(config-vrrp-if-gei-0/1)#vrrp 1 ipv4 10.0.0.1
R1(config-vrrp-if-gei-0/1)#vrrp 2 ipv4 10.0.0.2
R1(config-vrrp-if-gei-0/1)end
```

R2上的配置如下：

```
R2(config)#interface gei-0/1
R2(config-if-gei-0/1)#no shutdown
R2(config-if-gei-0/1)#ip address 10.0.0.2 255.255.0.0
R2(config-if-gei-0/1)#exit
R2(config)#vrrp
R2(config-vrrp)#interface gei-0/1
R2(config-vrrp-if-gei-0/1)#vrrp 1 ipv4 10.0.0.1
R2(config-vrrp-if-gei-0/1)#vrrp 2 ipv4 10.0.0.2
R2(config-vrrp-if-gei-0/1)#end
```

配置验证

查看R1的VRRP配置和生效情况

```
R1#show vrrp ipv4 brief
Interface   vrID Pri Time A P L State   Master addr VRouter addr
gei-0/1     1    255 1000 A P   Master  10.0.0.1    10.0.0.1
gei-0/1     2    100 1000 P     Master  10.0.0.1    10.0.0.2
/* A：是否Owner。P：是否抢占。L：是否自学习MASTER的VRRP报文发送时间间隔*/

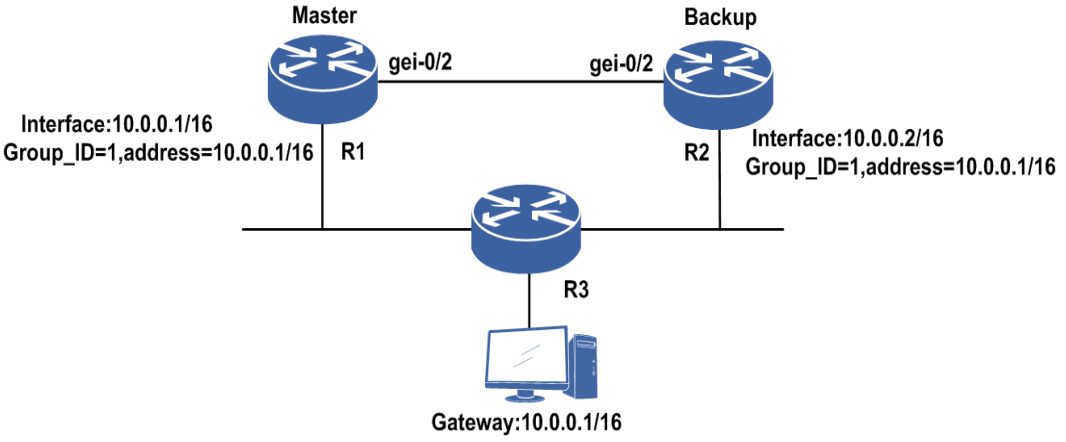
R1#show vrrp interface gei-0/1 vrid 1
gei-0/1 - vrID 1
  Vrrp configure info:          /*VRRP配置信息*/
    IP version 4, VRRP version 3
    Virtual IP address is 10.0.0.1
    Virtual MAC address is 0000.5e00.0101
    Advertise time is 1.000 (s)
    Configured priority is 100
    Preemption enable, delay 0 (s)
    Reload delay 0 (s)
    No authentication data
    Check ttl enable
    Vrrp accept mode enable
    Out-interface send-mode is all
    Tracked interface items: 0
       Interface                    State  Policy        Reduce-Priority
    Tracked detect items: 0
    Admin-group is None
  Vrrp run info:           /*VRRP在当前接口的运行信息*/
    State is Master          /*VRRP运行状态*/
      1 state changes, last state change 07:57:25 7 day(s)
/*切换次数与上次切换时系统已经运行的时间，如果尚未发生过切换，这个时间为0*/
    Current priority is 255        /*当前优先级，Owner状态优先级为最高255*/
    Master router is local
      Master router address is 10.0.0.1
      Master router priority is 255
      Master Advertisement interval is 1.000 (s)
      Master Down interval is 3.003 (s), no learn
```

10.3.4 VRRP 心跳线配置实例

配置说明

如*图 10-5*所示，本例中R1和R2之间运行VRRP协议。VRRP虚拟地址选用R1的接口地址10.0.0.1，R1将作为主用路由器。

图 10-5 VRRP 心跳线配置实例拓扑图



配置思路

1.进入要配置使能VRRP的接口，为其配置网络IP地址。

2.全局模式下进入VRRP配置模式，再进入要配置VRRP的接口。

3.分别为R1，R2配置相同的VRRP组号及虚拟地址。为使R1作为主用路由器，可以在R1设备上配置较高的优先级，或者直接配成IP地址拥有者（用R1的接口IP地址做虚拟地址，此时R1拥有最高优先级255）。

4.在R1，R2的VRRP接口配置模式下，分别为VRRP组配置报文出接口，要保证报文在这一对出接口上是可以互相收发的。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-0/2
R1(config-if-gei-0/2)#no shutdown
R1(config-if-gei-0/2)#ip address 10.0.0.1 255.255.0.0
R1(config-if-gei-0/2)#exit
R1(config)#vrrp
R1(config-vrrp)#interface gei-0/2
R1(config-vrrp-if-gei-0/2)#vrrp 1 ipv4 10.0.0.1
R1(config-vrrp-if-gei-0/2)#vrrp 1 out-interface gei-0/1
R1(config-vrrp-if-gei-0/2)#end
```

R2上的配置如下：

```
R2(config)#interface gei-0/2
R2(config-if-gei-0/2)#no shutdown
R2(config-if-gei-0/2)#ip address 10.0.0.2 255.255.0.0
R2(config-if-gei-0/2)#exit
R2(config)#vrrp
R2(config-vrrp)#interface gei-0/2
R2(config-vrrp-if-gei-0/2)#vrrp 1 ipv4 10.0.0.1
R2(config-vrrp-if-gei-0/2)#vrrp 1 out-interface gei-0/1
R2(config-vrrp-if-gei-0/2)#end
```

配置验证

查看R1的VRRP配置和生效情况：

```
R1#show vrrp ipv4 brief
Interface    vrID Pri Time A P L State   Master addr VRouter addr
gei-0/2       1  255 1000 A P    Master   10.0.0.1     10.0.0.1
/*A：是否Owner。P：是否抢占。L：是否自学习MASTER的VRRP报文发送时间间隔*/

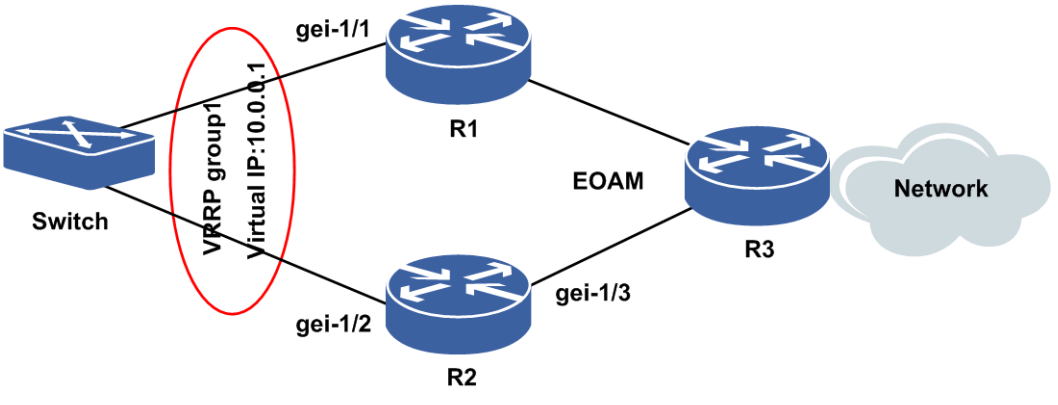
R1#show vrrp interface gei-0/2 vrid 1
gei-0/2 - vrID 1
Vrrp configure info: /*VRRP配置信息*/
IP version 4, VRRP version 3
Virtual IP address is 10.0.0.1
Virtual MAC address is 0000.5e00.0101
Advertise time is 1.000(s)
Configured priority is 100
Preemption enable, delay 0(s)
Reload delay 5 (s)
No authentication data
Check ttl enable
Vrrp accept mode enable
Out-interface send-mode is all
Out-interface(heartbeat line) is gei-0/1
Tracked interface items: 0
      Interface                    State  Policy        Reduce-Priority
Tracked detect items: 0
Admin-group is None
Vrrp run info:      /*VRRP在当前接口的运行信息*/
State is Master     /*VRRP运行状态*/
0 state changes, last state change 00:00:00
/*切换次数与上次切换时系统已经运行的时间，如果尚未发生过切换，这个时间为0*/
Current priority is 255 /*当前优先级，Owner状态优先级为最高255*/
Master router is local
Master router address is 10.0.0.1
Master router priority is 255
Master Advertisement interval is 1.000(s)
Master Down interval is 3.003(s), no learn
```

10.3.5 VRRP Track 配置实例

配置说明

如*图 10-6*所示，本例中R1和R2之间运行VRRP协议。VRRP虚拟地址为10.0.0.1。

图 10-6VRRP Track 配置实例拓扑图



配置思路

1.进入要配置使能VRRP的接口，为其配置网络IP地址。

2.全局模式下进入VRRP配置模式，再进入要配置VRRP的接口。

3.分别为R1和R2配置相同的VRRP组号及虚拟地址。为使R2作为主用路由器，可以在R2设备上配置较高的优先级，或者直接配成IP地址拥有者（用R2的接口IP地址做虚拟地址，此时R2拥有最高优先级255）。

4.进入R2的业务可靠性管理模式，配置检测对象（object），R1和R2上配置EFM的检测对象。

5.进入R2的VRRP接口配置模式下，使能VRRP的跟踪检测对象功能，跟踪步骤4当中配置的检测对象，并配置相应的策略。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ip address 10.0.0.2 255.255.255.0
R1(config-if-gei-1/1)#exit

R1(config)#vrrp
R1(config-vrrp)#interface gei-1/1
R1(config-vrrp-if-gei-1/1)#vrrp 1 ipv4 10.0.0.1
R1(config-vrrp-if-gei-1/1)#exit
R1(config-vrrp)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#ip address 10.0.0.3 255.255.255.0
R2(config-if-gei-1/2)#exit

R2(config)#efm
R2(config-efm)#set ethernet-oam function enable
R2(config-efm)#interface gei-1/3
R2(config-efm-if-gei-1/3)#set ethernet-oam function enable
R2(config-efm-if-gei-1/3)#set ethernet-oam link-monitor function enable
R2(config-efm-if-gei-1/3)#exit
R2(config-efm)#exit

R2(config)#samgr
R2(config-samg)#track 1 efm interface gei-1/3
R2(config-samg)#exit

R2(config)#vrrp
R2(config-vrrp)#interface gei-1/2
R2(config-vrrp-if-gei-1/2)#vrrp 1 ipv4 10.0.0.1
R2(config-vrrp-if-gei-1/2)#vrrp 1 priority 150
R2(config-vrrp-if-gei-1/2)#vrrp 1 track object 1 link-type
R2(config-vrrp-if-gei-1/2)#exit
R2(config-vrrp)#exit
```

R3上的配置如下：

```
R3(config)#efm
```

```
R3(config-efm)#set ethernet-oam function enable
R3(config-efm)#interface gei-1/4
R3(config-efm-if-gei-1/4)#set ethernet-oam function enable
R3(config-efm-if-gei-1/4)#set ethernet-oam link-monitor function enable
R3(config-efm-if-gei-1/4)#exit
R3(config-efm)#exit
```

配置验证

查看R2的VRRP track配置和生效情况：

```
R2#show vrrp ipv4 brief
Interface vrID Pri Time A P L State   Master addr   VRouter addr
gei-1/2    1   150 1000    P    Master 10.0.0.3      10.0.0.1
/*A：是否Owner。P：是否抢占。L：是否自学习MASTER的VRRP报文发送时间间隔*/

R2#show vrrp interface gei-1/2
gei-1/2 - vrID 1
  Vrrp configure info:
    IP version 4, VRRP version 3
    Run mode is standard
    Virtual IP address is 10.0.0.1
    Virtual MAC address is 0000.5e00.0101
    Advertise time is 1.000 (s)
    Configured priority is 150
    Preemption enable, delay 0 (s)
    Reload delay 0 (s)
    No authentication data
    Check ttl enable
    Vrrp accept mode enable
    Vrrp backup route mode disable
    Out-interface send-mode is all
    VLAN-Range send-mode is rotation
    Tracked interface items: 0
       Interface                State  Policy       Reduce-Priority
    Tracked detect items: 1
      Track name: efm  Track type: object  Detect type: efm
      Policy type: link
      Track state: up
    Admin-group is None
  Vrrp run info:
    State is Master
      5 state changes, last state change 13:11:34 2 day(s)
    Current priority is 150
    Master router is local
      Master router address is 10.0.0.3
      Master router priority is 150
      Master Advertisement interval is 1.000 (s)
      Master Down interval is 3.570 (s), no lear
```

10.4 Ping Detect

Ping Detect（自动侦测）利用ICMP的Request/Response报文来检测目的地的可达性，并将检测结果反馈到与之联动的备份功能模块触发其主备切换，从而提供了基于网络层应用可达性的备份功能。

10.4.1 配置 Ping Detect

本节介绍Ping Detect（自动侦测）的配置步骤和命令。

1.配置Ping Detect。

步骤	命令	功能
1	inspur(config)#**detect-group** <*group-number*>	配置一个检测组，组号的范围：1~100
2	inspur(config-detect-group-number)#**option** {**and** | **or**}	配置检测对象逻辑“与”、“或”关系 **and**：组内所有条目通才算组通 **or**：组内任一条目通就算组通
3	inspur(config-detect-group-number)#**list** <*list-number*>	配置检测组的检测列表，表的范围：1~10
4	inspur(config-detect-group-number-list-number)#**item** <*item-number*>[**vrf** <*vrf-name*>]<*des-ip-address*>[<*next-ip-address*>| **interface** <*interface-name*>]	配置检测列表的检测条目，配置该条目的地址，并指明下一跳地址和出接口
5	inspur(config-detect-group-number-list-number)#**option** {**and** | **or**}	配置检测对象逻辑“与”、“或”关系 **and**：列表内所有条目通才算列表通 **or**：列表内任一条目通就算列表通
6	inspur(config-detect-group-number)#**retry-times** <*retry-times*>	配置检测组传递给Ping模块的重传次数，范围为1~10，默认值为2
7	inspur(config-detect-group-number)#**loop-time** <*seconds*>	配置检测组的循环检测时间，范围：2~86400，单位：秒，默认为15秒
8	inspur(config-detect-group-number)#**time-out** <*seconds*>	配置检测组传递给Ping模块的超时时间，范围：1~20，单位：秒，默认为2秒
9	inspur(config-samgr)#**track** <*name*> **ping-detect group** <*group-number*>	在Samgr配置模式下使能Ping Detect功能

2.验证配置结果。

命令	功能
inspur#**show running-config ping-detect**	显示Ping Detect的配置，不显示默认值
inspur#**show running-config ping-detect all**	显示Ping Detect的配置，显示默认值

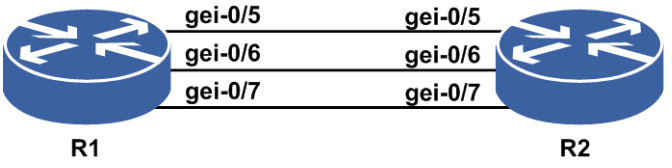
命令	功能
inspur#**show samgr track**	显示Samgr Track Ping Detect的信息
inspur#**show samgr track-group**	显示Samgr track-group的信息
inspur#**show samgr brief**	查看Ping Detect检测的结果

10.4.2 Ping Detect 基本配置实例

配置说明

如*图 10-7*所示，R1和R2上有5、6、7三个口相连，要在R1和R2之间配置一个检测组。

图 10-7 Ping Detect 基本配置实例



R1与R2上的接口地址如下：

接口		IP地址	掩码
R1	gei-0/5	100.0.0.15	255.255.255.0
	gei-0/6	101.0.0.15	255.255.255.0
	gei-0/7	102.0.0.15	255.255.255.0
R2	gei-0/5	100.0.0.20	255.255.255.0
	gei-0/6	101.0.0.20	255.255.255.0
	gei-0/7	102.0.0.20	255.255.255.0

配置思路

1.配置一个检测组。

2.在R1上配置检测组的检测条目，将这三个条目加入其中。

3.根据需要设置检测组的各个参数。

4.在Samgr配置模式下使能Ping Detect功能，并通过**show**命令查看结果。

5.设置检测对象的逻辑关系为**And**，加入一个ping不通的检测条目，查看结果；再将逻辑关系设置为**Or**，查看结果。

配置过程

R1上的配置如下：

```
inspur(config)#detect-group 1
inspur(config-detect-group-1)#list 1
inspur(config-detect-group-1-list-1)#item 1 100.0.0.20
inspur(config-detect-group-1-list-1)#item 2 101.0.0.20
inspur(config-detect-group-1-list-1)#item 3 102.0.0.20
inspur(config-detect-group-1)#!
inspur(config)#samgr
inspur(config-samgr)#track test ping-detect group 1
inspur(config-samgr)#exit
```

配置验证

查看R1上的Ping Detect配置和生效情况：

```
inspur(config)#show samgr brief
The total of track at this Router is 1.
=============================================================================
Track-nameDetect-type App-num State
testping-detect 0 up
```

设置检测对象的逻辑关系为**And**，再加入一条ping不通的条目：

```
inspur(config-detect-group-1-list-1)#option and
 /*设置检测对象的逻辑关系为"and"*/
inspur(config-detect-group-1-list-1)#item 4 1.2.3.4
inspur(config-detect-group-1-list-1)#!
inspur(config)#show samgr brief
The total of track at this Router is 1.
=============================================================================
Track-name Detect-type App-num State
 test ping-detect 0 L-down
```

设置检测对象的逻辑关系为**Or**，再查看结果：

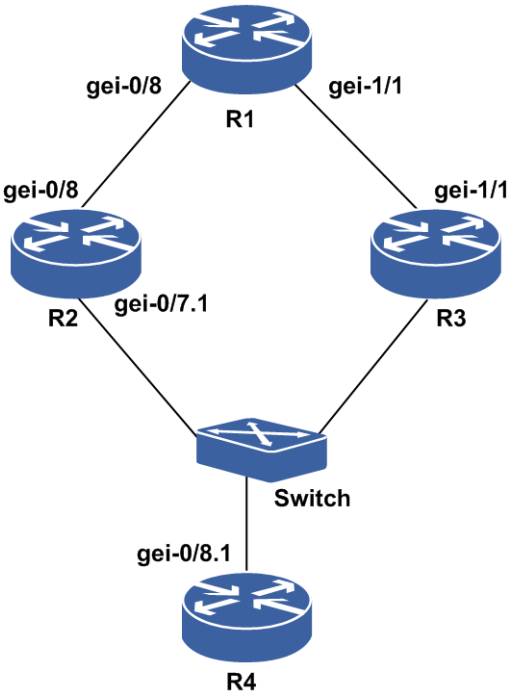
```
inspur(config-detect-group-1-list-1)#option or
 /*设置检测对象的逻辑关系为"or"*/
inspur(config-detect-group-1-list-1)#!
inspur(config)#show samgr brief
The total of track at this Router is 1.
=============================================================================
Track-name Detect-type App-num State
test ping-detect 0 up
```

10.4.3 直连路由与 Track Ping 联动配置实例

配置说明

以*图 10-8*为例，介绍直连路由与track ping联动的基本功能。

图 10-8 直连路由与 track ping 联动配置图



配置思路

1.在R1、R2与R4上分别配置IP地址，并启动OSPF协议，最终路由器之间相互建OSPF邻居。

2.在R2上先配置ping-detect检测组，再配置samgr的track对象，最后在接口gei-0/8上绑定track对象。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-0/8
R1(config-if-gei-0/8)#no shutdown
R1(config-if-gei-0/8)#ip address 71.88.1.2 255.255.255.0
R1(config-if-gei-0/8)#exit

R1(config)#router ospf 19
R1(config-ospf-19)#router-id 22.22.22.22
R1(config-ospf-19)#area 0
R1(config-ospf-19-area-0)#network 71.88.1.0 0.0.0.255
R1(config-ospf-19-area-0)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-0/8
R2(config-if-gei-0/8)#no shutdown
R2(config-if-gei-0/8)#ip address 71.88.1.1 255.255.255.0
R2(config)#interface gei-0/7.1
R2(config-if-gei-0/7.1)#ip address 41.52.17.2 255.255.255.0
R2(config-if-gei-0/7.1)#exit

R2(config)#vlan-configuration
R2(config-vlan)#interface gei-0/7.1
```

```
R2(config-vlan-if-gei-0/7.1)#encapsulation-dot1q 1
R2(config-vlan-if-gei-0/7.1)#exit

R2(config)#router ospf 19
R2(config-ospf-19)#router-id 22.11.11.22
R2(config-ospf-19)#area 0
R2(config-ospf-19-area-0)#network 71.88.1.0 0.0.0.255
R2(config-ospf-19-area-0)#network 41.52.17.0 0.0.0.255
R2(config-ospf-19-area-0)#exit
R2(config-ospf-19)#exit

R2(config)#detect-group 10

R2(config-detect-group-10)#option or
R2(config-detect-group-10)#retry-times 3
R2(config-detect-group-10)#loop-time 12
R2(config-detect-group-10)#time-out 3
R2(config-detect-group-10)#list 1
R2(config-detect-group-10-list-1)#option or
R2(config-detect-group-10-list-1)#item 9 41.52.17.3 41.52.17.2 interface
gei-0/7.1
R2(config-detect-group-10-list-1)#item 3 19.19.19.1
R2(config-detect-group-10-list-1)#item 6 200.11.12.101
R2(config-detect-group-10-list-1)#item 7 30.0.12.3
R2(config-detect-group-10-list-1)#item 8 100.10.11.201
R2(config-detect-group-10-list-1)#item 4 1.1.50.1
R2(config-detect-group-10-list-1)#!


R2(config)#samgr
R2(config-samgr)#track abc ping-detect group 10
R2(config-samgr)#exit
R2(config)#interface gei-0/8
R2(config-if-gei-0/8)#track abc
R2(config-if-gei-0/8)#exit
```

R4上的配置如下：

```
R4(config)#interface gei-0/8.1
R4(config-if-gei-0/8.1)#ip address 1.2.3.4 255.255.255.0
R4(config-if-gei-0/8.1)#ip address 41.52.17.3 255.255.255.0 secondary
R4(config-if-gei-0/8.1)#interface mac-address offset 23
R4(config-if-gei-0/8.1)#exit

R4(config)#vlan-configuration
R4(config-vlan)#interface gei-0/8.1
R4(config-vlan-if-gei-0/8.1)#encapsulation-dot1q 1
R4(config-vlan-if-gei-0/8.1)#exit

R4(config)#router ospf 19
R4(config-ospf-19)#router-id 33.33.33.33
R4(config-ospf-19)#area 0
R4(config-ospf-19-area-0)#network 41.52.17.0 0.0.0.255
R4(config-ospf-19-area-0)#exit
R4(config-ospf-19)#exit
```

配置验证

在R2上查看track对象的状态，此时R2上的track状态是up的，查看协议表中此时是有接口gei-0/8直连地址的添加。

```
R2(config)#show samgr brief
The total of track at this Router is 1.
Track-name            Detect-type       App-num     State   TransState
abc                  ping-detect        1          up      T-ok

R2#show ip protocol routing network 71.88.1.0
```

```
Protocol routes:
status codes: *valid, >best, i-internal, s-stale

    Dest            NextHop     RoutePrf   RouteMetric  Protocol
*>  71.88.1.0/24     71.88.1.1     0          0          direct
 *  71.88.1.0/24     71.88.1.0     110        1          ospf
*>  71.88.1.1/32     71.88.1.1     0          0          address
```

对gei-0/7.1进行**shutdown**操作后，查看R2上的track状态为down，gei-0/8的直连路由会被删除。

```
R2#show samgr brief
The total of track at this Router is 1.
Track-name        Detect-type       App-num     State
abc              ping-detect        1          L-down

R2#show ip protocol routing network 71.88.1.0
Protocol routes:
status codes: *valid, >best, i-internal, s-stale

Dest             NextHop        RoutePrf   RouteMetric Protocol
```

10.5 EFM

EFM是IEEE定义的检测监控和维护直连链路的标准，主要用于接入侧链路的监控检测。

EFM提供物理上点对点直连链路运行状态的统计监控，最大可能的监控该链路的运行状况，包括帧传输出错率、链路收发速率比较、丢失统计等。同时，EFM也能检测通告系统的紧急故障事件，如系统不可恢复故障事件等，使得二层链路上传输质量有一定的检测保证，做到监控并实时了解其运行状态，有助于网络管理员进行维护，减轻维护成本。

远端环回是EFM提供的一种链路检测功能，主要包括检测链路帧丢失情况以及处理相关的统计功能。远端环回为手动触发，有中断其它业务的可能，所以一般在需要检测的时候开启，检测结束后可以通过手动关闭该功能，恢复正常非检测状态。

10.5.1 配置 EFM

配置EFM的基本属性和功能，用来监控检测接入链路。

1.配置EFM的全局属性。

步骤	命令	功能
1	inspur(config)#**efm**	进入EFM配置模式
2	inspur(config-efm)#**set ethernet-oam function** {**enable** | **disable**}	配置开启或关闭EFM模块全局功能，默认关闭
3	inspur(config-efm)#**set ethernet-oam oui** <*word*>	配置EFM厂家标示**oui**字段，默认值为INSPUR
4	inspur(config-efm)#**set ethernet-oam**	配置EFM总体环回控制超时时

步骤	命令	功能
	remote-timeout <*value*>	间，范围：1~10，单位：秒，默认为3秒

2.配置EFM的接口属性。

步骤	命令	功能
1	inspur(config-efm)#**interface** <*interface-name*>	进入EFM接口配置模式
2	inspur(config-efm-if-interface-name)#**set ethernet-oam function** {**enable** | **disable**}	设置开启或关闭指定接口的EFM功能
3	inspur(config-efm-if-interface-name)#**set ethernet-oam rmt-loopback** {**start**| **stop**}	设置开启或关闭EFM远端环回功能
4	inspur(config-efm-if-interface-name)#**set ethernet-oam rmt-loopback-mode** {**enable** | **disable**}	设置指定接口是否响应环回请求，默认为响应
5	inspur(config-efm-if-interface-name)#**set ethernet-oam rmt-loopback-guard recovery-forward**	指定接口不响应环回请求，强制恢复本端状态到转发状态
6	inspur(config-efm-if-interface-name)#**set ethernet-oam link-monitor function** {**enable** | **disable**}	设置开启或关闭指定接口的链路监控功能
7	inspur(config-efm-if-interface-name)#**set ethernet-oam link-monitor frame threshold** <*th-value*>[**window** <*win-value*>]	设置链路监控中错误帧统计窗口值和极限值 <*th-value*>，错误帧极限值，范围为1~65535，单位为个数，默认为1 <*win-value*>，错误帧窗口值，范围为1~60，单位为秒，默认为1秒
8	inspur(config-efm-if-interface-name)#**set ethernet-oam link-monitor symbol-period threshold** <*th-value*>[**window** <*win-value*>]	设置链路监控中错误符号统计窗口值和极限值 <*th-value*>，错误符号极限值，范围为1~65535，单位为个数，默认为1 <*win-value*>，错误符号窗口值，范围为1~65535，单位为100万个，默认为1
9	inspur(config-efm-if-interface-name)#**set ethernet-oam link-monitor frame-period threshold** <*th-value*>[**window** <*win-value*>]	设置链路监控中错误帧周期统计窗口值和极限值 <*th-value*>，错误帧周期极限值，范围为1~65535，单位为个数，默认为1 <*win-value*>，错误帧周期窗口值，范围为1~65535，单位为

步骤	命令	功能
		1万个，默认为1
10	inspur(config-efm-if-interface-name)#**set ethernet-oam link-monitor frame-second threshold** <*th-value*>[**window** <*win-value*>]	设置链路监控中错误帧秒周期统计窗口值和极限值 <*th-value*>，错误帧秒周期极限值，范围为1~900，单位为帧秒个数，默认为1 <*win-value*>，错误帧秒周期窗口值，范围为1~900，单位为秒，默认为1秒
11	inspur(config-efm-if-interface-name)#**set ethernet-oam link-timeout** {<*timeout-value1*>|**fast** <*timeout-value2*>[**period** <*period-value*>]}	设置链路超时与发包周期时间： <*timeout-value1*>，超时时间，范围3~20，默认为5，单位1秒 <*timeout-value2*>，超时时间，范围3~200，默认为50，单位100 ms <*period-value*>，发包周期时间，范围1~10，默认为10，单位100 ms
12	inspur(config-efm-if-interface-name)#**set ethernet-oam mode** {**active** | **passive**}	设置EFM配置模式，默认为**active**
13	inspur(config-efm-if-interface-name)#**set ethernet-oam rmt-loopback** {**start** | **stop**}	开启或关闭EFM接口的链路环回功能

3.验证配置结果。

命令	功能
inspur#**show ethernet-oam** [<*interface-name*>{**discovery** | **link-monitor** | **statistics**}]	查看EFM当前全局配置或接口配置及状态

4.维护EFM。

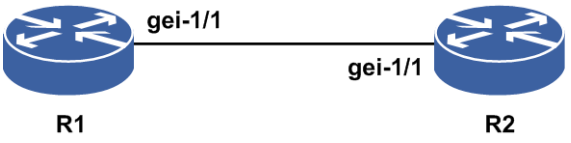
命令	功能
inspur#**debug ethernet-oam** {**interface** <*interface-name*>| **packet interface** <*interface-name*>[{**dual** | **in** | **out**} **type** {**all** | **information** | **lpbk-ctrl** | **notify** | **org-spec** | **reqst-varb** | **respse-varb**} **mode** {**all-time** | **numberr** <*num-value*>}| **all**}]	EFM的报文收发的debug开关，使用**no**命令关闭所有打开的开关

10.5.2 EFM 连接建立配置实例

配置说明

如*图10-9*所示，R1和R2直连，在R1、R2直连接口上配置EFM，建立连接。

图 10-9 EFM 连接建立



配置思路

1.R1直连R2的接口上配置EFM，开启指定接口的EFM使能开关和link-monitor开关，并全局使能EFM。

2.R2直连R1的接口上配置EFM，开启指定接口的EFM使能开关和link-monitor开关，并全局使能EFM。

3.R1、R2上show ethernet-oam discovery，查看R1与R2的EFM连接建立状况。

4.R1、R2上show ethernet-oam link-monitor，查看R1与R2之间的链路错误计数。

配置过程

R1的配置如下：

```
R1#configure terminal
R1(config)#efm
R1(config-efm)#interface gei-1/1
R1(config-efm-if-gei-1/1)#set ethernet-oam function enable
R1(config-efm-if-gei-1/1)#set ethernet-oam link-monitor funciton enable
R1(config-efm-if-gei-1/1)#exit
R1(config-efm)#set ethernet-oam oui R1
R1(config-efm)#set ethernet-oam function enable
R1(config-efm)#exit
```

R2的配置如下：

```
R2#configure terminal
R2(config)#efm
R2(config-efm)#interface gei-1/1
R2(config-efm-if-gei-1/1)#set ethernet-oam function enable
R2(config-efm-if-gei-1/1)#set ethernet-oam link-monitor funciton enable
R2(config-efm-if-gei-1/1)#exit
R2(config-efm)#set ethernet-oam oui R2
R2(config-efm)#set ethernet-oam function enable
R2(config-efm)#exit
```

配置验证

1.R1上**show ethernet-oam discovery**查看链路EFM协商状况：

```
R1(config)#show ethernet-oam gei-1/1 discovery
  PortId 32: Ethernet Oam enable
  Local DTE
  ----------
  Config:
  Mode             :active
  Org-Specific      :support
  Remote Loopback   :support
  Variable Retrieval:support
  Period Time       :10*(100ms)
  Link time out     :50*(100ms)

  Status:                          /*本地状态*/
  Parser           :forward         /*接收器转发状态*/
  Multiplexer       :forward         /*发送器发送状态*/
  Stable           :yes            /*本地链路状态"满意"*/
  Discovery         :done            /*链路发现完成*/
  Loopback          :off            /*没有开启环回*/
  PDU max size      :1518            /*本地支持的最大报文长度*/
  PDU Revision      :1               /*本地配置修改过1次*/
  Unidirection      :nonsupport

  Remote DTE
  -----------
  Config:
  Mode             :active
  Link Monitor      :support
  Unidirection      :nonsupport
  Org-Specific      :support
  Remote Loopback   :support
  Variable Retrieval:support
  PDU max size      :1518
  Remote OUI(hex)   :52-32-00

  Status:                                /*远端状态*/
  Parser           :forward               /*处于发送模式*/
  Multiplexer       :forward               /*处于发送模式*/
  Stable           :yes                  /*远端链路状态"满意"*/
  Mac Address       :1622.30c4.e999         /*远端设备MAC地址*/
  PDU Revision      :0                    /*远端配置修改过0次*/
```

2.R1上**show ethernet-oam link-monitor**查看链路错误计数：

```
R1(config)#show ethernet-oam gei-1/1 link-monitor
  Link Monitoring of Interface: gei-1/1
  Link Monitoring enable
  Error Symbol Period Event:
    Symbol Window           : 1(million symbols)
    Error Symbol Threshold    : 1(symbol)
    Error Symbols           : 0
    Local Total Error Symbols : 0
    Remote Total Error Symbols: 0
    Local Total Error Events  : 0
    Remote Total Error Events : 0
  Error Frame Event:
    Frame Window            : 1(s)
    Error Frame Threshold     : 1(frame)
    Error Frames            : 0
    Local Total Error Frames  : 0
    Remote Total Error Frames : 0
    Local Total Error Events  : 0
    Remote Total Error Events : 0
  Error Frame Period Event:
    Period Window           : 1(ten thousand frames)
    Error Period Threshold    : 1(frame)
    Error Frames            : 0
    Local Total Error Frames  : 0
    Remote Total Error Frames : 0
```

```
  Local Total Error Events  : 0
  Remote Total Error Events : 0
Error Frame Seconds Event:
  Error Seconds Window      : 1(s)
  Error Seconds Threshold   : 1(s)
  Error Frame Seconds       : 0(s)
  Local Total Error Frame Seconds  : 0(s)
  Remote Total Error Frame Seconds : 0(s)
  Local Total Error Frame Seconds Events  : 0
  Remote Total Error Frame Seconds Events : 0
```

3.R2上**show ethernet-oam discovery**查看链路EFM协商状况：

```
R2(config)#show ethernet-oam gei-1/1 discovery
  PortId 66: Ethernet Oam enable
  Local DTE
  ----------
  Config:
  Mode            :active
  Org-Specific     :support
  Remote Loopback   :support
  Variable Retrieval:support
  Period Time      :10*(100ms)
  Link time out    :50*(100ms)

  Status:
  Parser          :forward
  Multiplexer      :forward
  Stable          :yes
  Discovery        :done
  Loopback         :off
  PDU max size     :1518
  PDU Revision     :0
  Unidirection     :nonsupport

  Remote DTE
  -----------
  Config:
  Mode            :active
  Link Monitor     :support
  Unidirection     :nonsupport
  Org-Specific     :support
  Remote Loopback   :support
  Variable Retrieval:support
  PDU max size     :1514
  Remote OUI(hex)   : 52-31-00

  Status:
  Parser          :forward
  Multiplexer      :forward
  Stable          :yes
  Mac Address      :1210.1210.1211
  PDU Revision     :1
```

4.R2上**show ethernet-oam link-monitor**查看链路错误计数：

```
R2(config)#show ethernet-oam gei-1/1 link-monitor
  Link Monitoring of Interface: gei-1/1
  Link Monitoring enable
  Error Symbol Period Event:
    Symbol Window           : 1(million symbols)
    Error Symbol Threshold    : 1(symbol)
    Error Symbols           : 0
    Local Total Error Symbols : 0
    Remote Total Error Symbols: 0
    Local Total Error Events  : 0
    Remote Total Error Events : 0
  Error Frame Event:
    Frame Window            : 1(s)
    Error Frame Threshold     : 1(frame)
```

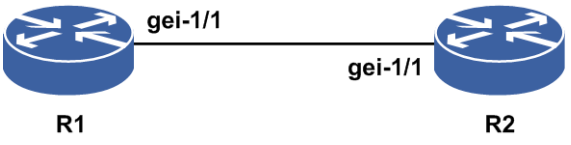
```
    Error Frames            : 0
    Local Total Error Frames  : 0
    Remote Total Error Frames : 0
    Local Total Error Events  : 0
    Remote Total Error Events : 0
  Error Frame Period Event:
    Period Window           : 1(ten thousand frames)
    Error Period Threshold    : 1(frame)
    Error Frames            : 0
    Local Total Error Frames  : 0
    Remote Total Error Frames : 0
    Local Total Error Events  : 0
    Remote Total Error Events : 0
  Error Frame Seconds Event:
    Error Seconds Window      : 1(s)
    Error Seconds Threshold   : 1(s)
    Error Frame Seconds       : 0(s)
    Local Total Error Frame Seconds  : 0(s)
    Remote Total Error Frame Seconds : 0(s)
    Local Total Error Frame Seconds Events  : 0
    Remote Total Error Frame Seconds Events : 0
```

10.5.3 EFM 远端环回配置实例

配置说明

如*图* 所示，R1和R2直连，在R1、R2直连接口上配置EFM，R1开启远端环回，R2环回报文。

图 10-10 EFM 远端环回



配置思路

1.R1直连R2的接口上配置EFM，全局使能EFM。

2.R2直连R1的接口上配置EFM，全局使能EFM。

3.R1与R2建立EFM连接后，R1开启远端环回。

4.R1、R2上show ethernet-oam discovery，查看R1与R2的EFM连接建立状况。

配置过程

R1的配置如下：

```
R1#configure terminal
R1(config)#efm
R1(config-efm)#interface gei-1/1
R1(config-efm-if-gei-1/1)#set ethernet-oam function enable
R1(config-efm-if-gei-1/1)#set ethernet-oam link-monitor funciton enable
```

```
R1(config-efm-if-gei-1/1)#exit
R1(config-efm)#set ethernet-oam oui R1
R1(config-efm)#set ethernet-oam function enable
R1(config-efm)#exit
```

R2的配置如下：

```
R2#configure terminal
R2(config)efm
R2(config-efm)#interface gei-1/1
R2(config-efm-if-gei-1/1)#set ethernet-oam function enable
R2(config-efm-if-gei-1/1)#set ethernet-oam link-monitor funciton enable
R2(config-efm-if-gei-1/1)#exit
R2(config-efm)#set ethernet-oam oui R2
R2(config-efm)#set ethernet-oam function enable
R2(config-efm)#exit
```

EFM连接建立后，R1上开启远端环回：

```
R1#configure terminal
R1(config)efm
R1(config-efm)#interface gei-1/1
R1(config-efm-if-gei-1/1)#set ethernet-oam rmt-loopback start
R1(config-efm-if-gei-1/1)#exit
R1(config-efm)#exit
```

配置验证

在建立EFM连接的这条链路上，R1向R2发送的除OAMPDU以外的其它报文，R2收到报文后都直接将其环回给R1。

```
R1(config-efm)#show ethernet-oam gei-1/1 discovery
  PortId 3: Ethernet Oam enable
  Local DTE
  ----------
  Config:
  Mode            :active
  Org-Specific     :support
  Remote Loopback   :support
  Variable Retrieval:support
  Period Time      :10*(100ms)
  Link time out    :50*(100ms)

  Status:
  Parser          :discard
  Multiplexer      :forward
  Stable          :yes
  Discovery        :done
  Loopback         :on(Master)
  PDU max size     :1518
  PDU Revision     :3
  Unidirection     :nonsupport

  Remote DTE
  -----------
  Config:
  Mode            :active
  Link Monitor     :support
  Unidirection     :nonsupport
  Org-Specific     :support
  Remote Loopback   :support
  Variable Retrieval:support
  PDU max size     :1518
  Remote OUI(hex)   :52-32-00

  Status:
  Parser          :loopback
```

```
Multiplexer       :discard
Stable           :yes
Mac Address       :00ee.ff10.2102
PDU Revision      :1
```

10.6 CFM

CFM是逻辑上的点对点连通性检测功能，检测两逻辑点的互通性。CFM可以有效地对虚拟桥局域网进行检查、隔离和报告连接性故障，是数据链路层中用来执行链路监控、检测与定位的一项主要协议。CFM可以在大多数支持全双工点到点或模拟点到点的链路上完成以太网数据链路层的链路检测，而不依赖于特定的系统接口。

CFM主要有以下三大功能：

- 故障探测：MEP使用周期发送和接收的CCM消息来对网络的连通性进行检测，主要可以检测出连通性失败和非意愿的连通性（错误连接的情况）。
- 故障确认和隔离：此功能属于管理性的行为，管理员通过LBM/LBR进行故障的确认，再进行一定的隔离操作。
- 路径发现：MEP使用LTM/LTR消息进行发现，跟踪一个MEP到另外一个MEP或MIP之间所经过的路径。

10.6.1 配置 CFM

配置CFM的基本属性和功能，用来进行点对点的连通性检测。

1.配置CFM功能。

步骤	命令	功能
1	inspur(config)#**cfm**	进入CFM配置模式
2	inspur(config-cfm)#**set cfm** {**disable** | **enable**}	设置开启或关闭CFM全局功能，默认关闭
3	inspur(config-cfm)#**create md index** <*index*> **name-format** <*format*>[**name** <*md-name*>] **level** <*level*>	创建一个维护域 <*level*>为维护域等级，范围0~7，数值越大等级越高
4	inspur(config-cfm)#**md index** < *index* >	进入维护域模式
5	inspur(config-cfm-md-index)#**create ma index** <*index*> **name-format** <*format*> **name** < *ma-name*>[**vid** <*vid*>]	创建一个维护联盟
6	inspur(config-cfm-md-index)#**ma index** <*index*>	进入维护联盟模式
7	inspur(config-cfm-md-index-ma-index)#**set ccminterval** <*interval*>	配置维护联盟的CCM间隔，取值1-7，分别对应3.3 ms、10 ms、100 ms、1 s、10 s、60 s、

步骤	命令	功能
		600 s七种间隔
8	inspur(config-cfm-md-index-ma-index)#**create mep mep-id** *<mepid>* **direction** {**down** | **up**} **interface** *<interface-name>*	创建MEP
9	inspur(config-cfm-md-index-ma-index)#**create rmep mepid** *<mepid >* **remote-mac** *<mac-address>*	创建RMEP *<mepid >*，有效范围1~8191，本MA内不能重复，包括本地MEP *<mac-address>*，远端MEP的MAC地址
10	inspur(config-cfm-md-index-ma-index)#**create mip session-id** *<session-id>* **interface** *<interface-name>*	创建MIP
11	inspur(config-cfm-md-index-ma-index)#**set mep** *<mepid>* **state** {**enable**|**disable**}	开启或关闭MEP的本地管理功能，对RMEP来说则是开启或关闭RMEP的CCM检测
12	inspur(config-cfm-md-index-ma-index)#**set mep** *<mepid>* **ccm-send** {**enable**|**disable**}	开启或关闭MEP的CCM发包功能，仅对本地MEP有效 *<mepid >*，范围1~8191，可配置本地MEP和远端MEP
13	inspur(config-cfm-md-index-ma-index)#**set mep** *<mepid>* **alarm-lowest-pri** *<priority>*	配置MEP的最低故障告警等级，限制MEP可触发告警的故障等级，范围为1-9，默认为1
14	inspur(config-cfm-md-index-ma-index)#**set mep** *<mepid>* **1dm** {**enable** | **disable**}[**frame-size** *<frame size>*| **interval** *<interval>*| **require-time** *<time>*| **rmep-id** *<mepid>*]	开启或关闭按需的单向时延检测功能
15	inspur(config-cfm-md-index-ma-index)#**set mep** *<mepid>* **ddm** {**enable** | **disable**}[**frame-size** *<frame size>*| **interval** *<interval>*| **require-time** *<time>*| **rmep-id** *<mepid>*]	开启或关闭按需的双向时延检测功能
16	inspur(config-cfm-md-index-ma-index)#**set mep** *<mepid>* **1mm** {**enable** | **disable**}[**interval** *<interval>*| **require-time** *<time>*| **rmep-id** *<mepid>*]	开启或关闭按需的单相帧丢失检测功能
17	inspur(config-cfm-md-index-ma-index)#**set mep** *<mepid>* **dlm** {**enable** | **disable**}[**frame-size** *<frame size>*| **interval** *<interval>*| **require-time** *<time>*| **rmep-id***<mepid>*]	开启或关闭主动的双向帧丢检测失功能
18	inspur(config-cfm-md-index-ma-index)#**set mep** *<mepid>* **ais** {**interval** *<interval>*| **state** {**enable** | **disable**}}	设置开启或关闭以太网告警指示信号功能，默认关闭
19	inspur(config-cfm-md-index-ma-index)#**set mep** *<mepid>* **priority** *<priority>*	配置本地MEP的CCM/LTM

步骤	命令	功能
		的优先级，范围为0-7，默认7
20	inspur(config-cfm-md-index-ma-index)#**set mep** <*mepid*> **lck** {**interval** <*interval*>| **state** {**enable**	**disable**}}	设置开启或关闭CFM以太网锁定信号功能，默认关闭
21	inspur(config-cfm-md-index-ma-index)#**set mep** <*mepid*> **client-level** <*priority*>	配置本地MEP的用户层级，范围1-7
22	inspur(config-cfm-md-index-ma-index)#**set mep** <*mepid*> **proactive** {**1dm**	**dmm**}{**enable** [**frame-size** <*frame size*>| **interval** <*interval*>| **rmep-id** <*mepid*>]| **disable**}	开启或关闭主动的单向、双向时延检测功能

frame-size <*frame size*>：帧的大小，范围：64、128、256、512、1024、1280、1518。

interval <*interval*>：发送周期，范围：1~60，默认：1秒。

require-time<*time*>：发送时长，范围：10~86400，单位：秒。

2.配置检测报文。

命令	功能
inspur#**cfm loopback md** <*md-index*> **ma** <*ma-index*> **local-mep** <*mepid*> **type unicast** <*mac-address*>[**repeat** <*time*>][**size** <*length*>][**timeout** <*second*>]	发送环回报文LBM
inspur#**cfm linktrace md** <*md-index*> **ma** <*ma-index*> **local-mep** < *mepid*><*mac-address*>[**timeout2** <*second*>][**ttl** <*value*>]	发送链路跟踪报文LTM，time out默认为5，ttl默认为64

<*md-index*>：维护域索引，范围1~65535。

<*ma-index*>：维护联合索引，范围1~65535。

<*mepid*>：本地MEPID，范围1~8191，唯一标识MA内一个本地MEP。

repeat <*time*>：一次发送的LBM报文个数，范围1~200，默认为3。

size <*length*>：LBM中携带的Data TLV字段长度，范围1~400，默认为0。

timeout <*second*>：LBM等待超时的时间长度，单位：秒，范围1~10，默认为5 s。

timeout2 <*second*>：等待LTR超时的时间间隔，单位：秒，范围5~10，默认为5 s。

ttl <*value*>：LTM可以转发的最大跳数，范围1~64，默认为64。

3.PW接口模式下配置MIP。

步骤	命令	功能
1	inspur(config-cfm)#**interface** *<IfName>*	进入PW接口模式
2	inspur(config-cfm-if-IfName)#**mip level** *<level>*	在PW接口模式下配置MIP 使用**no**命令取消配置

4.验证配置结果。

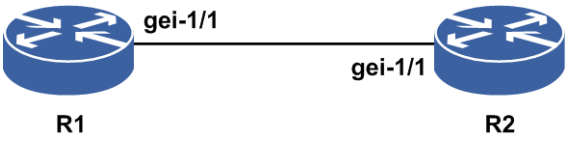
命令	功能
inspur#**show cfm status**	查看CFM全局配置状态
inspur#**show cfm md** {*<md-index>*|**all**}	查看指定维护域信息
inspur#**show cfm ma** {*<ma-index>*|**all**} **md** *<md-index>*	查看指定维护联盟详细信息
inspur#**show cfm mp** {*<mpid>*|**all**} **md** *<md-index>* **ma** *<ma-index>*	查看指定MP详细配置及状态信息
inspur#**show cfm mip** {**all-interface** | **interface** *<specify-interface>*}	查看指定MIP配置信息

10.6.2 CFM 快速连续性检测配置实例

配置说明

如*图 10-10*所示，R1和R2直连，在R1、R2直连接口上配置CFM，建立连接。

图 10-10 CFM 快速连续性检测



配置思路

1.R1、R2上创建同名、同ID的MD和MA，全局使能CFM。

2.R1、R2直连接口上创建同level的本地mep，并以对端的mac和mep id创建远端mep；再分别使能本地mep和ccm报文发送，使能远端mep。

3.R1、R2上show cfm mp查看mep标志位，查看R1与R2的CFM连接建立状况。

配置过程

R1的配置如下：

```
R1#configure terminal
R1(config)#cfm
R1(config-cfm)#set cfm enable
R1(config-cfm)#create md index 1 name-format 2 name MD1 level 4
R1(config-cfm)#md index 1
R1(config-cfm-md-1)#create ma index 1 name-format 2 name MA1
R1(config-cfm-md-1)#ma index 1
R1(config-cfm-md-1-ma-1)#create mep mepid 1 direction down interface gei-1/1
R1(config-cfm-md-1-ma-1)#set ccminterval 1          /*快速检测*/
R1(config-cfm-md-1-ma-1)#set mep 1 state enable
R1(config-cfm-md-1-ma-1)#set mep 1 ccm-send enable
R1(config-cfm-md-1-ma-1)#create rmep mepid 2 remote-mac 00ee.efab.ede3
R1(config-cfm-md-1-ma-1)#set mep 2 state enable
R1(config-cfm-md-1-ma-1)#end
```

R2的配置如下：

```
R2#configure terminal
R2(config)#cfm
R2(config-cfm)#set cfm enable
R2(config-cfm)#create md index 1 name-format 2 name MD1 level 4
R2(config-cfm)#md index 1
R2(config-cfm-md-1)#create ma index 1 name-format 2 name MA1
R2(config-cfm-md-1)#ma index 1
R2(config-cfm-md-1-ma-1)#create mep mepid 2 direction down interface gei-1/1
R2(config-cfm-md-1-ma-1)#set ccminterval 1
R2(config-cfm-md-1-ma-1)#set mep 2 state enable
R2(config-cfm-md-1-ma-1)#set mep 2 ccm-send enable
R2(config-cfm-md-1-ma-1)#create rmep mepid 1 remote-mac 0016.1514.1312
R2(config-cfm-md-1-ma-1)#set mep 1 state enable
R2(config-cfm-md-1-ma-1)#end
```

配置验证

1.R1上**show cfm mp all md 1 ma 1**查看链路状况：

```
R1(config)#show cfm mp all md 1 ma 1

MP type                              : Local MEP
  Direction                           : down
  MEPID                              : 1
  Level                              : 4
  Primary VID                         : 0
  Assign port                         : gei-1/1
  Priority                           : 7
  LowestAlarmPriority                  : 1
  Client level                       : invalid
  Admin state                        : enable
  Carrying Interface Status TLV        : disable
  Capability of setting line protocol   : disable
  Interwork configuration mode         : stopping-cc
  Interwork working mode              : stopping-cc
  CCM state/interval                 : enable/3.3ms
  AIS state/interval                 : disable/1s
  LCK state/interval                 : disable/1s
  LM state                           : disable
  On-demand DM state                   : disable
  Proactive DM state                   : disable
  TST state                          : disable

--------------------------------------------------------------------------
  PresentRDI            : 0          MADefectIndication     : 0
  SomeRDIDefect         : 0          SomeMACstatusDefect    : 0
  SomeRMEPCCMDefect      : 0          ErrorCCMDefect         : 0
  UnexpectedLevelDefect   : 0          UnexpectedPeriodDefect  : 0
  UnexpectedMACDefect    : 0          UnexpectedMEPIDDefect   : 0
  XconCCMDefect         : 0          AISRcvdFlag           : 0
  LCKRcvdFlag           : 0
```

```
------------------------------------------------------------------------
  TotalSendCCMs          : 62225      TotalRcvdCCMs          : 62225
  RightRcvdCCMs          : 62225      DefErrorCCMs           : 0
  DiscardCCMs            : 0          DefXconCCMs            : 0
  TotalSendLBMs          : 0          TotalRcvdLBRs          : 0
  TotalRcvdLBMs          : 0          TotalSendLBRs          : 0

------------------------------------------------------------------------

MP type                  : Remote MEP
  MEPID                  : 2
  Level                  : 4
  RemoteMAC              : 0a0a.0b12.1015
  Admin state            : enable
  CCM interval           : 3.3ms

------------------------------------------------------------------------
  RMEPLastRDI            : 0
  RMEPCCMdefect          : false
  Remote ifOperStatus    : null

------------------------------------------------------------------------
  LMMCount               : 0          DLMCount               : 0
  LMMFrameSendRemote     : 0          DLMFrameSendRemote     : 0
  LMMFrameSendLocal      : 0          DLMFrameSendLocal      : 0
  LMMFrameLossRemote     : 0          DLMFrameLossRemote     : 0
  LMMFrameLossLocal      : 0          DLMFrameLossLocal      : 0
  LMMAveFrameLossRemote  : 0          DLMAveFrameLossRemote  : 0
  LMMAveFrameLossLocal   : 0          DLMAveFrameLossLocal   : 0
  LMMHighFrameLossRemote : 0          DLMHighFrameLossRemote : 0
  LMMHighFrameLossLocal  : 0          DLMHighFrameLossLocal  : 0
  LMMTotalFrameLossRemote : 0         DLMTotalFrameLossRemote : 0
  LMMTotalFrameLossLocal : 0          DLMTotalFrameLossLocal : 0
  LMMFrameLossRatioRemote : 0.000000   DLMFrameLossRatioRemote : 0.000000
  LMMFrameLossRatioLocal : 0.000000   DLMFrameLossRatioLocal : 0.000000

------------------------------------------------------------------------
  Proactive DM Count     :
   1DMFrameTimeDelay     : 0s, 0ns
   1DMFrameTimeDelayChg  : 0s, 0ns
   DMMFrameTimeDelay     : 0s, 0ns
   DMMFrameTimeDelayChg  : 0s, 0ns
  On-demand DM Count     :
   1DMFrameTimeDelay     : 0s, 0ns
   1DMFrameTimeDelayChg  : 0s, 0ns
   DMMFrameTimeDelay     : 0s, 0ns
   DMMFrameTimeDelayChg  : 0s, 0ns

------------------------------------------------------------------------
```

2.R2上**show cfm mp all md 1 ma 1**查看链路状况：

```
R2(config)#show cfm mp all md 1 ma 1

MP type                          : Local MEP
  Direction                      : down
  MEPID                          : 2
  Level                          : 4
  Primary VID                    : 0
  Assign port                    : gei-1/1
  Priority                       : 7
  LowestAlarmPriority            : 1
  Client level                   : invalid
  Admin state                    : enable
  Carrying Interface Status TLV  : disable
  Capability of setting line protocol  : disable
  Interwork configuration mode   : stopping-cc
  Interwork working mode         : stopping-cc
  CCM state/interval             : enable/3.3ms
```

```
  AIS state/interval                 : disable/1s
  LCK state/interval                 : disable/1s
  LM state                          : disable
  On-demand DM state                 : disable
  Proactive DM state                 : disable
  TST state                         : disable

------------------------------------------------------------------------
  PresentRDI            : 0         MADefectIndication     : 0
  SomeRDIDefect         : 0         SomeMACstatusDefect    : 0
  SomeRMEPCCMDefect     : 0         ErrorCCMDefect         : 0
  UnexpectedLevelDefect : 0         UnexpectedPeriodDefect : 0
  UnexpectedMACDefect   : 0         UnexpectedMEPIDDefect  : 0
  XconCCMDefect         : 0         AISRcvdFlag            : 0
  LCKRcvdFlag           : 0

------------------------------------------------------------------------
  TotalSendCCMs         : 2254      TotalRcvdCCMs          : 2200
  RightRcvdCCMs         : 2200      DefErrorCCMs           : 0
  DiscardCCMs           : 0         DefXconCCMs            : 0
  TotalSendLBMs         : 0         TotalRcvdLBRs          : 0
  TotalRcvdLBMs         : 0         TotalSendLBRs          : 0

------------------------------------------------------------------------

MP type                : Remote MEP
  MEPID                : 1
  Level                : 4
  RemoteMAC            : 0022.936a.9400
  Admin state          : enable
  CCM interval         : 3.3ms

------------------------------------------------------------------------
  RMEPLastRDI          : 0
  RMEPCCMdefect        : false
  Remote ifOperStatus  : null

------------------------------------------------------------------------
  LMMCount             : 0         DLMCount               : 0
  LMMFrameSendRemote   : 0           DLMFrameSendRemote     : 0
  LMMFrameSendLocal    : 0           DLMFrameSendLocal      : 0
  LMMFrameLossRemote   : 0           DLMFrameLossRemote     : 0
  LMMFrameLossLocal    : 0           DLMFrameLossLocal      : 0
  LMMAveFrameLossRemote : 0          DLMAveFrameLossRemote  : 0
  LMMAveFrameLossLocal : 0           DLMAveFrameLossLocal   : 0
  LMMHighFrameLossRemote : 0         DLMHighFrameLossRemote : 0
  LMMHighFrameLossLocal : 0          DLMHighFrameLossLocal  : 0
  LMMTotalFrameLossRemote : 0        DLMTotalFrameLossRemote : 0
  LMMTotalFrameLossLocal : 0         DLMTotalFrameLossLocal : 0
  LMMFrameLossRatioRemote : 0.000000   DLMFrameLossRatioRemote : 0.000000
  LMMFrameLossRatioLocal : 0.000000   DLMFrameLossRatioLocal : 0.000000

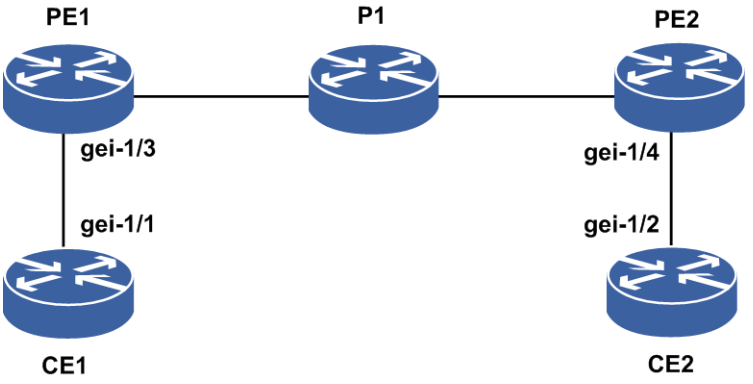
------------------------------------------------------------------------
  Proactive DM Count     :
   1DMFrameTimeDelay     : 0s, 0ns
   1DMFrameTimeDelayChg  : 0s, 0ns
   DMMFrameTimeDelay     : 0s, 0ns
   DMMFrameTimeDelayChg  : 0s, 0ns
  On-demand DM Count     :
   1DMFrameTimeDelay     : 0s, 0ns
   1DMFrameTimeDelayChg  : 0s, 0ns
   DMMFrameTimeDelay     : 0s, 0ns
   DMMFrameTimeDelayChg  : 0s, 0ns
  ------------------------------------------------------------------------
```

10.6.3 跨越 L2VPN 连通性检测配置实例

配置说明

如*图 10-11*所示L2VPN组网环境，在CE1、PE1、PE2和CE2上分别配置CFM的mep、mip结点，检测链路CE1—PE1—PE2—CE2的连通性。

图 10-11 跨越 L2VPN 连通性检测



配置思路

1.CE1、CE2、PE1和PE2上分别配置同名、同ID的MD和MA。

2.CE1和CE2的接口，参照“CFM快速连续性检测”实例，配置为一对CFM连续检测组；CE1、CE2打开告警。

3.PE1和PE2的公网侧接口和AC侧接口，分别配置mip结点，并全局使能CFM。

4.CE1向PE1、PE2、CE2上的mip、mep做cfm linktrace、cfm loopback操作，检查链路连通性。

配置过程

CE1的配置如下：

```
CE1(config)#cfm
CE1(config-cfm)#set cfm enable
CE1(config-cfm)#create md index 1 name-format 2 name MD1 level 4
CE1(config-cfm)#md index 1
CE1(config-cfm-md-1)#create ma index 1 name-format 2 name MA1 vid 1
/*L2VPN AC侧子接口的VLAN值*/
CE1(config-cfm-md-1)#ma index 1
CE1(config-cfm-md-1-ma-1)#create mep mepid 1 direction down interface
gei-1/1.1
CE1(config-cfm-md-1-ma-1)#set ccminterval 1          /*快速检测*/
CE1(config-cfm-md-1-ma-1)#set mep 1 state enable
CE1(config-cfm-md-1-ma-1)#set mep 1 ccm-send enable
CE1(config-cfm-md-1-ma-1)#create rmep mepid 2 remote-mac 00ee.efab.ede3
CE1(config-cfm-md-1-ma-1)#set mep 2 state enable
CE1(config-cfm-md-1-ma-1)#exit
CE1(config-cfm-md-1)#exit
CE1(config-cfm)#exit
```

```
CE1(config)#logging on
CE1(config)#exit

CE1#terminal monitor
```

CE2的配置如下：

```
CE2(config)#cfm
CE2(config-cfm)#set cfm enable
CE2(config-cfm)#create md index 1 name-format 2 name MD1 level 4
CE2(config-cfm)#md index 1
CE2(config-cfm-md-1)#create ma index 1 name-format 2 name MA1 vid 1
/*L2VPN AC侧子接口的VLAN值*/
CE2(config-cfm-md-1)#ma index 1
CE2(config-cfm-md-1-ma-1)#create mep mepid 2 direction down interface
gei-1/2.1
CE2(config-cfm-md-1-ma-1)#set ccminterval 1
CE2(config-cfm-md-1-ma-1)#set mep 2 state enable
CE2(config-cfm-md-1-ma-1)#set mep 2 ccm-send enable
CE2(config-cfm-md-1-ma-1)#create rmep mepid 1 remote-mac 0016.1514.1312
CE2(config-cfm-md-1-ma-1)#set mep 1 state enable
CE2(config-cfm-md-1-ma-1)#exit
CE2(config-cfm-md-1)#exit
CE2(config-cfm)#exit

CE2(config)#logging on
```

PE1的配置如下：

```
PE1(config)#cfm
PE1(config-cfm)#set cfm enable
PE1(config-cfm)#interface pw1
PE1(config-cfm-if-pw1)#mip level 4
PE1(config-cfm-if-pw1)#exit
PE1(config-cfm)#create md index 1 name-format 2 name MD1 level 4
PE1(config-cfm)#md index 1
PE1(config-cfm-md-1)#create ma index 1 name-format 2 name MA1 vid 1
PE1(config-cfm-md-1)#ma index 1
PE1(config-cfm-md-1-ma-1)#create mip session-id 1 interface gei-1/3.1
PE1(config-cfm-md-1-ma-1)#end
```

PE2的配置如下：

```
PE2(config)#cfm
PE2(config-cfm)#set cfm enable
PE2(config-cfm)#interface pw1
PE2(config-cfm-if-pw1)#mip level 4
PE2(config-cfm-if-pw1)#exit
PE2(config-cfm)#create md index 1 name-format 2 name MD1 level 4
PE2(config-cfm)#md index 1
PE2(config-cfm-md-1)#create ma index 1 name-format 2 name MA1 vid 1
PE2(config-cfm-md-1)#ma index 1
PE2(config-cfm-md-1-ma-1)#create mip session-id 1 interface gei-1/4.1
PE2(config-cfm-md-1-ma-1)#end
```

配置验证

CE1上向PE1、PE2、CE2上做cfm linktrace（trace）、cfm loopback（ping）操作，若链路正常，则trace和ping回应正确；另外，若链路从好变坏，CE1、CE2上会产生cfm的告警。以下为CE2向CE1做的ping和trace操作。

```
CE2#cfm linktrace md 1 ma 1 local-mep 1 0016.1514.1312
Trace the link to 0a0a.0b12.1015. Per-Hop timeout is 5 seconds. TransID is 1.
Trace sent via gei-1/2 on level 4. Type Ctrl+C to abort.
------------------------------------------------------------------------
-----
                                        Ingress     Egress     Relay
```

```
  Hops     MAC ADDRESS     Forwarded      Action      Action      Action
-------------------------------------------------------------------------
-----
F  1       00d0.d0c0.e21f  Forwarded      IngOk       EgrOk       RlyFDB
F  2       0022.2324.251f  Forwarded      IngOk       EgrOk       RlyFDB
!  3       0016.1514.1312  Not Forwarded   IngOk                   RlyHit
Trace complete
```

10.7 BFD

BFD能够在系统之间的任何类型通道上进行故障检测，这些通道包括直连的物理链路、虚电路、隧道、MPLS LSP、多跳路由通道以及非直连的通道。BFD实现故障检测具有简单性、单一性，专注于转发故障的快速检测，可以帮助网络以良好的QoS实现语音、视频及其它点播业务的传输。

10.7.1 配置 BFD

配置BFD的基本属性和功能，为两个不同的转发系统之间提供失效检测。

1.配置实例化BFD。

步骤	命令	功能
1	inspur(config)#**bfd**	进入BFD配置模式
2	inspur(config-bfd)#**session** <*session-name*>{**l2-bfd interface** <*interface-name*> **source** <*src-ip-address*>| **link-bfd** {**ipv4** | **ipv6**}<*src-ip-address*><*dst-ip-address*> **interface** <*interface-name*>[**vrf** <*vrf-name*>]| **peer-bfd** {**ipv4** | **ipv6**}<*src-ip-address*><*dst-ip-address*>[**vrf** <*vrf-name*>]| **ldp-bfd fec-address** <*src-ipv4-address*><*mask-length*>[**vrf** <*vrf-name*>]| **pw-bfd pw-name** <*pw-name*>| **rsvp-bfd te_tunnel** <*tunnel-id*>}	在BFD配置模式下，配置实例化的BFD <*src-ip-address*>，建立会话的源地址（必需是本地地址） <*dst-ip-address*>，建立会话的目的地址（不局限为直连地址） <*interface-name*>，指定会话的出接口（如果不指定，发送报文时就不会关心出接口，只要能够从本地发送出去就可以）
3	inspur(config-bfd)#**echo source ipv4** <*src-ip-address*>	配置单臂BFD使用的源地址
4	inspur(config-bfd)#**interface** <*interface-name*>	在BFD配置模式下，指定需要配置会话参数的接口
5	inspur(config-bfd-interface-name)#**time-negotiation interval** <*interval*> **min-rx** <*min-rx*> **multiplier** <*multiplier*>	配置BFD会话的收发包时间以及检测倍数 包含该命令的模式有：BFD接口模式、PEER-BFD实例模式、RSVP-BFD实例模式、PW-BFD实例模式、L2-BFD实例模式

步骤	命令	功能
6	inspur(config-bfd-interface-name)#**single-arm-echo enable**	配置BFD接口下单臂回声功能
7	inspur(config-bfd-interface-name)#**min-echo-rx-interval** <*echo-interval*>	配置BFD接口下单臂回声功能时间参数
8	inspur(config-bfd-peer-session-name)#**pkt-len min** <*min-pkt-length*> **max** <*max-pkt-length*>	实例化模式下配置大包检测功能 包含该命令的模式有：LINK-BFD实例模式、PEER-BFD实例模式
9	inspur(config-bfd-peer-session-name)#**multiport** {**enable** | **disable**}	配置修改目的端口号 命令模式：PEER-BFD实例模式
10	inspur(config-bfd-peer-session-name)#**dscp** <*DSCP value*>	配置BFD报文的DSCP值 包含该命令的模式有：LINK-BFD实例模式、PEER-BFD实例模式、LDP-BFD实例模式、RSVP-BFD实例模式、PW-BFD实例模式、L2-BFD实例模式
11	inspur(config-bfd-l2-session-name)#**discriminator ld** <*local-discriminator*> **rd** <*remote-discriminator*>	配置会话的本端和远端标识符，命令模式：L2-BFD实例模式
12	inspur(config-bfd)#**default destination** <*multicast-ipv4-address*>	在BFD配置模式下，配置二层链路BFD的默认组播目的地址

<*interval*>：发送检测报文的时间间隔，范围10~990，单位：ms。

<*min-rx-interval*>：接收检测报文的最小时间间隔，范围10~990，单位：ms。

<*multiplier*>：检测倍数，范围3~50。

<*min-pkt-length*>：BFD最小检测包长，范围24~512，缺省值：24，单位：byte。

<*max-pkt-length*>：BFD最大检测包长，范围24~512，缺省值：24，单位：byte。

enable：设置报文中UDP端口号为3784。

disable：设置报文中UDP端口号为4784。

<*DSCP value*>：BFD报文的DSCP值，范围0~63，缺省值：56。

<*local-discriminator*>：会话本端标识符，范围：1~2048。

<*remote-discriminator*>：会话远端标识符，范围：1~2048。

<*multicast-ipv4-address*>：检测二层链路的BFD会话的组播目的地址，范围：224.0.0.111~224.0.0.250，缺省值：224.0.0.250。

2.配置静态路由的BFD检测。

命令	功能
inspur(config)#**ip route vrf** <*vrf-name*><*prefix*><*net-mask*>{<*forwarding-router's-address*>[**globle**]|<*interface-name*>[<*forwarding-router's-address*>]}[<*distance-metric*>][**metric** <*metric-number*>] **bfd enable**	配置私网静态路由，并开启该链路的BFD监测功能
inspur(config)#**ip route** <*prefix*><*net-mask*>{<*forwarding-router's-address*>|<*interface-name*>[<*forwarding-router's-address*>]}[<*distance-metric*>][**metric** <*metric-number*>] **bfd enable**	配置公网静态路由，并开启该链路的BFD监测功能

<*forwarding-router's-address*>：下一跳的IP地址，十进制点分形式。

globle：私网路由指定公网下一跳，注意该选项和**bfd enable**不同时支持。

<*distance-metric*>：管辖距离，默认为1，范围：1~255。

<*metric-number*>：路由的度量值，默认为1，范围：1~255。

在配置静态路由时确认到达目的端的唯一链路，并通过**bfd enable**选项开启对这条链路的BFD检测功能。

3.配置OSPF路由的BFD检测。

步骤	命令	功能
1	inspur(config)#**router ospf** <*process-id*>	创建指定进程号的OSPF进程/进入指定的OSPF进程
2	inspur(config-ospf-id)#**bfd** [**area** <*area-id* >]	开启所有接口的BFD功能，或者开启指定area的所有接口上的BFD功能
3	inspur(config-ospf-id)#**interface** <*interface-name*>	选择一个需要开启BFD功能的接口
4	inspur(config-ospf-id-if-interface-name)#**bfd**	开启当前接口的BFD功能

在OSPF协议配置模式下开启所有接口的BFD，也可以选择性的开启所有绑定到指定区域的接口的BFD，或者进入OSPF协议的接口配置模式，开启当前接口的BFD功能。

4.配置IS-IS路由的BFD检测。

步骤	命令	功能
1	inspur(config)#**router isis** [<*process-id*>][**vrf** <*vrf-name*>]	创建/进入IS-IS路由协议进程
2	inspur(config-isis-id)#**interface** <*interface-name*>	在IS-IS路由配置模式下指定需要启用BFD的接口
3	inspur(config-isis-id-if-interface-name)#**bfd-enable**	启用IS-IS的BFD功能

在启用IS-IS协议的接口上开启BFD功能。当这个接口与对端建立了IS-IS邻接关系后，在这一对邻接接口的直连链路上基于IS-IS协议的BFD会话就形成了。

5.配置BGP路由的BFD检测。

步骤	命令	功能
1	inspur(config)#**router bgp** <*as-number*>	在路由器上配置BGP功能
2	inspur(config-bgp)#**neighbor** {<*ipv4-address*>|<*ipv6-address*>|<*peer-group-name*>} **fall-over bfd**	配置启动BFD链路失效检测机制

根据BGP邻居是直连或非直连，可以配置单跳（直连链路）BFD检测，或配置多跳（非直连）BFD检测。

6.配置LDP协议的BFD检测。

步骤	命令	功能
1	inspur(config)#**mpls ldp instance** <*1-65535*>[**vrf** <*vrf-name*>]	使能LDP沿着普通的逐跳路由路径建立LSP，并进入LDP配置模式
2	inspur(config-ldp)#**bfd** <*FEC address*><*mask length*> **interval** <*interval*> **min-rx** < *min-rx*> **multiplier** <*multiplier*>[**source** <*ip-address*>]	配置LDP LSP BFD相关参数，并触发创建LSP的BFD会话

<*FEC address*>：指定建立BFD的LSP地址，一般为一个远端地址网段。

<*mask length*>：指定远端网址的子网掩码长度，范围：0~32。

<*interval*>：指定期望的报文最小发送间隔时间，范围：10~990，单位：ms。

<*min_rx*>：指定期望的报文最小接收间隔时间，范围：10~990，单位：ms。

<*multiplier*>：指定检测超时的倍数，范围：3~50。

LDP BFD只需要单向配置，配置时指定LSP远端地址，反向的LDP BFD会话将自动建立。

7.配置RSVP协议的BFD检测功能。

命令	功能
inspur(config-mpls-te-if-interface-name)#**bfd**	MPLS-TE的实接口模式下开启接口BFD功能
inspur(config-mpls-te-tunnel-te_tunnel-number)#**tunnel mpls traffic-eng bfd interval** <*interval*> **min-rx** < *min-rx* > **multiplier** <*multiplier*>	MPLS-TE的tunnel接口模式下开启tunnel LSP BFD

<*interval*>：指定BFD控制报文的最小发送间隔，单位：毫秒，范围：10~990。

<*min-rx*>：指定BFD控制报文的最小接收间隔，单位：毫秒，范围：10~990。

<*multiplier*>：指定BFD控制报文的检测倍数，范围：3~50。

8.配置LOCAL/REMOTE描述符。

命令	功能
inspur(config-bfd-l2-instance-name)#**discriminator ld** <*ld*> **rd** <*rd*>	配置静态配置会话的LOCAL/REMOTE描述符

<*ld*>，指定会话的本地标识符，范围：1~2048。

<*rd*>，指定会话的远端标识符，范围：1~2048。

9.配置VRRP关联BFD功能。

命令	功能
inspur(config-samgr)#**track** <*track-object-name*> **bfd session** <*bfd-session-name*>	在SAMGR下面配置track对象
inspur(config-vrrp-if-interface-name)#**vrrp** <*vrid*> **track** {**group** | **object**}<*string*>{**link-type** | **peer-type** | **priority-decrement** <*1-254*>}	在VRRP接口配置模式下配置VRRP检测的事件组或检测对象及其策略类型

10.配置VPWS BFD功能。

命令	功能
inspur(config-vpws-vpws-name-pw-pw-number-neighbour-peer-router-id)#**vccv bfd capability** {**basic** | **status**} **encapsulation** {**raw** | **ip**}	在VPWS配置模式下配置VPWS BFD

11.配置BFD报文检测长度。

命令	功能
inspur(config-bfd)#**session** <*session-name*> **link-bfd ipv4** | **ipv6** <*src-ip-address*><*dst-ip-address*> **interface** <*interface-name*>[**vrf** <*vrf-name*>]	在BFD配置模式下，配置实例化的BFD
inspur(config-bfd-link-session-name)#**pkt-len min** <*24-512*> **max** <*24-512*>	在实例化的BFD配置模式下配置BFD报文检测长度

12.验证配置结果。

命令	功能
inspur#**show bfd neighbors ip detail**[**location** <*board-name*>]	显示IP类型BFD会话的详细信息
inspur#**show bfd neighbors ip brief**[**location** <*board-name*>]	显示IP类型BFD会话的概要信息
inspur#**show bfd neighbors ldp brief**[**location** <*board-name*>]	显示LDP类型BFD会话的概要信息

命令	功能
inspur#**show bfd neighbors ldp detail**[**location** <*board-name*>]	显示LDP类型BFD会话的详细信息
inspur#**show bfd neighbors rsvp** {**lsp** | **passive** | **tunnel**} **brief** [**location** <*board-name*>]	显示RSVP类型BFD会话的概要信息
inspur#**show bfd neighbors rsvp** {**lsp** | **passive** | **tunnel**} **detail** [**location** <*board-name*>]	显示RSVP类型BFD会话的详细信息
inspur#**show bfd neighbors pw brief**[**location** <*board-name*>]	显示PW类型BFD会话的概要信息
inspur#**show bfd neighbors pw detail**[**location** <*board-name*>]	显示PW类型BFD会话的详细信息
inspur#**show bfd neighbors l2 brief**[**location** <*board-name*>]	显示L2类型BFD会话的概要信息
inspur#**show bfd neighbors l2 detail**[**location** <*board-name*>]	显示L2类型BFD会话的详细信息
inspur#**show bfd statistics** [**location** <*board-name*>]	显示设备BFD基本信息
inspur#**show bfd neighbors local-disc** <*local-discriminator*>	指定本端标识符显示BFD信息

13.维护BFD。

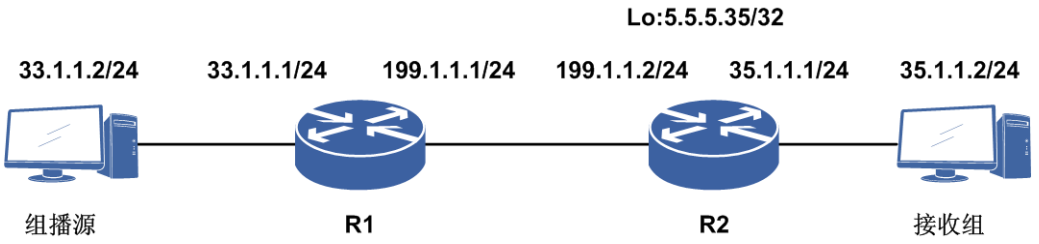
命令	功能
inspur#**debug bfd packet**	在BFD会话建立时显示发送和接收的建链报文的概要信息
inspur#**debug bfd event**	在BFD会话建立时显示BFD会话的状态变化的信息
inspur#**debug bfd byte**	在BFD会话建立时显示发送和接收的建链报文的报文信息（UDP数据区域的报文）
inspur#**debug bfd error**	在BFD会话建立时显示BFD建链过程中的错误信息
inspur#**debug bfd all**	同时开启packet、event、byte、error打印

10.7.2 PIM BFD 配置实例

配置说明

如*图 10-12*配置BFD关联PIM。

图 10-12 PIM BFD 配置实例拓扑图



配置思路

1.配置相应接口地址。

2.进入组播配置模式。

3.进入PIM配置模式。

4.进入接口启动PIM-SM。

5.在组播PIM模式的接口下，开启BFD。

配置过程

R1的配置如下：

```
R1(config)#interface gei-2/3
R1(config-if-gei-2/3)#ip address 199.1.1.1 255.255.255.0
R1(config-if-gei-2/3)#exit
R1(config)#interface gei-2/7
R1(config-if-gei-2/7)#ip address 33.1.1.1 255.255.255.0
R1(config-if-gei-2/7)#exit

R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-2/3
R1(config-mcast-pim-if-gei-2/3)#pimsm
R1(config-mcast-pim-if-gei-2/3)#bfd-enable
R1(config-mcast-pim-if-gei-2/3)#exit
R1(config-mcast-pim)#interface gei-2/7
R1(config-mcast-pim-if-gei-2/7)#pimsm
R1(config-mcast-pim-if-gei-2/7)#dr-priority 20
R1(config-mcast-pim-if-gei-2/7)#exit
```

R2的配置如下：

```
R2(config)#interface gei-3/8
R2(config-if-gei-3/8)#ip address 199.1.1.2 255.255.255.0
R2(config-if-gei-3/8)#exit
R2(config)#interface gei-3/7
R2(config-if-gei-3/7)#ip address 35.1.1.1 255.255.255.0
R2(config-if-gei-3/7)#exit
R2(config)#interface loopback5
R2(config-if-loopback5)#ip address 5.5.5.35 255.255.255.255
R2(config-if-loopback5)#exit

R2(config)#ip multicast-routing
R2(config-mcast)#router pim
R2(config-mcast-pim)#interface gei-3/8
R2(config-mcast-pim-if-gei-3/8)#pimsm
R2(config-mcast-pim-if-gei-3/8)#bfd-enable
```

```
R2(config-mcast-pim-if-gei-3/8)#exit
R2(config-mcast-pim)#interface gei-3/7
R2(config-mcast-pim-if-gei-3/7)#pimsm
R2(config-mcast-pim-if-gei-3/7)#dr-priority 20
R2(config-mcast-pim-if-gei-3/7)#exit
```

配置验证

在R1上通过**show ip pim interface**查看接口状态：

```
R1(config)#show ip pim interface
Address     Interface     State Nbr   Hello  DR        DR       PIM     Mode
                            Count Period Priority           Silent
33.1.1.1    gei-2/7       Up    0     30     20      33.1.1.1  Disabled S
199.1.1.1   gei-2/3       Up    1     30     1       199.1.1.2 Disabled S
```

在R1上通过**show ip pim neighbor**查看邻居状态：

```
R1(config)#show ip pim neighbor
Neighbor Address  Interface      DR Priority   Uptime     Expires   Ver
199.1.1.2        gei-2/3        1            00:07:48   00:01:23  V2
```

在R1上通过**show bfd neighbor ip brief**查看BFD状态：

```
R1(config)#show bfd neighbor ip brief
LocalAddr      PeerAddr      LD       RD       Hold   State    Interface
199.1.1.1      199.1.1.2     2053     2054     150    UP       gei-2/3

R1(config)#show bfd neighbor ip detail
------------------------------------------------------------------------------
--
LocalAddr: 199.1.1.1
PeerAddr : 199.1.1.2
Local Discr:2053          Remote Discr:2054          State:UP
Holdown(ms):150           Interface: gei-2/3
Vpnid:0                  VRF Name:---
BFD Type:SingleHop
Instance Name:
------------------------------------------------------------------------------
--
Version:1               Dest UDP Port:3784       Final Bit:1
Local Diag:0            Demand Mode:0            Poll Bit:0
MinTxInt:50             MinRxInt:50              Multiplier:3
Received MinTxInt:50     Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24        Max BFD Length:24

Rx Count:4352           Rx Interval (ms) min/max/avg:30    /100   /59
Tx Count:4159           Tx Interval (ms) min/max/avg:50    /120   /59
Registered Protocols:PIM
Uptime:0 day(s),0 hour(s),6 minute(s)
Control Plane Rcv Phy Interface Name: gei-2/3
==============================================================================
=
```

在R2上通过**show ip pim neighbor**查看邻居状态：

```
R2(config)#show ip pim neighbor
Neighbor Address  Interface      DR Priority   Uptime     Expires   Ver
199.1.1.1        gei-3/8        1            00:07:48   00:01:23  V2
```

在R2上通过**show bfd neighbor ip brief**查看BFD状态：

```
R2(config)#show bfd neighbor ip brief
LocalAddr      PeerAddr       LD       RD       Hold   State    Interface
199.1.1.2      199.1.1.1      2055     2054     150    UP       gei-3/8

RP3(config)#show bfd neighbor ip detail
------------------------------------------------------------------------------
```

```
--
LocalAddr: 199.1.1.2
PeerAddr : 199.1.1.1
Local Discr:2055          Remote Discr:2054          State:UP
Holdown(ms):150           Interface: gei-3/8
Vpnid:0                  VRF Name:---
BFD Type:SingleHop
Instance Name:
------------------------------------------------------------------------
--
Version:1               Dest UDP Port:3784       Final Bit:1
Local Diag:0             Demand Mode:0           Poll Bit:0
MinTxInt:50             MinRxInt:50             Multiplier:3
Received MinTxInt:50     Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24        Max BFD Length:24

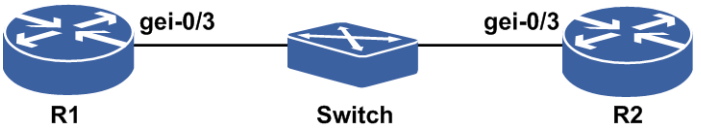
Rx Count:804             Rx Interval (ms) min/max/avg:40    /100   /59
Tx Count:813             Tx Interval (ms) min/max/avg:40    /80    /59
Registered Protocols:PIM
Uptime:0 day(s),0 hour(s),1 minute(s)
Control Plane Rcv Phy Interface Name: gei-3/8
========================================================================
==
```

10.7.3 静态单跳 BFD 配置实例

配置说明

目前静态单跳BFD与静态多跳BFD是不关联路由的，两者之间最大区别就是静态单跳BFD必须配置出接口，而静态多跳BFD是不配置出接口的。如*图 10-13*所示，R1上配置静态单跳BFD不关联路由，R2配置静态路由的BFD。

图 10-13 静态单跳 BFD



配置思路

1.R1上配置静态单跳BFD。

2.R2配置静态路由的BFD。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-0/3
R1(config-if-gei-0/3)#no shutdown
R1(config-if-gei-0/3)#ip address 172.20.130.213 255.255.255.0
R1(config-if-gei-0/3)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 172.20.96.1 255.255.255.255
```

```
R1(config-if-loopback1)#exit
R1(config)#bfd
R1(config-bfd)#session test link-bfd ipv4 172.20.130.213 172.20.130.214
interface gei-0/3
R1(config-bfd-link-test)#!
```

R2上的配置如下：

```
R2(config)#interface gei-0/3
R2(config-if-gei-0/3)#no shutdown
R2(config-if-gei-0/3)#ip address 172.20.130.214 255.255.255.0
R2(config-if-gei-0/3)#exit
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 172.20.108.1 255.255.255.255
R2(config-if-loopback1)#exit
R2(config)#ip route 172.20.96.1 255.255.255.255 172.20.130.213
bfd enable
```

配置验证

正确配置后，R1上的静态单跳BFD和R2上的静态路由单跳BFD会话应该能够成功建立，可以用如下命令查看结果：

用**show bfd neighbors** [**ip brief**|**ip detail**]来查看验证R1上的静态单跳BFD和R2上的静态路由单跳BFD会话是否生效。

R1上静态单跳BFD生效情况查看：

```
R1#show bfd neighbors ip brief
LocalAddr      PeerAddr       LD     RD    Hold    State   Interface
172.20.130.213  172.20.130.214  1      58    150     UP      gei-0/3

R1#show bfd neighbors ip detail
LocalAddr:172.20.130.213
PeerAddr :172.20.130.214
Local Discr:2153          Remote Discr:2395          State:UP

Holdown(ms):150           Interface: gei-0/3
Vpnid:0                  VRF Name:---
BFD Type:SingleHop
Instance Name:test
--------------------------------------------------------------------------
--
Version:1               Dest UDP Port:3784       Final Bit:1
Local Diag:0             Demand Mode:0           Poll Bit:1
MinTxInt:50             MinRxInt:50             Multiplier:3
Received MinTxInt:50     Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24        Max BFD Length:24

Rx Count:0              Rx Interval (ms) min/max/avg:0     /0     /0
Tx Count:0              Tx Interval (ms) min/max/avg:0     /0     /0
Registered Protocols:INSTANCE
Uptime:0 day(s),0 hour(s),0 minute(s)
Control Plane Rcv Phy Interface Name: gei-0/3
==========================================================================
===
```

R2上的静态路由单跳BFD会话生效情况查看：

```
R2#show bfd neighbors ip brief
LocalAddr      PeerAddr       LD     RD     Hold   State   interface
172.20.130.214  172.20.130.213  58     1      150    UP      gei-0/3

R2#show bfd neighbors ip detail
--------------------------------------------------------------------------
---
```

```
LocalAddr:172.20.130.214
PeerAddr :172.20.130.213
Local Discr:2395          Remote Discr:2153          State:UP

Holdown(ms):150           Interface: gei-0/3
Vpnid:0                  VRF Name:---
BFD Type:SingleHop
Instance Name:
--------------------------------------------------------------------------
--
Version:1                Dest UDP Port:3784       Final Bit:1
Local Diag:0             Demand Mode:0            Poll Bit:1
MinTxInt:50              MinRxInt:50              Multiplier:3
Received MinTxInt:50      Received MinRxInt:50      Received Multiplier:3
Length:24                Min Echo Interval:0
Min BFD Length:24         Max BFD Length:24

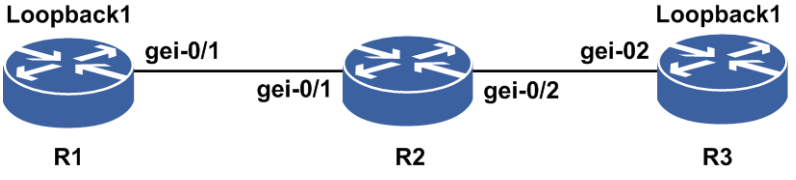
Rx Count:0               Rx Interval (ms) min/max/avg:0     /0     /0
Tx Count:188             Tx Interval (ms) min/max/avg:0     /0     /0
Registered Protocols:STATIC
Uptime:0 day(s),0 hour(s),0 minute(s)
Control Plane Rcv Phy Interface Name: gei-0/3
==========================================================================
==
```

10.7.4 静态多跳 BFD 配置实例

配置说明

目前静态单跳BFD与静态多跳BFD是不关联路由的，两者之间最大区别就是静态单跳BFD必须配置出接口，而静态多跳BFD是不配置出接口的。如*图 10-14*所示，R1上配置静态多跳BFD不关联路由，R3配置BGP多跳BFD。

图 10-14 静态多跳 BFD



配置思路

1.R1上配置静态多跳BFD。

2.R3配置BGP多跳BFD。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-0/1
R1(config-if-gei-0/1)#no shutdown
R1(config-if-gei-0/1)#ip address 172.20.130.18 255.255.255.0
R1(config-if-gei-0/1)#exit
```

```
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 172.20.96.1 255.255.255.255
R1(config-if-loopback1)#exit

R1(config)#router ospf 1
R1(config-ospf-1)#area 0
R1(config-ospf-1-area-0)#network 172.20.130.0 0.0.0.255
R1(config-ospf-1-area-0)#network 172.20.96.1 0.0.0.0
R1(config-ospf-1-area-0)#exit

R1(config)#router bgp 18004
R1(config-bgp)#neighbor 172.20.108.2 remote-as 18004
R1(config-bgp)#neighbor 172.20.108.2 update-source loopback1
R1(config-bgp)#exit
R1(config)#bfd
R1(config-bfd)#session test peer-bfd ipv4 172.20.96.1 172.20.108.2
R1(config-bfd-session-test)#end
```

R2上的配置如下：

```
R2(config)#interface gei-0/1
R2(config-if-gei-0/1)#no shutdown
R2(config-if-gei-0/1)#ip address 172.20.130.17 255.255.255.0
R2(config-if-gei-0/1)#exit
R2(config)#interface gei-0/2
R2(config-if-gei-0/2)#no shutdown
R2(config-if-gei-0/2)#ip address 172.20.140.221 255.255.255.0
R2(config-if-gei-0/2)#exit
R2(config)#interface loopback1
R2(config-if-loopback1)#ip address 172.20.96.2 255.255.255.255
R2(config-if-loopback1)#exit

R2(config)#router ospf 1
R2(config-ospf-1)#area 0
R2(config-ospf-1-area-0)#network 172.20.130.0 0.0.0.255
R2(config-ospf-1-area-0)#network 172.20.140.0 0.0.0.255
R2(config-ospf-1-area-0)#network 172.20.96.2 0.0.0.0
R2(config-ospf-1-area-0)#exit
```

R3上的配置如下：

```
R3(config)#interface gei-0/2
R3(config-if-gei-0/2)#no shutdown
R3(config-if-gei-0/2)#ip address 172.20.140.222 255.255.255.0
R3(config-if-gei-0/2)#exit
R3(config)#interface loopback1
R3(config-if-loopback1)#ip address 172.20.108.2 255.255.255.255
R3(config-if-loopback1)#exit

R3(config)#router ospf 1
R3(config-ospf-1)#area 0
R3(config-ospf-1-area-0)#network 172.20.140.0 0.0.0.255
R3(config-ospf-1-area-0)#network 172.20.108.2 0.0.0.0
R3(config-ospf-1-area-0)#exit

R3(config)#router bgp 18004
R3(config-bgp)#neighbor 172.20.96.1 remote-as 18004
R3(config-bgp)#neighbor 172.20.96.1 update-source loopback1
R3(config-bgp)#neighbor 172.20.96.1 fall-over bfd
R3(config-bgp)#exit
R3(config-bfd)#session test peer-bfd ipv4 172.20. 108.2 172.20.96.1
R3(config-bfd-session-test)#end
```

配置验证

正确配置后，R1上的静态多跳BFD和R3上的BGP多跳BFD会话应该能够成功建立，可以用如下命令查看结果：

用**show bfd neighbors** [**ip brief**|**ip detail**]来查看验证R1上的静态多跳BFD和R3上的BGP多跳BFD会话是否生效。

R1上静态多跳BFD生效情况查看：

```
R1(config)#show bfd neighbors ip brief
LocalAddr       PeerAddr       LD      RD      Hold    State    Interface
172.20.96.1    172.20.108.2    6       1       150     UP       ---

R1(config)#show bfd neighbors ip detail
------------------------------------------------------------------------------
--
LocalAddr: 172.20.96.1
PeerAddr : 172.20.108.2
Local Discr:2395          Remote Discr:2153          State:UP

Holdown(ms):150           Interface:---
Vpnid:0                  VRF Name:
BFD Type:MultiHop
Instance Name:test
------------------------------------------------------------------------------
--
Version:1               Dest UDP Port:3784       Final Bit:1
Local Diag:0            Demand Mode:0            Poll Bit:1
MinTxInt:50             MinRxInt:50              Multiplier:3
Received MinTxInt:50     Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24        Max BFD Length:24

Rx Count:190            Rx Interval (ms) min/max/avg:191     /200     /200
Tx Count:188            Tx Interval (ms) min/max/avg:200     /220     /220
Registered Protocols:INSTANCE
Uptime:0 day(s),0 hour(s),0 minute(s)
Control Plane Rcv Phy Interface Name:
==============================================================================
==
```

R3上的BGP多跳BFD会话生效情况查看：

```
R3(config)#show bfd neighbors ip brief
LocalAddr       PeerAddr       LD       RD       Hold   State     Interface
172.20.108.2    172.20.96.1     1        6       150    UP         -----

R3(config)#show bfd neighbors ip detail
------------------------------------------------------------------------------
--
LocalAddr:172.20.108.2
PeerAddr :172.20.96.1
Local Discr:2056          Remote Discr:2127          State:UP

Holdown(ms):150           Interface:---
Vpnid:0                  VRF Name:---
BFD Type:MultiHop
Instance Name:test
------------------------------------------------------------------------------
--
Version:1               Dest UDP Port:4784       Final Bit:1
Local Diag:0            Demand Mode:0            Poll Bit:1
MinTxInt:50             MinRxInt:50              Multiplier:3
Received MinTxInt:50     Received MinRxInt:50     Received Multiplier:3
Length:24               Min Echo Interval:0
Min BFD Length:24        Max BFD Length:24

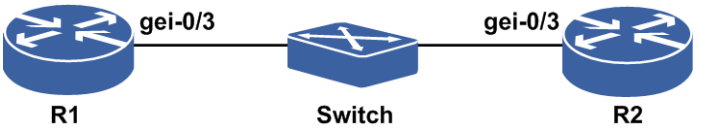
Rx Count:50             Rx Interval (ms) min/max/avg:50    /50    /48
Tx Count:40             Tx Interval (ms) min/max/avg:48    /48    /46
Registered Protocols:BGP
Uptime:0 day(s),0 hour(s),0 minute(s)
Control Plane Rcv Phy Interface Name: gei-0/2
==============================================================================
==
```

10.7.5 单臂 ECHO 配置实例

配置说明

在两台直连的设备中，其中一台设备支持BFD功能，另一台设备不支持BFD功能。为了能够更加快速的检测链路故障，在支持BFD功能的设备上开启单臂ECHO功能。不支持BFD功能的设备接收到该BFD报文后，直接将报文环回，从而达到快速检测链路的目的，如*图 10-15*所示。

图 10-15 单臂 ECHO 组网示意图



配置思路

R1上配置单臂ECHO功能。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-0/3
R1(config-if-gei-0/3)#no shutdown
R1(config-if-gei-0/3)#ip address 12.1.1.1 255.255.255.0
R1(config-if-gei-0/3)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
R1(config-if-loopback1)#exit
R1(config)#bfd
R1(config-bfd)#echo source ipv4 1.1.1.1
R1(config-bfd)#interface gei-0/3
R1(config-bfd-if-gei-0/3)#single-arm-echo enable
R1(config-bfd-if-gei-0/3)#exit
R1(config-bfd)#session 1 link-bfd ipv4 12.1.1.1 12.1.1.2 interface gei-0/3
R1(config-bfd-link-1)#!
```

R2上的配置如下：

```
R2(config)#interface gei-0/3
R2(config-if-gei-0/3)#no shutdown
R2(config-if-gei-0/3)#ip address 12.1.1.2 255.255.255.0
R2(config-if-gei-0/3)#exit
```

配置验证

正确配置后，R1上的BFD会话应该能够成功建立，可以用如下命令查看结果：

用**show bfd neighbors** [**ip brief**|**ip detail**]命令来查看验证R1上的BFD会话是否生效。

R1上BFD生效情况查看：

```
R1#show bfd neighbors ip brief
LocalAddr       PeerAddr        LD       RD       Hold   State     Interface
12.1.1.1        12.1.1.2        2050     0        1500   UP        gei-0/3
R1#show bfd neighbors ip detail
------------------------------------------------------------------------------
--
LocalAddr:12.1.1.1
PeerAddr :12.1.1.2
Track Action:---
Local Discr:2050          Remote Discr:0           State:UP
Holddown(ms):1500         Interface:gei-0/3
Vpnid:0                  VRF Name:
BFD Type:SingleHop
Instance Name:1
Detect Mode:Single-arm-echo
------------------------------------------------------------------------------
--
Version:1                Dest UDP Port:3785       Final Bit:0
Local Diag:0             Demand Mode:0            Poll Bit:0
MinTxInt:50              MinRxInt:50              Multiplier:3
Received MinTxInt:4506    Received MinRxInt:50     Received Multiplier:3
Length:24                Min Echo Interval:500
Min BFD Length:24         Max BFD Length:24

Rx Count:5134            Rx Interval (ms) min/max/avg:476   /477   /476
Tx Count:5133            Tx Interval (ms) min/max/avg:476   /477   /476

Penalty:0
Dampen state:N
Dampen Left:---
Negotiate fail notify:OFF
Negotiate fail notify time:300(s)
Registered Protocols:INSTANCE
Uptime:0 day(s),0 hour(s),40 minute(s),47 second(s)
Control Plane Rcv Phy Interface Name:gei-0/3
Debug packet/byte/error/event:OFF/OFF/OFF/OFF
==============================================================================
==
R1#
```

10.8 主备倒换

主备倒换是指主用主控卡与备用主控卡的切换，即当主用主控出现异常（掉电或是人为重启等），在备用主控在线的情况下，系统会自动主备倒换。这种切换对上层应用是透明的。

主备主控卡的倒换屏蔽了主控卡异常的影响，对上层应用没有任何影响，保证了系统数据信息的及时处理。

除了主用主控被重启等情况下会触发自动主备倒换，还可以通过执行主备倒换命令或使用主控板上的主备倒换按键进行主备倒换。

主备倒换是由主控卡上运行的相应进程模块来实现的，主备倒换实现控制主备单板的倒换流程：

1.控制应用进程倒换的顺序，给应用进程发送备转主、主转备消息，即应用程序的主

备倒换。

2.设置单板的主备状态，并与通讯模块交互切换与外围单板的通讯链路，即通信链路切换。

在此期间，应用进程中间状态的切换与数据同步（包括数据同步时间点的选择等）都由应用进程自己完成。

对于主备配置的单板，当主板发生故障时需要备板及时感知并进行主备倒换，因此需要有一个伙伴板扫描线程来实时感知伙伴板状态。当主备状态或在位状态发生变化时，需要及时通知主控相应进程来触发主备倒换流程。

在伙伴板扫描线程中，当线程扫描到主用板异常且备用正常，就会触发倒换。倒换的过程由主控相应的进程模块实现。

10.8.1 配置主备倒换

主备倒换分为强制倒换和优雅倒换。本节介绍主备倒换的配置步骤和命令。

相关信息

执行主备倒换的方式有：命令主备倒换、拔插主用主控板、EXCH按键倒换、reset键重启主用主控板、当主用主控板故障时倒换到备用主控板。

所有的主备倒换都可以归类为强制倒换（force）或优雅倒换（grace），现分类如下：

- 强制倒换：自动倒换发生在**force**命令倒换、拔插主用主控板卡、reset键重启倒换、主用主控板故障时
- 优雅倒换：**grace**命令倒换、EXCH按键倒换

强制倒换和优雅倒换的区别：

- 强制倒换（除**force**命令倒换外）不检查是否具备主备倒换的条件，无论板卡当前状态如何，直接将主用板卡重启以达到主备倒换的目的。

  使用**force**命令倒换会检查倒换发生的一些必要条件，如：备板在线、文件初始化是否完成和数据库初始化是否完成等。当这些必要条件不满足时不允许倒换。

- 优雅倒换会检查是否具备主备倒换的条件，如备板是否在线、版本同步是否完成，进程是否上电，数据库同步是否完成等。

1.配置主备倒换前，查看主备同步状态。

正确执行主备倒换的前提是设备的主备主控板都在线，并且运行正常、主备数据库同步完成。所以在执行主备倒换之前，应先通过以下命令分别查看备用主控是否在线、备用主控与主用主控之间的同步状态。

命令	功能
inspur#**show processor**	查看主备主控板卡是否在线
inspur#**show synchronization**	查看主备主控板卡的逻辑实体的同步状态

2.配置主备倒换。

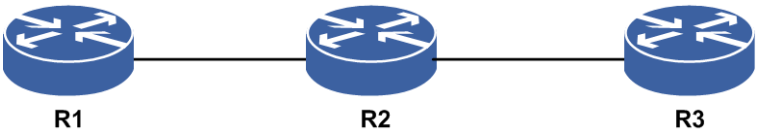
命令	功能
inspur#**redundancy switch sc force** [<*Line*>]	执行强制倒换
inspur#**redundancy switch sc grace** [<*Line*>]	执行优雅倒换

10.8.2 主备倒换配置实例

配置说明

组网环境如*图10-16*所示，初始三台设备正常工作，工作一段时间后，R2进行主备倒换。

图 10-16 主控主备倒换配置实例示意图



配置过程

1.设备正常工作，主用主控板ACT灯亮，备用主控板ACT灯灭，主备主控板RUN灯1Hz闪烁，主备主控板的Alarm灯灭

2.执行以下操作之一进行主备倒换：

i.执行主控主备倒换命令

ii.按下主用主控的reset键

iii.拔插主用主控板

iv.按下主用主控板的EXCH键

3.主备倒换结束后，面板灯亮正常，除主备倒换告警外，无其他异常告警产生

配置主控主备倒换命令如下：

```
inspur#redundancy switch sc grace
Proceed with redundancying switch SC? [yes/no]:yes
```

配置验证

查看配置结果：

```
倒换前：
inspur#show processor
================================================================================
======
```

```
================================================================================
======
Character: CPU current character in system
MSC : Master-SC in the system
SSC : Slave-SC in the system
N/A : None-SC in the system
CPU(5s) : CPU usage ratio measured in 5 seconds
CPU(1m) : CPU usage ratio measured in 1 minute
CPU(5m) : CPU usage ratio measured in 5 minutes
Peak : CPU peak usage ratio measured in 1 minute
PhyMem : Physical memory (megabyte)
FreeMem : Free memory (megabyte)
Mem : Memory usage ratio
================================================================================
======
================================================================================
======

          Character CPU(5s) CPU(1m) CPU(5m) Peak PhyMem FreeMem Mem
================================================================================
======
PIU-2/0 N/A 3% 3% 3% 3% 256 71 72.266%
--------------------------------------------------------------------------------
------
PIU-3/0 N/A 3% 3% 3% 3% 256 71 72.266%
--------------------------------------------------------------------------------
------
PIU-6/0 N/A 3% 4% 3% 4% 256 72 71.875%
--------------------------------------------------------------------------------
------
PIU-8/0 N/A 3% 4% 4% 6% 512 318 37.891%
--------------------------------------------------------------------------------
------
PIU-9/0 N/A 3% 3% 3% 3% 512 298 41.797%
--------------------------------------------------------------------------------
------
MPFU-12/0 MSC 16% 21% 19% 42% 4096 707 82.739%
--------------------------------------------------------------------------------
------
MPFU-13/0 SSC 16% 16% 16% 19% 4096 1336 67.383%
--------------------------------------------------------------------------------
------
inspur#
```

/* MPFU-12/0的character显示为MSC，表示这是当前的主用主控板。MPFU-13/0的character显示SSC，表示这是当前的备用主控板。主控在12槽位*/

倒换后：

```
inspur#show processor
================================================================================
======
================================================================================
======
Character: CPU current character in system
MSC : Master-SC in the system
SSC : Slave-SC in the system
N/A : None-SC in the system
CPU(5s) : CPU usage ratio measured in 5 seconds
CPU(1m) : CPU usage ratio measured in 1 minute
CPU(5m) : CPU usage ratio measured in 5 minutes
Peak : CPU peak usage ratio measured in 1 minute
PhyMem : Physical memory (megabyte)
FreeMem : Free memory (megabyte)
Mem : Memory usage ratio
================================================================================
======
================================================================================
======

 Character CPU(5s) CPU(1m) CPU(5m) Peak PhyMem FreeMem Mem
```

```
================================================================================
======
PIU-2/0 N/A 3% 3% 3% 3% 256 71 72.266%
--------------------------------------------------------------------------------
------
PIU-3/0 N/A 3% 3% 3% 3% 256 71 72.266%
--------------------------------------------------------------------------------
------
PIU-6/0 N/A 3% 4% 3% 4% 256 72 71.875%
--------------------------------------------------------------------------------
------
PIU-8/0 N/A 3% 4% 4% 6% 512 318 37.891%
--------------------------------------------------------------------------------
------
PIU-9/0 N/A 3% 3% 3% 3% 512 298 41.797%
--------------------------------------------------------------------------------
------
MPFU-12/0 SSC 16% 21% 19% 42% 4096 707 82.739%
--------------------------------------------------------------------------------
------
MPFU-13/0 MSC 16% 16% 16% 19% 4096 1336 67.383%
--------------------------------------------------------------------------------
------
inspur#
/* MPFU-12/0的character显示为SSC，表示这是当前的备用主控板。MPFU-13/0的character
显示MSC，表示这是当前的主用主控板。经过主备倒换，13槽位的主控卡由备用升为主用，12槽位
的主控卡由主用降为备用*/
```

11 策略模板

11.1.1 策略模板简介

IR12000智能路由器支持的策略模板功能包括：

·AAA模板

·业务可靠性管理

·时间控制列表（time-range）

·访问控制列表（ACL）

·IP前缀列表（prefix-list）

·Route-map

策略模板功能都是需要被其它业务调用才能发挥作用，可以为其它业务提供某种策略和控制机制，如控制认证授权方法、控制业务生效时间等。

策略模板不被调用时，不会对任何业务产生影响，只是作为预先配置好的策略模板存在。只要其他业务对策略模板所提供的策略机制感兴趣，就可以调用策略模板。

各种策略模板一旦被调用，就会对调用该策略模板的业务产生相应的影响，使得这些业务在应用中变得更加灵活。

11.2 AAA

AAA是认证（Authentication）、授权（Authorization）、计费（Accounting）的缩写，如何安全、有效、可靠地保护网络资源的合理使用和用户的利益成为所有网络服务提供者必须解决的问题。AAA服务就是针对这个问题，为网络运营商提供一个对用户进行有效管理的平台。

·AAA中对用户的网络认证是指对用户身份的验证。

·授权是指在用户通过认证之后确定其可以享受的服务。

·计费是记录用户使用网络资源情况的详细信息，这些信息是计费的依据。

AAA由客户端和服务器组成：

·客户端为驻留在路由器上的程序，负责组织数据发送到指定的服务端、接收服务器的响应信息，并根据服务器的响应结果进行配置，通知应用做不同的处理。

·服务端一般为运行在远程计算机上的AAA服务器程序，负责接收用户的连接请求，并对用户身份进行验证，返回用户配置信息。

实现AAA的协议主要包括RADIUS协议和TACACS+协议。

11.2.1 配置 AAA

配置AAA主要是配置方法列表，分为认证、授权、计费三类。配置好方法列表后，可以根据配置的方法对用户进行认证、授权、计费。

1.配置认证功能。

步骤	命令	功能
1	inspur(config)#**aaa-authentication-template** <*number*>	配置认证模板，并进入认证配置模式，<*number*>范围为1~2128
2	inspur(config-aaa-authen-template)# **aaa-authentication-type** {**none**|**local**|**radius**|**local-radius**|**radius-local**|**radius-none**|**local-tacacs**|**tacacs**|**tacacs-local**|**tacac-none**|**diameter**}	配置认证模板下的认证方式
3	inspur(config-aaa-authen-template)# **authentication-radius-group** <*group-number*>	配置RADIUS认证组，前提是RADIUS组已配置，<*group-number*>范围为1~2000
	inspur(config-aaa-authen-template)# **authentication-tacacs-group** <*tacacs-name*>	配置TACACS认证组，前提是TACACS组已配置，<*tacacs-name*>范围是1~31个字符
4	inspur(config-aaa-authen-template)# **authentication-diameter-group** <*group-number*>	配置DIAMETER认证组，<*group-number*>范围：1~10
5	inspur(config-aaa-authen-template)# **description** < *description* >	配置描述信息，长度为1~31个字符

local-radius：先本地认证，如果用户不存在，再进行RADIUS认证；如果本地认证拒绝，不进行RADIUS认证。

radius-local：先RADIUS认证，如果RADIUS配置错误或认证超时再进行本地认证；如果RADIUS认证拒绝，不进行本地认证。

radius-none：先RADIUS认证，如果RADIUS配置错误或超时，则直接通过认证。

local-tacacs：先本地认证，如果用户不存在，再进行TACACS认证；如果本地认证拒绝，不进行TACACS认证。

tacacs：TACACS远程认证。

tacacs-local：先TACACS认证，如果TACACS配置错误或超时再进行本地认证；如果TACACS认证拒绝，不进行本地认证。

tacacs-none：先TACACS认证，如果TACACS配置错误或超时，不认证。

2.配置授权功能。

步骤	命令	功能
1	inspur(config)#**aaa-authorization-template** <*number*>	配置授权模板，进入授权配置模式，<*number*>范围为1~2128

步骤	命令	功能
2	inspur(config-aaa-author-template)# **aaa-authorization-type** {**none**|**local** |**loacl-radius** |**loacl-tacacs** |**radius** |**radius-local** |**tacacs** |**tacacs-local**}	配置授权模板下的授权方式
3	inspur(config-aaa-author-template)# **authorization-radius-group** <*group-number*>	配置RADIUS授权组，前提RADIUS组已存在，<*group-number*>范围为1~2000
	inspur(config-aaa-author-template)# **authorization-tacacs-group** <*tacacs-name*>	配置TACACS授权组，前提TACACS组已存在，<*tacacs-name*>范围是1~31个字符
4	inspur(config-aaa-author-template)# **description** < *description* >	在授权模式下，配置描述信息，长度为1~31个字符

loacl-radius：无本地授权后转RADIUS授权。

loacl-tacacs：无本地授权后转TACACS授权。

radius-local：RADIUS授权超时转local方式。

tacacs-local：TACACS授权超时转local方式。

3.配置计费功能。

步骤	命令	功能
1	inspur(config)#**aaa-accounting-template** <*number*>	配置计费模板，进入计费配置模式，<*number*>范围1~2128
2	inspur(config-aaa-acct-template)#**aaa-accounting-type** {**none** | **radius** | **tacacs**}	配置计费模板下的计费方式
3	inspur(config-aaa-acct-template)#**accounting-radius-group first** <*group-number*>[**second** <*group-number*>]	配置RADIUS计费组，前提是RADIUS组已配置，<*group-number*>范围为1~2000
	inspur(config-aaa-acct-template)#**accounting-tacacs-group** <*tacacs-name*>	配置TACACS计费组，前提是TACACS组已配置
4	inspur(config-aaa-acct-template)#**description** < *description* >	配置描述信息，长度为1~31个字符

4.验证配置结果。

命令	功能
inspur#**show running-config aaa**	查看AAA相关配置
inspur#**show aaa-authentication-template** [<*number*>]	查看认证模板相关配置
inspur#**show aaa-authorization-template** [<*number*>]	查看授权模板相关信息

命令	功能
inspur#**show aaa-accounting-template** [<*number*>]	查看计费模板相关信息

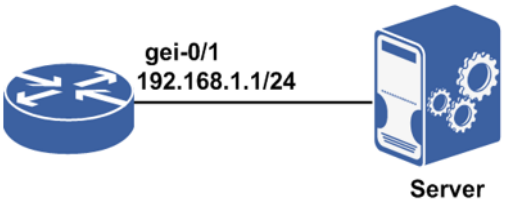
11.2.2 AAA 配置实例

配置说明

AAA是指认证、授权、计费，在IR12000上可以对认证、授权、计费分别配置模板。而在认证模板中有**tacacs+**、**radius**、**local**、**none**认证以及几种认证的组合方法。授权模板中有**local**、**none**、**tacacs**、**radius**授权以及几种授权的组合方法。计费模板中有**tacacs**、**radius**和**none**方法。本配置实例AAA认证和授权模板中方法为**tacacs+**，计费模板方法为**radius**。

如*图 11-1*所示的配置实例为指定认证和授权的方法是**tacacs+**。

图 11-1 AAA 配置实例拓扑图



1.配置AAA认证、授权、计费模板。这些认证模板是分开配置的。

AAA认证模板中有**tacacs+**、**radius**、**local**、**none**以及几种认证的组合方法。在组合认证方法中如**radius-local** ，**radius**是优先选择方法，仅当RADIUS无响应时才会转为**local**方法。

在各模板中配置完方法后，要在各模板下配置方法对应的服务器组（**local**和**none**方法无需配置）。

2.AAA的使用场景：配置用户管理模块认证、授权模板。将AAA模板绑定到用户管理模块模板中。使得用户登录时按照AAA当中的配置去进行认证、授权。如不在用户管理当中使用AAA，用户登录时AAA不发挥作用。

配置思路

1.请先明确需要使用的认证、授权、计费方法各采用哪种，在配置AAA模板之前必须先创建这种方法所对应的服务器组。（比如本例中示范配置认证方法选用**tacacs+**，则需要先创建响应的TACACS+服务器组）否则在AAA模板中为指定的方法配置认证/授权/计费的服务器时将提示服务器组不存在，无法配置成功。

2.AAA当中的任意一种都是独立进行配置的，方便其他业务灵活使用这些模板。创建需要的模板（认证/授权/计费），并指定一个序列号。

3.在该模板当中指定一种方法，如果指定的方法是**tacacs+**或者**radius**相关的，则需要再为这个方法指定一个服务器组。

4.配置好AAA模板后，AAA只作为模板存在。只有当其他业务调用时，AAA模板方可生效。

配置过程

IR12000上的配置如下：

```
/*使能设备的TACACS+服务，配置认证模板和授权模板所需要使用的TACACS+服务器组
（详细配置参见TACACS章节）*/
inspur(config)#tacacs enable
inspur(config)#tacacs-server host 10.1.1.1 key inspur
inspur(config)#tacplus group-server inspurgroup
inspur(config-sg)#server 10.1.1.1
inspur(config-sg)#exit

/*配置radius*/
inspur(config)#radius authentication-group 1
inspur(config-authgrp-1)#server 1 10.1.1.1 master key inspur
inspur(config-authgrp-1)#algorithm round-robin
inspur(config-authgrp-1)#max-retries 3
inspur(config-authgrp-1)#timeout 30
inspur(config-authgrp-1)#deadtime 0
inspur(config-authgrp-1)#exit

inspur(config)#aaa-authentication-template 2001
inspur(config-aaa-authen-template)#aaa-authentication-type tacacs-local
inspur(config-aaa-authen-template)#authentication-tacacs-group inspurgroup
inspur(config-aaa-authen-template)#exit
inspur(config)#aaa-authorization-template 2001
inspur(config-aaa-author-template)#aaa-authorization-type local-tacacs
inspur(config-aaa-author-template)#authorization-tacacs-group inspurgroup
inspur(config-aaa-author-template)#exit
inspur(config)#aaa-accounting-template 1
inspur(config-aaa-acct-template)#aaa-accounting-type radius
inspur(config-aaa-acct-template)#accounting-radius-group first 1
inspur(config-aaa-acct-template)#exit
```

配置验证

查看AAA相关配置信息：

```
inspur(config)#show running-config aaa
!<aaa>
aaa-authentication-template 2001
  aaa-authentication-type tacacs-local
  authentication-tacacs-group inspurgroup
$
aaa-authorization-template 2001
  aaa-authorization-type local-tacacs
  authorization-tacacs-group inspurgroup
$
aaa-accounting-template 1
  aaa-accounting-type radius
  accounting-radius-group first 1
$
!</aaa>
```

11.3 Time-range

Time-range主要是为其它应用模块提供一种唤醒/催眠服务。用户可以配置多个time-range，每个time-range有一个名字，在一个time-range中可以定义多个相对时间段以及一个绝对时间段。

Time-range必须配置在以下四种情况下才能够生效：

- 只配置了绝对时间段，且当前系统时间在配置的绝对时间段内，time-range生效。
- 只配置了相对时间段，且无论配置了几个相对时间段，只要当前系统时间在任意一个相对时间段内，则time-range生效。
- 既配置了绝对时间，又配置了相对时间，那么系统时间必须同时在绝对时间段内及在任意一个相对时间段内，time-range才能生效。
- 创建time-range列表后，没有添加时间段。那么系统时间即在空的time-range列表中，状态始终为激活状态生效。

11.3.1 配置 Time-range

配置Time-range的功能，为其他应用模块提供一种唤醒/催眠服务。

1.配置Time-range。

步骤	命令	功能
1	`inspur(config)#`**time-range enable**	开启time-range功能，并初始化相关数据
2	`inspur(config)#`**time-range** <*time-range-name*>	创建一个time-range，并进入time-range配置模式
3	`inspur(config-tr-name)#`**absolute** {[**start** <*start-time*><*start-date*>],[**end** <*end-time*><*end-date*>]}	为当前的time-range配置一个绝对时间段规则，一个time-range只能有一个绝对时间段
4	`inspur(config-tr-name)#`**periodic** [<*days-of-week*>]<*hh:mm:ss*> **to** [<*days-of-week*>]<*hh:mm:ss*>	为当前的time-range配置一个相对时间段规则，一个time-range可以有多个相对时间段

<*start-time*>：绝对时间段的开始时间，格式为"hh:mm:ss"，秒数必须是15的倍数。

<*start-date*>：绝对时间段的开始日期，格式为"mm-dd-yyyy"，year范围：2001~2037。

<*end-time*>：绝对时间段的结束时间，格式为"hh:mm:ss"，秒数必须是15的倍数。

<*end-date*>：绝对时间段的结束日期，格式为"mm-dd-yyyy"，year范围：2001~2037。

<*hh:mm:ss*>：表示"小时:分钟:秒"，秒数必须是15的倍数。

<*days-of-week*>：表示一周中特定的某天和某些天，可以为Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、Sunday，还可以是daily、weekend（周六、周日）、weekdays（周一至周五）。

2.验证配置结果。

命令	功能
inspur#**show time-range** < *time-range-name*>	查看某个time-range的状态信息
inspur#**show time-range**	查看所有time-range的状态信息

3.维护Time-range。

命令	功能
inspur#**time-range disable** [**clear**]	禁用time-range功能，clear清除配置
inspur#**debug time-range** [**change-to** {**inactive** | **active**}]	Time-range状态发生转换时在控制台打印系统时间、time-range的名字、转换前状态、转换后状态等
inspur#**show debug time-range**	显示TimeRange状态发生转换时的TimeRange列表

11.3.2 Time-range 列表配置实例

配置说明

1.单台设备的time-range列表容量上限是2048个，一个time-range列表中最多可以配置24个时间段。

2.时间段有两种，绝对（absolute）和相对（periodic）。绝对时间段由指定的时间及指定的日期构成，相对时间段由指定的时间和一周中的某一天组成，相对时间会以一周为单位循环重复。

3.一个列表当中可以选择根据需要设置绝对、相对时间段。注意只能有一个绝对时间，相对时间可以有多个。

4.time-range在4种情况下能够生效。

- 只配置了绝对时间段，并且当前系统时间在配置的绝对时间段内。
- 只配置了相对时间段。无论配置了几个相对时间段，只要当前系统时间符合任何一个相对时间段，则认为该time-range当前有效。
- 既有绝对时间，又有相对时间。系统时间必须同时符合绝对时间及任意一个相对时间，才能认为time-range有效。
- 创建time-range列表后，没有添加时间段。空的time-range列表，状态始终为active。

配置思路

本例示范配置一个名为test的time-range列表，其中配置一个绝对时间，指定时间段为：2011年1月14日上午9：30至2011年1月15日上午9：30，配置两个相对时间段，分别为每天上午8：00至8：30，以及周六凌晨零点至周日晚间22：00点。

根据time-range生效原则第三条，只有当绝对时间和相对时间的交集，才是time-range的有效时间。当系统时间处于这个有效时间范围内，time-range生效。

这个time-range配置产生的结果是：

2011年1月15日（这个日期为周五）上午的8：00至8：30，以及2011年1月15日凌晨零点至上午9：30，在这两个时间范围内time-range test状态为active，其中第一个交集时间被第二个交集所包含，对时间段生效没有阻碍。

配置步骤如下：

1.开启time-range功能，创建time-range列表。

2.确认需要触发业务的时间点，在time-range列表当中根据需要配置时间段。

3.确认机架的系统时间，以保证time-range的时间参照系是正确的。

配置过程

1.开启time-range功能，创建时间列表：

```
inspur(config)#time-range enable
inspur(config)#time-range test
inspur(config-tr-test)#
```

2.配置时间段：

```
inspur(config-tr-test)#?
  absolute  Specify an absolute entry
  commit    Commit the configuration
  end       Exit to privilege mode
  exit      Exit to previous command-mode
  no        Negate a command or set its defaults
  periodic  Specify a periodic entry
  ping      Send echo messages
  ping6     Send IPv6 echo messages
  rollback  Rollback the configuration
  show      Show running system information
  trace     Trace route to destination
  trace6    Trace route to destination using IPv6
  inspur(config-tr-test)#absolute ?
 end End point of the time range
 start Begin point of the time range
/*配置绝对时间段，可根据需要选择配置起、止时间点，表示在一个明确的时间和日期内生效。
（可以仅配置开始时间，表示从某个时刻开始一直生效；也可以仅配置结束时间，表示从某个
时刻开始失效）*/

inspur(config-tr-test)#absolute start ?
hh:mm:ss Starting time
inspur(config-tr)#absolute start 9:30:00 ?
 mm-dd-yyyy Starting date (year: 2001-2037)
inspur(config-tr)#absolute start 9:30:00 1-14-2011 ?
 end End point of the time range
 <cr>
inspur(config-tr)#absolute start 9:30:00 1-14-2011 end ?
hh:mm:ss Ending time
inspur(config-tr)#absolute start 9:30:00 1-14-2011 end 9:30:00 1-15-2011
```

```
/*配置了一个绝对时间段，指定生效时间限定在2011年1月14日上午9：30至2011年1月15日
上午9：30之间，如果列表内仅有这一个时间段配置，则根据time-range生效原则第一条，
在这个绝对时间内time-range一直生效。
如果本列表内还有其他时间段，则只要这个绝对时间段和本列表内的任意一个相对时间段存在交集，
在交集内time-range就能生效（绝对时间仅能配置一个，所以其他时间段只能是相对时间）*/

inspur(config-tr-test)#periodic ?
 daily From Monday to Sunday
 friday Friday
 monday Monday
 saturday Saturday
 sunday Sunday
 thursday Thursday
 tuesday Tuesday
 wednesday Wednesday
 weekdays From Monday to Friday
 weekend Saturday and Sunday
/*配置相对时间，与配置绝对时间不同的是：不能指定具体日期，而是指定一周内的某天，
或者是每天（daily）、周一至周五（weekdays）、周末（weedend）*/

inspur(config-tr-test)#periodic daily ?
hh:mm:ss Starting time
inspur(config-tr-test)#periodic daily 8:00:00 ?
 to The ending point of the time range
inspur(config-tr-test)#periodic daily 8:00:00 to 8:30:00 ?
 <cr>
inspur(config-tr-test)#periodic daily 8:00:00 to 8:30:00
/*配置了一个相对时间段，指定生效时间在每天的上午8：00至8：30以内*/

inspur(config-tr-test)#periodic saturday 00:00:00 to ?
 hh:mm:ss Ending time
 sunday Sunday
/*配置相对时间段，起始时间选择一周中的周六(Saturday)，则结束时间只能选择在
一周中排列在周六后的唯一天：周日(Sunday)*/

inspur(config-tr-test)#periodic saturday 00:00:00 to sunday 22:00:00
/*配置了相对时间段，指定生效时间在周六凌晨零点至周日晚22：00点*/
inspur(config-tr)#exit
/*配置完成，退出time-range配置模式，继续进行其它配置*/
```

3.确认系统时间是否正确：

```
inspur(config)#show clock
09:37:09 UTC Fri Jan 14 2011
inspur(config)#
/*系统时间是time-range的参照系，仅当系统时间处于time-range指定时间段的有效范围内，
time-range才能生效，所以使用时请务必保证系统时间设置正确*/
```

配置验证

1.查看time-range配置结果：

```
inspur(config)#show running-config time-range
!<time-range>
time-range enable
time-range test
 absolute start 09:30:00 01-14-2011 end 09:30:00 01-15-2011
 periodic daily 08:00:00 to 08:30:00
 periodic saturday 00:00:00 to sunday 22:00:00
 $
!</time-range>
/*命令show running-config中显示的配置结果和前面配置的一样，有一个绝对时间段和两个相
对时间段*/
```

2.查看time-range，当系统时间不在设置的时间段以内（此时time-range test的状态为inactive）：

```
inspur(config)#show time-range test
Current time is 09:38:20 01-14-2011 Friday
time-range test <inactive>
 absolute start 09:30:00 01-14-2011 end 09:30:00 01-15-2011
 periodic daily 08:00:00 to 08:30:00
 periodic saturday 00:00:00 to sunday 22:00:00
```

3.查看time-range，当系统时间在设置的时间段以内（此时time-range的状态为active）：

```
inspur(config)#show time-range test
Current time is 03:59:33 01-15-2011 Saturday
time-range test <active>
 absolute start 09:30:00 01-14-2011 end 09:30:00 01-15-2011
 periodic daily 08:00:00 to 08:30:00
 periodic saturday 00:00:00 to sunday 22:00:00
```

11.3.3 ACL 调用 time-range 配置实例

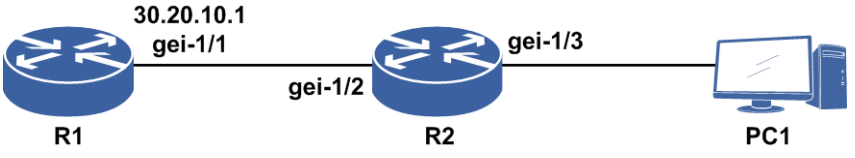
配置说明

Time-range本身的配置可以划定time-range active时间区域，time-range本身的active状态不能对用户操作进行任何约束，所以time-range必须通过绑定对应的ACL，使相应的ACL进入active状态以限定此ACL可以生效的时间域。

实际应用中，比方说某公司对于员工上班时间不允许浏览外网，在下班时间又允许员工浏览外网进行设定，以上就可以设定时间域，就是在上班这段时间对于公司内部发出的任何请求都予以deny，其他时间可以正常登录。

如*图 11-2*所示，假设PC1通过R2发送Telnet请求给R1，而R1只希望在某个时间段收到PC1的登录请求，而其他时间段收不到PC1的登录请求。那么可以先创建一个对应的time-range，将这个time-range绑定一个ACL，在端口gei-1/3的入方向上绑定这个ACL，这样就能实现在特定时间段来过滤掉PC1来的Telnet报文（也可以绑定在gei-1/2的出方向上）。

图 11-2 ACL 调用 time-range 配置实例拓扑图



只需要创建一个time-range，绑定到如下的ACL，给这个ACL添加规则：要求对匹配PC1的IP地址，协议类型是TCP，端口类型是Telnet的报文在time-range所指定的时间域内做deny处理。再将这个ACL绑定到gei-1/3的入方向或者gei-1/2的出方向即可。

这样配置后，只有在time-range指定的时间域内，对应的绑定的ACL才会生效，在这个时间域内PC1不能登录到R1，只要过了这个time-range生效的时间段，PC1又可以登录到R1。

配置思路

1.创建一个time-range，用户在创建时可以赋予一个自定义的名称，注意名称长度最长支持31个字符。

2.创建列表后就进入了time-range配置模式，在这里添加时间段。

3.根据实际配置的需要，将time-range绑定到对应的ACL，使对应的ACL在对应的时间段生效。

配置过程

R2上的配置如下。

1.创建一个time-range：

```
R2(config)#time-range enable
/*使能time-range，在没有使能time-range情况下不能创建time-range*/
R2(config)#time-range test
R2(config-tr-test)#
/*创建time-range名为test*/
```

2.给这个列表添加时间段：

```
R2(config-tr-test)#periodic daily 09:00:00 to 17:00:00
/*每天的09:00:00点开始，到17:00:00点结束*/
R2(config-tr-test)#exit
```

3.绑定到ACL（创建的ACL如下）：

```
R2(config)#ipv4-access-list test
R2(config-ipv4-acl)#rule 1 deny tcp 10.20.30.20 0.0.0.0 eq telnet
30.20.10.1 0.0.0.0 time-range test
R2(config-ipv4-acl)#rule 2 permit any
R2(config-ipv4-acl)#exit
R2(config)#ipv4-access-group interface gei-1/3 ingress test
/*绑定成功，ACL只在time-range生效的时间段起作用*/
```

配置验证

直接查看time-range信息，显示目前系统的时间以及每个time-range的名称和配置的时间段以及time-range的状态（active或者inactive）：

```
R2(config)#show time-range
Current time is 08:36:03 10-26-2012 Friday
time-range test <inactive>
periodic daily 09:00:00 to 17:00:00
```

查看一个指定的time-range信息：

```
R2(config)#show time-range test
Current time is 08:37:28 10-26-2012 Friday
time-range test <inactive>
periodic daily 09:00:00 to 17:00:00
```

11.3.4 SQA 调用 time-range 配置实例

配置说明

对于想要对登录IR12000智能路由器的用户进行RADIUS认证时，IR12000智能路由器作为发出认证请求的Client端，与一台RADIUS Server进行通信。为保证RADIUS认证可靠运行，需要验证IR12000智能路由器和RADIUS Server之间的连通性。这个连通性验证可以用ICMP类型的SQA进行，而SQA检测的时间点可以通过time-range进行控制。

下面以如*图* **11-3**所示组网图来进行配置举例。

图 11-3 SQA 调用 time-range 配置实例组网图



配置思路

1.配置一个time-range，根据需要设置时间点。

2.配置SQA实例，根据组网场景设置SQA检测类型为ICMP。

3.配置SQA检测开始的时间由指定的time-range来控制。

配置过程

1.配置一个time-range，根据需要设置时间点：

```
inspur(config)#show clock
10:20:47 UTC Thu Jan 13 2011

inspur(config)#time-range enable
inspur(config)#time-range 1
inspur(config-tr-1)#absolute start 10:30:00 1-13-2011
inspur(config-tr-1)#exit
```

提示：

配置SQA使用time-range指定检查时间功能，只能触发一次。不论这个time-range有几个有效时间，总是仅以第一个有效时间为准触发检查。 后续time-range再次进入有效时间时，不会触发SQA检查。

2.配置SQA实例，根据组网场景设置SQA检测类型为ICMP：

```
inspur(config)#sqa-test 1
inspur(config-sqa)#type-icmp vrf inspur 169.1.109.130
inspur(config-sqa)#
```

3.配置SQA检测开始的时间由指定的time-range来控制：

```
inspur(config-sqa)#sqa-begin timerange 1
inspur(config-sqa)#exit
```

提示：

配置SQA检测开始时间时，如果指定的time-range为空列表，其效果相当于立即检测。

配置验证

执行命令**show sqa-test**查看配置结果：

```
inspur(config)#show sqa-test 1
test number:1
test type: ICMP
vrf:inspur
destination IP:169.1.109.130
repeat:1
tos: 0
ttl: 255
size: 36
inte-time:100
send trap:disable
timerange name: 1
```

当time-range尚未到时，执行命令**show sqa-result**的输出如下：

```
inspur(config)#show clock
10:22:41 UTC Thu Jan 13 2011
inspur(config)#show sqa-result icmp
inspur(config)#
```

当time-range到时，执行命令**show sqa-result**查看输出如下：

```
inspur#show sqa-result icmp
icmp test[1] result
SendPackets:1  ResponsePackets:0
Completion:success  Destination IP Address: 169.1.109.130
Min/Max/Avg/Sum RTT:0/0/0/0ms
Min/Max/Avg/Sum Positive Jitter:0/0/0/0ms
Min/Max/Avg/Sum Negative Jitter:0/0/0/0ms
Min/Max/Avg/Sum Jitter:0/0/0/0ms
Packet loss rate:100%
Last Probe Time:2012-9-13 10:30:4
```

以上输出的含义为：在2012年9月13日上午10点30分04秒发生了检测，IR12000设备向目的地址为169.1.109.130的主机发送一个icmp echo request请求，没有收到回应。

没有收到回应可能的原因有：网络环境导致该IP地址不可达、169.1.109.130这个主机未开启ICMP服务、169.1.109.130主机的防火墙设置为不响应icmp echo request。

11.4 ACL

ACL是一种对流量进行分类的方法，使用该方法可以实现如port-ACL、URPF、PBR等功能。

ACL的实现主要依据报文中的字段对报文进行筛选过滤，最为常见的是依据IP报文中的五元组属性，即源IP地址、目的IP地址、协议类型、源端口号和目的端口号。

一张ACL列表可以有多条规则（rule），每条规则都描述了一定的匹配条件。对于给定的报文，从第一条规则开始判读是否匹配，一旦匹配则返回规则内设定的动作（permit/deny）。在某些应用中，该动作已扩展为由业务模块自行定制，例如ACL在

策略路由中的应用等。

11.4.1 配置 ACL

配置ACL规则并绑定到指定接口下，实现流分类功能。

1.配置ACL规则。

步骤	命令	功能
1	inspur(config)#**ipv4-access-list** *<name>*	创建/配置ACL列表
2	inspur(config-ipv4-acl)#**rule** [*<rule-id>*]{**permit** | **deny**}{*<source>*[*<source-wildcard>*]| **any**}[**time-range** *<time-range-name>*][**log**]	配置标准的基于源地址的ACL规则
	inspur(config-ipv4-acl)#**rule** [*<rule-id>*]{**permit** | **deny**}{*<0-255>*| **ip** |*<protocol-type>*}{*<source><source-wildcard>*| **any**}{*<destination><destination-wildcard>*| **any**}[{**tos** *<tos-value>*| **precedence** *<precedence-value>*| **dscp** *<dscp-value>*}][**range** *<1-255>***-***<1-255>*}][**fragments**][**ttl** {{**eq** | **ge** | **le** | **neq**}*<TTL_value>*| **range** *<TTL_ValueRange>*}][**time-range** *<time-range-name>*][**log**]	配置扩展的ACL规则
	inspur(config-ipv4-acl)#**rule** [*<rule-id>*]{**permit** | **deny**} **tcp** {*<source><source-wildcard>*| **any**}[{*<operator>*{*<0-65535>*|*<source-porttype>*}| **range** *<0-65535>***-***<0-65535>*}]{*<destination><destination-wildcard>*| **any**}[{*<operator>*{*<0-65535>*|*<destination-porttype>*}| **range** *<0-65535>***-***<0-65535>*}][{[**established**] ,[**syn**{+ | -}]}][{**tos** *<tos-value>*| **precedence** *<precedence-value>*| **dscp** *<dscp-value>*}][**fragments**][**ttl** {{**eq** | **ge** | **le** | **neq**}*<TTL_value>*| **range** *<TTL_ValueRange>*}][**time-range** *<time-range-name>*][**log**]	配置基于TCP协议的的ACL规则
	inspur(config-ipv4-acl)#**rule** [*<rule-id>*]{**permit** | **deny**} **udp** {*<source><source-wildcard>*| **any**}[{*<operator>*{*<0-65535>*|*<source-porttype>*}| **range** *<0-65535>***-***<0-65535>*}]{*<destination><destination-wildcard>*| **any**}[{*<operator>*{*<0-65535>*|*<destination-porttype>*}| **range** *<0-65535>***-***<0-65535>*}][{**tos** *<tos-value>*| **precedence** *<precedence-value>*| **dscp** *<dscp-value>*}][**fragments**][**ttl** {{**eq** | **ge** | **le** | **neq**}*<TTL_value>*| **range** *<TTL_ValueRange>*}][**time-range** *<time-range-name>*][**log**]	配置基于UDP协议的的ACL规则
	inspur(config-ipv4-acl)#**rule** [*<rule-id>*]{**permit** | **deny**} **icmp** {*<source><source-wildcard>*| **any**}{*<destination><destination-wildcard>*| **any**}[{*<icmp-type-value>*|*<icmp-type>*}[*<icmp-code>*]][{**tos** *<tos-value>*| **precedence** *<precedence-value>*| **dscp** *<dscp-value>*}][**fragments**][**ttl** {{**eq** | **ge** | **le** | **neq**}*<TTL_value>*| **range** *<TTL_ValueRange>*}][**time-range**	配置基于ICMP协议的的ACL规则

	<*time-range-name*>[**log**]	

<*rule-id*>：规则在ACL表中的唯一标识，该ID决定了规则在表中的顺序，范围1~2147483644。如不指定rule-id，系统默认插入表的末位，并按默认初始序号（base）和步长（increment）来分配rule-id（默认初始序号为10，默认步长是10）。

<*0-255*>：要匹配的协议类型，代表IP协议号的范围0~255。

ip：表示任意类型的网络协议。

<*protocol-type*>：IP协议类型，可以是关键字**igmp**、**gre**、**ospf**、**pim**、**vrrp**中的一个。

<*source-wildcard*>：源IPv4地址的反掩码，为十进制点分形式。

<*destination-wildcard*>：目的IPv4地址的反掩码，为十进制点分形式。

<*operator*> **range**：针对端口的操作类型，可以是关键字eq（等于）、ge（大于等于）、le（小于等于）、range（属于）中的一个，其中range后需要指定2个port操作数确定一个端口区间，区间的起始值不能大于结束值。

<*source-port*>：源端口号，值范围为0~65535。

<*destination-port*>：目的端口号，值范围为0~65535。

precedence <*value*>：优先级precedence，值范围为0~7。

tos <*value*>：ToS字段，值范围为0~15。

dscp <*value*>：DSCP字段，值范围0~63。

time-range ：设置time-range参数，通过这个配置为ACL增加时间属性，使ACL仅在指定时段生效。

established：TCP建链关键字，仅对TCP可用。

log：统计计数。

<*icmp-type*>：ICMP报文类型字段，可以是关键字echo-reply、unreachable、source-quench、redirect、alternate-address、echo、router-advertisement、router-solicitation、time-exceeded、parameter-problem、timestamp-request、timestamp-reply、information-request中的一个。

<*icmp-type-value*>：ICMP报文类型字段，范围0~255。

<*icmp-code*>：ICMP消息类型，范围0~255。

syn{**+** | **-**}：TCP头部SYN标志的取值，“-”表示校验不携带该标志的报文，“+”表示校验携带该标志的报文。

eq | **ge** | **le** | **neq**：对TTL的操作类型，关键字eq（等于），ge（大于等于），le（小于等于），neq（不等于）。

<*TTL_value*>：TTL的值，范围1~255。

<*TTL_ValueRange*>：TTL的范围值，范围<1-255>-<1-255>，起始值不可大于结束值。

2.复制ACL列表。

命令	功能

命令	功能
inspur(config)#**copy** {**ipv4-access-list** | **ipv4-mixed-access-list** | **link-access-list**}<*src-acl-name*><*dst-acl-name*>	复制ACL列表

3.将ACL规则绑定到接口上。

命令	功能
inspur(config)#**ipv4-access-group interface** <*interface-name*>{**ingress** | **egress**}<*acl-name*>	在全局模式下，将一个ACL绑定到一个或多个接口的指定方向
inspur(config-if-interface-name)#**ipv4-access-group** {**ingress** | **egress**}<*acl-name*>}	在接口模式下，绑定一个ACL到当前接口的指定方向

4.验证配置结果。

命令	功能
inspur#**show ipv4-access-lists** [|{**begin**|**exclude**|**include**}]	显示ACL列表信息
inspur#**show ipv4-access-lists brief** [**name** <*acl-name*>][|{**begin**|**exclude**|**include**}]	显示ACL列表简要信息
inspur#**show ipv4-access-lists usage** <*interface-name*>{**ingress**|**egress**} **port-acl** [|{**begin**|**exclude**|**include**}]	显示ACL规则被命中的次数（仅适用于配置了log的规则）
inspur#**show ipv4-access-lists name** <*acl-name*>[{**from** <*rule-id*>}{**to** <*rule-id*>}][**usage** <*interface-name*>{**ingress**|**egress**} **port-acl**][|{**begin**|**exclude**|**include**}]	显示指定名称的ACL列表的信息
inspur#**show ipv4-access-lists config** [|{**begin**|**exclude**|**include**}]	显示整机的ACL资源使用情况
inspur#**show ipv4-access-groups** [{[**by-access-list** <*acl-name*>],[**by-direction** {**ingress** | **egress**}],[**by-interface** <*interface-name*>}]	显示绑定信息

5.维护ACL。

命令	功能
inspur(config-ipv4-acl)#**move** < *target-rule-id*>< *target-New-rule-id*>	调整改变ACL列表中规则的编号顺序
inspur(config-ipv4-acl)#**no rule** {<*rule-id*>| **all** }	删除指定ACL规则/所有规则
inspur(config)#**resequence-access-list ipv4** <*acl-name*>[<*base*>[<*increment*>]]	重新编号
inspur(config)#**acl clean**	删除所有类型的ACL配置即接口上ACL的绑定

11.4.2 配置 Link ACL

配置Link ACL规则并绑定到指定接口下，实现流分类功能。

1.配置ACL规则。

步骤	命令	功能
1	`inspur(config)#`**link-access-list** *<name>*	创建/配置ACL列表
2	`inspur(config-link-acl)#`**rule** [*<rule-id>*]{**permit** | **deny**}[**link-protocol** *<link-protocol>*]{**source-mac from** *<source-mac-address>* **to** *<source-mac-address>*[**from** *<source-mac-address>* **to** *<source-mac-address>*]| **any** |*<source-mac-address><source-mac-address-mask>*}{**destination-mac from** *<destination-mac-address>* **to** *<destination-mac-address>*[**from** *<destination-mac-address>* **to** *<destination-mac-address>*]| **any** |*<destination-mac-address><destination-mac-address-mas>*}[{[**outer-cos** *<outer-cos-value>*],[**inner-cos** *<inner-cos-value>*],[**inner-vlan** *<Inner_Vlan>*],[**outer-vlan** *<Outer_Vlan>*]}][**time-range** *<time-range-name>*][**log**]	配置基于MAC地址的ACL规则

<rule-id>：规则在ACL表中的唯一标识，该ID决定了规则在表中的顺序，范围1~2147483644。如不指定rule-id，系统默认插入表的末位，并按默认初始序号（base）和步长（increment）来分配rule-id（默认初始序号为10，默认步长是10）。

<link-protocol>：二层协议类型。

<source-mac-address>：源MAC地址，为XXXX.XXXX.XXXX形式。

<source-mac-address-mask>：源MAC地址的反掩码，为XXXX.XXXX.XXXX形式。

<destination-mac-address>：目的MAC地址，为XXXX.XXXX.XXXX形式。

time-range：设置time-range参数，通过这个配置为ACL增加时间属性，使ACL仅在指定时段生效。

outer-cos*<outer-cos-value>*：外层CoS。

inner-cos*<inner-cos-value>*：内层CoS。

outer-vlan*<Outer_Vlan>*：外层VLAN。

inner-vlan*<Inner_Vlan>*：内层VLAN。

source-mac：配置源MAC地址范围。

destination-mac：配置目的MAC地址范围。

log：设定对rule规则的过滤统计。

2.将ACL规则绑定到接口上。

命令	功能
inspur(config)#**link-access-group interface** <*interface-name*>{**ingress** | **egress**}<*acl-name*>	在全局模式下，将一个ACL绑定到一个或多个接口的指定方向
inspur(config-if-interface-name)#**link-access-group** {**ingress** | **egress**}<*acl-name*>}	在接口模式下，绑定一个ACL到当前接口的指定方向

3.验证配置结果。

命令	功能
inspur#**show link-access-lists** [|{**begin** | **exclude** | **include**}]	显示ACL列表信息
inspur#**show link-access-lists brief** [**name** <*acl-name*>][|{**begin** | **exclude** | **include**}]	显示ACL列表简要信息
inspur#**show link-access-lists usage** <*interface-name*>{**ingress** | **egress**} **port-acl** [|{**begin** | **exclude** | **include**}]	显示ACL规则被命中的次数（仅适用于配置了log的规则）
inspur#**show link-access-lists name** <*acl-name*>[{**from** <*rule-id*>}{**to** <*rule-id*>}][**usage** <*interface-name*>{**ingress** | **egress**} **port-acl**][|{**begin** | **exclude** | **include**}]	显示指定名称的ACL列表的信息
inspur#**show link-access-lists config** [|{**begin** | **exclude** | **include**}]	显示整机的ACL资源使用情况
inspur#**show link-access-groups** [{[**by-access-list** <*acl-name*>],[**by-direction** {**ingress** | **egress**}],[**by-interface** <*interface-name*>}]	显示绑定信息

4.维护ACL。

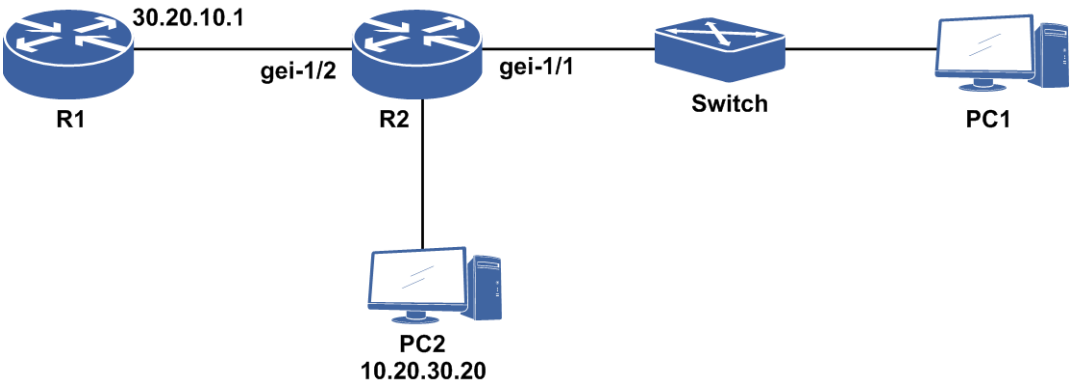
命令	功能
inspur(config-link-acl)#**move** < *target-rule-id*>< *target-New-rule-id*>	调整改变ACL列表中规则的编号顺序
inspur(config-link-acl)#**no rule** {<*rule-id*>| **all** }	删除指定ACL规则/所有规则
inspur(config)#**resequence-access-list link** <*acl-name*>[<*base*>[<*increment*>]]	重新编号

11.4.3 ACL 配置实例

配置说明

在如*图 11-4*所示的网络中，假设PC1和PC2都通过R2发送Telnet请求给R1，而R1希望只收到PC1的登录请求，而不收到PC2的登录请求。那么可以在gei-1/1的入方向上绑定ACL来过滤掉PC2来的Telnet报文（也可以绑定在gei-1/2的出方向上。）

图 11-4 ACL 配置实例拓扑图



这时只需要创建一个ACL，给这个ACL添加规则：要求对匹配PC2的IP地址，协议类型是TCP，端口类型是telnet的报文作deny处理；除此以外的所有报文作permit处理。再将这个ACL绑定到gei-1/1的入方向或者gei-1/2的出方向即可。

这样配置后，即使PC2获得了R1的telnet用户名和密码，发出的请求也不会到达R1，报文在到达R2后就被丢弃。同时R1和PC2的其他通信不受影响。

配置思路

1.创建一个ipv4-access-list，用户在创建时可以赋予一个自定义的名称，注意名称长度最长支持31个字符。

2.创建列表后就进入了IPv4 ACl配置模式，在这里添加rule，每个rule可以指定一种报文类型，并且规定此种报文是被permit或deny。

3.根据流量过滤的需要，将定制的ipv4-access-list绑定在需要过滤流量的接口的入方向或者出方向。

配置过程

R2上的配置如下：

```
R2(config)#ipv4-access-list test
R2(config-ipv4-acl)#rule 10 deny tcp 10.20.30.20 0.0.0.0 eq telnet
 30.20.10.1 0.0.0.0
R2(config-ipv4-acl)#rule 20 permit any
R2(config-ipv4-acl)#exit
R2(config)#ipv4-access-group interface gei-1/1 ingress test
```

配置验证

查看配置的ACL，提供了三种方式查看配置的ACL：

方式一：

```
R2(config)#show ipv4-access-lists brief /*显示每个ACL的名称和配置的rule数量*/
No.     ACL                 RuleSum
-------------------------------------------------
1       test                  2
```

查看ACL绑定接口的情况：

```
R2(config)#show ipv4-access-groups
Interface name|vlan             Direction  ACL name
-------------------------------------------------------------
gei-1/1                        Ingress    test
```

方式二：

```
R2(config)#show ipv4-access-lists name test
/*可以查看一个ACL，指定名称后可以选择简要查看或完整查看，缺省为完整查看*/
ipv4-access-list test
2/2 (showed/total)
   10 deny tcp 10.20.30.20 0.0.0.0 eq telnet 30.20.10.1 0.0.0.0
   20 permit any
R2(config)#show ipv4-access-lists brief name test
No.      ACL                            RuleSum
-----------------------------------------------------
1        test                             2
```

方式三：

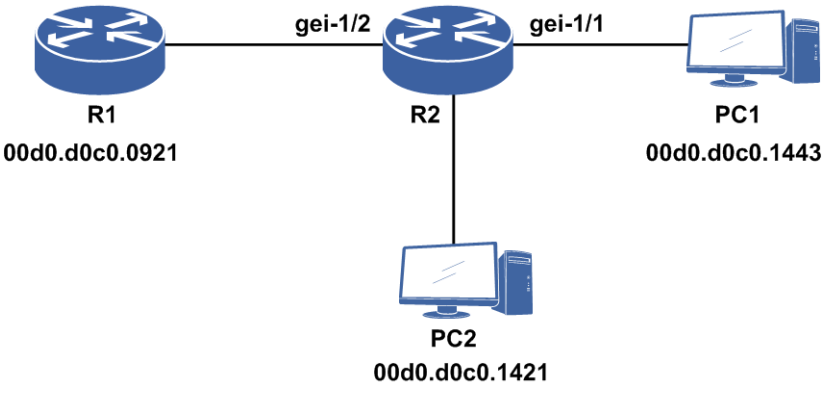
```
R2(config)#show ipv4-access-lists
/*查看整机配置的所有ACL，模式为完整查看*/
ipv4-access-list test
2/2 (showed/total)
  10 deny tcp 10.20.30.20 0.0.0.0 eq telnet 30.20.10.1 0.0.0.0
  20 permit any
```

11.4.4 Link ACL 配置实例

配置说明

如*图 11-5*所示，组网示例中假设PC1和PC2都通过R2发送报文给R1，而R1希望只收到PC1的报文，而不收到PC2的报文。那么可以在gei-1/1的入方向或者gei-1/2的出方向上绑定Link ACL来过滤掉PC2发来的报文。

图 11-5 Link ACL 配置组网示意图



这种情况下需要创建一个Link ACL，给这个Link ACL添加规则：规则可以是具体的源MAC/目的MAC地址、源MAC/目的MAC地址段、outer-vlan/inner-vlan匹配、outer-cos/inner-cos匹配及link-protocol号等，要求对匹配PC2的相应规则的报文作deny处理，除此以外的所有报文作permit处理。再将这个Link ACL绑定到gei-1/1的入方向或者gei-1/2的出方向。

配置后， PC2发出的报文不会到达R1，报文在到达R2后就被丢弃，同时R1和PC2的

其它通信则不受影响。

配置思路

1.创建一个link-access-list，创建时可以赋予一个自定义的名称，最长支持31个字符。

2.创建列表后进入Link ACl配置模式，添加rule，每个rule可以指定一种报文类型（本实例配置匹配MAC地址的报文），并且规定此种报文是被permit或deny。

3.根据流量过滤的需要，将定制的link-access-list绑定在需要过滤流量的接口的入方向或者出方向。

配置过程

R2上的配置如下：

```
R2(config)#link-access-list test
R2(config-link-acl)#rule deny 00d0.d0c0.1421 0000.0000.0000 any
R2(config-link-acl)#rule permit any any
R2(config-ipv4-acl)#exit
R2(config)#link-access-group interface gei-1/1 ingress test
```

配置验证

在R2上查看配置的Link ACL，提供了三种方式查看配置的Link ACL：

•方式一

```
/*只显示每个Link ACL的名称和配置的rule数量*/
R2(config)#show link-access-lists brief
No.     ACL                          RuleSum
-------------------------------------------------------
1       test                         2

/*查看Link ACL绑定接口的情况*/
R2 (config)#show link-access-groups
Interface name|vlan          Direction  ACL name
-----------------------------------------------------------------
gei-1/1                   Ingress    test
```

•方式二

```
/*可以查看一个Link ACL，指定名称后可以选择简要查看或完整查看，缺省为完整查看*/
R2(config)#show link-access-lists name test
link-access-list test
 2/2 (showed/total)
   10 deny 00d0.d0c0.1421 0000.0000.0000 any
   20 permit any any

R2(config)#show link-access-lists brief name test
No.     ACL                          RuleSum
-------------------------------------------------------
1       test                         2
```

•方式三

```
/*完整查看整机配置的所有Link ACL*/
R2(config)#show link-access-lists
link-access-list test
 2/2 (showed/total)
   10 deny 00d0.d0c0.1421 0000.0000.0000 any
   20 permit any any
```

11.5 Prefix-list

Prefix-list是一种按照路由前缀过滤的列表，由过滤列表和过滤列表中的规则两部分组成。

通过使用前缀列表（prefix-list），可以对指定的路由前缀设置**permit**或**deny**动作，以此控制由这个前缀所发起的各种行为是否被准许，对网络提供必要的安全保障。

前缀列表可以被组播、OSPF、IS-IS、BGP等多种业务使用。

11.5.1 配置 prefix-list

配置前缀列表功能，对指定的路由前缀进行过滤，为网络提供必要的安全保障。

1.配置prefix-list。

命令	功能
inspur(config)#**ip prefix-list** <*prefix-list-name*>{[**seq** <*seq-number*>]{**deny** | **permit**}<*network-num*><*len*>[**ge** <*value*>][**le** <*value*>]| **description** <*LINE*>}	配置前缀列表

<*prefix-list-name*>：前缀列表名称，最长31字符。

seq <*seq-number*>：指定前缀列表序列号，范围1~4294967294。

<*network-num*>：v4格式的IP地址。

<*len*>：掩码长度，范围0~32。

permit：如果待过滤的IP地址在该表项的前缀范围内，表示通过该表项的过滤并不再进行后续的匹配；若待过滤的IP地址不在该表项的前缀范围内则继续进行后续表项的匹配查找。

deny：如果待过滤的IP地址在该表项的前缀范围内，表示通不过该表项的过滤并且不再进行后续表项的匹配；若待过滤的IP地址不在该表项的前缀范围内则继续进行后续表项的匹配。

ge <*value*>：指定IP地址前缀的匹配范围后还需该匹配的地址前缀长度大于等于该值，该值范围1~32。

le <*value*>：指定IP地址前缀的匹配范围后还需该匹配的地址前缀长度小于等于该值，该值范围1~32。

description <*LINE*>：前缀列表说明描述信息，最大长度79字符。

2.配置组播调用prefix-list。

步骤	命令	功能
1	inspur(config)#**ip multicast-routing**	进入IP组播配置模式
2	inspur(config-mcast)#**router pim**	启用IP组播协议PIM-SM
3	inspur(config-mcast-pim)#**rp-candidate** <*interface-name*>[**group-list** <*prefix-list-name*>][**priority** <*priority*>]	配置路由器使其通告自己为候选RP 候选RP优先级的范围：0~255
4	inspur(config-mcast-pim)#**static-rp** <*ip-address*>[**group-list** <*prefix-list-name*>][**priority** <*priority*>]	配置静态RP地址 静态RP优先级缺省为192，范围：0~255

3.配置OSPF调用prefix-list。

步骤	命令	功能
1	inspur(config-ospf-process-id)#**distribute-list prefix** <*prefix-list-name*>{**in** | **out**}	对前缀符合prefix-list的路由进行控制（不符合的将按照deny处理） distribute-list的**in**命令，用于过滤owner为OSPF的路由 distribute-list的**out**命令，在5、7型LSA生成以后，用于控制外部路由导入OSPF域，是redistribute命令的补充
2	inspur(config-ospf-id)#**distribute-list prefix** <*prefix-list-name*> **gateway** <*prefix-list-name*> **in**	在in方向，对前缀和GW分别符合所制定的prefix-list的OSPF路由进行控制（不符合的将按照deny处理）

4.配置BGP调用prefix-list。

步骤	命令	功能
1	inspur(config)#**router bgp** <*as-number*>	配置BGP实例
2	inspur(config-bgp)#**neighbor** {<*ipv4-address*>|<*ipv6-address*>|<*peer-group-name*>} **prefix-list** <*prefix-list name*>{**in** | **out**}	配置BGP使用prefix-list，**in** | **out**表示应用于输出还是输入路由

5.配置Route-map调用prefix-list。

命令	功能
inspur(config-route-map)#**match ip address prefix-list** <*prefix-list-name*>	Route-map当中配置match前缀列表，前缀列表名称最长31字符

6.验证配置结果。

命令	功能
inspur#**show ip prefix-list** [{<*detail*>|<*summary*>}][<*prefix-list-name*>]	显示配置的IP地址过滤列表相关信息

11.5.2 Prefix-list 基本配置实例

配置说明

- 本例将示范配置名为test的prefix-list，配置准许192.168.120.0/24和192.168.110.1/32的路由前缀通过，允许192.168.100.0掩码长度在24-32之间的路由前缀通过。
- 配置的效果将是：调用这个prefix-list的业务，路由前缀严格匹配192.168.120.0/24和192.168.110.1/32的才能通过，掩码长度在24位到32位，前24位匹配192.168.100.0的路由前缀能够通过，其余的前缀都被deny。
- 配置中缺省sequence，默认的sequence id是从5开始，以5递增。

配置思路

逐一配置prefix-list规则。

配置过程

```
inspur(config)#ip prefix-list test permit 192.168.120.1 24
inspur(config)#ip prefix-list test permit 192.168.110.1 32
inspur(config)#ip prefix-list test permit 192.168.100.0 24 le 32
```

配置验证

使用**show running-config prefix-list**命令查看prefix-list的配置结果：

```
inspur(config)#show running-config prefix-list
!<prefix-list>
ip prefix-list test seq 5 permit 192.168.120.0 24
ip prefix-list test seq 10 permit 192.168.110.1 32
ip prefix-list test seq 15 permit 192.168.100.0 24 le 32
!</prefix-list>
```

11.5.3 组播调用 prefix-list 配置实例

配置说明

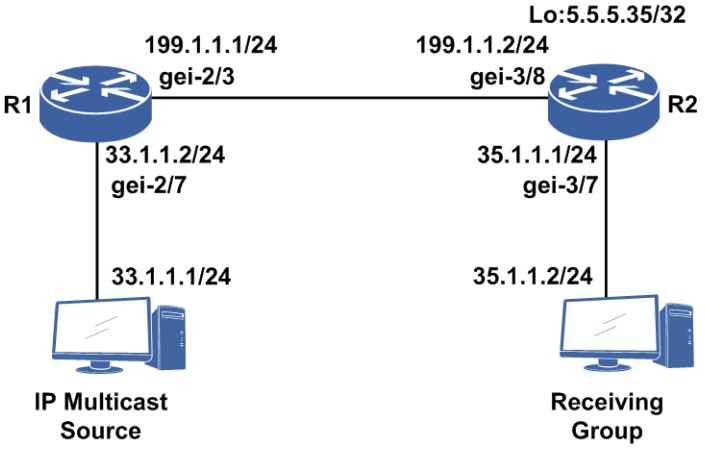
组播PIM-SM同时支持静态RP和动态RP配置。

·使用静态RP，需要在PIM域中的所有PIM路由器上配置静态RP。

·使用动态RP，在PIM域内选择几台PIM路由器，配置C-RP（Candidate-RP），从C-RP中竞选产生RP，同时必须配置C-BSR（Candidate-BootStrap Router），由C-BSR竞选产生BSR。

以动态RP为例，如*图 11-6*所示，R1端组播源加入，R2端IGMP组加入，在R2上配置C-BSR，同时配置group-list为inspur的C-RP，其中inspur为prefix-list列表的名称，组范围为225.0.0.0/24。

图 11-6 组播调用 prefix-list 配置实例组网图



配置思路

1.配置相应接口。

2.进入组播配置模式。

3.进入PIM配置模式。

4.在R2上配置loopback5为C-BSR，同时配置loopback5为C-RP，RP匹配的前缀列表范围为225.0.0.0/24。

5.进入接口启动PIM-SM。

6.在R1上配置到RP的单播路由，在R2上配置到组播源的单播路由（本例配置了静态路由，也可以配置IGP路由）。

配置过程

R1的配置如下：

```
R1(config)#interface gei-2/3
R1(config-if-gei-2/3)#ip address 199.1.1.1 255.255.255.0
R1(config-if-gei-2/3)#exit
R1(config)#interface gei-2/7
R1(config-if-gei-2/7)#ip address 33.1.1.1 255.255.255.0
R1(config-if-gei-2/7)#exit
R1(config)#ip multicast-routing
R1(config-mcast)#router pim
R1(config-mcast-pim)#interface gei-2/3
R1(config-mcast-pim-if-gei-2/3)#pimsm
```

```
R1(config-mcast-pim-if-gei-2/3)#exit
R1(config-mcast-pim)#interface gei-2/7
R1(config-mcast-pim-if-gei-2/7)#pimsm
R1(config-mcast-pim-if-gei-2/7)#exit
R1(config-mcast-pim)#exit
R1(config-mcast)#exit
R1(config)#ip route 5.5.5.35 255.255.255.255 199.1.1.2
```

R2的配置如下：

```
R2(config)#ip prefix-list inspur permit 225.0.0.0 24
R2(config)#interface gei-3/8
R2(config-if-gei-3/8)#ip address 199.1.1.2 255.255.255.0
R2(config-if-gei-3/8)#exit
R2(config)#interface gei-3/7
R2(config-if-gei-3/7)#ip address 35.1.1.1 255.255.255.0
R2(config-if-gei-3/7)#exit
R2(config)#ip multicast-routing
R2(config-mcast)#router pim
R2(config-mcast-pim)#bsr-candidate loopback5
R2(config-mcast-pim)#rp-candidate loopback5 group-list inspur
R2(config-mcast-pim)#interface gei-3/8
R2(config-mcast-pim-if-gei-3/8)#pimsm
R2(config-mcast-pim-if-gei-3/8)#exit
R2(config-mcast-pim)#interface gei-3/7
R2(config-mcast-pim-if-gei-3/7)#pimsm
R2(config-mcast-pim-if-gei-3/7)#dr-priority 20
R2(config-mcast-pim-if-gei-3/7)#exit
R2(config-mcast-pim)#exit
R2(config-mcast)#exit
R2(config)#ip route 33.1.1.0 255.255.255.0 199.1.1.1
```

配置验证

在R1上通过**show ip pim rp mapping**查看RP信息：

```
R1(config)#show ip pim rp mapping
Group(s): 225.0.0.0/24(SM)
RP: 5.5.5.35, v2, Priority:192
BSR: 5.5.5.35, via bootstrap
Uptime: 00:00:28, expires: 00:02:02

Group(s): 0.0.0.0/0(NOUSED)

R1(config)#show ip pim rp hash 225.0.0.1
rp address: 5.5.5.35
```

11.5.4 OSPF 调用 prefix-list 配置实例

配置说明

1.在ospfv2配置模式配置distribute-list带prefix，用于过滤与prefix-list匹配的ospfv2路由：

- 使用**distribute-list prefix-list** <*prefix-list-name*> **in**命令，用于过滤owner为OSPF的路由。
- 使用**distribute-list prefix-list** <*prefix-list-name*> **out**命令，在5，7型LSA生成以后，用于控制外部路由导入OSPF域，是redistribute命令的补充。

- 不配置**distribute-list**命令，即不进行路由的过滤和externalLSA的导入控制。

2.使用in命令过滤路由的时候要小心，鉴于OSPF路由之间的关联性，有如下几个建议：

- 最好不要过滤2型LSA对应的路由，否则会导致网络拓扑不全。
- 允许某3型路由进入的时候，注意确保对应的ABR路由存在，如果不存在，可在模板设置中将对应路由允许。
- 允许某5型路由进入的时候，注意确保forwarding address路由的存在，如果不存在，也要在模板设置中将对应路由允许。

3.当调用的prefix-list列表本身并不存在的时候，调用的效果相当于permit any。

4.由于非空的prefix-list列表的末尾都有缺省规则deny all，即未配置为permit的前缀都会被deny，所以如果要deny某些路由，需要注意加配permit all，将其他的路由前缀permit。

配置思路

1.配置prefix-list模板，将前缀为23.2.2.0/24的OSPF路由deny，其余路由permit。

2.在ospfv2 distribute-list中调用这个prefix-list。

配置过程

1.配置prefix-list，用于将如下路由表中前缀为23.2.2.0/24的路由过滤掉。

```
inspur(config)#show ip forwarding route ospf
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
status codes: *valid, >best
Dest          Gw        Interface   Owner  Pri Metric
*>1.1.1.0/24   26.1.1.22 gei-1/1     OSPF   110 101
*>11.1.1.0/24  26.1.1.22 gei-1/1     OSPF   110 101
*>12.1.1.0/24  23.1.1.22 gei-1/3     OSPF   110 20
*>16.1.1.0/24  26.1.1.22 gei-1/1     OSPF   110 101
*>23.2.2.0/24  23.1.1.22 gei-1/3     OSPF   110 20
*>26.1.3.0/24  26.1.1.22 gei-1/1     OSPF   110 101
*>100.1.1.0/24 23.1.1.22 gei-1/3     OSPF   110 20

inspur(config)#ip prefix-list inspur deny 23.2.2.0 24
inspur(config)#ip prefix-list inspur permit 0.0.0.0 0 le 32
/*这条配置可以实现permit any*/
```

2.在路由通告过滤中使用distribute-list带prefix。

```
inspur(config)#router ospf 1
inspur(config-ospf-1)#distribute-list prefix inspur in
inspur(config-ospf-1)#exit
/*如果是应用在distribute的out方向，需要先配置redistribute*/
```

配置验证

查看经过过滤之后的路由表，确定过滤路由成功：

```
inspur(config)#show ip forwarding route ospf
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest          Gw       Interface   Owner Pri Metric
*>1.1.1.0/24   26.1.1.22 gei-1/1    OSPF  110 101
*>11.1.1.0/24  26.1.1.22 gei-1/1    OSPF  110 101
*>12.1.1.0/24  23.1.1.22 gei-1/3    OSPF  110 20
*>16.1.1.0/24  26.1.1.22 gei-1/1    OSPF  110 101
*>26.1.3.0/24  26.1.1.22 gei-1/1    OSPF  110 101
*>100.1.1.0/24 23.1.1.22 gei-1/3    OSPF  110 20
```

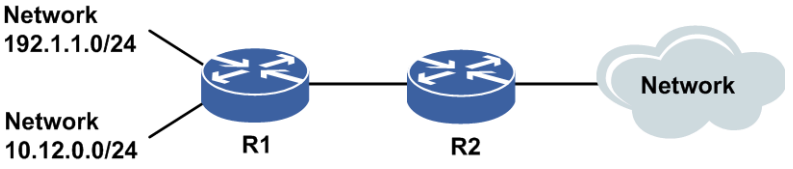
11.5.5 BGP 调用 prefix-list 配置实例

配置说明

如*图 11-7*所示，R1接入了多个网络，其中的两个网络是192.1.1.0/24和10.12.0.0/24。R1和R2间建立BGP邻居，R2希望只学习到网络192.1.1.0/24的路由。

可以通过配置prefix-list来控制路由的学习，即允许R1向R2通告192.1.1.0/24的路由，而不通告10.12.0.0/24的路由。

图 11-7 BGP 调用 prefix-list 配置实例组网图



配置思路

1.R1和R2上起BGP邻居。

2.R1上导入两条路由到BGP当中。

3.R1上配置prefix-list，准许某些路由M通过，限制其它路由N通过。

4.R1上配置在BGP当中对邻居R2通告路由使用该prefix-list进行通告过滤。

5.配置结果是R1向R2通告BGP路由时，通告M路由，而不通告N路由；在R2上查看路由，有BGP通告的M路由，无N路由。

配置过程

1.R1、R2上配置BGP邻居（省略）。

2.R1上导入路由。

i.本例中使用**network**命令通告R1上的路由，先查R1上有哪些路由存在：

```
R1(config)#show ip forwarding route
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: user-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
status codes: *valid, >best
   Dest          Gw          Interface       Owner  Pri Metric
*> 1.1.1.1/32    100.1.3.1   gei-0/2         Static   1   0
*> 10.12.0.0/24  10.12.0.1   gei-0/3         Direct   0   0
*> 10.12.0.1/32  10.12.0.1   gei-0/3         Address  0   0
*> 100.1.3.0/24  100.1.3.2   gei-0/2         Direct   0   0
*> 100.1.3.2/32  100.1.3.2   gei-0/2         Address  0   0
*> 100.1.31.0/24 100.1.31.1  smartgroup30.10  Direct   0   0
*> 100.1.31.1/32 100.1.31.1  smartgroup30.10  Address  0   0
*> 100.10.1.0/24 100.10.1.1  gei-0/4         Direct   0   0
*> 100.10.1.1/32 100.10.1.1  gei-0/4         Address  0   0
*> 100.10.2.0/24 100.10.2.1  gei-0/4.1       Direct   0   0
*> 100.10.2.1/32 100.10.2.1  gei-0/4.1       Address  0   0
*> 100.10.2.2/32 100.10.2.2  gei-0/4.1       Static   1   0
*> 100.20.1.0/24 100.20.1.1  gei-0/7         Direct   0   0
*> 100.20.1.1/32 100.20.1.1  gei-0/7         Address  0   0
*> 192.1.1.0/24  192.1.1.1   gei-0/9         Direct   0   0
*> 192.1.1.1/32  192.1.1.1   gei-0/9         Address  0   0
```

ii.在R1上通告上面目的地址为1.1.1.1/32、10.12.0.0/24、192.1.1.0/24的三条路由：

```
R1(config)#router bgp 1
R1(config-bgp)#network 1.1.1.1 255.255.255.255
R1(config-bgp)#network 192.1.1.0 255.255.255.0
R1(config-bgp)#network 10.12.0.0 255.255.255.0
R1(config-bgp)#exit
```

iii.在R1上验证配置结果：

```
R1(config)#show running-config bgp
!<bgp>
router bgp 1
  synchronization
  network 1.1.1.1 255.255.255.255
  network 192.1.1.0 255.255.255.0
  network 10.12.0.0 255.255.255.0
  neighbor 100.10.1.2 remote-as 2
  neighbor 100.10.1.2 activate
  address-family ipv4 multicast
  $
  address-family l2vpn vpls
  $
  address-family vpnv4
  $
  address-family vpnv4 mcast
  $
  address-family vpnv4 multicast
  $
  address-family ipv6
    synchronization disable
  $
  address-family ipv6 multicast
  $
  address-family vpnv6
```

```
  $
  address-family route-target
  $
$
!</bgp>
```

iv.在R1上查看路由通告的结果：

```
R1(config)#show ip bgp route
Status codes: * valid, > best, i-internal, s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete
   Network      NextHop   Metric LocPrf RtPrf Path
*> 1.1.1.1/32    1.1.1.1   0      0          i
*> 10.12.0.0/24  10.12.0.1 0      0          i
*> 192.1.1.0/24  192.1.1.1 0      0          i
```

v.在R2上查看BGP学习路由情况：

```
R2(config)#show ip forwarding route bgp
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
status codes: *valid, >best
  Dest         Gw        Interface   Owner Pri Metric
*> 1.1.1.1/32   100.10.1.1 gei-0/4    BGP   20  0
*> 10.12.0.0/24 100.10.1.1 gei-0/4    BGP   20  0
*> 192.1.1.0/24 100.10.1.1 gei-0/4    BGP   20  0
```

3.在R1上配置prefix-list，准许步骤2中导入的部分路由192.1.1.0/24：

```
R1(config)#ip prefix-list inspur permit 192.1.1.0 24
R1(config)#show running-config prefix-list
!<prefix-list>
ip prefix-list inspur seq 5 permit 192.1.1.0 24
!</prefix-list>
```

4.R1上配置在BGP当中对邻居R2通告路由使用该prefix-list。

i.配置对邻居R2通告路由使用prefix-list inspur：

```
R1(config)#router bgp 1
R1(config-bgp)#neighbor 100.10.1.2 prefix-list inspur out
R1(config-bgp)#exit
```

ii.查看R1上的配置结果：

```
R1(config)#show running-config bgp
!<bgp>
router bgp 1
  synchronization
  network 1.1.1.1 255.255.255.255
  network 192.1.1.0 255.255.255.0
  network 10.12.0.0 255.255.255.0
  neighbor 100.10.1.2 remote-as 2
  neighbor 100.10.1.2 activate
  neighbor 100.10.1.2 prefix-list inspur out
  ……
!</bgp>
```

5.在R2上查看最终学习到的路由：

```
R2(config)#show ip forwarding route bgp
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
```

```
          ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
          GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
          GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
  status codes: *valid, >best
     Dest        Gw        Interface   Owner Pri Metric
  *> 192.1.1.0/24 100.10.1.1 gei-0/4     BGP   20   0
```

配置验证

在R1上查看prefix-list和BGP配置：

```
R1#show running-config prefix-list
!<prefix-list>
ip prefix-list inspur seq 5 permit 192.1.1.0 24
!</prefix-list>

inspur#show running-config bgp
!<bgp>
router bgp 1
  synchronization
  network 1.1.1.1 255.255.255.255
  network 192.1.1.0 255.255.255.0
  network 10.12.0.0 255.255.255.0
  neighbor 100.10.1.2 remote-as 2
  neighbor 100.10.1.2 activate
  neighbor 100.10.1.2 prefix-list inspur out
  ……
!</bgp>
```

在R2上查看BGP配置：

```
R2#show running-config bgp
!<bgp>
router bgp 2
  synchronization
  neighbor 100.10.1.1 remote-as 1
  neighbor 100.10.1.1 activate
  ……
!</bgp>
```

在R1上查看BGP的路由通告

```
R1#show ip bgp route
Status codes: * valid, > best, i-internal, s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete
  Network         NextHop   Metric LocPrf RtPrf Path
*> 1.1.1.1/32     1.1.1.1    0          0     i
*> 10.12.0.0/24   10.12.0.1  0          0     i
*> 192.1.1.0/24   192.1.1.1  0          0     i
```

在R2上查看BGP路由学习情况：

```
R2#show ip bgp summary
Neighbor  Ver As MsgRcvd MsgSend Up/Down  State/PfxRcd
100.10.1.1 4  1  125     120     01:00:13     1

RouterB#show ip bgp route
Status codes: * valid, > best, i-internal, s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete
   Network     NextHop     Metric LocPrf RtPrf Path
*> 192.1.1.0/24 100.10.1.1   20          1     i
```

在R2上使用**show ip forwarding route bgp**命令查看转发路由表中BGP属性的路由，能看到从R1学习到的路由只有prefix-list当中唯一permit的192.1.1.0/24，说明配置成功：

```
R2#show ip forwarding route bgp
IPv4 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
 MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
 ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
 GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
 GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
status codes: *valid, >best;
  Dest         Gw        Interface   Owner Pri Metric
*> 192.1.1.0/24 100.10.1.1 gei-0/4     BGP   20  0
```

11.5.6 Route-map 调用 prefix-list 配置实例

配置说明

Route-map和prefix-list一样，都是一种模板。在某些业务中，并不直接调用prefix-list，而是通过route-map先调用prefix-list，再在业务中调用route-map的方式实现业务对prefix-list的调用。

比如IS-IS在重分配和泄露命令中并不直接关联prefix-list，而是通过route-map间接进行地址前缀的prefix-list匹配（IS-IS的这种调用将在route-map章节中进行介绍）。

配置思路

1.配置prefix-list。

2.在route-map中match匹配这个prefix-list。

配置过程

1.创建要调用的ip prefix-list：

```
inspur(config)#ip prefix-list inspur permit 192.168.100.0 24
```

2.配置route-map调用prefix-list：

```
inspur(config)#route-map inspur1
inspur(config-route-map)#match ip address prefix-list inspur
inspur(config-route-map)#exit
```

配置验证

用**show ip prefix-list** *<prefix-list-name>*命令查看配置的prefix-list是否正确：

```
inspur(config)#show ip prefix-list inspur
ip prefix-list inspur :
seq 5 permit 192.168.100.0 24
```

用**show route-map** *<route-map-name>*命令查看配置的route-map是否正确：

```
inspur(config)#show route-map inspur1
[route-map inspur1] IP type: IPv4
route-map inspur1 permit 10
match ip address prefix-list inspur
```

11.6 Route-Map

Route-Map是功能强大的过滤和修改器，作为一个策略模板，Route-Map在路由设备上广泛应用于策略路由和路由策略：

- Route-Map应用于接口的入方向，用于对接口进入的特定流量指定路由，称为策略路由。
- Route-Map应用于路由协议，用于干预路由的产生、发布、选择，从而达到优化路由表的效果，称为路由策略。

Route-Map作为一个策略模板，仅当作为策略路由应用到接口或者作为路由策略应用到路由协议时，才能生效。

11.6.1 配置路由策略

配置路由策略的相关属性和功能，包括基本属性、路由属性以及在路由协议中如何调用路由策略。

1.配置路由策略的基本属性。

步骤	命令	功能
1	inspur(config)#**route-map** <*route-map-name*>[**permit**|**deny**][<*sequence-number*>]	创建用于路由策略的route-map，并且进入路由映射配置模式
2	inspur(config-route-map)#**match ip address *(**<*access-list-name*>**)**	配置match项，匹配类型为IPv4路由条目的目的网段/目的地址，选择使用ACL进行匹配
	inspur(config-route-map)#**match ip address prefix-list *(**<*prefix-list-name*>**)**	配置match项，匹配类型为IPv4路由条目的目的网段/目的地址，选择使用prefix-list进行匹配
	inspur(config-route-map)#**match ip metric *(**<*metric-value*>**)**	匹配路由的metric值，可根据需要连配多个
	inspur(config-route-map)#**match ip tag *(**<*tag-value*>**)**	匹配路由的tag值，OSPF和Static路由带此属性，可根据需要连配多个
	inspur(config-route-map)#**match as-path *(**<*as-path-list-number*>**)**	匹配BGP协议路由as-path的属性，可根据需要连配多个
	inspur(config-route-map)#**match community-list *(**<*community-list-number*>**)**	匹配BGP协议路由的community属性，可根据需要连配多个
	inspur(config-route-map)#**match extcommunity-list**	匹配BGP/VPN路由的extcommunity属性，可根据需

步骤	命令	功能
	***(**<*community-list-number*>**)**	要连配多个
	inspur(config-route-map)#**match route-type** {**external** [**type-1** | **type-2**]|**internal**|**level-1**|**level-2**|**local**}	匹配路由类型
	inspur(config-route-map)#**match as-path-length** {**ge** | **le** | **eq**}<*as-path length*>	匹配as-path的长度，范围：0~255
	inspur(config-route-map)#**match as-path-unique-length** {**ge** | **le** | **eq**}<*as-path unique length*>	匹配as-path-unique的长度，范围：0~255
	inspur(config-route-map)#**match ip metric** {**ge** | **le** | **eq**}<*metric-value*>	匹配路由的metric值，取值范围：0~4294967295
	inspur(config-route-map)#**match origin** {**egp** | **igp** | **incomplete**}	匹配orgin属性，可以选择EGP、IGP或者未知类型
	inspur(config-route-map)#**match ip source** [**prefix-lilst**]{<*access-list-name*>|<*prefix-list-name*>}	匹配source的值，可以使用ACL或者前缀列表的名称配置
	inspur(config-route-map)#**match ip next-hop** *[<*access-list-name*>]	匹配类型为IPv4路由的下一跳地址，选择使用ACL进行匹配

<*route-map-name*>：路由映射的名称，长度为1~31个字符。

permit | **deny**：一个Route-map当中可以有一至多个sequence，各个序列的属性可以灵活配置为**permit**或者**deny**。**permit**表示匹配后执行路由策略，**deny**表示无论是否匹配，皆不执行任何动作。

<*sequence-number*>：Route-map的序列号，每个route-map支持一至多个序列，在进行匹配时，所有路由按照序列号由小到大的顺序进行匹配，一旦匹配上，根据当前sequence的属性决定是否执行路由策略。

<*access-list-name*>：Match类型为ipv4-access-list，将路由和ACL进行匹配。

prefix-list <*prefix-list-name*>：Match类型为prefix-list，将路由和前缀列表进行匹配。

ip metric *(<*metric-value*>**)**：Match类型为ip metric，取值区间为0~4294967295，可根据需要连配多个。

ip tag *(<*tag-value*>**)**：Match类型为ip tag，取值区间为0~4294967295，可根据需要连配多个。

as-path *(<*as-path-number*>**)**：Match类型为as-path，取值区间为1~199，可根据需要连配多个。

community-list *(<*community-list-number*>**)**：Match类型为community-list，取值区间为1~499，可根据需要连配多个。

extcommunity-list *(<*community-list-number*>**)**：Match类型为extcommunity-list，取值区间为1~500，可根据需要连配多个。

route-type {**external** [**type-1**|**type-2**]|**internal**|**level-1**|**level-2**|**local**}：Match类型为

route-type，根据需要选择路由类型，不能连配，但是可以配置多条此类型的match项。

{ge | le | eq}：ge表示大于某值，le表示小于某值，eq表示等于某值。

2.配置路由策略的路由属性。

命令	功能
inspur(config-route-map)#**set as-path prepend *(***<as number>***)**	配置路由策略中的路由属性，设置as-path属性，可根据需要连配多个，BGP协议独有
inspur(config-route-map)#**set community** {**none** | **additive***{**no-advertise** | **no-export** | **no-export-subconfed** | **internet** |*<0-65535>*:*<0-65535>*|*<1-4294967295>*})}	设置团体属性，BGP协议独有
inspur(config-route-map)#**set extcommunity rt-trans** {{**remove** | **additive** *****{*<0-65535>*:*<0-4294967295>*|*<1-65535>*.*<0-65535>*:*<0-65535>*| **A.B.C.D:***<0-65535>*}}|{*<0-65535>*:*<0-4294967295>*| *<1-65535>*.*<0-65535>*:*<0-65535>*| **A.B.C.D:***<0-65535>*})}	设置扩展团体属性，BGP协议独有
inspur(config-route-map)#**set extcommulity soo-trans** {*<0-65535>*:*<0-4294967295>*|*<1-65535>*.*<0-65535>*:*<0-65535>*| **A.B.C.D:***<0-65535>*| **remove**}	设置扩展团体属性，BGP协议独有
inspur(config-route-map)#**set dampening** *<half-life><reuse><suppress><max-suppress-time>*	设置路由的阻尼因素，BGP协议独有
inspur(config-route-map)#**set local-preference** *<value>*	设置路由的local-preference属性，BGP协议独有
inspur(config-route-map)#**set origin** {**igp**|**egp** |**incomplete** }	设置路由起源属性，BGP协议独有
inspur(config-route-map)#**set level** *<level-value>*	设置IS-IS路由属性，IS-IS协议中用到
inspur(config-route-map)#**set next-hop** *<ip-address>*[**...***<ip-address>*]	设置路由的下一跳
inspur(config-route-map)#**set ip metric** [+|-]*<metric-value>*	设置路由的metric值
inspur(config-route-map)#**set ip metric-type** {**internal** |**external** |**type-1** |**type-2** }	设置路由选择协议的尺度类型
inspur(config-route-map)#**set ip tag** *<tag-value>*	设置IP tag值，OSPF和Static路由会有的属性

<*half-life***>**：改变路由阻尼因素的半衰期，范围为1~45。

<*reuse***>**：改变路由阻尼因素的重新使用值，范围为1~20000。

<*suppress***>**：改变路由阻尼因素的路由抑制值，范围为1~20000。

<*max-suppress-time***>**：改变路由阻尼因素的最大抑制时间，通常路由抑制时间到达该值以后，惩罚值不再增加，范围为1~255。

3.配置RIP调用路由策略。

步骤	命令	功能
1	inspur(config)#**router rip**	进入RIP配置模式
2	inspur(config-rip)#**redistribute** <*protocol*>[**process-id**][**metric** <*metric-value*>][**route-map** <*route-map-name*>]	重分配其它路由协议的路由到RIP中

[**process-id**]：实例号，在重分配OSPF或者ISIS路由时需要配置实例号，OSPF：1~65535；IS-IS：0~65535，如果不配置缺省为0。

<*protocol*>：路由再分配的源路由协议，可以是以下关键词：ospf-ext，ospf-int，static，bgp-ext，bgp-int，connected，isis-1，isis-2，isis-1-2，nat，natpt，ps-busi-addr，ps-user-addr，subscriber-aggregation，subscriber-host，user-special。

metric <*metric-value*>>：指定以多大的路由权值引入路由，如果不指定，则按缺省路由权（default-metric）引入，范围1~16。

route-map <route-map-name>：用于再分配的路由映射名称，长度为1~31个字符。RIP通过在该重分配命令中使用到ROUTE-MAP路由策略。

4.配置IS-IS调用路由策略。

步骤	命令	功能
1	inspur(config)#**router isis** [<*process-id*>][**vrf** <*vrf-name*>]	进入IS-IS路由配置模式功能
2	inspur(config-isis-id)#**redistribute** <*protocol*>[**level-1**][**level-1-2**][**level-2**][**metric-type** <*metric-type*>][**metric** <*metric-value*>][**route-map** <*route-map-name*>]	在IS-IS路由模式下，配置重分发
3	inspur(config-isis-id)#**router-leak level-2 into level-1 route-map** <*route-map-name*>	在IS-IS路由模式下，配置路由泄漏

<*protocol*>：路由来源，可以为connected、static、rip、is-is <process-id>、ospf <process-id>、bgp、nat、natpt、ps-busi-addr、ps-user-addr、sl-nat64-ipv4、subscriber-aggregation、subscriber-host、user-special，若重分配IS-IS或OSPF路由，则需要指定相应的实例号。

level-1：设置重分发的路由信息进入Level-1。

level-1-2：设置重分发的路由信息同时进入Level-1和Level-2。

level-2：设置重分发的路由信息进入Level-2。

<*metric-type*>：设置重分发的路由是携带external还是internal的metric值。

<*metric-value*>：metric值，范围0~4261412864。

route-map <*route-map-name*>：引用一个route-map。

5.配置OSPF调用路由策略。

步骤	命令	功能
1	inspur(config-ospf-process-id)#**redistribute** {**sl-nat64-ipv4**|**user-special**|**nat**|**natpt**|**subscriber-host**|**subscriber-aggregation**|**static**|**connected**|**rip**|{**ospf-int**|**ospf-ext**}<*process-id*>|{**isis-1**|**isis-2**|**isis-1-2**}[<*process-id*>]|{**bgp-ext**|**bgp-int**}[{[**as** <*1-65535*>**/**<*1-65535*>**.**<*0-65535*>],[**peer** <*peer-address*>]}]|{**ps-busi-addr**|**ps-user-addr**}[**with-originate-metric**]}[{[**tag**|<*tag-value*>],[**metric** <*metric-value*>],[**metric-type** {**ext-2**|**ext-1**}],[**route-map** <*map-tag*>]}]	在OSPF路由模式下，配置重分发

重分发路由来源，可以为connected、static、rip、is-is <process-id>、ospf-int <process-id>、ospf-ext <process-id>、bgp-int、、bgp-ext、nat、natpt、ps-busi-addr、ps-user-addr、sl-nat64-ipv4、subscriber-aggregation、subscriber-host、user-special，若重分配IS-IS或OSPF路由，则需要指定相应的实例号。

<*metric-type*>：设置重分发的路由类型是ext-1或者ext-2。

<*metric-value*>：metric值，范围1~16777214。

route-map <*route-map-name*>：引用一个route-map。

6.配置BGP调用路由策略。

步骤	命令	功能
1	inspur(config)#**router bgp** {<*1~65535*>|<*1~65535*>**.**<*0~65535*>}	进入BGP路由配置模式
2	inspur(config-bgp)#**redistribute** <*protocol*>[**route-map** <*route-map-name*>[**metric** <*metric-value*>]]	配置重分配将其他协议类型的路由到BGP <*protocol*>，协议类型，如果是OSPF或者IS-IS还需给出实例号 <*route-map-name*>，路由的路由映射名称，长度为1~31个字符
3	inspur(config-bgp)#**bgp dampening** [**route-map** <*route-map-name*>]	使BGP路由阻尼有效或修改各种BGP路由阻尼因素
4	inspur(config-bgp)#**neighbor** [<*ipv4-address*>|< *peer-group-name*>] **route-map** < *route-map-name*>{ **in** | **out**}	对邻居/邻居对等体组通告来的路由，或通告给邻居/邻居对等体组的路由进行过滤，或设置路由的优先级 **in** | **out**，表示应用于输出还是输入路由
5	inspur(config-bgp)#**address-family ipv4 vrf** <*vrf-name*>	进入IPv4 vrf地址族配置模式

步骤	命令	功能
6	inspur(config-bgp-af-ipv4-vrf-name)#**aggregate-address** < *ip-address*>< *net-mask*>[**attribute-map** < *route-map-name*>][**suppress-map**< *route-map-name*>][**as-set**][**summary-only**][**strict**]	在VRF路由表中创建一条聚合策略 **attribute-map**，属性图 **suppress-map**，抑制图

7.配置VRF调用路由策略。

步骤	命令	功能
1	inspur(config)#**ip vrf** <*vrf-name*>	创建VRF
2	inspur(config-vrf-name)#**rd** <*route-distinguisher*>	配置RD
3	inspur(config-vrf-name)#**route-target** [**import** | **export** | **both**]<*extended-community* >	创建与VRF关联的route-target扩展团体属性
4	inspur(config-vrf-name)#**address-family ipv4**	激活IPv4 vrf地址族
5	inspur(config-vrf-name-af-ipv4)#**import map** <*route-map-name*>	配置与VRF关联的导入路由映射
	inspur(config-vrf-name-af-ipv4)#**export map** <*route-map-name*>	配置与VRF关联的导出路由映射

8.验证配置结果。

命令	功能
inspur(config)#**show running-config rip**	查看各路由协议当中是否使用了路由策略（显示RIP协议的配置）
inspur(config)#**show running-config isis**	查看各路由协议当中是否使用了路由策略（显示ISIS协议的配置）
inspur(config)#**show running-config ospfv2** | **ospfv3**	查看各路由协议当中是否使用了路由策略（显示OSPF协议的配置）
inspur(config)#**show running-config bgp**	查看各路由协议当中是否使用了路由策略（显示BGP协议的配置）
inspur(config)#**show running-config vrf**	查看vrf是否使用了路由策略（显示VRF的配置）
inspur(config)#**show ip vrf detail** [<*vrf-name*>]	查看VRF的具体配置信息，可指定查看某个目标VRF实例的配置
inspur(config)#**show ip vrf** [<*vrf-name*>]	查看VRF的配置信息
inspur(config)#**show ip vrf brief** [<*vrf-name*>]	查看VRF的简要信息
inspur(config)#**show ip vrf summary**	查看VRF的概要配置信息

命令	功能
inspur(config)#**show route-map** [<*route-map-name*>]	查看具体的route-map模板的配置

11.6.2 配置策略路由

本节介绍策略路由的配置步骤和命令。

1.配置策略路由的基本属性。

步骤	命令	功能
1	inspur(config)#**route-map** <*route-map-name*>[**permit** | **deny**][<*sequence-number*>]	创建用于策略路由的route-map，并且进入路由映射配置模式
2	inspur(config-route-map)#**match ip address *(**<*access-list-name*>**)**	在路由映射配置模式下配置match项，对与访问表匹配的包进行策略路由 ACL既可以是标准型的又可以是扩展型的
3	inspur(config-route-map)#**set ip next-hop *(**<*ip-address*>**)**[**track** <*sqa-name*>]	当数据包可被策略路由时，把数据包路由到指定的下一跳，可以设置10个IP地址
	inspur(config-route-map)#**set ip path interface** <*interface-name*> **next-hop** <*ip-address*>	当数据包可被策略路由时，将数据包路由到指定的以太出接口和下一跳，只能配置一个
	inspur(config-route-map)#**set interface *(**<*interface-name*>**)**	当数据包可被策略路由时，把数据包路由到指定接口上
	inspur(config-route-map)#**set ip tos** <*tos-value*>	设置IP tos值
	inspur(config-route-map)#**set ip precedence** <*precedence-value*>	设置IP报头优先级
	inspur(config)#**ip policy interface** < *interface-name*> **route-map** < *route-map-name*>	配置对报文进行基于策略路由的快速转发

<*route-map-name*>：路由映射的名称，长度为1~31个字符。

permit：如果路由映射符合匹配条件，允许再分配策略路由标志。

deny：如果路由映射符合匹配条件，不允许再分配策略路由标志。

<*sequence-number*>：序列号，范围0~65535。

2.配置VRF策略路由。

步骤	命令	功能
1	inspur(config)#**route-map** <*route-map-name*>[**permit** | **deny**][<*sequence-number*>]	创建用于策略路由的route-map，并且进入路由映射配置模式
2	inspur(config-route-map)#**set vrf** <*vrf-name*>	配置VRF的名字，当数据包符合用于策略路由的路由映像的一个匹配项而可被策略路由时，使用**set vrf**命令把数据包路由到指定VPNID上
3	inspur(config-route-map)#**set vrf** <*vrf-name*> **ip next-hop** <*ip-address*>[**track** <*sqa-name*>]	设置指定VRF的某个下一跳路径
4	inspur(config-route-map)#**set global**	将私网VRF接入侧的数据报文策略到普通出接口所在链路上
5	inspur(config-route-map)#**set global** [**ip next-hop** <*ip-address*>]	将指定私网VRF接入侧的数据报文策略到公网某个下一跳路径

3.验证配置结果。

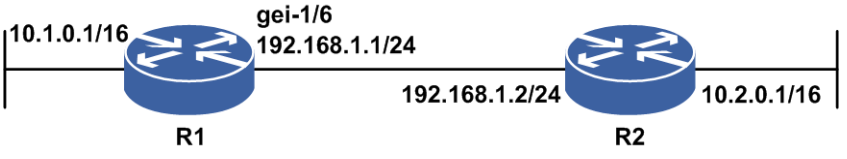
命令	功能
inspur#**show route-map**<*route-map-name*>	显示route-map的信息
inspur#**show running-config pbr**	显示接口上PBR的绑定信息

11.6.3 RIP 重分配路由策略配置实例

配置说明

如*图 11-8*所示，在R1和R2上运行RIP，通告各自的RIP路由，可重分发其他路由，以重分发静态路由为例。

图 11-8 RIP 重分配路由策略配置实例示意图



配置思路

1.接口配置IPv4地址。

2.在接口所在网段上启动RIP协议。

3.重分发其他路由，配置重分发命令。

4.为重分发命令关联route-map名称。

5.配置route-map策略。

6.查看配置结果，确认两台设备分别能够学到对端通告的路由。

配置过程

R1的配置如下：

```
R1(config)#router rip
R1(config-rip)#redistribute static route-map www
R1(config-rip)#network 192.168.1.0 0.0.0.255
R1(config-rip)#exit
R1(config)#ip route 3.3.3.0 255.255.255.0 loopback1 4      /*不是最优路由，不会被通告*/
R1(config)#ip route 3.3.3.0 255.255.255.0 gei-1/6 30.0.0.6 3
R1(config)#ip route 5.5.5.0 255.255.255.0 loopback2
R1(config)#route-map www permit 10
R1(config-route-map)#set ip metric 10
R1(config-route-map)#exit
```

R2的配置如下：

```
R2(config)#router rip
R2(config-rip)#network 192.168.1.0 0.0.0.255
R2(config-rip)#exit
```

配置验证

在R1和R2上利用**show**命令来查看RIP、route-map和静态路由的配置信息，以及RIP的路由表和IPv4的路由信息。

R1上的路由信息：

```
R1(config)#show running-config rip
!<rip>
router rip
  redistribute static route-map www
  network 192.168.1.0 0.0.0.255
$
!</rip>

R1(config)#show running-config static
!<static>
ip route 3.3.3.0 255.255.255.0 loopback1 4
ip route 3.3.3.0 255.255.255.0 gei-1/6 30.0.0.6 3
ip route 5.5.5.0 255.255.255.0 loopback2
!</static>

R1(config-route-map)#show running-config route-map
!<route-map>
route-map www permit 10
  set ip metric 10
$
!</route-map>

R1(config)#show ip rip database
Routes of rip:
```

```
h : is possibly down,in holddown time
f : out holddown time before flush

   Dest          Metric     RtPrf    InstanceID  Time      From
*> 3.0.0.0/8      10         254      0          00:00:24  0.0.0.0
*> 3.3.3.0/2410 3 0 00:00:000.0.0.0
*> 5.0.0.0/8      10         254      0          00:00:24  0.0.0.0
*> 5.5.5.0/24     10         1        0          00:00:00  0.0.0.0
*> 192.168.1.0/24 0          0        0          00:00:00  0.0.0.0
```

R2上的路由信息：

```
R2(config)#show running-config rip
!<rip>
router rip
  network 192.168.1.0 0.0.0.255
$
!</rip>

R2(config)#show ip rip database
Routes of rip:
h : is possibly down,in holddown time
f : out holddown time before flush

Dest               Metric     RtPrf    InstanceID  Time          From
*> 3.0.0.0/8        11         120      0          00:00:10      192.168.23.115
*> 5.0.0.0/8        11         120      0          00:00:10      192.168.23.115
*> 192.168.1.0/24    0          0        0          00:00:00      0.0.0.0

R2(config)#show ip protocol routing
Protocol routes:
status codes: *valid, >best, i-internal, s-stale

    Dest             NextHop         RoutePrf   RouteMetric Protocol
*>  3.0.0.0/8         192.168.23.115  120        11          rip
*>  5.0.0.0/8         192.168.23.115  120        11          rip
*>  192.168.1.0/24     192.168.23.111  0          0           connected
*>  192.168.1.2/32     192.168.23.111  0          0           connected
```

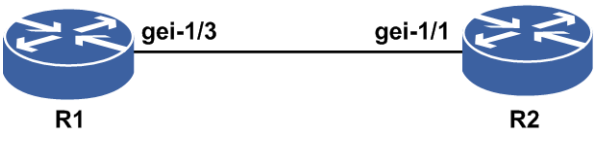
11.6.4 IS-IS 路由策略配置实例

配置说明

如*图 11-9*所示，R1和R2在level-1-2建立邻居，状态为up。

R1上配置2条静态路由，在IS-IS level-1中重分发静态路由带route-map参数。

图 11-9 IS-IS 路由策略配置实例示意图



配置思路

1.R1和R2配置成level-1-2，建立邻居。

2.在R1上配置route-map testisis。

3.在R1上配置若干静态路由。

4.在R1上重分发静态路由带route-map参数。

配置过程

1.R1和R2配置成level-1-2，建立邻居。

在R1上配置ISIS：

```
R1(config)#router isis 44
R1(config-isis-44)#system-id 5555.5555.5555
R1(config-isis-44)#area 44
R1(config-isis-44)#is-type level-1-2
R1(config-isis-44)#metric-style narrow
R1(config-isis-44)#interface gei-1/3
R1(config-isis-44-if-gei-1/3)#ip router isis
R1(config-isis-44-if-gei-1/3)#exit
R1(config-isis-44)#exit
```

在R2上配置ISIS：

```
R2(config)#router isis 44
R2(config-isis-44)#system-id 2222.2222.2222
R2(config-isis-44)#area 44
R2(config-isis-44)#is-type level-1-2
R2(config-isis-44)#metric-style narrow
R2(config-isis-44)#interface gei-1/1
R2(config-isis-44-if-gei-1/1)#ip router isis
R2(config-isis-44-if-gei-1/1)exit
R2(config-isis-44)#exit
```

2.在R1上配置route-map testisis：

```
R1(config)#route-map testisis permit 10
R1(config-route-map)#set level level-1
R1(config-route-map)#set ip metric 10
R1(config-route-map)#set ip metric-type external
R1(config-route-map)#exit
```

3.在R1上配置3条静态路由：

```
R1(config)#ip route 1.2.3.4 255.255.255.255 192.168.1.103
R1(config)#ip route 20.0.0.0 255.255.255.0 192.168.5.203
R1(config)#ip route 168.178.19.0 255.255.255.0 177.77.16.2
```

4.在R1上重分发静态路由带route-map参数：

```
R1(config)#router isis 44
R1(config-isis-44)#redistribute static route-map testisis
R1(config-isis-44)#exit
```

配置验证

IS-IS配置结果：

```
R1(config)#show running-config isis
!<isis>
router isis 44
  area 44
  system-id 5555.5555.5555
  is-type level-1-2
  metric-style narrow
  redistribute static route-map testisis
```

```
  interface gei-1/3
    ip router isis
  $
$
!</isis>
R2(config)#show running-config isis
!<isis>
router isis 44
  area 44
  system-id 2222.2222.2222
  is-type level-1-2
  metric-style narrow
  interface gei-1/1
    ip router isis
  $
$
!</isis>
```

ROUTE-MAP配置结果：

```
R1(config)#show route-map testisis
 [route-map testisis] IP type: IPv4
route-map testisis permit 10
  set level level-1
  set ip metric 10
  set ip metric-type external
```

静态路由配置结果：

```
R1(config)#show ip forwarding route static
IPv4 Routing Table:
status codes: *valid, >best
Dest            Gw            Interface     Owner     Pri Metric
*> 1.2.3.4/32     192.168.1.103   gei-3/2       Static    1   0
*> 20.0.0.0/24    192.168.5.203   gei-3/3       Static    1   0
*> 168.178.19.0/24 177.77.16.2    smartgroup47    Static    1   0
```

验证配置后是否达到预期效果，在R1上看层1的路由：

narrow模式metric-type external ， metric=10+64=74,

默认条件下重分发路由进入层2，配置了route-map后，路由只重分发进层1。

```
R1(config)#show isis database level-1 detail process-id 44
Process ID:44
IS-IS Level-1 Link State Database:
LSPID              LSP Seq Num    LSP Checksum    LSP Holdtime   ATT/P/OL
R1.00-00*           0x6           0xd6dc          1142           0/0/0
    NLPID:          0xcc
    Area Address:    00
    Ip Address:      55.1.1.1
    Hostname:        R1
    Metric: 10       IS neighbor R1.02
    Metric: 10       IP-Internal 55.1.1.0 255.255.255.0
LSPID              LSP Seq Num    LSP Checksum    LSP Holdtime   ATT/P/OL
R1.00-01*           0x8           0x9223          934            0/0/0
    Metric: 74       IP-External 1.2.3.4 255.255.255.255
    Metric: 74       IP-External 20.0.0.0 255.255.255.0
    Metric: 74       IP-External 168.178.19.0 255.255.255.0
    Hostname:        R1
```

在R2上查看R1通告过来的3条ISIS路由信息：

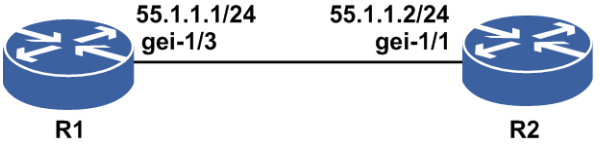
```
R2(config)#show ip forwarding route isis-l1
IPv4 Routing Table:
status codes: *valid, >best
   Dest            Gw        Interface          Owner     Pri Metric
*> 1.2.3.4/32        55.1.1.1   gei-1/1            ISIS-L1   115 84
*> 20.0.0.0/24       55.1.1.1   gei-1/1            ISIS-L1   115 84
*> 168.178.19.0/24    55.1.1.1   gei-1/1            ISIS-L1   115 84
```

11.6.5 OSPF 路由策略配置实例

配置说明

如*图 11-10*所示，R1上的接口放入OSPF区域1中，R2上的接口放入OSPF区域1中，R1和R2建立OSPF邻居，状态为full。在R1上配置3条静态路由，把静态路由在OSPF中带route-map参数重分发。

图 11-10 OSPF 路由策略配置实例示意图



配置思路

1.R1和R2在区域1建立邻居。

2.在R1上配置route-map。

3.在R1上配置几条静态路由。

4.R1上配置OSPF重分发静态路由带route-map参数。

配置过程

步骤1：R1和R2直连接口配置同网段地址，用于建立OSPF邻居。

```
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#ip address 55.1.1.1 255.255.255.0
R1(config-if-gei-1/3)#exit
R1(config)#router ospf 2
R1(config-ospf-2)#area 1
R1(config-ospf-2-area-1)#network 55.1.1.0 0.0.0.255
R1(config-ospf-2-area-1)#exit
R1(config-ospf-2)#exit

R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 55.1.1.2 255.255.255.0
R2(config-if-gei-1/1)#exit
R2(config)#router ospf 2
R2(config-ospf-2)#area 1
R2(config-ospf-2-area-1)#network 55.1.1.0 0.0.0.255
R2(config-ospf-2-area-1)#exit
```

步骤2：R1上配置route-map。

```
R1(config)#route-map ff
R1(config-route-map)#match ip metric 0
R1(config-route-map)#set ip metric 50
R1(config-route-map)#set ip metric-type type-1
R1(config-route-map)#set ip tag 100
R1(config-route-map)#exit
```

步骤3：R1上配置若干条静态路由。

```
R1(config)#ip route 1.2.3.4 255.255.255.255 192.168.1.103
R1(config)#ip route 20.0.0.0 255.255.255.0 192.168.5.203
R1(config)#ip route 168.178.19.0 255.255.255.0 177.77.16.2
```

步骤4：在R1上配置OSPF中重分配静态路由带route-map参数。

```
R1(config)#router ospf 2
R1(config-ospf-2)#redistribute static route-map ff
R1(config-ospf-2)#exit
```

配置验证

查看R1上的配置结果，以及R1上的静态、OSPF路由。

```
R1(config-route-map)#show route-map ff
[route-map ff] IP type: IPv4
route-map ff permit 10
  match ip metric 0
  set ip metric 50
  set ip metric-type type-1
  set ip tag 100

R1(config)#show ip forwarding route static
IPv4 Routing Table:
Status codes: *valid, >best
Dest             Gw             Interface     Owner     Pri Metric
*> 1.2.3.4/32     192.168.1.103   gei-3/2       Static    1   0
*> 20.0.0.0/24    192.168.5.203   gei-3/3       Static    1   0
*> 168.178.19.0/24 177.77.16.2    smartgroup47   Static    1   0

R1(config)#show running-config | begin router ospf
router ospf 2
 area 1
   network 10.0.0.0 0.0.0.255
 $
  redistribute static route-map ff
$

R1(config)#show ip ospf database process 2

          OSPF Router with ID (61.61.61.1) (Process ID 2)

              Router Link States (Area 0.0.0.1)

Link ID        ADV Router     Age     Seq#        Checksum   Link count
61.61.61.1      61.61.61.1     138     0x80000003   0xa7a1     1
1.2.3.2         1.2.3.2        140     0x80000003   0x8526     1

              Net Link States (Area 0.0.0.1)

Link ID        ADV Router     Age     Seq#        Checksum
55.1.1.1        61.61.61.1     138     0x80000001   0x394f

              Type-5 AS External Link States

Link ID        ADV Router     Age     Seq#        Checksum   Tag
20.0.0.0        61.61.61.1     189     0x80000001   0xd7f9     100
1.2.3.4         61.61.61.1     189     0x80000001   0x6e6d     100
168.178.19.0     61.61.61.1     189     0x80000001   0x1a5d     100
```

在R2上查看OSPF路由的属性。

```
R2(config-ospfv2)#show ip forwarding route ospf
IPv4 Routing Table:
Status codes: *valid, >best
   Dest             Gw        Interface          Owner      Pri Metric
*> 1.2.3.4/32        55.1.1.1   gei-1/1            OSPF       110 51
*> 20.0.0.0/24       55.1.1.1   gei-1/1            OSPF       110 51
```

```
*> 168.178.19.0/24    55.1.1.1   gei-1/1          OSPF       110 51
```

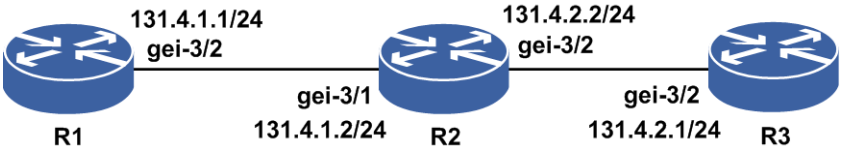
11.6.6 BGP 路由策略配置实例

配置说明

如*图 11-11*所示，R1和R2建立EBGP邻居，R2和R3建立IBGP邻居， R1向R2通告路由。

在R2上配置route-map test1，应用在R2连接R1的in方向上，在R2上配置route-map test2，应用在R2连接R3的out方向上。

图 11-11 BGP 路由策略配置实例



配置思路

1.R1和R2建立EBGP邻居，R2和R3建立IBGP邻居。

2.R1向R2通告若干BGP路由，R2及R3应正常学习到。

3.R2上配置ipv4-access-list 1，ipv4-access-list 2，route-map test1，route-map test2。

4.R2上将route-map test1应用在R2连接R1邻居的in方向上，将route-map test2应用在R2连接R3邻居的out方向上。

提示：

·Route-map分别应用在入接口和出接口时，注意区别（区别：set操作在in方向上只有community和local-preference生效，在out方向上都可以生效）。

·Route-map 中 BGP 协 议 的 专 用 选 项 有 （ set： community-list 、 dampening 、 local-preference、origin、as-path、Match： as-path、community-list)。

配置过程

1.将三台路由器之间直连接口配置同网段地址，配置EBGP邻居。

R1上的配置如下：

```
R1(config)#interface gei-3/2
R1(config-if-gei-3/2)#no shutdown
R1(config-if-gei-3/2)#ip address 131.4.1.1 255.255.255.0
R1(config-if-gei-3/2)#exit
R1(config)#router bgp 1011
R1(config-bgp)#neighbor 131.4.1.2 remote-as 200
R1(config-bgp)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-3/1
```

```
R2(config-if-gei-3/1)#no shutdown
R2(config-if-gei-3/1)#ip address 131.4.1.2 255.255.255.0
R2(config-if-gei-3/1)#exit
R2(config)#interface gei-3/2
R2(config-if-gei-3/2)#no shutdown
R2(config-if-gei-3/2)#ip address 131.4.2.2 255.255.255.0
R2(config-if-gei-3/2)#exit
R2(config)#router bgp 200
R2(config-bgp)#neighbor 131.4.1.1 remote-as 1011
R2(config-bgp)#neighbor 131.4.2.1 remote-as 200
R2(config-bgp)#exit
```

R3上的配置如下：

```
R3(config)#interface gei-3/2
R3(config-if-gei-3/2)#no shutdown
R3(config-if-gei-3/2)#ip address 131.4.2.1 255.255.255.0
R3(config-if-gei-3/2)#exit
R3(config)#router bgp 200
R3(config-bgp)#neighbor 131.4.2.2 remote-as 200
R3(config-bgp)#exit
```

2.R1向R2通告5个BGP路由。

```
R1(config)#router bgp 1011
R1(config-bgp)#network 7.7.7.0 255.255.255.0
R1(config-bgp)#network 8.8.8.0 255.255.255.0
R1(config-bgp)#network 9.9.9.0 255.255.255.0
R1(config-bgp)#network 7.7.8.0 255.255.255.0
R1(config-bgp)#network 7.7.9.0 255.255.255.0
R1(config-bgp)#exit
```

3.R2上配置route-map test1及其中嵌套使用的ACL列表。

```
R2(config)#ipv4-access-list 1
R2(config-ipv4-acl)#rule 1 permit 7.7.7.0 0.0.0.255
R2(config-ipv4-acl)#exit
R2(config)#ipv4-access-list 2
R2(config-ipv4-acl)#rule 1 permit 8.8.8.0 0.0.0.255
R2(config-ipv4-acl)#exit

R2(config)#route-map test1 permit 10
R2(config-route-map)#match ip address 1
R2(config-route-map)#match ip address 2
R2(config-route-map)#set local-preference 30000
R2(config-route-map)#exit
R2(config)#route-map test2 permit 10
R2(config-route-map)#match ip address 1
R2(config-route-map)#match ip metric 5
R2(config-route-map)#match as-path 1
R2(config-route-map)#match community-list 1
R2(config-route-map)#exit
R2(config)#route-map test2 permit 20
R2(config-route-map)#match ip address 2
R2(config-route-map)#set as-path prepend 2
R2(config-route-map)#set local-preference 200
R2(config-route-map)#set next-hop 10.1.1.0
R2(config-route-map)#set origin incomplete
R2(config-route-map)#exit
```

4.R2上将route-map test1应用在连接R1邻居的in方向上，将route-map test2应用在R2连接R3邻居的out方向上。

```
R2(config)#router bgp 200
R2(config-bgp)#neighbor 131.4.1.1 route-map test1 in
R2(config-bgp)#neighbor 131.4.2.1 route-map test2 out
R2(config-bgp)#exit
```

配置验证

1.在步骤2，通告路由后，R2和R3上皆应该能学到5条路由。

```
R2(config)#show ip bgp route
Status codes: * valid, > best, i-internal, s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete

Dest NextHop Metric LocPrf RtPrf Path
*>   7.7.7.0/24  131.4.1.1     0              20     1011 i
*>   7.7.8.0/24  131.4.1.1     0              20     1011 i
*>   7.7.9.0/24  131.4.1.1     0              20     1011 i
*>   8.8.8.0/24  131.4.1.1     0              20     1011 i
*>   9.9.9.0/24  131.4.1.1     0              20     1011 i

R3(config)#show ip bgp route
Status codes: * valid, > best, i-internal, s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete

Dest NextHop Metric LocPrf RtPrf Path
*>i  7.7.7.0/24  131.4.1.1     0     100     200    1011 i
*>i  7.7.8.0/24  131.4.1.1     0     100     200    1011 i
*>i  7.7.9.0/24  131.4.1.1     0     100     200    1011 i
*>i  8.8.8.0/24  131.4.1.1     0     100     200    1011 i
*>i  9.9.9.0/24  131.4.1.1     0     100     200    1011 i
```

2.步骤4，R2上绑定了路由策略后，R2上仅能学到匹配route-map test1当中嵌套的match项的路由7.7.7.0/24和8.8.8.0/24，未匹配到的路由学不到。

3.对应同一条路由策略下，使用多个match项时，macth项之间是与关系，所以route-map test2 permit 10没有匹配到，所以7.7.7.0这条路由不会通告给R3。

4.使用BGP路由策略后的效果：

```
R2(config)#show ip bgp summary /*R2从R1上学习到了2条BGP路由*/
Neighbor   Ver   As   MsgRcvd   MsgSend  Up/Down    State/PfxRcd
131.4.1.1  4     1011 34        33       00:16:23        2
131.4.2.1  4     200  32        33       00:16:23        0
R2(config)#show ip bgp route /*2条BGP路由信息*/
Status codes: * valid, > best, i-internal, s-stale
Origin codes: i-IGP, e-EGP, ?-incomplete

     Dest             NextHop     Metric  LocPrf    RtPrf  Path
*>   7.7.7.0/24       131.4.1.1     0     30000     20     1011 i
*>   8.8.8.0/24       131.4.1.1     0     30000     20     1011 i
```

2条BGP路由的详细信息。

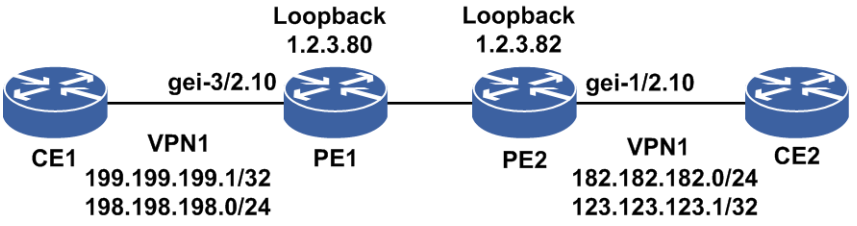
```
R2(config)#show ip bgp route network 7.7.7.0 mask 255.255.255.0
BGP routing table entry for 7.7.7.0/24
  2d18h received from 131.4.1.1 (1.2.3.1)
   origin i,nexthop 131.4.1.1,metric 0,localpref 30000,rtpref 20,best,
   as path [1011]
   as4 path
R2(config)#show ip bgp route network 8.8.8.0 mask 255.255.255.0
BGP routing table entry for 8.8.8.0/24
  2d18h received from 131.4.1.1 (1.2.3.1)
   origin i,nexthop 131.4.1.1,metric 0,localpref 30000,rtpref 20,best,
   as path [1011]
   as4 path
  2d18h advertised to 131.4.2.1 (1.2.3.2)
   origin ?,nexthop 10.1.1.0,metric 0,localpref 200,
   as path [2 1011]
   as4 path
```

11.6.7 VRF 路由策略配置实例

配置说明

VRF路由策略配置实例组网如*图* **11-12**所示。

图 11-12 VRF 路由策略配置实例示意图



1.如*图 11-40*所示建立L3VPN基本组网，PE1和PE2在相同的AS，建立MP-IBGP邻居。

2.PE1上有VRF test1，其中通告了本地Loopback地址生成的Address路由199，和对接CE1的直连路由198。

3.PE2上有VRF test1，其中通告了本地Loopback地址生成的Address路由123，和对接CE2的直连路由182。

4.两个PE上VRF test1路由表当中有本地和远端的路由（182、123和199、 198都有）。

5.PE1上配置VRF test1当中采用route-map路由策略：

对入向的182、123网段路由进行如下策略：允许从VPN邻居导入182.182.182.0 24 ge 32路由。

对出向的199和198网段进行如下策略：允许向VPN邻居通告199.199.199.1 32路由。

6.配置后路由策略生效结果验证。

配置思路

1.配置CE1–PE1–PE2–CE2的L3VPN基本组网环境。

2.两台PE的私网路由表内能学到配置说明中规划的所有路由。

3.在PE1上配置route-map，其中定义将要实施路由策略的路由信息的特征，即定义一组匹配规则。可以以路由信息中的不同属性作为匹配依据进行设置，如目的地址、发布路由信息的路由器地址等。

4.PE1上配置VRF实例中应用route-map，实现对路由的导入/导出、路由发布接收和引入时的策略。

配置过程

1.在PE1和PE2上配置L3VPN基本组网：

PE1的配置如下：

```
PE1(config)#ip vrf test1
PE1(config-vrf-test1)#rd 10:10
PE1(config-vrf-test1)#route-target both 10:10
PE1(config-vrf-test1)#address-family ipv4
PE1(config-vrf-test1-af-ipv4)#exit
PE1(config-vrf-test1)#exit

PE1(config)#interface loopback30
PE1(config-if-loopback30)#ip vrf forwarding test1
PE1(config-if-loopback30)#ip address 199.199.199.1 255.255.255.255
PE1(config-if-loopback30)#exit
PE1(config)#interface gei-3/2.10
PE1(config-if-gei-3/2.10)#ip vrf forwarding test1
PE1(config-if-gei-3/2.10)#ip address 198.198.198.1 255.255.255.0
PE1(config-if-gei-3/2.10)#exit

PE1(config)#vlan-configuration
PE1(config-vlan)#interface gei-3/2.10
PE1(config-subvlan-if-gei-3/2.10)#encapsulation-dot1q 10
PE1(config-subvlan-if-gei-3/2.10)#exit
PE1(config-vlan)#exit

PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 1.2.3.80 255.255.255.255
PE1(config-if-loopback1)#exit

PE1(config)#router bgp 200
PE1(config-bgp)#neighbor 1.2.3.82 remote-as 200
PE1(config-bgp)#neighbor 1.2.3.82 update-source loopback1
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 1.2.3.82 activate
PE1(config-bgp-af)#exit
PE1(config-bgp)#address-family ipv4 vrf test1
PE1(config-bgp-af)#redistribute address
PE1(config-bgp-af)#redistribute connected
PE1(config-bgp-af)#end
```

PE2的配置如下：

```
PE2(config)#ip vrf test1
PE2(config-vrf-test1)#rd 10:10
PE2(config-vrf-test1)#route-target both 10:10
PE2(config-vrf-test1)#address-family ipv4
PE2(config-vrf-test1-af-ipv4)#exit
PE2(config-vrf-test1)#exit

PE2(config)#interface loopback10
PE2(config-if-loopback10)#ip vrf forwarding test1
PE2(config-if-loopback10)#ip address 123.123.123.1 255.255.255.255
PE2(config-if-loopback10)#exit
PE2(config)#interface gei-1/2.10
PE2(config-if-gei-1/2.10)#ip vrf forwarding test1
PE2(config-if-gei-1/2.10)#ip address 182.182.182.1 255.255.255.0
PE2(config-if-gei-1/2.10)#exit

PE2(config)#vlan-configuration
PE2(config-vlan)#interface gei-1/2.10
PE2(config-subvlan-if-gei-1/2.10)#encapsulation-dot1q 10
PE2(config-subvlan-if-gei-1/2.10)#exit
PE2(config-vlan)#exit

PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 1.2.3.82 255.255.255.255
PE2(config-if-loopback1)#exit

PE2(config)#router bgp 200
PE2(config-bgp)#neighbor 1.2.3.80 remote-as 200
PE2(config-bgp)#neighbor 1.2.3.80 update-source loopback1
PE2(config-bgp)#address-family vpnv4
```

```
PE2(config-bgp-af)#neighbor 1.2.3.80 activate
PE2(config-bgp-af)#exit
PE2(config-bgp)#address-family ipv4 vrf test1
PE2(config-bgp-af)#redistribute address
PE2(config-bgp-af)#redistribute connected
PE2(config-bgp-af)#end
```

2.检查PE1、PE2上的VRF路由。

PE1上显示：

```
PE1(config)#show ip forwarding route vrf test1
IPv4 Routing Table:
Status codes: *valid, >best
   Dest            Gw            Interface          Owner      Pri Metric
*> 123.123.123.1/32   1.2.3.82       posgroup2          BGP        200 0
*> 182.182.182.0/24   1.2.3.82       posgroup2          BGP        200 0
*> 182.182.182.1/32   1.2.3.82       posgroup2          BGP        200 0
*> 198.198.198.0/24   198.198.198.1   gei-3/2.10         Direct     0   0
*> 198.198.198.1/32   198.198.198.1   gei-3/2.10         Address    0   0
*> 199.199.199.1/32   199.199.199.1   loopback30         Address    0   0
```

PE2上显示：

```
PE2(config)#show ip forwarding route vrf test1
IPv4 Routing Table:
Status codes: *valid, >best
   Dest            Gw            Interface          Owner      Pri Metric
*> 123.123.123.1/32   123.123.123.1   loopback10         Address    0   0
*> 182.182.182.0/24   182.182.182.1   gei-1/2.10         Direct     0   0
*> 182.182.182.1/32   182.182.182.1   gei-1/2.10         Address    0   0
*> 198.198.198.0/24   1.2.3.80       posgroup2          BGP        200 0
*> 198.198.198.1/32   1.2.3.80       posgroup2          BGP        200 0
*> 199.199.199.1/32   1.2.3.80       posgroup2          BGP        200 0
```

3.在PE1上配置route-map，并应用到VRF当中。

配置route-map test1，用于限制export方向的路由通告。

```
PE1(config)#ip prefix-list test1 seq 5 permit 199.199.199.1 32
PE1(config)#route-map test1
PE1(config-route-map)#match ip address prefix-list test1
PE1(config-route-map)#exit
```

配置route-map test2，用于限制import方向的路由通告。

```
PE1(config)#ip prefix-list test2 seq 5 permit 182.182.182.0 24 ge 32
PE1(config)#route-map test2
PE1(config-route-map)#match ip address prefix-list test2
PE1(config-route-map)#exit
```

在vrf test1当中应用route-map。

```
PE1(config)#ip vrf test1
PE1(config-vrf-test1)#address-family ipv4
PE1(config-vrf-test1-af-ipv4)#export map test1
PE1(config-vrf-test1-af-ipv4)#import map test2
PE1(config-vrf-test1-af-ipv4)#end
```

4.在PE1、PE2上检查VRF路由表，看VRF路由策略是否生效。

PE1上查看：

```
PE1(config)#show ip forwarding route vrf test1
IPv4 Routing Table:
status codes: *valid, >best
 Dest Gw Interface Owner Pri Metric
*> 182.182.182.1/32 1.2.3.82 posgroup2 bgp 200 0
```

```
  *> 198.198.198.0/24 198.198.198.1 gei-3/2.10 direct 0 0
  *> 198.198.198.1/32 198.198.198.1 gei-3/2.10 address 0 0
  *> 199.199.199.1/32 199.199.199.1 loopback30 address 0 0
```

PE2上查看：

```
  PE2(config)#show ip forwarding route vrf test1
  IPv4 Routing Table:
  status codes: *valid, >best
   Dest Gw Interface Owner Pri Metric
  *> 123.123.123.1/32 123.123.123.1 loopback10 address 0 0
  *> 182.182.182.0/24 182.182.182.1 gei-1/2.10 direct 0 0
  *> 182.182.182.1/32 182.182.182.1 gei-1/2.10 address 0 0
  *> 199.199.199.1/32 1.2.3.80 posgroup2 bgp 200 0
```

配置验证

PE1上配置成功，使用**show running-config**命令时应有如下配置：

```
PE1#show running-config bgp
!<bgp>
router bgp 200
  neighbor 1.2.3.82 remote-as 200
  neighbor 1.2.3.82 activate
  neighbor 1.2.3.82 update-source loopback1
  address-family ipv4 vrf test1
    redistribute address
    redistribute connected
  $
  address-family vpnv4
  neighbor 1.2.3.82 activate
  $
$
!</bgp>

PE1#show running-config vrf | begin test1
ip vrf test1
  rd 10:10
  route-target import 10:10
  route-target export 10:10
  address-family ipv4
    import map test2
    export map test1
  $
$
!</vrf>

PE1#show route-map test1
[route-map test1] IP type: IPv4
route-map test1 permit 10
  match ip address prefix-list test1
PE1#show route-map test2
[route-map test2] IP type: IPv4
route-map test2 permit 10
  match ip address prefix-list test2
PE1#show ip prefix-list test1
ip prefix-list test1 :
    seq 5 permit 199.199.199.1 32
PE1#show ip prefix-list test2
ip prefix-list test2 :
    seq 5 permit 182.182.182.0 24 ge 32
```

从export方向上（路由导入），PE1上的vrf test1路由表应该从使用VRF路由策略前的：

```
PE1(config)#show ip forwarding route vrf test1
IPv4 Routing Table:
Status codes: *valid, >best
```

```
   Dest             Gw             Interface          Owner      Pri Metric
*> 123.123.123.1/32   1.2.3.82       posgroup2          BGP        200 0
*> 182.182.182.0/24   1.2.3.82       posgroup2          BGP        200 0
*> 182.182.182.1/32   1.2.3.82       posgroup2          BGP        200 0
*> 198.198.198.0/24   198.198.198.1   gei-3/2.10         Direct     0   0
*> 198.198.198.1/32   198.198.198.1   gei-3/2.10         Address    0   0
*> 199.199.199.1/32   199.199.199.1   loopback30         Address    0   0
```

变更为：

```
PE1(config)#show ip forwarding route vrf test1
IPv4 Routing Table:
Status codes: *valid, >best
   Dest             Gw             Interface          Owner      Pri Metric
*> 182.182.182.1/32   1.2.3.82       posgroup2          BGP        200 0
*> 198.198.198.0/24   198.198.198.1   gei-3/2.10         Direct     0   0
*> 198.198.198.1/32   198.198.198.1   gei-3/2.10         Address    0   0
*> 199.199.199.1/32   199.199.199.1   loopback30         Address    0   0
```

其中路由导入（import方向）的路由策略test2，过滤了从对端PE2通告过来的两条路由：

```
*> 123.123.123.1/32   1.2.3.82       posgroup2          BGP        200 0
*> 182.182.182.0/24   1.2.3.82       posgroup2          BGP        200 0
```

因为在route-map test2当中指定了匹配**ip prefix-list test2 seq 5 permit 182.182.182.0 24 ge 32**的路由才进行学习，即：

```
*> 182.182.182.1/32   1.2.3.82       posgroup2          BGP        200 0
```

PE1上使用路由导出（export方向）的路由策略test1，对出向路由通告进行了策略，所以该策略使用后，在PE2上vrf test1路由表应该从原先的：

```
PE2(config)#show ip forwarding route vrf test1
IPv4 Routing Table:
Status codes: *valid, >best
   Dest             Gw             Interface          Owner      Pri Metric
*> 123.123.123.1/32   123.123.123.1   loopback10          Address    0   0
*> 182.182.182.0/24   182.182.182.1   gei-1/2.10          Direct     0   0
*> 182.182.182.1/32   182.182.182.1   gei-1/2.10          Address    0   0
*> 198.198.198.0/24   1.2.3.80       posgroup2          BGP        200 0
*> 198.198.198.1/32   1.2.3.80       posgroup2          BGP        200 0
*> 199.199.199.1/32   1.2.3.80       posgroup2          BGP        200 0
```

变化为：

```
PE2(config)#show ip forwarding route vrf test1
IPv4 Routing Table:
Status codes: *valid, >best
   Dest             Gw             Interface          Owner      Pri Metric
*> 123.123.123.1/32   123.123.123.1   loopback10          Address    0   0
*> 182.182.182.0/24   182.182.182.1   gei-1/2.10          Direct     0   0
*> 182.182.182.1/32   182.182.182.1   gei-1/2.10          Address    0   0
*> 199.199.199.1/32   1.2.3.80       posgroup2          BGP        200 0
```

可以看到从远端1.2.3.80学习到的路由仅有一条：

```
*> 199.199.199.1/32   1.2.3.80       posgroup2          BGP        200 0
```

这一条是匹配route-map test1当中定义的match条件ip prefix-list test1 seq 5 permit 199.199.199.1 32的。

匹配不上的两条被过滤掉，这两条为：

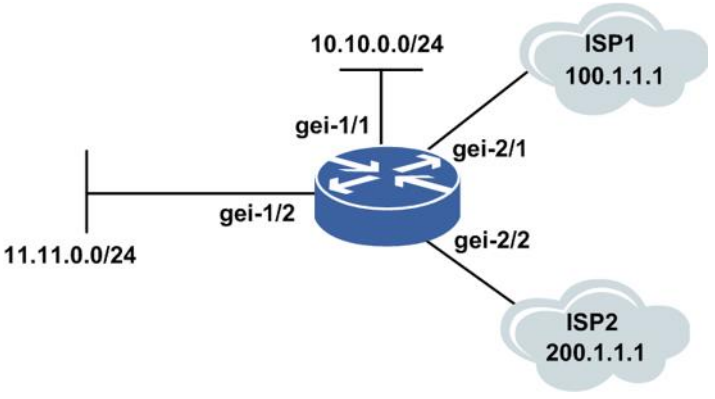
```
*> 198.198.198.0/24   1.2.3.80       posgroup2          BGP        200 0
*> 198.198.198.1/32   1.2.3.80       posgroup2          BGP        200 0
```

11.6.8 本地不同接口接入的策略路由配置实例

配置说明

如*图 11-13*所示，路由器通过不同的接口接入两个子网的用户，而且有两个ISP出口可供使用，要求根据用户的IP地址选择不同的出口，IP地址属于10.10.0.0/24子网的用户业务使用ISP1出口，而IP地址属于11.11.0.0/24子网的用户业务使用ISP2出口。

图 11-13 本地不同接口接入的策略路由配置实例



配置思路

1.配置接口地址。

2.建立ACL定义要控制的流量。

3.创建route-map，关联ACL并定义动作。

4.将route-map关联至相应的接口上。

配置过程

IR12000上的配置如下：

```
inspur(config)#interface gei-1/1
inspur(config-if-gei-1/1)#description To User1
inspur(config-if-gei-1/1)#ip address 10.10.0.254 255.255.255.0
inspur(config-if-gei-1/1)#exit

inspur(config)#interface gei-1/2
inspur(config-if-gei-1/2)#description To User2
inspur(config-if-gei-1/2)#ip address 11.11.0.254 255.255.255.0
inspur(config-if-gei-1/2)#exit

inspur(config)#interface gei-2/1
inspur(config-if-gei-2/1)#description To ISP1
inspur(config-if-gei-2/1)#ip address 100.1.1.2 255.255.255.252
inspur(config-if-gei-2/1)#exit

inspur(config)#interface gei-2/2
inspur(config-if-gei-2/2)#description To ISP2
inspur(config-if-gei-2/2)#ip address  200.1.1.2 255.255.255.252
```

```
inspur(config-if-gei-2/2)#exit

inspur(config)#ip route 0.0.0.0 0.0.0.0 100.1.1.1
inspur(config)#ipv4-access-list 10
inspur(config-ipv4-acl)#rule 1 permit 10.10.0.0 0.0.0.255
inspur(config-ipv4-acl)#exit

inspur(config)#ipv4-access-list 20
inspur(config-ipv4-acl)#rule 1 permit 11.11.0.0 0.0.0.255
inspur(config-ipv4-acl)#exit

/*将与ACL 10匹配的报文转发到100.1.1.1*/
inspur(config)#route-map source-ip permit 10
inspur(config-route-map)#match ip address 10
inspur(config-route-map)#set ip next-hop 100.1.1.1
inspur(config-route-map)#exit

/*将与ACL 20匹配的报文转发到200.1.1.1*/
inspur(config)#route-map source-ip permit 20
inspur(config-route-map)#match ip address 20
inspur(config-route-map)#set ip next-hop 200.1.1.1
inspur(config-route-map)#exit

/*将route-map source-ip绑定至接口上*/
inspur(config)#ip policy interface gei-1/1 route-map source-ip

/*将route-map source-ip绑定至接口上*/
inspur(config)#ip policy interface gei-1/2 route-map source-ip
```

在本案例中，会出现以下三种情况：

1.当ISP1和ISP2出口均正常时，10.10.0.0/24和11.11.0.0/24子网的用户业务分别走ISP1、ISP2出口。

2.当ISP1正常、ISP2出口异常时，两个子网的用户业务都走ISP1出口，此时11.11.0.0/24子网的用户业务利用的是默认路由。

3.当ISP1异常、ISP2出口正常时，11.11.0.0/24子网的用户业务正常，而10.10.0.0/24子网的用户业务中断。

配置验证

查看route-map的配置内容：

```
inspur(config)#show route-map source-ip
[route-map source-ip] IP type: IPv4
route-map source-ip permit 10
match ip address 10
set ip next-hop 100.1.1.1
route-map source-ip permit 20
match ip address 20
set ip next-hop 200.1.1.1
```

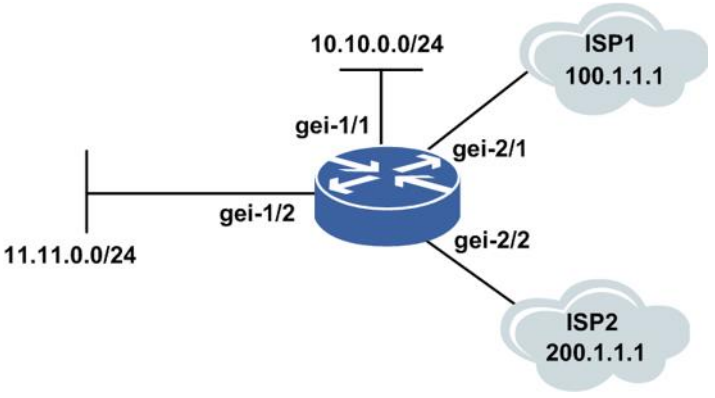
11.6.9 本地同一个接口接入的策略路由配置实例

配置说明

如*图 11-14*所示，当不同子网的用户通过路由器的同一个接口接入时，策略路由器的

配置要做相应的变化。

图 11-14 本地同一个接口接入的策略路由配置实例



配置思路

1.配置接口地址。

2.建立ACL定义要控制的流量。

3.创建route-map，关联ACL并定义动作。

4.将route-map关联至相应的接口上。

配置过程

IR12000的配置：

```
inspur(config)#interface gei-1/1
inspur(config-if-gei-1/1)#description To User
inspur(config-if-gei-1/1)#ip address 192.168.1.1 255.255.255.252
inspur(config-if-gei-1/1)#exit

inspur(config)#interface gei-2/1
inspur(config-if-gei-2/1)#description To ISP1
inspur(config-if-gei-2/1)#ip address 100.1.1.2 255.255.255.252
inspur(config-if-gei-2/1)#exit

inspur(config)#interface gei-2/2
inspur(config-if-gei-2/2)#description To ISP2
inspur(config-if-gei-2/2)#ip address 200.1.1.2 255.255.255.252
inspur(config-if-gei-2/2)#exit

inspur(config)#ip route 10.10.0.0 255.255.255.0 192.168.1.2
inspur(config)#ip route 11.11.0.0 255.255.255.0 192.168.1.2
```

配置route-map的内容：

```
/*配置Route-map中应用的ACL列表信息*/
inspur(config)#ipv4-access-list 10
inspur(config-ipv4-acl)#rule 1 permit 10.10.0.0 0.0.0.255
inspur(config-ipv4-acl)#exit

inspur(config)#ipv4-access-list 20
inspur(config-ipv4-acl)#rule 1 permit 11.11.0.0 0.0.0.255
inspur(config-ipv4-acl)#exit
```

```
/*配置Route-map信息，Sequence号分别为10、20*/
inspur(config)#route-map source-ip permit 10
inspur(config-route-map)#match ip address 10

/*将与ACL 10匹配的报文转发到100.1.1.1，200.1.1.1作为备用出口*/
inspur(config-route-map)#set ip next-hop 100.1.1.1 200.1.1.1
inspur(config-route-map)#exit
inspur(config)#route-map source-ip permit 20
inspur(config-route-map)#match ip address 20

/*将与ACL 20匹配的报文转发到200.1.1.1，100.1.1.1作为备用出口*/
inspur(config-route-map)#set ip next-hop 200.1.1.1 100.1.1.1
inspur(config-route-map)#exit
```

配置将route-map应用于接口：

```
/*将Route-map Source-ip绑定至接口上*/
inspur(config)#ip policy interface gei-1/1 route-map source-ip
```

本例中，两个ISP出口互为备用，会出现以下两种情况：

1.当ISP1和ISP2出口均正常时，10.10.0.0/24和11.11.0.0/24子网的用户业务分别走ISP1、ISP2出口。

2.当其中一个出口故障时，相应子网的用户业务将走备用出口。所以只要两个出口不同时出现异常，业务将不会中断。

配置验证

查看route-map的配置内容：

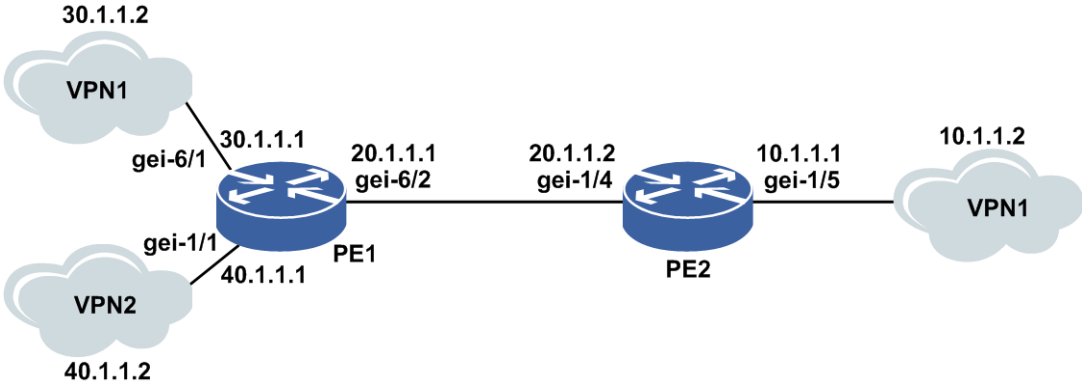
```
inspur(config)#show route-map source-ip
[route-map source-ip] IP type: IPv4
route-map source-ip permit 10
  match ip address 10
  set ip next-hop 100.1.1.1 200.1.1.1
route-map source-ip permit 20
  match ip address 20
  set ip next-hop 200.1.1.1 100.1.1.1
```

11.6.10 远端 VRF 策略路由配置实例

配置说明

如*图 11-15*所示，路由器通过不同的接口接入多个子网的用户，若vpn1内的某些用户需要访问vpn2内的网络，可以通过远端VRF策略路由来实现。

图 11-15 远端 VRF 策略路由配置实例拓扑图



配置过程

PE1上的配置如下：

```
/*接口配置*/
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 1.2.3.30 255.255.255.255
PE1(config-if-loopback1)#exit

PE1(config)#ip vrf vpn1

PE1(config-vrf-vpn1)#rd 1:1
PE1(config-vrf-vpn1)#route-target both 1:1
PE1(config-vrf-vpn1)#address-family ipv4
PE1(config-vrf-vpn1-af-ipv4)#exit
PE1(config-vrf-vpn1)#exit
PE1(config)#ip vrf vpn2
PE1(config-vrf-vpn2)#rd
PE1(config-vrf-vpn2)#rd 1:2
PE1(config-vrf-vpn2)#route-target both 1:2
PE1(config-vrf-vpn1)# address-family ipv4
PE1(config-vrf-vpn1-af-ipv4)#exit
PE1(config-vrf-vpn1)#exit

PE1(config)#interface gei-6/1
PE1(config-if-gei-6/1)#description to vpn1
PE1(config-if-gei-6/1)#ip vrf forwarding vpn1
PE1(config-if-gei-6/1)#ip address 30.1.1.1 255.255.255.0
PE1(config-if-gei-6/1)#exit

PE1(config)#interface gei-1/1
PE1(config-if-gei-1/1)#description to vpn2
PE1(config-if-gei-1/1)#ip vrf forwarding vpn2
PE1(config-if-gei-1/1)#ip address 40.1.1.1 255.255.255.0
PE1(config-if-gei-1/1)#exit

PE1(config)#interface gei-6/2
PE1(config-if-gei-6/2)#ip address 20.1.1.1 255.255.255.0
PE1(config-if-gei-6/2)#exit

/*配置OSPF*/
PE1(config)#router ospf 1 vrf vpn1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 30.1.1.0 0.0.0.255
PE1(config-ospf-1-area-0)#exit
PE1(config)#router ospf 2 vrf vpn2
PE1(config-ospf-2)#area 0
PE1(config-ospf-2-area-0)#network 40.1.1.0 0.0.0.255
PE1(config-ospf-2-area-0)#exit
```

```
PE1(config)#router ospf 3
PE1(config-ospf-3-area-0)#area 0
PE1(config-ospf-3-area-0)#network 1.2.3.30 0.0.0.0
PE1(config-ospf-3-area-0)#network 20.1.1.0 0.0.0.255
PE1(config-ospf-3-area-0)#exit

/*配置BGP*/
PE1(config)#router bgp 1
PE1(config-bgp)#neighbor 1.2.3.29 remote-as 2
PE1(config-bgp)#neighbor 1.2.3.29 ebgp-multihop ttl 8
PE1(config-bgp)#neighbor 1.2.3.29 update-source loopback1
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 1.2.3.29 activate
PE1(config-bgp-af)#exit
PE1(config-bgp)#address-family ipv4 vrf vpn1
PE1(config-bgp-af)#redistribute ospf-int 1
PE1(config-bgp-af)#redistribute ospf-ext 1
PE1(config-bgp-af)#exit
PE1(config-bgp)#address-family ipv4 vrf vpn2
PE1(config-bgp-af)#redistribute ospf-int 2
PE1(config-bgp-af)#redistribute ospf-ext 2
PE1(config-bgp-af)#exit
PE1(config-bgp)#exit

/*配置LDP*/
PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#interface gei-6/2
PE1(config-ldp-1-if-gei-6/2)#exit
PE1(config-ldp-1)#router-id loopback1 force
PE1(config-ldp-1)#exit
```

PE2上的配置如下：

```
/*配置接口*/
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 1.2.3.29 255.255.255.255
PE2(config-if-loopback1)#exit

PE2(config)#ip vrf vpn1
PE2(config-vrf-vpn1)#rd 1:1
PE2(config-vrf-vpn1)#route-target both 1:1
PE2(config-vrf-vpn1)#address-family ipv4
PE2(config-vrf-vpn1-af-ipv4)#exit
PE2(config-vrf-vpn1)#exit
PE2(config)#ip vrf vpn2
PE2(config-vrf-vpn2)#rd
PE2(config-vrf-vpn2)#rd 1:2
PE2(config-vrf-vpn2)#route-target both 1:2
PE2(config-vrf-vpn2)#address-family ipv4
PE2(config-vrf-vpn2-af-ipv4)#exit
PE2(config-vrf-vpn2)#exit
PE2(config)#interface gei-1/4
PE2(config-if-gei-1/4)#ip address 20.1.1.2 255.255.255.0
PE2(config-if-gei-1/4)#exit

PE2(config)#interface gei-1/5
PE2(config-if-gei-1/5)#description to vpn1
PE2(config-if-gei-1/5)#ip vrf forwarding vpn1
PE2(config-if-gei-1/5)#ip address 10.1.1.1 255.255.255.0
PE2(config-if-gei-1/5)#exit

/*配置OSPF*/
PE2(config)#router ospf 16
PE2(config-ospf-16)#area 0
PE2(config-ospf-16-area-0)#network 1.2.3.29 0.0.0.0
PE2(config-ospf-16-area-0)#network 20.1.1.0 0.0.0.255
PE2(config-ospf-16-area-0)#exit
```

```
/*配置BGP*/
PE2(config)#router bgp 2
PE2(config-bgp)#neighbor 1.2.3.30 remote-as 1
PE2(config-bgp)#neighbor 1.2.3.30 ebgp-multihop ttl 8
PE2(config-bgp)#neighbor 1.2.3.30 update-source loopback1
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 1.2.3.30 activate
PE2(config-bgp-af)#exit
PE2(config-bgp)#address-family ipv4 vrf vpn1
PE2(config-bgp-af)#redistribute ospf-int 16
PE2(config-bgp-af)#redistribute ospf-ext 16
PE2(config-bgp-af)#exit
PE2(config-bgp)#exit

/*配置LDP*/
PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#interface gei-1/4
PE2(config-ldp-1-if-gei-1/4)#exit
PE2(config-ldp-1)#router-id loopback1 force
PE2(config-ldp-1)#exit
```

配置route-map及应用过程如下：

```
/*配置route-map中ACL列表信息*/
PE2(config)#ipv4-access-list 2
PE2(config-ipv4-acl)#rule 1 permit 10.1.1.2 0.0.0.0
PE2(config-ipv4-acl)#exit

/*配置route-map信息*/
PE2(config)#route-map test
PE2(config-route-map)#match ip address 2
PE2(config-route-map)#set vrf vpn2
PE2(config-route-map)#exit

/*将route-map应用到PE2的gei-1/5接口上*/
PE2(config)#ip policy interface gei-1/5 route-map test
```

配置验证

当PE1与PE2之间的邻居建立完成后，查看vpn1下存在的路由如下：

```
PE2(config)#show ip protocol routing vrf vpn1
Routes of vpn:
status codes: *valid, >best, s-stale

    Dest           NextHop      Intag    Outtag    RtPrf    Protocol
*>  10.1.1.0/24     10.1.1.1     163845    notag     0       connected
*>  10.1.1.1/32     10.1.1.1     163844    notag     0       connected
*>  15.15.15.0/24    1.2.3.30     163914    163975    20      bgp-ext
*>  15.15.16.0/24    1.2.3.30     163913    163974    20      bgp-ext
*>  15.15.17.0/24    1.2.3.30     163912    163973    20      bgp-ext
*>  15.15.18.0/24    1.2.3.30     163911    163972    20      bgp-ext
*>  15.15.19.0/24    1.2.3.30     163910    163971    20      bgp-ext
*>  15.15.20.0/24    1.2.3.30     163909    163970    20      bgp-ext
*>  15.15.21.0/24    1.2.3.30     163908    163969    20      bgp-ext
*>  15.15.22.0/24    1.2.3.30     163907    163968    20      bgp-ext
*>  15.15.23.0/24    1.2.3.30     163906    163967    20      bgp-ext
*>  15.15.24.0/24    1.2.3.30     163905    163966    20      bgp-ext
*>  30.1.1.0/24     1.2.3.30     163903    163962    20      bgp-ext
*>  30.1.1.2/32     1.2.3.30     163904    163965    20      bgp-ext
```

查看vpn2下存在的路由如下：

```
PE2(config)#show ip protocol routing vrf vpn2
Routes of vpn:
status codes: *valid, >best, s-stale
    Dest           NextHop      Intag    Outtag   RtPrf    Protocol
*>  14.14.14.0/24   1.2.3.30     163926   163993   20       bgp-ext
*>  14.14.15.0/24   1.2.3.30     163925   163992   20       bgp-ext
*>  14.14.16.0/24   1.2.3.30     163934   164001   20       bgp-ext
*>  14.14.17.0/24   1.2.3.30     163933   164000   20       bgp-ext
*>  14.14.18.0/24   1.2.3.30     163932   163999   20       bgp-ext
*>  14.14.19.0/24   1.2.3.30     163931   163998   20       bgp-ext
*>  14.14.20.0/24   1.2.3.30     163930   163997   20       bgp-ext
*>  14.14.21.0/24   1.2.3.30     163929   163996   20       bgp-ext
*>  14.14.22.0/24   1.2.3.30     163928   163995   20       bgp-ext
*>  14.14.23.0/24   1.2.3.30     163927   163994   20       bgp-ext
```

在本案例中，如果PE1上的vpn1内部分用户需要访问vpn2的网络，可以通过配置route-map的match项，将需要访问的用户通过ACL规则配置进去，并设置route-map的set项，具体配置参见上述配置，注意的是，在PE1上要有访问vpn2的私网路由。

例如：10.1.1.2的用户想访问14.14.14.0/24网段，但是10.1.1.2用户是属于vpn1中的，而14.14.14.0网段是vpn2所属的网段，在PE2上用**show ip protocol routing vrf vpn2**命令能够查看到14.14.14.0网段的路由。此时可以通过远端VRF策略路由实现，set项配置为：**set vrf vpn2**即可。

11.7 EEM

EEM（Embeded Event Manager，嵌入式事件管理器）提供了一种分布式的、可扩展的、 可根据用户需求而灵活定制的，用于进行事件监控和故障恢复的机制。利用这种机制， 当被监控的事件发生，或者是达到某个门限值时，EEM提供了进行消息报告以及采取相 应动作的能力。一个完整的EEM的操作被称作 EEM Policy （EEM策略），EEM Policy包 括定义监控的事件以及当被监控事件发生时所要执行的动作。

随着客户的网络规模日益庞大，单纯依靠现有网管架构下网管服务器与网络设备之间的 主从模式，很难解决网络管理的成本、复杂性、扩展性以及出现故障时处理的及时性等 这些越来越有挑战性的问题。因此未来的网络管理需求要求网络设备本身具有更高的智 能，能够根据各种不同的预定条件或网管人员的要求对网络设备本身进行不同的操作， 减少网管人员的维护压力、提高对网络故障的响应速度。

EEM从根本上改变了网络设备的管理方式，使得网络设备由现有网络管理架构中的被动 报告者和应答者，转变成为积极主动的参与者。让网络设备本身变得更为智能、灵活， 帮助网络的运维人员更轻松、更及时、更准确地进行网络优化和故障排除。未来EEM的 发展将继续延伸网络设备的智能，实现构建真正“自诊断、自愈合”的网络的目标。

11.7.1 配置 EEM

配置EEM的变量和脚本文件。

1.配置环境

命令	功能
inspur(config)#**event manager environment** <variable-name> <value>	配置EEM环境变量。

	*<variable-name>*是变量名称，长 度为1~64个字符 *value*是变量值，长度为1~200个字符

2.配置脚本

步骤	命令	功能
1	inspur(config)#**event manager policy** *<policy-filename>* >	加载tcl脚本文件
2	inspur(config)#event manager run <policy-filename>	手动运行tcl脚本。<policy-filename>存 放 目 录为policy-filename

3.维护EEM

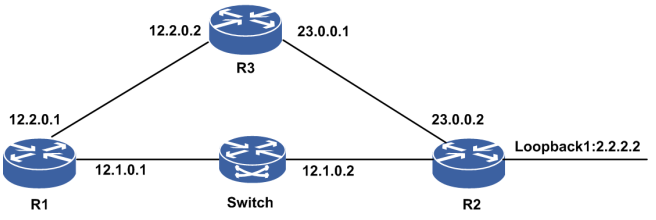
步骤	命令	功能
1	inspur#**debug event manager** {**all** | **tcl cli-library**}	打开EEM debug功能
2	inspur#**show event manager policy registered**	查看已经加载tcl脚本
3	inspur#**show event manager environment**	查看EEM环境变量

11.7.2 NONE 类型 EEM 配置实例

配置说明

如*图 11-16*所示，R1到R2 loopback1有两条路径，分别为p1：R1--SW--R2和p2：R1--R3--R2，其中R1--SW--R2路径优先，R1配置ping检测，检测R1--Swith--R2链路 是否可达。

图 11-16 EEM 配置实例



配置思路

每次执行tcl脚本时检测当前ping检测的状态，若状态为UP，则提高p1路由的优先级，使 其优先p2；若状态为down，则降低p1路由的优先级，使p2优先。

配置过程

1.R1配置2.2.2.2/32两条静态路由，下一跳分别为R2和R3，其中下一跳R2的路由优先。

```
ip route 2.2.2.2 255.255.255.255 12.1.0.2
ip route 2.2.2.2 255.255.255.255 12.2.0.2 2 metric 2
```

2.R1配置ping检测，检测下一跳R2是否可达。

```
detect-group 1
    loop-time 5
    list 1
       item 1 12.1.0.2
    $
$
```

3.编写none类型tcl脚本。

route.tcl：ping检测状态为down时，降低路由优先级；ping检测状态为up时，提高路 由优先级。

```
::eem::event_register_none
#
#
namespace imports
#
namespace import ::eem::*
#
# Body of policy
#
# when the track ping-detect status is down, we reduce the priority of the
static route
# when the track ping-detect status is up, we raise the priority of the static
route
#
::eem::event_register_none
#
# namespace imports
#
namespace import ::eem::*
#
# Body of policy


if [catch {cli_open} result] {
error $result $errorInfo
} else {
array set cli $result

}
cli_exec $cli(fd) "conf t"
cli_write $cli(fd) "show ping-detect detail group 1 "
set len 1
while {$len > 0} {
set info [cli_read_line $cli(fd)]
set info [string trim $info]
regsub -all {[[:blank:]]+} $info " " info set status [lindex [split $info]
1]
set len [string length $info]
if {0 == [string compare $status "Down"]} {
cli_exec $cli(fd) "ip route 2.2.2.2 255.255.255.255 12.1.0.2 metric 10"
break
}
if {0 == [string compare $status "Up"]} {
cli_exec $cli(fd) "ip route 2.2.2.2 255.255.255.255 12.1.0.2"
break
}
}
```

4.拷贝tcl脚本到设备/datadisk0/eem目录下。

```
inspur#copy ftp vrf mng //169.1.105.105/route.tcl@zsr:zsr root:
/datadisk0/eem/route.tcl
```

5.加载tcl脚本。

```
inspur(config)#event manager policy route.tcl
```

配置验证

1.断开Switch和R2之间的链路，运行tcl脚本。

```
inspur(config)#event manager run route.tcl
```

2.执行**show running-config static**命令，查看路由情况。

```
R1(config)#show running-config static
!<static>
ip route 2.2.2.2 255.255.255.255 12.1.0.2 metric 10
ip route 2.2.2.2 255.255.255.255 12.2.0.2 metric 2
!</static>
R1(config)#show ip forwarding route static
IPv4 Routing Table:
Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
         MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
         ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
         GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
         GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
Status codes: *valid, >best;
Dest           Gw           Interface           Owner           Pri  Metric
  *> 2.2.2.2/32  12.2.0.2     gei-2/6             Static            1     2
```

3.恢复switch和R2之间的链路，运行tcl脚本。

```
inspur(config)#event manager run route.tcl
```

4.执行show running-config static命令，查看路由情况。

```
R1(config)#show running-config static

  !<static>
  ip route 2.2.2.2 255.255.255.255 12.1.0.2
  ip route 2.2.2.2 255.255.255.255 12.2.0.2 metric 2
  !</static>
  R1(config)#show ip forwarding route static
  IPv4 Routing Table:
  Headers: Dest: Destination,  Gw: Gateway,  Pri: Priority;
  Codes  : BROADC: Broadcast, USER-I: User-ipaddr, USER-S: User-special,
           MULTIC: Multicast, USER-N: User-network, DHCP-D: DHCP-DFT,
           ASBR-V: ASBR-VPN, STAT-V: Static-VRF, DHCP-S: DHCP-static,
           GW-FWD: PS-BUSI, NAT64: Stateless-NAT64, LDP-A: LDP-area,
           GW-UE: PS-USER, P-VRF: Per-VRF-label, TE: RSVP-TE;
  Status codes: *valid, >best;
  Dest           Gw           Interface           Owner           Pri Metric
  *> 2.2.2.2/32  12.1.0.2     gei-2/2             Static           1    0
```

12 IPv6

12.1 IPv6 基础

IPv6（互联网协议第6版）是互联网协议的一个新版本，相对于IPv4主要改变如下：

·扩展的寻址能力

·简化的头格式

·对扩展和选项的增强支持

·流标签能力

·认证和保密能力

相比于近乎枯竭的IPv4地址，IPv6提供128位的地址空间，能提供巨大的地址容量：

·共有2^{128}个不同的IPv6地址。

·若按土地面积分配，每平方厘米可获得2.2×10^{20}个地址。

IPv6地址耗尽的机会是很小的。在可预见的很长时期内，IPv6的128位地址长度形成的巨大的地址空间能够为所有可以想象出的网络设备提供一个全球唯一的地址。

12.1.1 配置 IPv6

本节介绍IPv6基础功能的配置，包括配置ICMPv6和配置TCPv6。

1.配置ICMPv6。

如果一个路由器由于某些原因（查不到路由或者报文中的三层协议号错误等）不能处理一个IP包，则可能会产生ICMP错误报文，并直接回送到包的源节点，源节点将采取一些办法来纠正所报告的错误状态。

步骤	命令	功能
1	`inspur(config)#`**interface** *<interface-name>*	进入接口配置模式
2	`inspur(config-if-interface-name)#`**ipv6 forward unreachable**	通过配置该命令，转发面会把未知协议的报文或者查不到路由的报文上送控制面，由控制面给源节点回复一个ICMP不可达报文 缺省情况下，该功能不使能（触发ICMPv6错误报文的原包默认是在转发面丢弃的）
3	`inspur(config)#`**icmp-config**	进入ICMP配置模式

步骤	命令	功能
4	inspur(config-icmp)#**interface** {**byname** <*interface-byname*>|<*interface-name*>}	进入ICMP接口配置模式
5	inspur(config-icmp-if-interface-name)#**ipv6 unreachable**	使接口发送ICMPv6报文不可达的功能有效，该功能默认开启

<*interface-byname*>：接口别名，最长32字符。

<*interface-name*>：接口名称，字符类型，长度为1-32。

2.配置TCPv6。

TCPv6是基于IPv6的TCP连接，功能与TCPv4相同，这里不再赘述。

命令	功能
inspur(config)#**ipv6 tcp synwait-time** <*wait-time*>	设置等待试探建立一个TCP连接的时长，对以后建立的TCP连接起作用，范围：30~80，单位：秒，缺省：75秒
inspur(config)#**ipv6 tcp window-size** <*wait-size*>	设置TCP侦听方窗口大小，对当前已经建立的TCP连接无效，范围100~65535，单位：字节，缺省：65535字节
inspur(config)#**ipv6 tcp finwait-time** <*wait-time*>	设置等待关闭一个TCP连接的时长，范围：300~675，单位：秒，缺省：675秒
inspur(config)#**ipv6 tcp queuemax** <*packet-numbers*>	设置TCP最大输出队列长度，对当前已经建立的连接无效，范围：5~50，单位：包，缺省：5个

3.验证配置结果。

IPv6为提高传输效率，不支持中间节点分片。当报文在中间节点转发时，报文长度大于中间节点接口的IPv6 MTU，中间节点会发送ICMPv6错误报文通知给源节点路径上的MTU值，即PMTU。这样，报文发包时会在源节点进行分片。

命令	功能
inspur#**show ipv6 pmtu**	显示本设备上学习到的MTU值
inspur#**show tcp6 brief**	显示所有TCPv6连接的简要信息
inspur#**show tcp6 config**	显示TCPv6配置参数信息
inspur#**show tcp6 statistics**	显示TCPv6层的统计参数
inspur#**show tcp6 tcb** <*tcb-index*>	显示指定TCB对应TCPv6连接的相关参数

4.维护IPv6。

命令	功能
inspur#**clear tcp6 connect** {<*local-ipv6-address*>| **vrf** <*vrf-name*><*local-ipv6-address*>}<*local-port*><*remote-ipv6-address*><*remote-port*>	清除IPv6 TCP连接，包括Telnet，FTP，BGP等基于IPv6 TCP的连接
inspur#**clear tcp6 statistics**	清除IPv6 TCP统计信息
inspur(config)#**clear tcp6 tcb** <*tcb-index*>	清除指定索引的TCB连接，TCB索引取值范围：1~4294967295
inspur#**debug ipv6 packet** [**interface** <*interface-name*>][**protocol** {**tcp** | **udp** | **icmp**}][{**detail**}]	打开IPv6协议的debug功能，显示IPv6协议处理的调试信息，显示路由器是否在发送或接收IPv6报文，可以指定接口或者协议号或者详细信息进行打印
inspur#**debug ipv6 icmp**	打开ICMPv6协议的debug功能，显示ICMPv6协议处理的调试信息，显示路由器是否在发送或接收ICMP报文
inspur#**debug ipv6 tcp all**	打开IPv6 TCP协议相关的所有打印开关
inspur#**debug ipv6 tcp driver**	设置建立、关闭IPv6 TCP连接相关信息的调试开关
inspur#**debug ipv6 tcp packet**	设置IPv6 TCP发送、接收包的源、目的等信息的调试开关
inspur#**debug ipv6 tcp transactions**	设置TCP状态迁移等信息的调试开关
inspur#**debug ipv6 udp**	设置UDP发送、接收包的源和目的信息等的调试开关
inspur#**show debug ipv6**	显示已经打开的IPv6协议debug功能相关开关
inspur#**show debug icmp6**	显示已经打开的ICMPv6协议debug功能相关开关
inspur#**show debug tcp6**	显示已经打开的IPv6 TCP协议debug功能相关开关
inspur#**show debug udp6**	显示已经打开的IPv6 UDP协议debug功能相关开关

<*local-ipv6-address*>：本地IP地址，为十六进制冒分形式。

<*vrf-name*>：IP地址所属的VRF名称，长度为1~32个字符。

<*local-port*>：本地端口号，范围：1~65535。

<*remote-ipv6-address*>：远端IP地址，为十六进制冒分形式。

<*remote-port*>：远端端口号，范围：1~65535。

12.1.2 配置 IPv6 地址

为接口配置IPv6地址是管理和配置其它功能的前提。

1.配置IPv6地址。

步骤	命令	功能
1	inspur(config)#**interface** <*interface-name*>	进入接口配置模式
2	inspur(config-if-interface-name)#**ipv6 enable**	接口开启IPv6功能
3	inspur(config-if-interface-name)#**ipv6 address** <*ipv6-address*>/<*prefix-length*>	配置接口IPv6地址
	inspur(config-if-interface-name)#**ipv6 address link-local** <*X:X::X:X*>	配置接口IPv6 link local地址

<*ipv6-address*>：表示将要在接口上配置的地址，地址的格式（<*X:X::X:X*>）遵循RF中的规定，以16位为一组，中间用“:”格开，可以采用RFC中支持的简化形式。

<*prefix-length*>：表示IPv6地址的前缀长度，10进制格式（取值1~128），表示连续的IPv6地址的高多少位组成前缀。

<*X:X::X:X*>：表示link-local地址，要求配置是fe80::/64地址前缀格式。

2.配置IPv6功能的可选参数。

命令	功能
inspur(config-if-interface-name)#**ipv6 mtu** <*bytes*>	配置接口上发送IPv6报文的最大传输单元（MTU）值，单位：字节，范围：1280~9202，默认值为1500
inspur(config-if-interface-name)#**ipv6 dad-attemps** <*number*>	配置接口对地址进行重复地址检测（DAD）的最大次数，范围：1~10，缺省值3

3.验证配置结果。

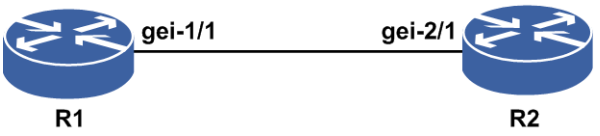
命令	功能
inspur#**show ipv6 interface** <*interface-name*>	显示IPv6接口的详细信息
inspur#**show ipv6 interface brief** <*interface-name*>	显示IPv6接口的简要信息

12.1.3 IPv6 地址配置实例

配置说明

如*图 12-1*所示，R1接口gei-1/1和R2接口gei-2/1直接连接，要求R1与R2能够互相ping6通。

图 12-1 IPv6 地址配置实例拓扑图



配置思路

1.配置R1和R2接口的IPv6地址。

2.测试配置结果，确认R1和R2能够ping6通。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ipv6 enable
R1(config-if-gei-1/1)#ipv6 address 3ffe:100::1/64
或者：
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ipv6 enable
R1(config-if-gei-1/1)#ipv6 address link-local fe80::1111:2222:3333:4444
R1(config-if-gei-1/1)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-2/1
R2(config-if-gei-2/1)#no shutdown
R2(config-if-gei-2/1)#ipv6 enable
R2(config-if-gei-2/1)#ipv6 address 3ffe:100::2/64
或者：
R2(config)#interface gei-2/1
R2(config-if-gei-2/1)#no shutdown
R2(config-if-gei-2/1)#ipv6 enable
R2(config-if-gei-2/1)#ipv6 address link-local fe80::5555:6666:7777:8888
R2(config-if-gei-2/1)#exit
```

配置验证

在R1上的验证如下：

```
R1#show ipv6 interface brief gei-1/1
gei-1/1                          [up/up]
    fe80::2d1:d1ff:fe3a:7be1
    3ffe:100::1/64
```

```
R1#ping6 3ffe:100::2
sending 5,100-byte ICMP echoes to 3ffe:100::2,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5), round-trip min/avg/max= 0/0/0 ms.
```

在R2上的验证如下：

```
R1#show ipv6 interface brief gei-2/1
gei-2/1                          [up/up]
    fe80::1422:30ff:fec4:e999
    3ffe:100::2/64
R2#ping6 3ffe:100::1
sending 5,100-byte ICMP echoes to 3ffe:100::1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5), round-trip min/avg/max= 0/0/0 ms.
```

12.2 NDP

NDP实现了IPv4中ARP、ICMP中的路由设备发现部分、重定向协议的所有功能，并具有邻居不可达检测机制。

当一个IPv6节点在网络上出现时，直接相连的链路上的其它IPv6节点可以通过NDP进行发现，进而获得其链路层地址。IPv6节点也能通过NDP来查找路由设备，维护路径上处于活动状态的邻居节点的可达性信息。

邻居发现的这些功能主要通过NDP报文实现，NDP分组装载在ICMPv6分组内部。NDP定义了5种ICMPv6分组类型，分别为：路由请求报文（RS）、路由通告报文（RA）、邻居请求报文（NS）、邻居通告报文（NA）和重定向报文。

12.2.1 配置 NDP

通过配置NDP协议功能，直连链路的节点间可以进行地址解析、邻居发现、节点维护和邻居不可达检测等。

1.进入接口配置模式。

命令	功能
inspur(config)#**interface** <*interface-name*>	进入接口配置模式

2.配置NDP功能属性的可选参数。

命令	功能
inspur(config-if-interface-name)#**ipv6 nd managed-config-flag**	设置接口发送的路由器通告报文的“管理地址配置”字段，即报文的M位值为1，缺省时值为0
inspur(config-if-interface-name)#**ipv6 nd other-config-flag**	设置接口发送的路由器通告报文的“其它已规定配置”字段，即报文的O位值为1，缺省时值为0
inspur(config-if-interface-name)#**ipv6 nd prefix** <*ipv6-prefix*>/<*prefix-length*> [{<*valid-lifetime*> <*preferred-lifetime*>} | **off-link** |	设置接口发送的路由器应答报文的前缀选项

命令	功能
no-autoconfig]	
inspur(config-if-interface-name)#**ipv6 nd ra-interval** <*seconds*>	配置接口发送路由器应答的时间间隔，单位：秒，取值范围3~1800，缺省为600
inspur(config-if-interface-name)#**ipv6 nd ra-lifetime** <*seconds*>	配置接口发送路由器应答的“路由器存活时间”字段的值，单位：秒，取值范围0~9000，缺省为1800
inspur(config-if-interface-name)#**ipv6 nd ra-linkmtu** <*ra-advlinkmtu*>	配置在路由器通告中的MTU字段的值，单位：字节，取值范围0~1500，缺省为1500
inspur(config-if-interface-name)#**ipv6 nd reachable-time** < *milliseconds*>	配置在远端邻居确认可达后多少时间内认为远端邻居是可达的，单位：毫秒，取值范围0~3600000，缺省为30000
inspur(config-if-interface-name)#**ipv6 nd retransmit-time** <*milliseconds*>	配置在路由器应答中的“重传计时器”字段的值，单位：毫秒，取值范围1000~360000，缺省为1000
inspur(config-if-interface-name)#**ipv6 nd suppress-ra**	配置路由器不发送路由器应答报文，缺省时值为1，不发送路由器应答报文
inspur(config-if-interface-name)#**ipv6 nd ra-curhoplimit**<*hoplimit*>	配置路由通告的跳数限制，取值范围0~255，缺省为64
inspur(config-if-interface-name)#**ipv6 nd staled-time**<*minutes*>	配置邻居缓存表中ND条目的stale状态时间，单位：分钟，范围：1~14400，缺省为1440
inspur(config-if-interface-name)#**ipv6 nd stale-switch**	设置在staled-time到达之前进行可达性检测，默认该开关关闭
inspur(config-if-interface-name)#**ipv6 dad-attemts** <*numbers*>	设置接口对地址进行重复地址检测的次数，配置范围是0~10，缺省检测次数为3
inspur(config-if-interface-name)#**ipv6 nd redirect**	开启发送ND重定向报文开关，缺省时该开关关闭
inspur(config-if-interface-name)#**ipv6 nd proxy**	开启接口间ND代理功能，缺省时不开启
inspur(config-if-interface-name)#**ipv6 nd inter-vlan-proxy**	开启相同接口不同VLAN间的ND代理功能，缺省时不开启
inspur(config-if-interface-name)#**ipv6 nd inner-vlan-proxy**	开启相同接口相同VLAN内的ND代理功能，缺省时不开启
inspur(config-if-interface-name)#**ipv6 nd ra-route-information prefix** <*ipv6-prefix*>**/**<*prefix-length*>[**route-lifetime** <*route-lifetime*>[**preferences** <*route-preference*>]]	接口配置IPv6协议的路由应答报文中的路由信息选项

<*valid-lifetime*>：前缀的有效生存时间，单位：秒，配置范围：0~4294967295，缺省为604800。

<*preferred-lifetime*>：首选生存时间，单位：秒，配置范围：0~4294967295，缺省为86400。

no-autoconfig：表示链路上的主机不能用本前缀作IPv6地址自动配置。

off-link：表明前缀的L位（在线标志）没有设置，缺省标记置1。该标志设置了的话，表示前缀可以用于在线确定，即属于此前缀的所有地址都在线；没有设置时，一些地址可以在线，一些则离线。

<*ipv6-prefix*>：包含在路由器通告中的网络前缀。

<*prefix-length*>：前缀长度。

<*route-lifetime*>：路由生存时间，单位：秒，配置范围：0~4294967295，缺省：4294967295秒。

<*route-preference*>：路由优先级，配置范围：0~3，缺省：0。

3.添加静态条目至邻居缓存表。

命令	功能
inspur(config-if-interface-name)#**nd 6 add** <*ipv6-address*><*hardware-address*>	在邻居缓存表中添加一条静态条目
inspur(config-if-supervlan)#**nd6 add** <*ipv6-address*><*hardware-address*><*interface*>	Supervlan接口下在邻居缓存表中增加一条静态条目

<*ipv6-address*>：邻居缓存表中的目的地址。

<*hardware-address*>：邻居缓存表中对应目的地址的硬件地址，48位的值，采用XXXX.XXXX.XXXX的形式，16位为1组，中间以“.”隔开。

<*interface*>：指定subvlan接口，仅对于supervlan接口配置模式可见且必须配置，其他接口配置模式下该参数不可见。

4.验证配置结果。

命令	功能
inspur#**show nd6 cache**[<*interface-name*>]	显示IPv6邻居缓存表的信息，加接口时只显示该接口下的邻居缓存条目 显示的结果不仅仅是通过NDP动态生成的邻居条目，还包含静态邻居缓存条目

5.维护NDP。

命令	功能
inspur(config-if-interface-name)#**nd 6 delete** <*ipv6-address*>	删除IPv6邻居缓存表中的一个条目
inspur#**clear nd-cache** [<*interface-name*>]	不加接口名，清除IPv6的邻居缓存表中所有的动态条目；加接口名，清除IPv6邻居缓存

命令	功能
	表中该接口下的动态条目，该命令只能在特权模式下使用
inspur#**debug ipv6 nd6**	打开所有有关ND协议debug功能开关
inspur#**show debug nd6**	显示已经打开的ND6协议debug功能相关开关

12.2.2 NDP 配置实例

配置说明

在路由器的gei-1/1接口下的NDP邻居表中配置静态条目。

配置思路

1.进入接口配置模式，在邻居缓存表中添加一条静态条目。

2.显示邻居缓存表的内容，确认是否添加成功。

配置过程

路由器上的配置过程如下：

```
inspur(config)#interface gei-1/1
inspur(config-if-gei-1/1)#no shutdown
inspur(config-if-gei-1/1)#nd6 add 780::1 0000.0a00.1345
```

配置验证

假设配置前路由器上的回显信息如下：

```
inspur#show nd6 cache
Total Cache Number Is:1
Only Current Valid Items Are Shown Below:
Address          Link-Address     Age          Status       Interface
3ffe:100::2       0023.e422.1134   23h56m2s      Stale        gei-1/1
```

配置后在路由器上验证配置结果如下：

```
inspur#show nd6 cache
Total Cache Number Is:12
Only Current Valid Items Are Shown Below:
Address          Link-Address     Age          Status       Interface
780::1           0000.0a00.1345   static        Reachable    gei-1/1
3ffe:100::2       0023.e422.1134   23h55m6s      Stale        gei-1/1
```

以上结果表示在NDP邻居表中添加一条静态条目成功。

12.3 IPv6 静态路由

静态路由是网络管理员通过手工配置指定的路由。当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。

静态路由不像动态路由那样根据路由算法建立路由表，也不能自动适应网络拓扑结构的变化。当网络发生故障或者拓扑发生变化后， 必须由网络管理员手工修改配置。

所有的静态路由项都必须明确下一跳地址，在发送报文时根据报文的目的地址寻找路由表中与之匹配的路由。只有指定了下一跳地址，链路层才能找到对应的链路层地址，并转发报文。

IPv6静态路由原理同IPv4静态路由，配置时使用IPv6地址。

12.3.1 配置 IPv6 静态路由

静态路由是由网络管理员根据路由需求手工进行配置的，可以达到对网络中路由行为的精确控制。

相关信息

配置静态路由时需要注意：

- 对于点到点接口，配置静态路由只需指定出接口。因为指定出接口即隐含指定了下一跳地址，此时认为与该接口相连的对端接口地址就是路由的下一跳地址。
- 对于以太接口，配置静态路由不允许单独指定其作为出接口。在应用中，如果必须指定以太接口为出接口，应该先指定出接口再指定下一跳地址。
- 对于Null接口，配置静态路由指定Null接口应用于黑洞路由，匹配该路由的流量都会被直接丢弃。

1.配置IPv6静态路由。

命令	功能
inspur(config)#**ipv6 route** [**vrf** {**mng** |<*vrf-name*>}]<*ipv6-address-mask*>{<*ipv6-address*>|<*interface-name*>[<*ipv6-address*>]}[<*distance*>][**metric** <*cost*>][**bfd enable**][**track** <*track-name*>][**name** <*static-description*>]	配置IPv6静态路由
inspur(config)#**ipv6 route** [**vrf** {**mng** |<*vrf-name*>}]<*ipv6-address-mask*>{<*ipv6-address*>}[<*distance*>][**metric** <*cost*>][**bfd enable**][**track** <*track-name*>][**name** <*static-description*>]	配置IPv6静态路由指定下一跳，<*ipv6-address*>可以为直连地址或非直连地址
inspur(config)#**ipv6 route** [**vrf** {**mng** |<*vrf-name*>}]<*ipv6-address-mask*>{<*interface-name*>[<*ipv6-address*>]}[<*distance*>][**metric** <*cost*>][**bfd enable**][**track** <*track-name*>][**name** <*static-description*>]	配置带出接口或是出接口+下一跳形式的IPv6静态路由
inspur(config)#**ipv6 route-static** [**vrf** <*vrf-name*>] **fast-reroute**	使能IPv6静态路由FRR路由计算功能
inspur(config)#**ipv6 route nexthop source**	配置IPv6静态路由指定BFD源

命令	功能
<*interface-name*>	端下一跳的出接口，只支持loopback口

参数解释：

vrf <*vrf-name*>：用于配置指定VRF中的静态路由，VRF名称长度为1～32个字符，管理口mng作为特殊的VRF。

<*distance*>：管辖距离，范围1～255。

metric<*cost*>：路由的度量值，范围0～255。

bfd enable：使能静态BFD功能。

name <*static-description*>]：静态路由描述功能，描述字符串为1-64个字符。

ipv6 route 命令使用说明：

- <*distance*>相当于路由协议的优先级，值越小，优先级越高。缺省情况下静态路由的优先级高于动态路由，默认为1，但是通过设置可使动态路由优先于静态路由。
- **bfd enable**为静态路由关联BFD检测的使能开关。取消BFD检测，采用删除路由或者配置相同路由而不配置BFD选项的方式。

ipv6 route nexthop source 命令使用说明：

- 此命令与静态路由配置命令配合使用。
- 如果命令绑定的接口无IP地址，则不创建BFD会话。当接口IPv6地址更新时才会通知静态路由创建BFD会话。

2.验证配置结果。

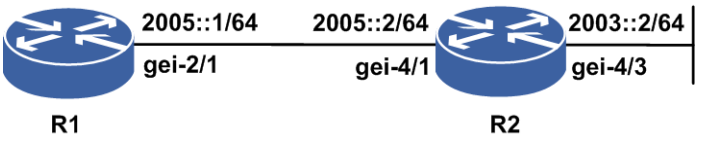
命令	功能
`inspur(config)#`**show running-config ipv6-static-route**	显示配置的IPv6静态路由信息
`inspur(config)#`**show ipv6 protocol routing static**	显示路由表中配置的静态路由及其有效性
`inspur(config)#`**show ipv6 forwarding route static**	显示转发表中静态路由的信息

12.3.2 下一跳直连的 IPv6 静态路由配置实例

配置说明

如*图 12-2*所示，R1和R2直连，地址为2005::/64网段，如果要从R1可以ping6通R2的2003::/64网段，可以通过在R1上加静态路由到2003::/64网段，下一跳为R1和R2直连的R2上的接口IPv6地址。

图 12-2 下一跳直连的 IPv6 静态路由配置实例拓扑图



配置思路

1.R1和R2直连地址间配置好2005::/64网段的IPv6地址。

2.在R2的直连接口上配置一个不同网段的2003::/64的IPv6地址。

3.通过在R1上加指向2003::/64网段的静态路由，R1可以ping6通R2的2003::/64网段地址。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/1
R1(config-if-gei-2/1)#no shutdown
R1(config-if-gei-2/1)#ipv6 enable
R1(config-if-gei-2/1)#ipv6 address 2005::1/64
R1(config-if-gei-2/1)#exit
R1(config)#ipv6 route 2003::/64 2005::2  /*配置静态路由*/
R1(config)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-4/1
R2(config-if-gei-4/1)#no shutdown
R2(config-if-gei-4/1)#ipv6 enable
R2(config-if-gei-4/1)#ipv6 address 2005::2/64
R2(config-if-gei-4/1)#exit
R2(config)#interface gei-4/3
R2(config-if-gei-4/3)#no shutdown
R2(config-if-gei-4/3)#ipv6 enable
R2(config-if-gei-4/3)#ipv6 address 2003::2/64
R2(config-if-gei-4/3)#exit
```

配置验证

R1上检查地址是否配置成功，接口是否up和静态路由是否添加成功，ping6 2003::2看是否可以ping6通。

```
R1(config)#show running-config-interface gei-2/1
!<if-intf>
interface gei-2/1
  ipv6 enable
  ipv6 address 2005::1/64
  no shutdown
$
!</if-intf>

R1(config)#show ipv6 interface gei-2/1
Interface gei-2/1  is up, line protocol is up
  IPv6 is enabled,  Hardware is Gigabit Ethernet
```

```
  HWaddr: 0020.231d.0e0e
  index 29
  Bandwidth 1000000 Kbits
  IPv6 MTU is 1500 bytes
  inet6 fe80::220:23ff:fe1d:e0e/64
  inet6 2005::1/64
  DAD attemps number:3
  ND reachable-time is 30000 milliseconds

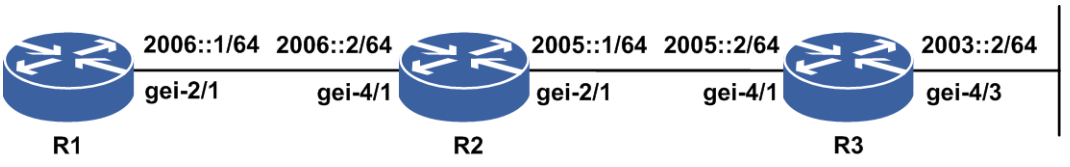
R1(config)#show running-config ipv6-static-route
!<ipv6-static-route>
ipv6 route 2003::/64 2005::2
!</ipv6-static-route>
R1#show ipv6 forwarding route static
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                            Owner    Metric
  Interface        Pri  Gw
2003::/64                        S        0
  gei-2/1          1    2005::2
```

12.3.3 下一跳非直连的 IPv6 静态路由配置实例

配置说明

如*图 12-3*所示，R1、R2和R3直连。R1如果将报文传给远端网络2003::/64，先必须将报文传给拥有IPv6地址2006::2的R2，R2要想将报文传给远端网络2003::/64，先必须将报文传给拥有IPv6地址2005::2的R3。

图 12-3 下一跳非直连的 IPv6 静态路由配置拓扑图



配置思路

1.R1上配置目的地址为2003::/64网段的静态路由，下一跳为2005::2。

2.R1上配置目的地址为2005::/64网段的静态路由，下一跳为2006::2。

配置过程

R1上的配置如下（R1、R2和R3的IPv6地址配置省略）：

```
R1(config)#ipv6 route 2003::/64 2005::2  /*配置下一跳非直连的静态路由*/
R1(config)#ipv6 route 2005::/64 2006::2  /*配置下一跳直连的静态路由*/
```

R2上的配置如下：

```
R2(config)#ipv6 route 2003::/64 2005::2
```

配置验证

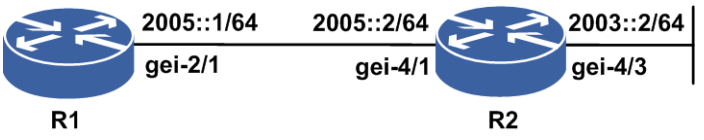
```
R1#show ipv6 forwarding route static
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                Owner    Metric
  Interface      Pri  Gw
2003::/64                            S          0
  gei-2/1        1    2006::2
2005::/64                            S          0
  gei-2/1        1    2006::2
```

12.3.4 IPv6 默认路由配置实例

配置说明

默认路由又称为缺省路由，也是一种特殊的静态路由。当路由表中的所有路由都选择失败的时候，为使报文有最终的一个发送地，将使用默认路由，从而大大减少了路由器的处理负担。以*图 12-4*所示举例，IPv6默认路由的配置。

图 12-4 IPv6 默认路由配置实例拓扑图



配置思路

1.配置接口IPv6地址。

2.配置默认路由，下一跳接口指定R2的gei-4/1的IPv6地址。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/1
R1(config-if-gei-2/1)#no shutdown
R1(config-if-gei-2/1)#ipv6 enable
R1(config-if-gei-2/1)#ipv6 address 2005::1/64
R1(config)#ipv6 route ::/0 2005::2
/*R2上接口的IPv6地址配置省略*/
```

配置验证

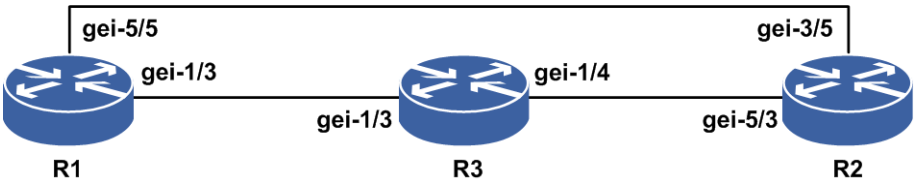
```
R1(config)#show ipv6 forwarding route static
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                            Owner    Metric
 Interface     Pri  Gw
::/0                            S          0
 gei-2/1       1    2005::2
```

12.3.5 IPv6 静态路由公网 FRR 配置实例

配置说明

FRR的功能在于当网络中链路或者节点失效后，为这些重要的节点或链路提供备份保护，实现快速重路由，减少链路或节点失效时对流量的影响，使流量实现快速恢复。以*图 12-5*所示的组网为例，配置IPv6静态路由公网FRR功能。

图 12-5 IPv6 静态路由公网 FRR 配置实例组网图



配置思路

1.在R1上打开公网IPv6静态路由备份路由计算开关。

2.配置作为主路由的IPv6静态路由。

3.配置作为备路由的IPv6静态路由，目的地址、掩码需与主路由一致，出接口需与主路由不同，优先级或metric需次于主路由。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#ipv6 enable
R1(config-if-gei-1/3)#ipv6 address 300::1/56
R1(config-if-gei-1/3)#exit
R1(config)#interface gei-5/5
R1(config-if-gei-5/5)#no shutdown
R1(config-if-gei-5/5)#ipv6 enable
R1(config-if-gei-5/5)#ipv6 address 500::1/56
R1(config-if-gei-5/5)#exit
R1(config)#ipv6 route-static fast-reroute   /*开启FRR功能*/
```

```
R1(config)#ipv6 route 1234::1/128 500::2
R1(config)#ipv6 route 1234::1/128 300::2 10
```

R3上的配置如下：

```
R3(config)#interface gei-1/3
R3(config-if-gei-1/3)#no shutdown
R3(config-if-gei-1/3)#ipv6 enable
R3(config-if-gei-1/3)#ipv6 address 300::2/56
R3(config-if-gei-1/3)#exit
R3(config)#interface gei-1/4
R3(config-if-gei-1/4)#no shutdown
R3(config-if-gei-1/4)#ipv6 enable
R3(config-if-gei-1/4)#ipv6 address 400::2/56
R3(config-if-gei-1/4)#exit
R3(config)# ipv6 route 1234::1/128 400::3
```

R2上的配置如下：

```
R2(config)#interface gei-5/3
R2(config-if-gei-5/3)#no shutdown
R2(config-if-gei-5/3)#ipv6 enable
R2(config-if-gei-5/3)#ipv6 address 400::3/56
R2(config-if-gei-5/3)#exit
R2(config)#interface gei-3/5
R2(config-if-gei-3/5)#no shutdown
R2(config-if-gei-3/5)#ipv6 enable
R2(config-if-gei-3/5)#ipv6 address 500::2/56
R2(config-if-gei-3/5)#exit
R2(config)#interface loopback5
R2(config-if-loopback5)#ipv6 enable
R2(config-if-loopback5)#ipv6 address 1234::1/128
R2(config-if-loopback5)#exit
```

配置验证

在R1上FRR配置验证如下：

```
R1(config)#show ipv6 forwarding route 1234::1
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                          Owner Metric
  Interface      Pri  Gw
1234::1/128                    S     0
  gei-5/5    1    500::2

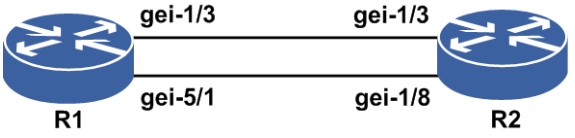
R1(config)#show ipv6 forwarding backup route 1234::1
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority, M/S: Master/Slave,
         Sta: Status;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Status codes: M: Master, S: Slave, I: Inuse, U: Unuse;
Dest                                 Owner    Metric
  Interface     Pri  M/S Sta  Gw
1234::1/128                           S       0
  gei-5/5       1    M   I    500::2
1234::1/128                           S       0
  gei-5/3       10   S   U    300::2
```

12.3.6 IPv6 静态路由私网 FRR 配置实例

配置说明

FRR的功能在于当网络中链路或者节点失效后，为这些重要的节点或链路提供备份保护，实现快速重路由，减少链路或节点失效时对流量的影响，使流量实现快速恢复。以*图 12-6*所示的组网为例，配置IPv6静态路由私网FRR功能。

图 12-6 IPv6 静态路由私网 FRR 配置实例组网图



配置思路

1.配置VRF，使能VRF的v6地址族。

2.在R1上打开私网IPv6静态路由的备份路由计算开关。

3.配置作为主路由的私网IPv6静态路由。

4.配置作为备路由的IPv6静态路由，VRF、目的地址、掩码需与主路由一致，出接口需与主路由不同，优先级或metric需次于主路由。

配置过程

R1上的配置如下：

```
R1(config)#ip vrf vpn
R1(config-vrf-vpn)#rd 1:3
R1(config-vrf-vpn)#address-family ipv6
R1(config-vrf-vpn-af-ipv6)#exit
R1(config-vrf-vpn)#exit

R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#ip vrf forwarding vpn
R1(config-if-gei-1/3)#ipv6 enable
R1(config-if-gei-1/3)#ipv6 address 300::1/56
R1(config-if-gei-1/3)#exit
R1(config)#interface gei-5/1
R1(config-if-gei-5/1)#no shutdown
R1(config-if-gei-5/1)#ip vrf forwarding vpn
R1(config-if-gei-5/1)#ipv6 enable
R1(config-if-gei-5/1)#ipv6 address 500::1/56
R1(config-if-gei-5/1)#exit
R1(config)#ipv6 route-static vrf vpn fast-reroute   /*开启FRR功能*/
R1(config)#ipv6 route vrf vpn 1234::1/128 500::2
R1(config)#ipv6 route vrf vpn 1234::1/128 300::2 10
```

R2上的配置如下：

```
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#no shutdown
R2(config-if-gei-1/3)#ipv6 enable
```

```
R2(config-if-gei-1/3)#ipv6 address 300::2/56
R2(config-if-gei-1/3)#exit
R2(config)#interface gei-1/8
R2(config-if-gei-1/8)#no shutdown
R2(config-if-gei-1/8)#ipv6 enable
R2(config-if-gei-1/8)#ipv6 address 500::2/56
R2(config-if-gei-1/8)#exit
R2(config)#interface loopback5
R2(config-if-loopback5)#ipv6 enable
R2(config-if-loopback5)#ipv6 address 1234::1/128
R2(config-if-loopback5)#exit
```

配置验证

R1上FRR配置验证如下：

```
R1(config)#show ipv6 forwarding route vrf vpn 1234::1
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                        Owner Metric
  Interface      Pri  Gw
1234::1/128                 S     0
  gei-5/1        1    500::2

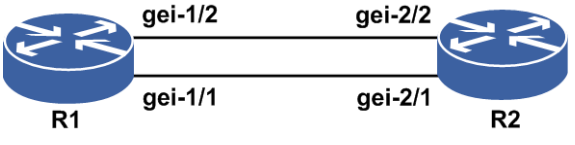
R1(config)#show ipv6 forwarding backup route vrf vpn 1234::1
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority, M/S: Master/Slave,
         Sta: Status;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Status codes: M: Master, S: Slave, I: Inuse, U: Unuse;
Dest                                Owner    Metric
  Interface     Pri  M/S Sta  Gw
1234::1/128                          S        0
  gei-5/5       1    M   I    500::2
1234::1/128                          S        0
  gei-5/3       10   S   U    300::2
```

12.3.7 IPv6 静态路由负荷分担配置实例

配置说明

负荷分担可使超出单个接口带宽的流量均分到多条链路上，实现流量在各条链路上的负载均衡。以*图 12-7*所示的组网为例，配置采用IPv6静态路由的负荷分担来实现负载均衡的功能。

图 12-7 静态路由负荷分担组网图



配置思路

1.配置接口地址，在R1、R2路由器上直连接口配置IPv6地址，在R2上配置loopback口地址。

2.在R1上配置到对端loopback口地址的2条IPv6静态路由，下一跳分别为对端直连的接口地址；2条IPv6静态路由的distance值和metric值必须相等。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ipv6 enable
R1(config-if-gei-1/1)#ipv6 address 300::1/56
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#ipv6 enable
R1(config-if-gei-1/2)#ipv6 address 500::1/56
R1(config-if-gei-1/2)#exit
R1(config)#ipv6 route 1234::1/128 500::2
R1(config)#ipv6 route 1234::1/128 300::2
```

R2上的配置如下：

```
R2(config)#interface gei-2/1
R2(config-if-gei-2/1)#no shutdown
R2(config-if-gei-2/1)#ipv6 enable
R2(config-if-gei-2/1)#ipv6 address 300::2/56
R2(config-if-gei-2/1)#exit
R2(config)#interface gei-2/2
R2(config-if-gei-2/2)#no shutdown
R2(config-if-gei-2/2)#ipv6 enable
R2(config-if-gei-2/2)#ipv6 address 500::2/56
R2(config-if-gei-2/2)#exit
R2(config)#interface loopback5
R2(config-if-loopback5)#ipv6 enable
R2(config-if-loopback5)#ipv6 address 1234::1/128
R2(config-if-loopback5)#exit
```

配置验证

用**show ipv6 forwarding route**命令查看R1上的路由转发表：

```
R1(config)#show ipv6 forwarding route 1234::1
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                          Owner Metric
  Interface      Pri  Gw
1234::1/128                    S     0
  gei-1/1        1    300::2
1234::1/128                    S     0
  gei-1/2        1    500::2
```

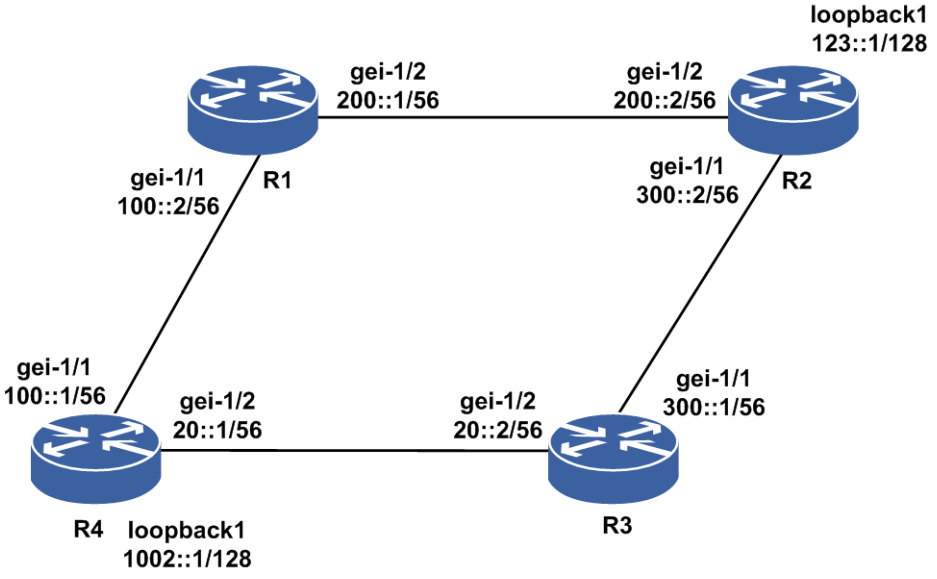
以上结果说明，到达目的地1234::1/128的下一跳有两个，分别是300::2和500::2，出接口分别是gei-1/1和gei-1/2，达到了负载均衡的目的。

12.3.8 IPv6 静态路由 BFD 源端下一跳配置实例

配置说明

创建IPv6静态路由多跳BFD会话时需要指定源端下一跳，这个功能目前只针对loopback口，BFD会话的本端地址选择配置的loopback口上的第一个非link-local地址。以*图 12-8*所示的拓扑为例，配置R4上的BFD会话本端地址选择loopback上的第一个非link-local地址。

图 12-8 IPv6 静态路由 BFD 源端下一跳组网图



配置思路

1.R4上配置与R1直连的接口地址，配置与R3直连的接口地址，配置loopback口地址，配置IPv6静态路由到达R2上loopback口地址，配置IPv6静态路由使能BFD，配置IPv6静态路由的BFD源端下一跳命令。

2.R1上配置与R4直连的接口地址，配置与R2直连的接口地址，配置到达R2上loopback口地址的IPv6静态路由。

3.R3上配置与R4直连的接口地址，配置与R2直连的接口地址，配置到达R2上loopback口地址的IPv6静态路由。

4.R2上配置与R1直连的接口地址，配置与R3直连的接口地址，配置loopback口地址，配置IPv6静态路由到达R4上loopback口地址，配置IPv6静态路由使能BFD，配置IPv6静态路由的BFD源端下一跳命令。

配置过程

R4上的配置如下：

```
R4(config)#interface gei-1/1
R4(config-if-gei-1/1)#no shutdown
R4(config-if-gei-1/1)#ipv6 enable
R4(config-if-gei-1/1)#ipv6 address 100::1/56
R4(config-if-gei-1/1)#exit
R4(config)#interface gei-1/2
R4(config-if-gei-1/2)#no shutdown
R4(config-if-gei-1/2)#ipv6 enable
R4(config-if-gei-1/2)#ipv6 address 20::1/56
R4(config-if-gei-1/2)#exit
R4(config)#interface loopback1
R4(config-if-loopback1)#ipv6 enable
R4(config-if-loopback1)#ipv6 address 1002::1/128
R4(config-if-loopback1)#exit
R4(config)#ipv6 route 123::1/128 100::2
R4(config)#ipv6 route 123::1/128 200::2
R4(config)#ipv6 route 1234::1/128 123::1 bfd enable
R4(config)#ipv6 route nexthop source loopback1
```

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ipv6 enable
R1(config-if-gei-1/1)#ipv6 address 100::2/56
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#ipv6 enable
R1(config-if-gei-1/2)#ipv6 address 200::1/56
R1(config-if-gei-1/2)#exit
R1(config)#ipv6 route 123::1/128 200::2
R1(config)#ipv6 route 1002::1/128 100::1
```

R3上的配置如下：

```
R3(config)#interface gei-1/1
R3(config-if-gei-1/1)#no shutdown
R3(config-if-gei-1/1)#ipv6 enable
R3(config-if-gei-1/1)#ipv6 address 300::1/56
R3(config-if-gei-1/1)#exit
R3(config)#interface gei-1/2
R3(config-if-gei-1/2)#no shutdown
R3(config-if-gei-1/2)#ipv6 enable
R3(config-if-gei-1/2)#ipv6 address 200::2/56
R3(config-if-gei-1/2)#exit
R3(config)#ipv6 route 123::1/128 300::2
R3(config)#ipv6 route 1002::1/128 200::1
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ipv6 enable
R2(config-if-gei-1/1)#ipv6 address 300::2/56
R2(config-if-gei-1/1)#exit
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#ipv6 enable
R2(config-if-gei-1/2)#ipv6 address 200::2/56
R2(config-if-gei-1/2)#exit
R2(config)#interface loopback1
R2(config-if-loopback1)#ipv6 enable
R2(config-if-loopback1)#ipv6 address 123::1/128
R2(config-if-loopback1)#exit
R2(config)#ipv6 route 1002::1/128 200::1
R2(config)#ipv6 route 1002::1/128 300::1
R2(config)#ipv6 route 1234::1/128 1002::1 bfd enable
R2(config)#ipv6 route nexthop source loopback1
```

配置验证

用**show bfd neighbors ip brief**命令在R2上查看BFD会话信息：

```
R2(config)#show bfd neighbors ip brief
LocalAddr         PeerAddr          LD   RD    Hold   State  Interface
1002:0:0:0:0:0:0:1 123:0:0:0:0:0:0:1  2051  2049   150    UP     ---
```

以上结果说明，R2和R4之间的多跳BFD会话创建成功，R2上BFD会话的对端地址为配置的下一跳地址，本端地址为本路由器上指定的源端接口的loopback1地址。

12.4 RIPng

RIP作为一种成熟的路由标准，在Internet中有着广泛的应用，特别是在一些中小型网络中。基于这种现状，同时考虑到RIP与IPv6的兼容性问题，IETF对现有技术进行改造，制定了IPv6下的RIP标准，即RIPng。

RIPng是基于UDP的协议，并且使用端口号521发送和接收数据包。RIPng的报文大致可分为两类：选路信息报文和用于请求信息的报文。

12.4.1 配置 RIPng

配置RIPng路由的相关属性和功能，包括协议参数、汇总路由、重分发协议路由等。

1.进入RIPng配置模式。

命令	功能
inspur(config)#**ipv6 router rip** [**vrf** <*vrf-name*>]	进入RIPng配置模式，带VRF参数表示进入RIPng-VRF模式

2.配置RIPng协议的可选参数。

命令	功能
inspur(config-ripng)#**timers basic** <*update*><*timeout*><*garbage*>	配置RIPng协议的定时器
inspur(config-ripng)#**default-metric** <*metric*>	配置RIPng路由的缺省度量值
inspur(config-ripng)#**port** <*1-65535*>	配置RIPng组播报文的监听端口，默认为521
inspur(config-ripng)#**offset-list** <*access-list-number*>{**in** | **out**}<*offset-metric*>	配置RIPng特定的接收（in）或发送（out）的路由metric偏移量，metric偏移值的范围为0~16

<*update*>：周期性发送报文的更新时间，单位：秒，范围5~65535秒，默认值是30秒。

<*timeout*>：路由无效的时间，单位：秒，范围5~65535秒，默认值是180秒。

<*garbage*>：路由从无效到删除的时间，单位：秒，范围5~65535秒，默认值是120

秒。

in | out：指定路由为接收/发送路由。

3.配置RIPng汇总路由和重分发协议路由。

命令	功能
inspur(config-ripng)#**summary-prefix** <*X:X::X:X/<0-128>*>	配置RIPng的汇总路由
inspur(config-ripng)#**redistribute** <*protocol*>[**metric** <*metric-value*>][**route-map** <*map-tag*>]	配置重分发协议路由

<*protocol*>：重分发的协议名称。

<*metric-value*>：重分发该协议的度量值，范围为1~16。

<*map-tag*>：重分发该协议所使用的路由图。

4.开启接口RIPng协议功能。

步骤	命令	功能
1	inspur(config-ripng)#**interface** <*interface-name*>	进入RIPng接口配置模式
2	inspur(config-ripng-if-interface-name)#**ipv6 rip enable**	在接口上开启RIPng功能

5.配置RIPng接口下的可选参数。

命令	功能
inspur(config-ripng-if-interface-name)#**ipv6 rip split-horizon**	在接口上进行水平分割，默认开启
inspur(config-ripng-if-interface-name)#**ipv6 rip poison-reverse**	在接口上进行毒性逆转，默认开启
inspur(config-ripng-if-interface-name)#**ipv6 rip interface active**	配置主动接口，使该接口只发送不接收报文
inspur(config-ripng-if-interface-name)#**ipv6 rip interface passive**	配置被动接口，使该接口只接收不发送报文
inspur(config-ripng-if-interface-name)#**ipv6 rip neighbor** <*X:X::X:X*>	配置RIPng协议的邻居地址，将单独往这个邻居发送单播报文
inspur(config-ripng-if-interface-name)#**ipv6 rip originate-default-route** [**only**]	在接口上产生RIPng协议的缺省路由

6.验证配置结果。

命令	功能

命令	功能
inspur(config)#**show ipv6 rip** [**vrf** <*vrf-name*>]	显示RIPng协议内容
inspur(config)#**show ipv6 rip database** [{**X:X::X:X/**<*0~128*>|<*X:X::X:X*>}][**vrf** <*vrf-name*>]	显示RIPng协议的路由数据库信息
inspur(config)#**show ipv6 rip interface** [**vrf** <*vrf-name*>]<*interface-name*>	显示启动了RIPng协议的接口信息

7.维护RIPng路由。

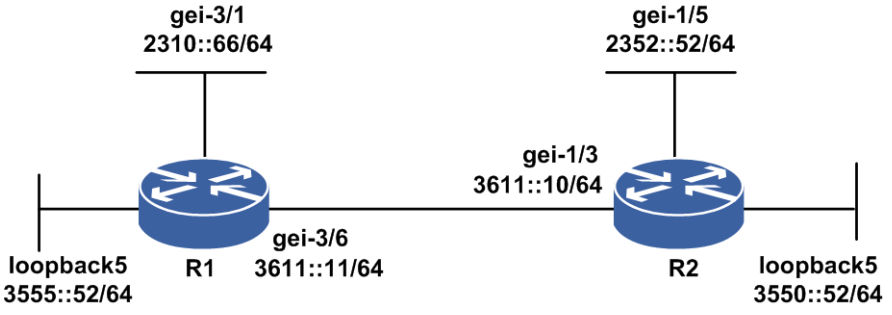
命令	功能
inspur#**clear ipv6 rip route** [**vrf** <*vrf-name*>]{<*X:X::X:X*>**/**<*0~128*>| **all**}	删除RIPng协议收到的路由，可以删除所有收到的路由，也可以有选择地删除某一条路由

12.4.2 RIPng 基本配置实例

配置说明

如*图 12-9*所示，在R1和R2上运行RIPng，通告各自的RIPng路由，以一个loopback地址为例，可重分发其他路由，以重分发直连路由为例。

图 12-9 RIPng 基本配置实例拓扑图



配置思路

1.接口使能IPv6，配置IPv6地址。

2.配置RIPng协议。

3.在接口上启用RIPng协议相关配置。

4.若需要重分发其他路由，配置重分发命令。

5.查看配置结果，确认两台设备正确建立邻居，分别能够学到对端通告的路由。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-3/6
R1(config-if-gei-3/6)#ipv6 enable
R1(config-if-gei-3/6)#ipv6 address  3611::11/64
R1(config-if-gei-3/6)#no shutdown
R1(config-if-gei-3/6)#exit
R1(config)#interface gei-3/1
R1(config-if-gei-3/1)#ipv6 enable
R1(config-if-gei-3/1)#ipv6 address  2310::66/64
R1(config-if-gei-3/1)#no shutdown
R1(config-if-gei-3/1)#exit
R1(config)#interface loopback5
R1(config-if-loopback5)#ipv6 enable
R1(config-if-loopback5)#ipv6 address  3555::52/64
R1(config-if-loopback5)#exit

R1(config)#ipv6 router rip
R1(config-ripng)#interface gei-3/6
R1(config-ripng-if-gei-3/6)#ipv6 rip enable
R1(config-ripng-if-gei-3/6)#exit
R1(config-ripng)#interface loopback5
R1(config-ripng-if-loopback5)#ipv6 rip enable
R1(config-ripng-if-loopback5)#exit
R1(config-ripng)#redistribute connected
R1(config-ripng)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#ipv6 enable
R2(config-if-gei-1/3)#ipv6 address 3611::10/64
R2(config-if-gei-1/3)#no shutdown
R2(config-if-gei-1/3)#exit
R2(config)#interface gei-1/5
R2(config-if-gei-1/5)#ipv6 enable
R2(config-if-gei-1/5)#ipv6 address 2352::52/64
R2(config-if-gei-1/5)#no shutdown
R2(config-if-gei-1/5)#exit
R2(config)#interface loopback5
R2(config-if-loopback5)#ipv6 enable
R2(config-if-loopback5)#ipv6 address 3550::52/64
R2(config-if-loopback5)#exit

R2(config)#ipv6 router rip
R2(config-ripng)#interface gei-1/3
R2(config-ripng-if-gei-1/3)#ipv6 rip enable
R2(config-ripng-if-gei-1/3)#exit
R2(config-ripng)#interface loopback5
R2(config-ripng-if-loopback5)#ipv6 rip enable
R2(config-ripng-if-loopback5)#exit
R2(config-ripng)#redistribute connected    /*配置重分发*/
R2(config-ripng)#exit
```

配置验证

在R1和R2上可以使用**show running-config ripng**命令查看RIPng的配置信息，使用**show ipv6 forwarding route ripng**命令查看路由信息。

R1上的路由信息：

```
R1#show running-config ripng
!<ripng>
```

```
ipv6 router rip
  redistribute connected
    interface gei-3/6
    ipv6 rip enable
  $
  interface loopback5
    ipv6 rip enable
  $
!</ripng>

R1#show ipv6 rip
RIPng protocol, port 521, multicast-group FF02::9
    administrative distance is 120
    default metric is 1
    updates every 30 seconds, expire after 180 seconds
    garbage collect after 120 seconds

The number of ripng routes:
    connect ripng route 3
    aggregate ripng route 0
    ripng route 2
  Redistribution:
    redistribute connected

R1#show ipv6 rip database
 2255::/64
     nexthop: ::, via: unknown
     metric:  16, tag:   0
 2355::/64
     nexthop: fe80::2d0:d0ff:feaf:cc10, via: gei-3/6
     metric:   2, tag:   0
 2356::/64
     nexthop: fe80::2d0:d0ff:feaf:cc10, via: gei-3/6
     metric:   2, tag:   0
 2357::/64
     nexthop: fe80::2d0:d0ff:feaf:cc10, via: gei-3/6
     metric:   2, tag:   0
 2358::/64
     nexthop: fe80::2d0:d0ff:feaf:cc10, via: gei-3/6
     metric:   2, tag:   0
 2310::/64
     nexthop: ::, via: unknown
     metric:  16, tag:   0
 3036::/64
     nexthop: ::, via: gei-3/6
     metric:   1, tag:   0
 3550::/64
     nexthop: fe80::2d0:d0ff:feaf:cc10, via: gei-3/6
     metric:   2, tag:   0
 3555::/64
     nexthop: ::, via: loopback5
     metric:   1, tag:   0
 3611::/64
     nexthop: ::, via: gei-3/6
     metric:   1, tag:   0

R1#show ipv6 forwarding route ripng
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                        Owner   Metric
  Interface    Pri  Gw
2352::/64                                    R       2
  gei-3/6  120  fe80:12::2d0:d0ff:feaf:cc10
3550::/64                                    R       2
  gei-3/6  120  fe80:12::2d0:d0ff:feaf:cc10

R1#ping6 2352::52
```

```
sending 5,100-byte ICMP echoes to 2352::52,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 0/0/0 ms.
```

R2的路由信息：

```
R2#show running-config ripng
!<ripng>
ipv6 router rip
  redistribute connected
    interface gei-1/3
    ipv6 rip enable
  $
interface loopback5
    ipv6 rip enable
!</ripng>

R2#show ipv6 rip
RIPng protocol, port 521, multicast-group FF02::9
    administrative distance is 120
    default metric is 1
    updates every 30 seconds, expire after 180 seconds
    garbage collect after 120 seconds

The number of ripng routes:
    connect ripng route 3
    aggregate ripng route 0
    ripng route 2
  Redistribution:
    redistribute connected

R2#show ipv6 rip database
 2255::/64
     nexthop: fe80::2d0:d0ff:fe78:99dd, via: gei-1/3
     metric:  16, tag:   0
 2355::/64
     nexthop: ::, via: unknown
     metric:   1, tag:   0
 2356::/64
     nexthop: ::, via: unknown
     metric:   1, tag:   0
2310::/64
     nexthop: fe80::2d0:d0ff:fe78:99dd, via: gei-1/3
     metric:  16, tag:   0
 3036::/64
     nexthop: fe80::2d0:d0ff:fe78:99dd, via: gei-1/3
     metric:   2, tag:   0
 3550::/64
     nexthop: ::, via: loopback5
     metric:   1, tag:   0
 3555::/64
     nexthop: fe80::2d0:d0ff:fe78:99dd, via: gei-1/3
     metric:   2, tag:   0
 3611::/64
     nexthop: ::, via: gei-1/3
     metric:   1, tag:   0

R2#show ipv6 forwarding route ripng
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;

Dest                                        Owner   Metric
  Interface    Pri   Gw
2310::/64                                    R       2
  gei-1/3  120   fe80:2e::2d0:d0ff:fe78:99dd
3555::/64                                    R       2
  gei-1/3  120   fe80:2e::2d0:d0ff:fe78:99dd
```

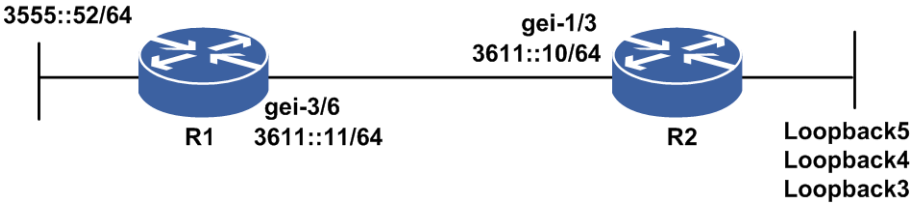
```
R2#ping6 2310::66
sending 5,100-byte ICMP echoes to 2310::66,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 0/0/0 ms.
```

12.4.3 RIPng 路由汇总配置实例

配置说明

如*图 12-10*所示，RIPng的路由可以进行路由汇总后再通告给邻居。

图 12-10 RIPng 路由汇总配置实例拓扑图



配置思路

1.按*图 4-53*所示搭建环境，并配置接口IPv6地址。

2.R1上接口启RIPng协议。

3.R2上配置Loopback地址，并且配合汇总路由，通告给R1。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-3/6
R1(config-if-gei-3/6)#ipv6 enable
R1(config-if-gei-3/6)#ipv6 address 3611::11/64
R1(config-if-gei-3/6)#no shutdown
R1(config-if-gei-3/6)#exit
R1(config)#ipv6 router rip
R1(config-ripng)#interface gei-3/6
R1(config-ripng-if-gei-3/6)#ipv6 rip enable
```

R2上的配置如下：

```
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#ipv6 enable
R2(config-if-gei-1/3)#ipv6 address 3611::10/64
R2(config-if-gei-1/3)#no shutdown
R2(config-if-gei-1/3)#exit
R2(config)#interface loopback5
R2(config-if-loopback5)#ipv6 enable
R2(config-if-loopback5)#ipv6 address 2001:db8:0:10::/64
R2(config-if-loopback5)#exit
R2(config)#interface loopback4
R2(config-if-loopback4)#ipv6 enable
R2(config-if-loopback4)#ipv6 address 2001:db8:0:11::/64
```

```
R2(config-if-loopback4)#exit
R2(config)#interface loopback3
R2(config-if-loopback3)#ipv6 enable
R2(config-if-loopback3)#ipv6 address 2001:db8:0:12::/64
R2(config-if-loopback3)#exit
R2(config)#ipv6 router rip
R2(config-ripng)#interface gei-1/3
R2(config-ripng-gei-1/3)#ipv6 rip enable
R2(config-ripng-gei-1/3)#exit
R2(config-ripng)#summary-prefix 2001:db8:0:10::/62
/*配置汇总路由，把loopback的几个路由汇总一个*/
```

配置验证

R1上学到的RIPng路由如下：

R1上的路由信息：

```
R1#show ipv6 forwarding route ripng
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                              Owner Metric
  Interface          Pri   Gw
2001:db8:0:10::/64                                  R     2
  gei-3/6        120  fe80:c::2d0:d0ff:fe00:500
2001:db8:0:10::/62                                  R     2
  gei-3/6        120  fe80:c::2d0:d0ff:fe00:500
2001:db8:0:11::/64                                  R     2
  gei-3/6        120  fe80:c::2d0:d0ff:fe00:500
2001:db8:0:12::/64                                  R     2
  gei-3/6        120  fe80:c::2d0:d0ff:fe00:500
```

12.5 OSPFv3

OSPFv2是IETF组织开发的一个基于链路状态的内部网关协议，具有适应范围广、收敛迅速、无自环、便于层级化网络设计等特点，因此在IPv4网络中获得了广泛应用。

IETF在保留OSPFv2优点的基础上针对IPv6网络修改形成了OSPFv3。OSPFv3主要用于在IPv6网络中提供路由功能，是IPv6网络中路由技术的主流协议。

与OSPFv2相比，OSPFv3在工作机制上与OSPFv2基本相同。

12.5.1 配置 OSPFv3

配置OSPFv3协议路由的相关属性和功能，包括协议属性、接口属性、汇总路由、重分发协议路由以及路由负荷分担等。

1.启用OSPFv3功能。

步骤	命令	功能
1	inspur(config)#**ipv6 router ospf**	启动OSPFv3进程实例，进入

步骤	命令	功能
	<*process-id*>[**vrf** <*vrf-name*>]	OSPFv3配置模式
2	inspur(config-ospfv3-process-id)#**router-id** <*router-id*>	指定一个OSPFv3进程实例的Router ID
3	inspur(config-ospfv3-process-id)#**area** <*area-id*>	配置OSPFv3的区域

<*process-id*>：OSPFv3进程号，范围：1~65535。

vrf <*vrf-name*>：VRF名称，长度1~32字符。

<*router-id*>：IP地址形式的OSPF路由器标识符。

只有通过**router-id**命令配置了路由器标识符后，OSPFv3实例才能正常运行。

2.配置OSPFv3协议属性。

命令	功能
inspur(config-ospfv3-process-id-area-id)#**authentication ipsec spi** <*spi-id*>{**md5** | **sha1** <*Hex-string*>[**rollover-interval** <*rollover-interval*>]}	配置OSPFv3的区域下所有接口认证密钥
inspur(config-ospfv3-process-id-area-id)#**bfd** <*disable* | **enable**>	配置区域下所有接口的双向转发检测（BFD， Bidirection Forwarding Detect）属性
inspur(config-ospfv3-process-id-area-id)#**default-cost** <*cost-value*>	配置区域的缺省度量值，范围0~16777215，缺省为1
inspur(config-ospfv3-process-id-area-id)#**encryption**{**ipsec spi** <*spi-id*> **esp 3des** | **aes-cbc 128** | **dst** | **null** [**hex-string**] **md5** | **sha1** <*Hex-string*>[**rollover-interval** <*rollover-interval*>]}	配置OSPFv3的接口加密
inspur(config-ospfv3-process-id-area-id)#**range X:X::X:X/**<*0-128*>[**advertise** | **not-advertise**]	配置区域的聚合地址范围 **advertise** | **not-advertise**，通告/不通告汇总3型链路状态
inspur(config-ospfv3-process-id-area-id)#**stub** [**no-summary**]	定义一个区域为stub区域，**no-summary**表示禁止区域边界路由器（ABR）将汇总路由信息发送到该stub区域
inspur(config-ospfv3-process-id-area-id)#**virtual-link** [**dead-interval** <*seconds*>][**hello-interval** <*seconds*>][**retransmit-interval** <*seconds*>][**transmit-delay** <*seconds*>]	定义OSPF虚链路
inspur(config-ospfv3-process-id)#**bfd enable**	配置所有接口的双向转发检测（BFD）功能
inspur(config-ospfv3-process-id)#**default-metric** <*metric-value*>	设置OSPFv3协议的缺省度量值，该值分配给重分发路由，范围1~16777214，缺省度量值为20

命令	功能
inspur(config-ospfv3-process-id)#**distribute-list** {**access-list** <*access-list-name*> **in** | **route-map** <*name of a route-map*> **in**}	distribute-list的**in**命令，用于过滤owner为OSPF的路由
inspur(config-ospfv3-process-id)#**timers spf** <*delay*><*holdtime*>	设置OSPFv3协议计算路由的时间间隔
inspur(config-ospfv3-process-id)#**fast-reroute per-prefix**	设置OSPFv3 FRR参数

<*spi-id*>：安全策略索引（security policy index）值，合法的十进制值为：256~32767。

<*Hex-string*>：md5-key字符长度为32字符；sha1-key字符长度为40字符。

<*rollover-interval*>：密钥生效延迟时间。参数的作用是当用户修改key值时，由于修改所有路由器上的key需要花费比较长的时间，因此需要进行一个平滑过渡的时期，该参数就是指平滑过渡的间隔时间，单位为分钟，范围：0~100000。

hello-interval <*seconds*>：虚拟链路上发送Hello报文的时间间隔，单位：秒，范围1~8192，缺省为10秒。

dead-interval <*seconds*>：虚拟链路上邻居死亡时间，单位：秒，范围1~8192，缺省为40秒。

retransmit-interval <*seconds*>：虚拟链路上报文重传间隔，单位：秒，范围1~8192，缺省为5秒。

transmit-delay <*seconds*>：虚拟链路上发送一个链路状态更新数据包的时延，单位：秒，范围1~8192，缺省为1秒。

<*delay*>：设置收到变化后导致路由重新计算的时间间隔，单位：秒，范围0~65535，缺省为5秒。

<*holdtime*>：路由计算中的时间间隔，单位：秒，范围0~65535，缺省为10秒。

3.配置OSPFv3汇总路由和重分发协议路由。

命令	功能
inspur(config-ospfv3-process-id)#**redistribute** <*protocol*>[**metric** <*metric-value*>][**metric-type** <*type*>][**route-map** <*name*>][**tag** <*number*>]	将其他协议的路由重分发到OSPFv3协议中
inspur(config-ospfv3-process-id)#**summary-prefix** <*X:X::X:X/<0-128>*>	为OSPF建立聚集地址，汇总正重新分配到OSPF的其他路由选择协议路径

<*protocol*>：重分配的协议名称，取值有：BGP、connected、IS-IS、RIP、static、aftr、sf-nat64、sl-nat64-ipv6、subscriber-host。

metric <*metric-value*>：设置重分配后的LSA的metric值，缺省情况下使用该实例的default-metric，范围：1~16777214。

metric-type <*metric-type*>：设置重分配后的LSA的metric-type，取值为ext-1或ext-2，缺省为ext-2。

tag <*number*>：为重分发到OSPF的路由设置标签，范围：0~4294967295。

4.配置OSPFv3路由负荷分担。

步骤	命令	功能
1	inspur(config-ospfv3-process-id)#**maximum-paths** <*number*>	配置协议支持负荷分担的路由数目，范围1~32，缺省为1条 路由表中最多保存32条等开销路由条目以进行负载均衡，此命令可以支持最多达32条相同度量值路径
2	inspur(config)#**interface** <*interface-name*>	进入接口配置模式
3	inspur(config-if-interface-name)#**load-sharing bandwidth** <*bandwidth-value*>	配置接口负荷分担的权重 ▸权重设置在出接口上，只有配置了优先级后，配置的权重才有效 ▸权重范围不同的接口其大小值也不同

5.配置OSPFv3接口属性。

步骤	命令	功能
1	inspur(config-ospfv3-process-id)#**area** <*area-id*>	接口开启OSPFv3协议功能
	inspur(config-ospfv3-process-id-area-id)#**interface** <*interface-name*>[**instance** <*0~255*>]	
2	inspur(config-ospfv3-process-id-area-id-if-interface-name)#**hello-interval** <*interval*>	指定接口上hello报文时间间隔，单位：秒，范围1~65535 ▸**point-to-point** 与 **broadcast** 类型接口的默认为10秒 ▸**non-broadcast** 与 **point-to-multipoint**类型接口的默认为30秒
	inspur(config-ospfv3-process-id-area-id-if-interface-name)#**retransmit-interval** <*interval*>	指定接口重传LSA的时间间隔，单位：秒，范围1~65535，默认为5秒
	inspur(config-ospfv3-process-id-area-id-if-interface-name)#**transmit-delay** <*interval*>	指定接口传输一个链路状态更新数据报文的时延，单位：秒，范围1~65535，默认为1秒
	inspur(config-ospfv3-process-id-area-id-if-interface-name)#**dead-interval** <*interval*>	指定接口上邻居的老化时间，单位：秒，范围1~65535 ▸**point-to-point** 与 **broadcast**

步骤	命令	功能
		类型接口的默认值为40秒 ▸**non-broadcase** 与**point-to-multipoint**类型接口的默认为120秒
	inspur(config-ospfv3-process-id-area-id-if-interface-name)#**cost** <*cost-value*>	设置接口开销，范围是1~65535
	inspur(config-ospfv3-process-id-area-id-if-interface-name)#**priority** <*value*>	设置接口优先级，范围0~255，默认为1
	inspur(config-ospfv3-process-id-area-id-if-interface-name)#**neighbor** <*X:X::X:X*>[[**cost** <*cost-value*>]|[**poll-interval** <*interval*>]|[**priority** <*value*>]]	配置接口类型为**non-broadcast**或**point-to-multipoint**的网络中的相邻路由器
	inspur(config-ospfv3-process-id-area-id-if-interface-name)#**network** {**broadcast**	**non-broadcast**	**point-to-multipoint** [**non-broadcast**]| **point-to-point**}	设置接口网络类型
	inspur(config-ospfv3-process-id-area-id-if-interface-name)#**authentication** [**null**	{**ipsec spi** <*spi-id*> **md5**	**sha1** <*Hex-string*>[**rollover-interval** <*rollover-interval*>]}]	配置OSPFv3的接口认证密钥
	inspur(config-ospfv3-process-id-area-id-if-interface-name)#**bfd** <*disable*	**enable**>	配置接口的双向转发检测（BFD， bidirection forwarding detect）属性
	inspur(config-ospfv3-process-id-area-id-if-interface-name)#**encryption** {**null** |**ipsec spi** <*spi-id*> **esp** [**3des**|**aes-cbc 128**|**des**|**null**]<*Hex-string*>[**md5**	**sha1**<*Hex-string*>][**rollover-interval** <*rollover-interval*>]}	配置OSPFv3的接口加密
	inspur(config-ospfv3-process-id-area-id-if-interface-name)#**ipv6-mtu-ignore**	配置DD报文交换过程中忽略MTU的匹配检查
	inspur(config-ospfv3-process-id-area-id-if-interface-name)#**linklsa-suppress** <*enable*>	配置抑制接口产生8型link LSA
	inspur(config-ospfv3-process-id-area-id-if-interface-name)#**fast-reroute** <*disable*>	关闭接口FRR功能

6.配置路由快速收敛OSPF前缀优先级。

命令	功能
inspur(config-ospfv3-process-id)#**prefix-priority** {**critical**	**high**	**medium**}{**prefix-name** <*prefix name*>| **tag** <*tag value*>}	配置OSPF的前缀优先级收敛命令，使匹配命令的LSA优先得到计算

<*prefix name*>：匹配prefix-list的名称，长度为1~31个字符。

<*tag value*>：匹配的tag值，范围为0~4294967295。

7.验证配置结果。

命令	功能
inspur(config)#**show ipv6 ospf** <*process-id*>	显示OSPFv3的实例信息
inspur(config)#**show ipv6 ospf database**	显示OSPFv3实例的数据库信息
inspur(config)#**show ipv6 ospf interface** [<*interface-name*>]	显示OSPFv3实例的接口信息
inspur(config)#**show ipv6 ospf neighbor**	显示OSPFv3实例的邻居信息
inspur(config)#**show ipv6 ospf request-list**	显示OSPFv3实例的请求列表信息
inspur(config)#**show ipv6 ospf retransmission-list**	显示OSPFv3实例的重传列表信息
inspur(config)#**show ipv6 ospf vertex**	显示OSPFv3实例的节点信息
inspur(config)#**show ipv6 ospf virtual-links**	显示OSPFv3实例的虚链信息

8.维护OSPFv3接口。

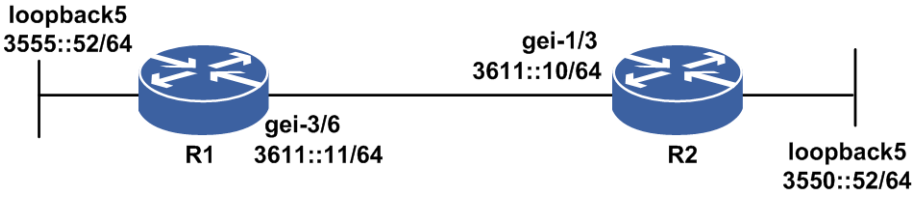
命令	功能
inspur(config-ospfv3)#**passive-interface** <*interface-name*>	禁止OSPFv3接口收发报文 一般接口可以正常收发OSPF协议报文，该命令禁止接口收发OSPF报文，主要用于调试、查错

12.5.2 OSPFv3 基本配置实例

配置说明

如*图 12-11*所示，R1和R2通过直连接口建链，通告各自的一个回环地址路由。

图 12-11 OSPFv3 配置实例拓扑图



配置思路

1.R1和R2直连接口使能IPv6，配置IPv6地址，并配置回环接口，使能IPv6，配置IPv6地址。

2.配置OSPFv3。

3.将各接口加入到OSPFv3区域0。

4.查看配置结果，确认两台设备正确建立邻居，分别能够学到对端通告的路由，分别能够ping通对端loopback接口。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-3/6
R1(config-if-gei-3/6)#no shutdown
R1(config-if-gei-3/6)#ipv6 enable
R1(config-if-gei-3/6)#ipv6 address 3611::11/64
R1(config-if-gei-3/6)#exit
R1(config)#interface loopback5
R1(config-if-loopback5)#ipv6 enable
R1(config-if-loopback5)#ipv6 address 3555::52/64
R1(config-if-loopback5)#exit

R1(config)#ipv6 router ospf 1
R1(config-ospfv3-1)#router-id 11.11.11.11
R1(config-ospfv3-1)#area 0
R1(config-ospfv3-1-area-0)#interface gei-3/6
R1(config-ospfv3-1-area-0-if-gei-3/6)#exit
R1(config-ospfv3-1-area-0)#interface loopback5
R1(config-ospfv3-1-area-0-if-loopback5)#exit
R1(config-ospfv3-1-area-0)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#no shutdown
R2(config-if-gei-1/3)#ipv6 enable
R2(config-if-gei-1/3)#ipv6 address 3611::10/64
R2(config-if-gei-1/3)#exit
R2(config)#interface loopback5
R2(config-if-loopback5)#ipv6 enable
R2(config-if-loopback5)#ipv6 address 3550::55/64
R2(config-if-loopback5)#exit

R2(config)#ipv6 router ospf 1
R2(config-ospfv3-1)#router-id 10.10.10.10
R2(config-ospfv3-1)#area 0
R2(config-ospfv3-1-area-0)#interface gei-1/3
R2(config-ospfv3-1-area-0-if-gei-1/3)#exit
R2(config-ospfv3-1-area-0)#interface loopback5
R2(config-ospfv3-1-area-0-if-loopback5)#exit
R2(config-ospfv3-1-area-0)#exit
```

配置验证

完成上述配置后，在两端设备上可以利用命令**show ipv6 ospf neighbor**和**show ipv6 forwarding route**查看建立的邻居信息和路由信息，分别从两台设

备上ping对端的loopback接口，都能ping通，说明配置成功。

在R1上查看和验证的结果如下：

```
R1(config)#show ipv6 ospf neighbor
OSPFv3 Process 1
Neighbor ID    Pri State     Dead Time   Interface ID    Interface
10.10.10.10    1   FULL/BDR  00:00:35       46        gei-3/6

R1#show ipv6 forwarding route 3550::55
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                        Owner    Metric
  Interface     Pri  Gw
3550::55/128                                 O          1
  gei-3/6   110  fe80:12::2d0:d0ff:feaf:cc10

R1#ping6 3550::55
sending 5,100-byte ICMP echo(es) to 3550:0:0:0:0:0:0:55,timeout is 2 second(s).
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 2/2/3 ms.
```

在R2上查看和验证的结果如下：

```
R2(config)#show ipv6 ospf neighbor
OSPFv3 Process 1
Neighbor ID    Pri   State    Dead Time   Interface ID  Interface
11.11.11.11    1    FULL/DR  00:00:37      18        gei-1/3

R2#show ipv6 forwarding route 3555::52
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                        Owner    Metric
  Interface     Pri  Gw
3555::52/128                                 O       1
  gei-1/3   110  fe80:2e::2d0:d0ff:fe78:99dd

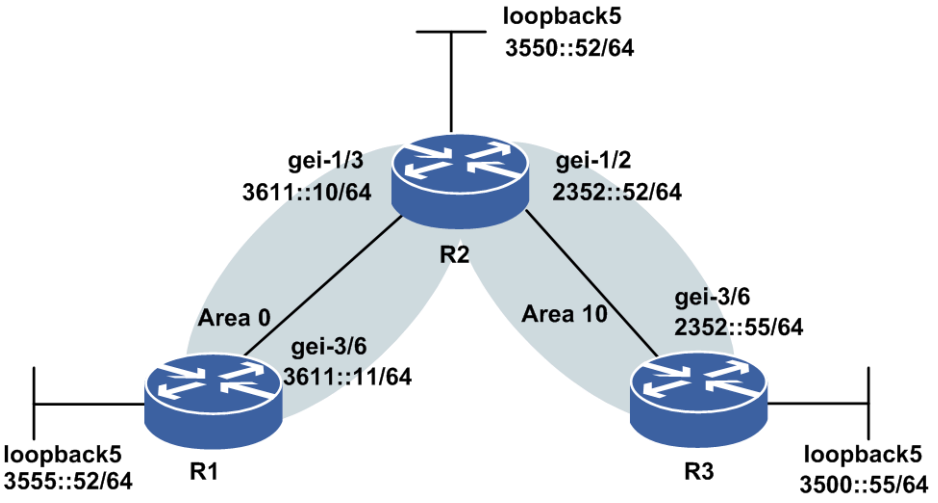
R2#ping6 3555::52
sending 5,100-byte ICMP echo(es) to 3555:0:0:0:0:0:0:52,timeout is 2 second(s).
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 2/3/4 ms.
```

12.5.3 OSPFv3 重分发配置实例

配置说明

如*图 12-12*所示，R1和R2通过直连接口建链，R1和R2在区域0建链，R2和R3在区域10建链，通告各自的一个回环地址路由，R1重分发直连路由。

图 12-12 OSPFv3 重分发配置拓扑图



配置思路

1.各接口使能IPv6，配置IPv6地址，并配置回环接口，使能IPv6，配置IPv6地址。

2.配置OSPFv3。

3.将各接口加入到OSPFv3，R1和R2在区域0建链，R2和R3在区域10建链，R1配置重分发直连路由。

4.查看配置结果，确认各设备正确建立邻居，分别能够学到另两台设备通告的路由，分别能够ping通其他设备通告的loopback接口。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-3/6
R1(config-if-gei-3/6)#no shutdown
R1(config-if-gei-3/6)#ipv6 enable
R1(config-if-gei-3/6)#ipv6 address  3611::11/64
R1(config-if-gei-3/6)#exit
R1(config)#interface loopback5
R1(config-if-loopback5)#ipv6 enable
R1(config-if-loopback5)#ipv6 address  3555::52/64
R1(config-if-loopback5)#exit

R1(config)#ipv6 router ospf 1
R1(config-ospfv3-1)#router-id 11.11.11.11
R1(config-ospfv3-1)#area 0
R1(config-ospfv3-1-area-0)#interface gei-3/6
R1(config-ospfv3-1-area-0-if-gei-3/6)#exit
R1(config-ospfv3-1-area-0)#redistribute connected
R1(config-ospfv3-1-area-0)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#no shutdown
R2(config-if-gei-1/3)#ipv6 enable
R2(config-if-gei-1/3)#ipv6 address 3611::10/64
R2(config-if-gei-1/3)#exit
```

```
R2(config)#interface gei-1/2
R2(config-if-gei-1/2)#no shutdown
R2(config-if-gei-1/2)#ipv6 enable
R2(config-if-gei-1/2)#ipv6 address 2352::52/64
R2(config-if-gei-1/2)#exit
R2(config)#interface loopback5
R2(config-if-loopback5)#ipv6 enable
R2(config-if-loopback5)#ipv6 address 3550::52/64
R2(config-if-loopback5)#exit

R2(config)#ipv6 router ospf 1
R2(config-ospfv3-1)#router-id 10.10.10.10
R2(config-ospfv3-1)#area 0
R2(config-ospfv3-1-area-0)#interface gei-1/3
R2(config-ospfv3-1-area-0-if-gei-1/3)#exit
R2(config-ospfv3-1-area-0)#interface loopback5
R2(config-ospfv3-1-area-0-if-loopback5)#exit
R2(config-ospfv3-1-area-0)#exit
R2(config-ospfv3-1)#area 10
R2(config-ospfv3-1-area-10-if-gei-1/2)#exit
R2(config-ospfv3-1-area-10)#exit
```

R3上的配置如下：

```
R3(config)#interface gei-3/6
R3(config-if-gei-3/6)#no shutdown
R3(config-if-gei-3/6)#ipv6 enable
R3(config-if-gei-3/6)#ipv6 address 2352::55/64
R3(config-if-gei-3/6)#exit
R3(config)#interface loopback5
R3(config-if-loopback5)#ipv6 enable
R3(config-if-loopback5)#ipv6 address 3500::55/64
R3(config-if-loopback5)#exit

R3(config)#ipv6 router ospf 1
R3(config-ospfv3-1)#router-id 1.1.1.5
R3(config-ospfv3-1)#area 10
R3(config-ospfv3-1-area-10)#interface gei-3/6
R3(config-ospfv3-1-area-10-if-gei-3/6)#exit
R3(config-ospfv3-1-area-10)#interface loopback5
R3(config-ospfv3-1-area-10-if-loopback5)#exit
R3(config-ospfv3-1-area-10)#exit
```

配置验证

完成上述配置后，在各设备上可以利用**show ipv6 ospf neighbor**和**show ipv6 forwarding route**命令查看建立的邻居信息和路由信息，互ping loopback接口，都能ping通，说明配置成功。

在R1上查看和验证的结果如下：

```
R1#show running-config ospfv3
!<ospfv3>
ipv6 router ospf 1
  router-id 11.11.11.11
  redistribute connected
 area 0.0.0.0
    interface gei-3/6
 $
  $
$
!</ospfv3>

R1#show ipv6 ospf neighbor
OSPFv3 Process 1
Neighbor ID   Pri   State      Dead Time   Interface ID    Interface
```

```
10.10.10.10    1   FULL/BDR     00:00:35       46       gei-3/6

R1#show ipv6 forwarding route 3550::52
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                        Owner    Metric
  Interface     Pri  Gw
3550::52/128                                 O       1
  gei-3/6    110  fe80:12::2d0:d0ff:feaf:cc10

R1#ping6 3550::52
sending 5,100-byte ICMP echo(es) to 3550:0:0:0:0:0:0:52,timeout is 2 second(s).
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 3/3/3 ms.

R1#show ipv6 forwarding route 3500::55
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                        Owner    Metric
  Interface     Pri  Gw
3500::55/128                                 O       2
  gei-3/6    110  fe80:12::2d0:d0ff:feaf:cc10

R1 #ping6 3500::55
sending 5,100-byte ICMP echo(es) to 3500:0:0:0:0:0:0:55,timeout is 2 second(s).
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 3/3/3 ms.
```

在R2上查看和验证的结果如下：

```
R2#show running-config ospfv3
!<ospfv3>
ipv6 router ospf 1
  router-id 10.10.10.10
 area 0.0.0.0
    interface gei-1/3
    $
    interface loopback5
    $
  $
  area 0.0.0.10
    interface gei-1/2
    $
  $
$
!</ospfv3>

R2#show ipv6 ospf neighbor
OSPFv3 Process 1
Neighbor ID    Pri   State     Dead Time  Interface ID  Interface
1.1.1.5        1     FULL/BDR  00:00:33     54          gei-1/2
11.11.11.11    1     FULL/DR   00:00:37     18          gei-1/3

R2#show ipv6 forwarding route 3555::52
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                        Owner    Metric
  Interface     Pri  Gw
3555::/64                                    O       20
  gei-1/3    110  fe80:2e::2d0:d0ff:fe78:99dd
```

```
R2#ping6 3555::52
sending 5,100-byte ICMP echo(es) to 3555:0:0:0:0:0:0:52,timeout is 2 second(s).
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 2/2/3 ms.
```

在R3上查看和验证的结果如下：

```
R3#show running-config ospfv3
!<ospfv3>
ipv6 router ospf 1
  router-id 1.1.1.5
 area 0.0.0.0
    interface gei-3/6
    $
  $
  area 0.0.0.10
    interface loopback5
    $
  $
$
!</ospfv3>

R3#show ipv6 ospf neighbor
OSPFv3 Process 1
Neighbor ID    Pri    State     Dead Time   Interface ID   Interface
10.10.10.10     1    FULL/DR   00:00:31       45        gei-3/6

R3#show ipv6 forwarding route 3555::52
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                          Owner    Metric
  Interface     Pri  Gw
3555::/64                                      O      20
  gei-3/6   110  fe80:36::2d0:d0ff:feaf:cc10

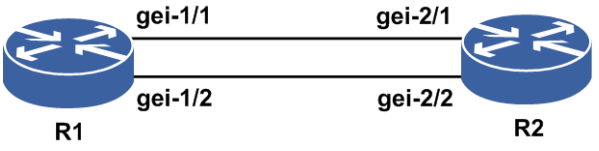
R3#ping6 3555::52
sending 5,100-byte ICMP echo(es) to 3555:0:0:0:0:0:0:52,timeout is 2 second(s).
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 2/3/7 ms.
```

12.5.4 OSPFv3 路由负荷分担配置实例

配置说明

如*图 12-13*所示负荷分担配置，最多支持32个下一跳，以2条下一跳举例。

图 12-13 OSPFv3 路由负荷分担配置实例示意图



配置思路

1.按*图 12-13*所示搭建环境。

2.配置接口地址和OSPFv3配置。

3.接口下配置负荷分担。

配置过程

R1的配置如下：

```
R1(config)#interface gei-2/1
R1(config-if-gei-2/1)#no shutdown
R1(config-if-gei-2/1)#ipv6 enable
R1(config-if-gei-2/1)#ipv6 address 2005::1/64
R1(config)#interface gei-2/2
R1(config-if-gei-2/2)#no shutdown
R1(config-if-gei-2/2)#ipv6 enable
R1(config-if-gei-2/2)#ipv6 address 2006::1/64
R1(config)#interface loopback11
R1(config-if-loopback11)#ip address 2.2.2.2 255.255.255.255
R1(config-if-loopback11)#exit

R1(config)#ipv6 router ospf 1
R1(config-ospfv3-1)#router-id 2.2.2.2
R1(config-ospfv3-1)#area 0
R1(config-ospfv3-1-area-0)#interface gei-2/1
R1(config-ospfv3-1-area-0)#interface gei-2/2   /*OSPFv3的配置*/
R1(config-ospfv3-1-area-0)#maximum-paths 2     /*配置负荷分担数量2*/
R1(config-ospfv3-1-area-0)#exit
```

R2的配置如下：

```
R2(config)#interface gei-2/1
R2(config-if-gei-2/1)#no shutdown
R2(config-if-gei-2/1)#ipv6 enable
R2(config-if-gei-2/1)#ipv6 address 2005::2/64
R2(config)#interface gei-2/2
R2(config-if-gei-2/2)#no shutdown
R2(config-if-gei-2/2)#ipv6 enable
R2(config-if-gei-2/2)#ipv6 address 2006::2/64
R2(config)#interface loopback11
R2(config-if-loopback11)#ip address 1.1.1.1 255.255.255.255
R2(config)#interface loopback10
R2(config-if-loopback10)#ipv6 enable
R2(config-if-loopback10)#ipv6 address 2000::2/64
R2(config-if-loopback10)#exit

R2(config)#ipv6 router ospf 1
R2(config-ospfv3-1)#router-id 1.1.1.1
R2(config-ospfv3-1)#area 0
R2(config-ospfv3-1-area-0)#interface gei-2/1    /*OSPFv3的配置*/
R2(config-ospfv3-1-area-0)#interface gei-2/2
R2(config-ospfv3-1-area-0)#interface loopback10
R2(config-ospfv3-1-area-0)#maximum-paths 2
R2(config-ospfv3-1-area-0)#exit
```

配置验证

在R1上使用**show ipv6 forwarding route ospf**命令查看到同一目的地址2000::2，两条相同代价的路由转发表。

12.6 IS-ISv6

IS-IS是一种扩展性很强的路由协议，从支持CLNS的路由协议扩展到支持IPv4。同样由于IS-IS强健的扩展性，使得IS-IS同样支持IPv6。

单拓扑IS-IS只能运行单个SPF算法，此时IPv4和IPv6对应的拓扑必须相同，有一定的限制。而多拓扑IS-IS可以运行多个SPF算法，IPv4和IPv6的拓扑可以不相同，带来了一定的灵活性。

相关RFC中定义了两个新的TLV类型来支持IS-ISv6协议：IPv6 Reachability TLV和IPv6 Interface Address TLV。

- IPv6 Reachability TLV的TLV类型值为236（0xEC），其TLV效果等同于IPv4的两个TLV：IP内部可达和IP外部可达。
- IPv6 Interface Address TLV的TLV类型值为232（0xE8），其TLV效果等同于IPv4中的TLV：IP端口地址。

IS-ISv6原理的工作原理和IS-ISv4的类似。

12.6.1 配置 IS-ISv6

配置IS-ISv6协议路由的相关属性和功能，包括基本属性、全局参数、汇总路由、重分发协议路由、路由负荷分担、快速重路由以及接口参数等。

1.配置IS-ISv6基本属性。

步骤	命令	功能
1	inspur(config)#**router isis** <*process-id*>[**vrf** <*vrf-name*>]	启动IS-ISv6路由协议进程
2	inspur(config-isis-process-id)#**system-id** <*system-id*>[**range** <*range-number*>]	配置路由实体的系统ID
	inspur(config-isis-process-id)#**area** <*area-address*>	配置IS-ISv6的区域地址

<*system-id*>：该实例的SystemID，6个字节的16进制字符串，以xxxx.xxxx.xxxx的形式输入。

<*range-number*>：SystemID的可扩展范围，范围0~32，缺省为0，实例将使用从SystemID到SystemID＋<*range-number*>的ID值。

<*area-address*>：区域地址，为1~13个字节的16进制字符串。

2.在IS-ISv6路由模式下，配置IS-ISv6全局参数。

如果网络中运行的都是IR12000设备，在配置IS-ISv6路由时，使用缺省参数即可。但在与别的厂家设备对接时，相关的接口参数和定时器可能需要加以调整，以使IS-ISv6协议在网络中能够更加高效的运行。

命令	功能

命令	功能
inspur(config-isis-process-id)#**enable**	开启IS-ISv6协议功能，配置**disable**命令关闭
inspur(config-isis-process-id)#**authentication-type** {**md5** | **text**}[**level-1** | **level-2**]	配置IS-ISv6路由实体的认证模式
inspur(config-isis-process-id)#**ignore-lsp-errors**	配置IS-ISv6忽略LSP的校验和错误
inspur(config-isis-process-id)#**is-type** {**level-1** | **level-2-only** | **level-1-2**}	配置路由器的路由level
inspur(config-isis-process-id)#**max-lsp-lifetime** <*interval*>	配置LSP的最大生存时间，单位：秒，范围1~65535，缺省为1200秒
inspur(config-isis-process-id)#**metric-style** {**narrow** | **wide**}	配置路由器的metric类型，**narrow**模式仅有6bits位来携带metric值，**wide**模式有24bits位来携带metric值，且支持携带更多的TLV
inspur(config-isis-process-id)#**authentication** {< *key*>| **encrypt** < *key*>}[**level-1** | **level-2**]	配置IS-ISv6的LSP/SNP认证密钥
inspur(config-isis-process-id)#**disable-snp-authentication**	关闭SNP认证 当配置LSP/SNP认证后，若仅需要开启LSP认证，配置该命令
inspur(config-isis-process-id)#**enable-snp-authentication**	开启SNP认证，关闭SNP认证后若要开启配置该命令
inspur(config-isis-process-id)#**hostname dynamic**{**disable** | **enable**}	配置IS-ISv6的动态主机名映射功能
inspur(config-isis-process-id)#**hello padding**	配置IS-ISv6在接口上发出的hello报文填充0，直到报文的大小等于接口的MTU

3.在IS-ISv6地址簇模式下，配置IS-ISv6全局参数。

步骤	命令	功能
1	inspur(config-isis-process-id)#**address-family ipv6**	进入IPv6地址族配置模式
2	inspur(config-isis-process-id-af)#**distance** <*1-255*>	配置IS-ISv6的路由优先级，范围是1~255，缺省为115
	inspur(config-isis-process-id-af)#**multi-topology**	启用多拓扑功能
	inspur(config-isis-process-id-af)#**set-overload-bit**	设定IS-ISv6的OL标志位
	inspur(config-isis-process-id-af)#**rou**	配置level-2向level-1路由泄露

步骤	命令	功能
	ter-leak level-2 into level-1 route-map *<map-tag>*	
	inspur(config-isis-process-id-af)#**distribute-list route-map** *<map-tag>* **in**	配置IS-ISv6的路由过滤策略
	inspur(config-isis-process-id-af)#**spf-interval** *<interval>*[**level-1** | **level-2**]	配置IS-ISv6的拓扑计算的最少时间间隔，单位：秒，范围1~120，缺省为3秒
	inspur(config-isis-process-id-af)#**prefix-priority** {**critical** | **high** | **medium**}{**acl-name** *<acl-name>*| **tag** *<value>*}[{**level-1** | **level-2**}]	配置IPv6前缀优先级

critical：设置关键的前缀规则。

high：设置较高的前缀规则。

medium：设置中间的前缀规则。

acl-name *<acl-name>*：ACL列表表明优先级，范围：1~31个字符。

tag *<value>*：设置一个标签表明优先级，范围：1~4294967295。

level-1：路由器处于Level-1区域。

level-2：路由器处于Level-2区域。

4.配置IS-ISv6汇总路由和重分发协议路由。

命令	功能
inspur(config-isis-process-id-af)#**redistribute** *<protocol>*[**level-1** | **level-1-2** | **level-2**][**metric** *<metric-value>*][**route-map** *<map-tag>*]	配置来自于别的路由协议的路由重分发到IS-ISv6中
inspur(config-isis-process-id-af)#**summary-prefix** *<ipv6-prefix>*[{[**metric** *<metric-value>*],[{**level-1** | **level-1-2** | **level-2**}]}	配置IS-ISv6汇总路由

<protocol>：路由来源，可以为connected、static、rip、isis <process-id>、ospf <process-id>、bgp、aftr、sf-nat64、sl-nat64-ipv6，若重分配ISIS/OSPF路由，则需要指定相应的实例号。

level-1 | **level-2** | **level-1-2**：路由器所在的区域，缺省为level-2。

metric *<metric-value>*：IS-ISv6路由的metric值。如果为**metric-style narrow**模式，范围：0~63；如果为**metric-style wide**模式，范围：0~4261412864。

<map-tag>：设置当前协议再分配的路由映射名称，长度为1~31个字符。

<ipv6-prefix>：IPv6网段前缀，格式为"X:X::X:X/<0-128>"。

5.配置IS-ISv6路由的负荷分担和快速重路由。

命令	功能

命令	功能
inspur(config-isis-process-id-af)#**maximum-paths** <*number*>	在IS-IS路由模式下，配置负荷分担， <*number*>表示支持的负荷分担条目，范围为1~32
inspur(config-isis-process-id-af)#**fast-reroute enable**	启用IS-IS快速重路由功能
inspur(config-isis-process-id-af)#**fast-reroute alternate-type** {**down-stream-path**}	设置IS-IS快速重路由类型

6.配置IS-ISv6接口参数。

步骤	命令	功能
1	inspur(config-isis-process-id)#**interface** <*interface-name*>	进入IS-ISv6接口配置模式
2	inspur(config-isis-process-id-if-interface-name)#**ipv6 router isis**	在接口上启用IS-ISv6协议功能
3	inspur(config-isis-process-id-if-interface-name)#**circuit-type** {**level-1** | **level-1-2** | **level-2-only**}	配置IS-ISv6接口能建立邻接关系的类型，默认为**level-1-2**类型
	inspur(config-isis-process-id-if-interface-name)#**csnp-interval** <*interval*>[**level-1** | **level-2**]	配置IS-ISv6在接口上发送CSNP的时间间隔，单位：秒，范围1~65535，在广播链路上缺省为10秒，在点到点链路上缺省为3600秒
	inspur(config-isis-process-id-if-interface-name)#**hello-interval** <*interval*>[**level-1** | **level-2**]	配置IS-ISv6在某接口上发出两个连续hello的时间间隔，单位：秒，范围1~65535，缺省为10秒
	inspur(config-isis-process-id-if-interface-name)#**hello-multiplier** <*multiplier*>[**level-1** | **level-2**]	配置邻居关系的保存时间与hello间隔时间的倍数，范围3~1000，缺省为3
	inspur(config-isis-process-id-if-interface-name)#**lsp-interval** <*interval*>[**level-1** | **level-2**]	配置IS-ISv6在接口上连续发送两个LSP报文的最小时间间隔，单位：秒，范围33~4294967040，缺省为33秒
	inspur(config-isis-process-id-if-interface-name)#**psnp-interval** <*interval*>[**level-1** | **level-2**]	配置IS-ISv6在接口上发送PSNP包的时间间隔，单位：秒，范围1~65535，缺省为3秒
	inspur(config-isis-process-id-if-interface-name)#**ipv6 metric** <*value*>[**level-1** | **level-2**]	配置IS-ISv6在接口上的metric，范围1~16777215，在启用多拓扑后生效，默认为10
	inspur(config-isis-process-id-if-interface-name)#**authentication-type** {**md5** | **text**}[**level-1** | **level-2**]	配置IS-ISv6 hello报文的认证模式
	inspur(config-isis-process-id-if-interface-name)#**authentication** {**key**| **encrypt** <*key*>}[**level-1** | **level-2**]	配置IS-ISv6 hello报文的认证

步骤	命令	功能
	inspur(config-isis-process-id-if-interface-name)#**priority** <*priority*>[**level-1** | **level-2**]	配置IS-ISv6在广播网接口上的优先级，范围0~127，缺省为64
	inspur(config-isis-process-id-if-interface-name)#**retransmit-interval** <*interval*>[**level-1** | **level-2**]	配置IS-ISv6在接口上重发LSP的重传间隔，单位：秒，缺省为5秒
	inspur(config-isis-process-id-if-interface-name)#**max-burst** <*number*>	设置IS-ISv6接口下LSP包一次最多发送的个数，范围1~50，缺省为20
	inspur(config-isis-process-id-if-interface-name)#**mesh-group** {<*mesh group number*>| **blocked**}	设置IS-ISv6接口下的mesh-group功能，范围1~4294967295
	inspur(config-isis-process-id-if-interface-name)#**network point-to-point**	启用LAN网络接口模拟点对点接口功能
	inspur(config-isis-process-id-if-interface-name)#**metric** <*value*>[**level-1** | **level-2**]	配置IS-ISv6在接口上的metric，范围1~16777215，默认为10

7.验证配置结果。

Command	Function
inspur(config)#**show isis adjacency** [**level-1**{ **process-id** }| **level-2**{ **process-id** }| **process-id** | **up-time** {**level-1**{ **process-id** }| **level-2**{ **process-id** }}]	显示当前IS-ISv6的邻居信息
inspur(config)#**show isis database** [**WORD**]|[**level-1**]|[**level-2**]**detail**{**WORD**|**Process-id**{**WORD**}}|**verbose** { **WORD**|[**level-1**]|[**level-2**]{**WORD**|**Process-id**{**WORD**}}| **Process-id**{**WORD**}	显示当前IS-ISv6的数据库
inspur(config)#**show isis circuits** [**process-id**|**detail**{**process-id**}]	显示当前IS-ISv6的端口信息
inspur(config)#**show isis** [**ipv6**] **topology** [**level-1**{**process-id**}| **level-2**{**process-id**}| **process-id**]	显示当前IS-ISv6的拓扑信息
inspur(config)#**show isis hostname** [**process-id**]	显示当前IS-ISv6的主机名映射信息
inspur(config)#**show isis mesh-groups**{**blocked** | **group**}[**process-id**]	显示IS-ISv6的mesh-groups信息
inspur(config)#**show isis ipv6 fast-reroute-topology** [{**level-1** | **level-2** | **process-id** <*process-id*>}]	显示快速重路由信息的拓扑

8.维护IS-ISv6路由接口。

命令	功能
inspur(config-isis-process-id-if-interfac	将一个接口配置成被动模式，设置

命令	功能
e-name)#**passive-mode**	了该命令的接口不能进行路由更新
inspur(config-isis-process-id-if-interfac e-name)#**ipv6 bfd-enable**	启用IS-ISv6在接口上的双向快速链路检测协议
inspur(config-isis-process-id-if-interfac e-name)#**ipv6 fast-reroute block**	本接口上不启用IPv6 fast-reroute功能

9.IS-ISv6的**debug**维护命令。

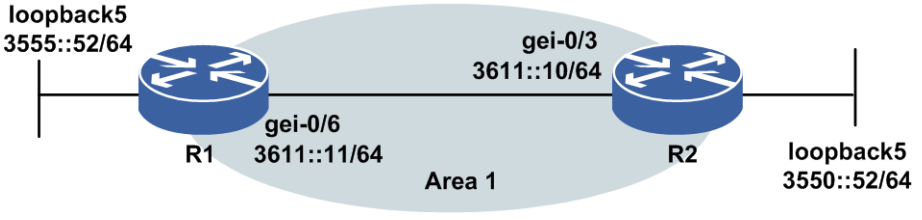
命令	功能
inspur#**debug isis all**	跟踪显示IS-ISv6的所有调试信息
inspur#**debug isis update-packets** [**process-id** *<0-65535>*]	跟踪显示IS-ISv6更新事件调试信息
inspur#**debug isis adj-packets** [**process-id** *<0-65535>*]	跟踪显示IS-ISv6邻居关系信息
inspur#**debug isis mpls traffic-eng events** [**process-id** *<0-65535>*]	跟踪显示ISIS MPLS事件调试信息
inspur#**debug isis spf-events** [**process-id** *<0-65535>*]	跟踪显示IS-ISv6路由计算事件调试信息
inspur#**debug isis snp-packets**[**process-id** *<0-65535>*]	跟踪显示IS-ISv6序列号数据包调试信息

12.6.2 单区域 IS-ISv6 配置实例

配置说明

如*图 12-14*所示为单区域IS-ISv6配置的典型图例，下面以该图说明IS-IS协议的基本配置。

图 12-14 单区域 IS-ISv6 配置实例拓扑图



配置思路

1.R1和R2直连接口使能IPv6，配置IPv6地址，并配置回环接口，使能IPv6，配置IPv6

地址。

2.配置IS-ISv6协议，两台设备，system-id不能相同，若设备同时有接口配置了IPv4的IS-IS，则可以将两台设备均设置为多拓扑，配置多拓扑需要先将IS-IS的metric类型设置为wide；若两台设备均无接口配置IPv4的IS-IS协议，则两端可用默认的单拓扑建立邻居；若设备有接口配置IPv4地址及IS-IS协议，两端也可以单拓扑来建立IS-ISv6，此时接口需同时配置IPv4地址和IPv6地址，且同时配置**ip router isis**和**ipv6 router isis**，本例中以多拓扑为例。

3.在各接口上启用IS-ISv6协议。

4.测试配置结果，确认两台设备已正确建立邻居，并正确计算出IPv6拓扑，从两台设备上分别能够ping6通对端loopback接口。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-0/6
R1(config-if-gei-0/6)#ipv6 enable
R1(config-if-gei-0/6)#ipv6 address 3611::11/64
R1(config-if-gei-0/6)#no shutdown
R1(config-if-gei-0/6)#exit
R1(config)#interface loopback5
R1(config-if-loopback5)#ipv6 enable
R1(config-if-loopback5)#ipv6 address 3555::52/64
R1(config-if-loopback5)#exit

R1(config)#router isis
R1(config-isis-0)#area 47.0005
R1(config-isis-0)#system-id 0000.0000.0011
R1(config-isis-0)#metric-style wide
R1(config-isis-0)#hostname dynamic disable
R1(config-isis-0)#interface gei-0/6
R1(config-isis-0-if-gei-0/6)#ipv6 router isis
R1(config-isis-0-if-gei-0/6)#exit
R1(config-isis-0)#interface loopback5
R1(config-isis-0-if-loopback5)#ipv6 router isis
R1(config-isis-0-if-loopback5)#exit
R1(config-isis-0)#address-family ipv6
R1(config-isis-0-af)#multi-topology
R1(config-isis-0-af)#end
```

R2上的配置如下：

```
R2(config)#interface gei-0/3
R2(config-if-gei-0/3)#ipv6 enable
R2(config-if-gei-0/3)#ipv6 address 3611::10/64
R2(config-if-gei-0/3)#no shutdown
R2(config-if-gei-0/3)#exit
R2(config)#interface loopback5
R2(config-if-loopback5)#ipv6 enable
R2(config-if-loopback5)#ipv6 address 3550::52/64
R2(config-if-loopback5)#exit

R2(config)#router isis
R2(config-isis-0)#area 47.0005
R2(config-isis-0)#system-id 0000.0000.0010
R2(config-isis-0)#metric-style wide
R2(config-isis-0)#hostname dynamic disable
R2(config-isis-0)#interface gei-0/3
R2(config-isis-0-if-gei-0/3)#ipv6 router isis
R2(config-isis-0-if-gei-0/3)#exit
R2(config-isis-0)#interface loopback5
```

```
R2(config-isis-0-if-loopback5)#ipv6 router isis
R2(config-isis-0-if-loopback5)#exit
R2(config-isis-0)#address-family ipv6
R2(config-isis-0-af)#multi-topology
R2(config-isis-0-af)#end
```

配置验证

配置完成以后，在两端设备上可以通过show命令查看配置信息，双方可正确建立邻居，并计算出拓扑，从两台设备上ping6对端的loopback接口，可以ping6通，说明配置成功。

R1上的配置验证，可以通过**show running-config isis**命令查看IS-IS的配置信息：

```
R1#show running-config isis
!<isis>
router isis 0
  area 47.0005
  system-id 0000.0000.0011
  hostname dynamic disable
  metric-style wide
  address-family ipv6
    multi-topology
  $
  interface gei-0/6
    ipv6 router isis
  $
  interface loopback5
    ipv6 router isis
  $
$
!</isis>
```

使用**show isis adjacency**命令查看邻居状态是否正常，主要看state字段是否为UP的，邻居状态建立以后显示UP状态：

```
R1#show isis adjacency
Interface    System id      State  Lev  Holds  SNPA(802.2)    Pri    MT
gei-0/6      0000.0010.0022  UP/UP  L1L2 7/6    00D0.D0AF.CC10 64/64  M
```

使用**show isis ipv6 topology**命令查看拓扑是否正确计算出来（若单拓扑环境，则使用**show isis topology**命令查看）。如果计算出来，则在执行结果中可以看到如下条目，metric为“--”，表示本机，metric为“**”，表示不可达：

```
R1#show isis ipv6 topology
Process ID: 0
IS-IS paths to Level-1 routers
System id      Metric    Next-Hop     Interface      SNPA
0000.0000.0010  10    0000.0010.0022   gei-0/6     00D0.D0AF.CC10
0000.0000.0011  --
IS-IS paths to Level-2 routers
System id      Metric    Next-Hop     Interface     SNPA
0000.0000.0010  10    0000.0010.0022   gei-0/6    00D0.D0AF.CC10
0000.0000.0011  --
```

使用**show isis circuits**命令查看接口信息，及DIS选举情况，如果接口状态为UP表示接口状态正常，如果为down，则表示不正常，需要查看链路状态，Level1-DR项显示为DIS的system-id：

```
R1#show isis circuits
Process ID: 0
IS-IS interface database:
Interface   State Lev  CirId Level1-DR         Level2-DR         Pri(L1/L2)
loopback5    Up   L1L2 0     Disabled          Disabled          64/64
gei-0/6      Up   L1L2 6     0000.0000.0010-03  0000.0000.0010-03 64/64
```

可以使用**show ipv6 forwarding route isis-l1**或**show ipv6 forwarding route isis-l2**命令查看通告的路由情况，路由通告正常的可以看到对端的loopback接口路由信息：

```
R1#show ipv6 forwarding route isis-l1
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                          Owner    Metric
  Interface     Pri   Gw
3550::/64                                      I1       20
  gei-0/6       115   fe80:12::2d0:d0ff:feaf:cc10
```

邻居建立和路由通告正常，可以ping6通对端loopback接口：

```
R1#ping6 3550::52
sending 5,100-byte ICMP echoes to 3550::52,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 0/0/0 ms.
```

同样在R2端验证配置结果如下：

```
R2#show running-config isis
!<isis>
router isis 0
  area 47.0005
  system-id 0000.0000.0010
  metric-style wide
  hostname dynamic disable
  address-family ipv6
    multi-topology
  $
  interface gei-0/3
    ipv6 router isis
  $
  interface loopback5
    ipv6 router isis
  $
$
!</isis>

R2#show isis adjacency
Interface    System id      State  Lev  Holds  SNPA(802.2)    Pri   MT
gei-0/3  0000.0000.0011 UP/UP  L1L2 25/25  00D0.D078.99DD 64/64 M

R2#show isis ipv6 topology
Process ID: 0
IS-IS paths to Level-1 routers
System id      Metric    Next-Hop      Interface     SNPA
0000.0000.0010 --
0000.0000.0011 10        0000.0000.0011 gei-0/3    00D0.D078.99DD
IS-IS paths to Level-2 routers
System id      Metric    Next-Hop      Interface     SNPA
0000.0000.0010 --
0000.0000.0011 10        0000.0000.0011 gei-0/3    00D0.D078.99DD

R2#show isis circuits
IS-IS interface database:
Interface   State Lev  CirId Level1-DR   Level2-DR    Pri(L1/L2)
loopback5     Up    L1L2 0   Disabled    Disabled     64/64
gei-0/3       Up    L1L2 3   Dis is me   Dis is me    64/64

R2#show ipv6 forwarding route isis-l1
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
```

```
Dest                                          Owner    Metric
  Interface     Pri   Gw
3555::/64                                      I1       20
  gei-0/3       115   fe80:2e::2d0:d0ff:fe78:99dd

R2#ping6 3555::52
sending 5,100-byte ICMP echoes to 3555::52,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 0/0/0 ms.
```

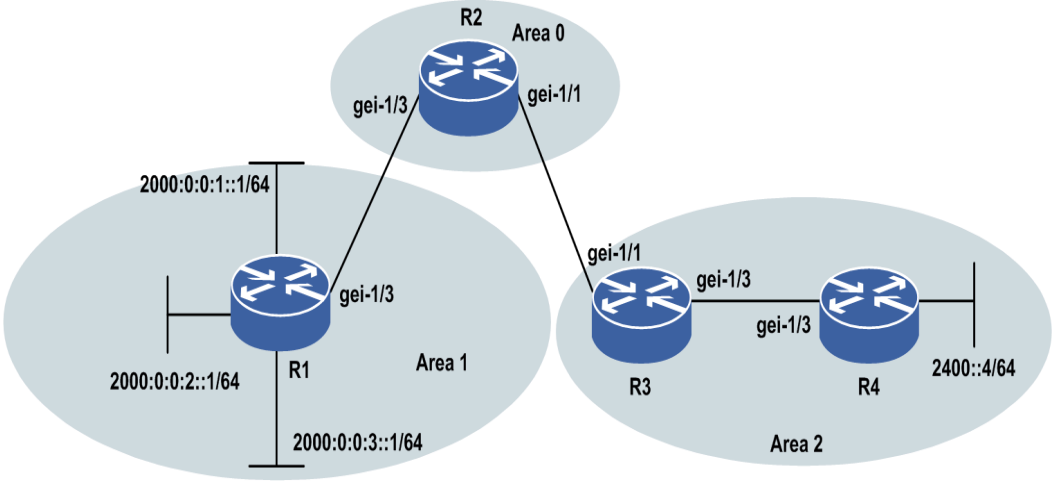
12.6.3 多区域 IS-ISv6 配置实例

配置说明

在网络较大时，应该考虑在IS-IS中使用多个区域。可根据地域及功能将相近的路由器划分在一个区域内，区域的划分有助于减少内存的需求。使区域内的路由器只需要维护较小的链路状态数据库。

如*图 12-15*所示是一个配置有多区域的IS-IS实例，其中R1属于区域1；R2属于区域0；R3，R4属于区域2。在R1中对区域1的网段进行了路由聚合，在R4上将默认路由再分配到了IS-IS中。

图 12-15 多区域 IS-ISv6 配置实例拓扑



配置思路

1.对各接口使能IPv6，配置IPv6地址，并配置回环接口，使能IPv6，配置IPv6地址。

2.配置IS-ISv6协议，每台设备的system-id不能相同，R2和R1、R3之间分别建立L2邻居，R3和R4之间建立L1邻居，同样以多拓扑为例。

3.在接口上启用IS-ISv6协议。

4.在R1设备上启用路由聚合。

5.在R4上重分发直连路由。

6.测试配置结果，确认各设备正确建立邻居，并正确计算出IPv6拓扑，各设备接口地址可ping6通。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#ipv6 enable
R1(config-if-gei-1/3)#ipv6 address 2003::1/64
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#exit
R1(config)#interface loopback1
R1(config-if-loopback1)#ipv6 enable
R1(config-if-loopback1)#ipv6 address 2000:0:0:1::1/64
R1(config-if-loopback1)#exit
R1(config)#interface loopback2
R1(config-if-loopback2)#ipv6 enable
R1(config-if-loopback2)#ipv6 address 2000:0:0:2::1/64
R1(config-if-loopback2)#exit
R1(config)#interface loopback3
R1(config-if-loopback3)#ipv6 enable
R1(config-if-loopback3)#ipv6 address 2000:0:0:3::1/64
R1(config-if-loopback3)#exit

R1(config)#router isis
R1(config-isis-0)#area 01
R1(config-isis-0)#system-id 0000.0000.0011
R1(config-isis-0)#is-type level-1-2
R1(config-isis-0)#metric-style wide
R1(config-isis-0)#interface gei-1/3
R1(config-isis-0-if-gei-1/3)#ipv6 router isis
R1(config-isis-0-if-gei-1/3)#circuit-type level-2-only
R1(config-isis-0-if-gei-1/3)#exit
R1(config-isis-0)#interface loopback1
R1(config-isis-0-if-loopback1)#ipv6 router isis
R1(config-isis-0-if-loopback1)#circuit-type level-2-only
R1(config-isis-0-if-loopback1)#exit
R1(config-isis-0)#interface loopback2
R1(config-isis-0-if-loopback2)#ipv6 router isis
R1(config-isis-0-if-loopback2)#circuit-type level-2-only
R1(config-isis-0-if-loopback2)#exit
R1(config-isis-0)#interface loopback3
R1(config-isis-0-if-loopback3)#ipv6 router isis
R1(config-isis-0-if-loopback3)#circuit-type level-2-only
R1(config-isis-0-if-loopback3)#exit
R1(config-isis-0)#address-family ipv6
R1(config-isis-0-af)#multi-topology           /*多拓扑配置*/
R1(config-isis-0-af)#summary-prefix 2000::/48  /*路由聚合*/
R1(config-isis-0-af)#end
```

R2上的配置如下：

```
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#ipv6 enable
R2(config-if-gei-1/3)#ipv6 address 2003::2/64
R2(config-if-gei-1/3)#no shutdown
R2(config-if-gei-1/3)#exit
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ipv6 enable
R2(config-if-gei-1/1)#ipv6 address 2001::2/64
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit

R2(config)#router isis
R2(config-isis-0)#area 00
R2(config-isis-0)#system-id 0000.0000.0012
R2(config-isis-0)#is-type level-2
R2(config-isis-0)#metric-style wide
```

```
R2(config-isis-0)#interface gei-1/1
R2(config-isis-0-if-gei-1/1)#ipv6 router isis
R2(config-isis-0-if-gei-1/1)#circuit-type level-2-only
R2(config-isis-0-if-gei-1/1)#exit
R2(config-isis-0)#interface gei-1/3
R2(config-isis-0-if-gei-1/3)#ipv6 router isis
R2(config-isis-0-if-gei-1/3)#circuit-type level-2-only
R2(config-isis-0-if-gei-1/3)#exit
R2(config-isis-0)#address-family ipv6
R2(config-isis-0-af)#multi-topology
R2(config-isis-0-af)#end
```

R3上的配置如下：

```
R3(config)#interface gei-1/1
R3(config-if-gei-1/1)#ipv6 enable
R3(config-if-gei-1/1)#ipv6 address 2001::3/64
R3(config-if-gei-1/1)#no shutdown
R3(config-if-gei-1/1)#exit
R3(config)#interface gei-1/3
R3(config-if-gei-1/3)#ipv6 enable
R3(config-if-gei-1/3)#ipv6 address 2300::3/64
R3(config-if-gei-1/3)#no shutdown
R3(config-if-gei-1/3)#exit

R3(config)#router isis
R3(config-isis-0)#area 02
R3(config-isis-0)#system-id 0000.0000.0013
R3(config-isis-0)#is-type level-1-2
R3(config-isis-0)#metric-style wide
R3(config-isis-0)#interface gei-1/1
R3(config-isis-0-if-gei-1/1)#ipv6 router isis
R3(config-isis-0-if-gei-1/1)#circuit-type level-2-only
R3(config-isis-0-if-gei-1/1)#exit
R3(config-isis-0)#interface gei-1/3
R3(config-isis-0-if-gei-1/3)#ipv6 router isis
R3(config-isis-0-if-gei-1/3)#circuit-type level-1
R3(config-isis-0-if-gei-1/3)#exit
R3(config-isis-0)#address-family ipv6
R3(config-isis-0-af)#multi-topology
R3(config-isis-0-af)#end
```

R4上的配置如下：

```
R4(config)#interface gei-1/3
R4(config-if-gei-1/3)#ipv6 enable
R4(config-if-gei-1/3)#ipv6 address 2300::4/64
R4(config-if-gei-1/3)#no shutdown
R4(config-if-gei-1/3)#exit
R4(config)#interface loopback4
R4(config-if-loopback4)#ipv6 enable
R4(config-if-loopback4)#ipv6 address 2400::4/64
R4(config-if-loopback4)#exit

R4(config)#ipv6 route ::/0 2400::1
R4(config)#router isis
R4(config-isis-0)#area 02
R4(config-isis-0)#system-id 0000.0000.0014
R4(config-isis-0)#is-type level-1
R4(config-isis-0)#default-information originate
R4(config-isis-0)#metric-style wide
R4(config-isis-0)#interface gei-1/3
R4(config-isis-0-if-gei-1/3)#ipv6 router isis
R4(config-isis-0-if-gei-1/3)#circuit-type level-1
R4(config-isis-0-if-gei-1/3)#exit
R4(config-isis-0)#interface loopback4
R4(config-isis-0-if-loopback4)#ipv6 router isis
R4(config-isis-0-if-loopback4)#circuit-type level-1
R4(config-isis-0)#address-family ipv6
R4(config-isis-0-af)#multi-topology
```

```
R4(config-isis-0-af)#redistribute static metric 10  /*重分发路由*/
R4(config-isis-0-af)#end
```

配置验证

配置完成以后，在各设备上可以通过show命令查看配置信息，可正确建立邻居，并计算出拓扑，可以ping6通各接口，说明配置成功。

R1上的配置验证，可以通过**show running-config isis**命令查看IS-IS的配置信息：

```
R1#show running-config isis
!<isis>
router isis 0
  area 01
  system-id 0000.0000.0011
  metric-style wide
  address-family ipv6
    multi-topology
    summary-prefix 2000::/48
  $
  interface gei-1/3
    ipv6 router isis
circuit-type level-2-only
  $
  interface loopback1
    ipv6 router isis
circuit-type level-2-only
  $
interface loopback2
    ipv6 router isis
circuit-type level-2-only
  $
interface loopback3
    ipv6 router isis
circuit-type level-2-only
  $
$
!</isis>
```

使用**show isis adjacency**命令查看邻居状态是否正常，主要看state字段是否为UP的，邻居状态建立以后显示UP状态，结果如下：

```
R1#show isis adjacency
Interface   System id      State  Lev  Holds  SNPA(802.2)   Pri  MT
gei-1/3 0000.0000.0012  UP     L2   7    00D0.D078.99D2  64   M
```

使用**show isis ipv6 topology**命令查看拓扑是否正确计算出来（若单拓扑环境，则使用**show isis topology**命令查看），如果计算出来，则在执行结果中可以看到如下条目，metric为“--”，表示本机，metric为“**”，表示不可达：

```
R1#show isis ipv6 topology
Process ID: 0
IS-IS paths to Level-1 routers
System id     Metric    Next-Hop     Interface        SNPA
0000.0000.0011 --
IS-IS paths to Level-2 routers
System id     Metric    Next-Hop     Interface       SNPA
0000.0000.0012 10    0000.0000.0012   gei-1/3     00D0.D078.99D2
0000.0000.0013 20    0000.0000.0012   gei-1/3     00D0.D078.99D2
0000.0000.0014 30    0000.0000.0012   gei-1/3     00D0.D078.99D2
0000.0000.0011 –
```

可以使用**show ipv6 forwarding route isis-l2**命令查看通告的路由情况，路由通告正常的可以看到对端的loopback接口路由信息：

```
R1#show ipv6 forwarding route isis-l2
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                          Owner     Metric
  Interface    Pri     Gw
2001::/64                                      I2        10
  gei-1/3      115     fe80:2e::2d0:d0ff:fe78:99d2
2300::/64                                      I2        20
  gei-1/3      115     fe80:2e::2d0:d0ff:fe78:99d2
2400::/64                                      I2        30
  gei-1/3      115     fe80:2e::2d0:d0ff:fe78:99d2
```

邻居建立和路由通告正常，可以ping6通R4的loopback接口：

```
R1#ping6 2400::4
sending 5,100-byte ICMP echoes to 2400::4,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max=97/120/156 ms.
```

同样在R2端验证配置结果如下：

```
R2#show running-config isis
!<isis>
router isis 0
  area 00
  system-id 0000.0000.0012
  is-type level-2-only
  metric-style wide
  address-family ipv6
    multi-topology
  $
  interface gei-1/1
    ipv6 router isis
    circuit-type level-2-only
  $
  interface gei-1/3
    ipv6 router isis
    circuit-type level-2-only
  $
$
!</isis>

R2#show isis adjacency
Interface    System id      State  Lev  Holds  SNPA(802.2)   Pri  MT
gei-1/3      0000.0000.0011 UP     L2   25  00D0.D078.99DD   64   M
gei-1/1      0000.0000.0013 UP     L2   25  00D0.D078.99D3   64   M

R2#show isis ipv6 topology
IS-IS paths to Level-2 routers
System id      Metric    Next-Hop      Interface        SNPA
0000.0000.0012 --
0000.0000.0011 10      0000.0000.0011   gei-1/3   00D0.D078.99DD
0000.0000.0013 10      0000.0000.0013   gei-1/1   00D0.D078.99D3
0000.0000.0014 20      0000.0000.0013   gei-1/1   00D0.D078.99D3

R2#show isis circuits
Process ID: 0
Interface   State Lev  CirId Level1-DR    Level2-DR      Pri(L1/L2)
gei-1/3     Up   L2   3     Disabled    Dis is me        64/64
gei-1/1     Up   L2   2     Disabled    0000.0000.0013-01 64/64

R2#show ipv6 forwarding route isis-l2
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
```

```
Dest                                          Owner    Metric
  Interface    Pri   Gw
2000::/48                                      I2       10
  gei-1/3      115  fe80:2e::2d0:d0ff:fe78:99dd
2300::/64                                      I2       10
  gei-1/1      115  fe80:2e::2d0:d0ff:fe78:99d3
2400::/64                                      I2       20
  gei-1/1      115  fe80:2e::2d0:d0ff:fe78:99d3
```

在R3端验证配置结果如下：

```
R3#show running-config isis
!<isis>
router isis 0
  area 02
  system-id 0000.0000.0013
  metric-style wide
  address-family ipv6
    multi-topology
  $
  interface gei-1/1
    ipv6 router isis
    circuit-type level-2-only
  $
  interface gei-1/3
    ipv6 router isis
    circuit-type level-1
  $
$
!</isis>

R3#show isis adjacency
Interface    System id      State  Lev  Holds  SNPA(802.2)  Pri  MT
gei-1/3  0000.0000.0014 UP     L1   25  00D0.D078.99D4  64   M
gei-1/1  0000.0000.0012 UP     L2   25  00D0.D078.99D2  64   M

R3#show isis ipv6 topology
Process ID: 0
IS-IS paths to Level-1 routers
System id      Metric    Next-Hop      Interface        SNPA
0000.0000.0013 --
0000.0000.0014 10      0000.0000.0014 gei-1/3     00D0.D078.99D4

IS-IS paths to Level-2 routers
System id      Metric     Next-Hop      Interface          SNPA
0000.0000.0013 --
0000.0000.0011 10      0000.0000.0012 gei-1/1     00D0.D078.99D2
0000.0000.0012 20      0000.0000.0012 gei-1/1     00D0.D078.99D2

R3#show ipv6 forwarding route
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
        D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
        S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                          Owner    Metric
  Interface     Pri     Gw
2000::/48                                      I2       20
  gei-1/1      115   fe80:2e::2d0:d0ff:fe78:99d4
2003::/64                                      I2       10
  gei-1/1      115   fe80:2e::2d0:d0ff:fe78:99d2
2400::/64                                      I1       10
  gei-1/1      115   fe80:2e::2d0:d0ff:fe78:99d2
```

在R4端验证配置结果如下：

```
R4#show running-config isis
!<isis>
router isis 0
  area 02
```

```
  system-id 0000.0000.0014
  is-type level-1
  metric-style wide
  address-family ipv6
    multi-topology
    redistribute connected metric 10
  $
  interface gei-1/1
    ipv6 router isis
    circuit-type level-1
  $
$
!</isis>

R4#show isis adjacency
Interface    System id      State  Lev  Holds  SNPA(802.2)   Pri  MT
gei-1/3  0000.0000.0013 UP     L1   25  00D0.D078.99D3   64   M

R4#show isis ipv6 topology
Process ID: 0
IS-IS paths to Level-1 routers
System id      Metric    Next-Hop      Interface        SNPA
0000.0000.0014 --
0000.0000.0013 10        0000.0000.0013 gei-1/3    00D0.1234.561F

R4#ping6 2000:0:0:1::1
sending 5,100-byte ICMP echoes to 2000:0:0:1::1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 56/93/102 ms.
```

12.7 BGP4+

BGP4+是对BGP协议的扩展，沿用了RFC中规定的BGP的基本消息格式，增加了用于传送IPv6路由信息的扩展属性，并按照RFC中的规定对所有IPv6路由进行处理。BGP4+同时支持RFC协议中规定的BGP路由反射、BGP联盟等扩展功能，有以下特点：

- 运行可靠，采用TCP作为其底层协议，用TCP端口179
- 只发送路由的更新信息
- 定期发送keepalives信号，来确保TCP连接的正常
- 拥有完善的度量值
- 拥有丰富的属性（attributes）和控制功能
- 专门用于大型网络

BGP4+的工作原理和BGP类似。

12.7.1 配置 BGP4+

配置BGP4+协议路由的相关属性和功能，包括基本功能、路由负荷分担等。

1.配置BGP4+基本功能。

IR12000智能路由器上BGP4+的基本配置命令与IPv4中对BGP的配置类似，只是增加了支持IPv6地址的功能配置。具体内容参考“IR12000智能路由器 配置指导（IPv4路由）”中“BGP配置”内容。

2.配置BGP4+路由负荷分担。

步骤	命令	功能
1	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
	inspur(config-bgp)#**address-family ipv6**	进入BGP IPv6地址族配置模式
2	inspur(config-bgp-af-ipv6)#**maximum-paths ibgp**< *number*>	配置协议支持负荷分担的路由数目，范围1~32，缺省为1（针对IBGP的负荷分担）
	inspur(config-bgp-af-ipv6)#**maximum-paths** < *number*>	配置协议支持负荷分担的路由数目，范围1~32，缺省为1（针对EBGP的负荷分担）
	inspur(config-bgp-af-ipv6)#**maximum-paths eibgp** <*number*>	配置协议支持负荷分担的路由数目，范围1~32，缺省为1（针对IBGP和EBGP路由形成的负荷分担）
3	inspur(config-bgp-af)#**bgp frr**	配置BGP FRR功能，备份路由数目默认值是1
4	inspur(config)#**interface** < *interface-name*>	进入接口配置模式
	inspur(config-if-interface-name)#**ip load-sharing** {**per-destination** | **per-packet**}	配置接口负荷分担模式：负荷分担是在出接口上配置的，默认情况下为**per-destination** 只有所有的接口配置为**per-packet**模式，负荷分担的模式才是**per-packet**

3.验证配置结果。

命令	功能
inspur(config)#**show ip bgp protocol**	显示本地BGP协议模块的配置信息
inspur(config)#**show bgp ipv6 unicast neighbor** [{<*ipv4-addr*>|<*ipv6-addr*>}]	查看BGP邻接关系，显示当前邻居状态
inspur(config)#**show bgp ipv6 unicast**	显示BGP路由选择表中的条目
inspur(config)#**show bgp ipv6 unicast summary**	显示所有BGP邻居连接的状态

4.维护BGP4+。

命令	功能
inspur#**debug ip bgp in**	跟踪显示BGP发出的notification报文，并列出错误号和子错误号
inspur#**debug ip bgp out**	跟踪显示BGP发出的notification报文，

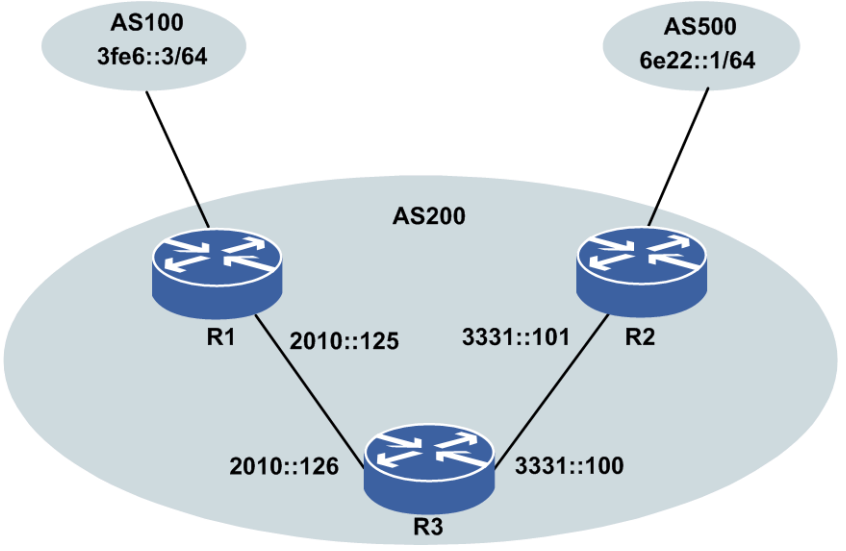
命令	功能
	并列出错误号和子错误号
inspur#**debug ip bgp keepalives**	BGP Keepalieve消息处理情况
inspur#**debug ip bgp updates**	BGP Update消息处理情况；可以具体到只对某个对等体相关的Update消息处理情况进行跟踪打印
inspur#**debug ip bgp events**	跟踪显示BGP连接的状态机迁移
inspur#**show debug bgp**	显示debug命令配置信息

12.7.2 BGP4+路由反射器配置实例

配置说明

如*图 12-16*所示的网络中，路由器R1、R2和R3间是IBGP，但是没有全连接。现在为了打破IBGP必须是全连接的连接规则，配置路由反射器，使得R3能够将IBGP邻居接收到的路由，转发给另外一个IBGP邻居。鉴于AS 200中的IBGP不是全连接，可以配置路由反射器来避免全连接。

图 12-16 BGP4+路由反射器配置拓扑图



配置思路

1.按照组网图对各接口使能IPv6，配置IPv6地址。

2.启动BGP。

3.指定邻居。

4.配置路由反射器簇ID，将邻居设置为路由反射器客户对等体。

配置过程

本实例接口IPv6地址配置省略。

R1上的配置如下：

```
R1(config)#router bgp 200
R1(config-bgp)#neighbor 3fe6::3 remote-as 100
R1(config-bgp)#neighbor 2010::126 remote-as 200
R1(config-bgp)#address-family ipv6
R1(config-bgp-af-ipv6)#neighbor 3fe6::3 activate
R1(config-bgp-af-ipv6)#neighbor 2010::126 activate
R1(config-bgp-af-ipv6)#end
```

R2上的配置如下：

```
R2(config)#router bgp 200
R2(config-bgp)#neighbor 6e22::1 remote-as 500
R2(config-bgp)#neighbor 3331::100 remote-as 200
R2(config-bgp)#address-family ipv6
R2(config-bgp-af-ipv6)#neighbor 6e22::1 activate
R2(config-bgp-af-ipv6)#neighbor 3331::100 activate
R2(config-bgp-af-ipv6)#end
```

R3上的配置如下：

```
R3(config)#router bgp 200
R3(config-bgp)#neighbor 2010::125 remote-as 200
R3(config-bgp)#neighbor 3331::101 remote-as 200
R3(config-bgp)#address-family ipv6
R3(config-bgp-af-ipv6)#neighbor 2010::125 activate
R3(config-bgp-af-ipv6)#neighbor 3331::101 activate
R3(config-bgp-af-ipv6)#neighbor 2010::125 route-reflector-client  /*配置反射
器*/
R3(config-bgp-af-ipv6)#neighbor 3331::101 route-reflector-client
R3(config-bgp-af-ipv6)#end
```

配置验证

通过R3上配置的反射器，R1和R2上的路由信息一致。

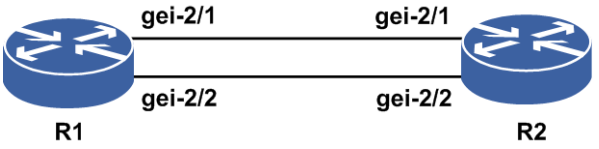
12.7.3 BGP4+路由负荷分担配置实例

配置说明

负荷分担可使超出单个接口带宽的流量均分到多条链路上，实现流量在各条链路上的负载均衡。

如*图 12-17*所示，以BGP4+协议为例，在同一邻居节点在同一区域有多条链路可达，且其链路代价相同，启用负荷分担，则可实现BGP4+的负荷分担。

图 12-17 BGP4+路由负荷分担配置实例



配置思路

1.对各接口开启IPv6，配置IPv6地址，并配置逐包的负荷分担（默认为逐流分担）；在R2上配置loopback1的IPv6地址。

2.启用并配置BGP4+协议。

3.在R1上配置BGP4+的负荷分担。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/1
R1(config-if-gei-2/1)#ipv6 enable
R1(config-if-gei-2/1)#ipv6 address 2000::1/64
R1(config-if-gei-2/1)#exit
R1(config)#interface gei-2/2
R1(config-if-gei-2/2)#ipv6 enable
R1(config-if-gei-2/2)#ipv6 address 2001::1/64
R1(config-if-gei-2/2)#exit
R1(config)#router bgp 100
R1(config-bgp)#neighbor 2000::2 remote-as 100
R1(config-bgp)#neighbor 2001::2 remote-as 100
R1(config-bgp)#address-family ipv6
R1(config-bgp-af-ipv6)#maximum-paths ibgp 16  /*配置负荷分担*/
R1(config-bgp-af-ipv6)#neighbor 2000::2 activate
R1(config-bgp-af-ipv6)#neighbor 2001::2 activate
R1(config-bgp-af-ipv6)#end

R1(config)#interface gei-2/1
R1(config-if-gei-2/1)#ip load-sharing per-packet
R1(config)#interface gei-2/2
R1(config-if-gei-2/2)#ip load-sharing per-packet
R1(config-if-gei-2/2)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-2/1
R2(config-if-gei-2/1)#ipv6 enable
R2(config-if-gei-2/1)#ipv6 address 2000::2/64
R2(config-if-gei-2/1)#exit
R2(config)#interface gei-2/2
R2(config-if-gei-2/2)#ipv6 enable
R2(config-if-gei-2/2)#ipv6 address 2001::2/64
R2(config-if-gei-2/2)#exit
R2(config)#interface loopback1
R2(config-if-loopback1)#ipv6 enable
R2(config-if-loopback1)#ipv6 address 2000:0:0:1::2/64
R2(config-if-loopback1)#exit

R2(config)#router bgp 100
R2(config-bgp)#neighbor 2000::1 remote-as 100
R2(config-bgp)#neighbor 2001::1 remote-as 100
```

```
R2(config-bgp)#address-family ipv6
R2(config-bgp-af-ipv6)#neighbor 2000::1 activate
R2(config-bgp-af-ipv6)#neighbor 2001::1 activate
R2(config-bgp-af-ipv6)#network 2000:0:0:1::2/128
R2(config-bgp-af-ipv6)#end
```

配置验证

在R1侧学习到的IBGP路由，用**show**命令验证配置结果：

```
R1#show ipv6 forwarding route bgp
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                              Owner  Metric
  Interface      Pri     Gw
2000:0:0:1::/64                     B      0
  gei-2/1        20      fe80:12::1
2000:0:0:1::/64                     B      0
  gei-2/2        20      fe80:16::1
```

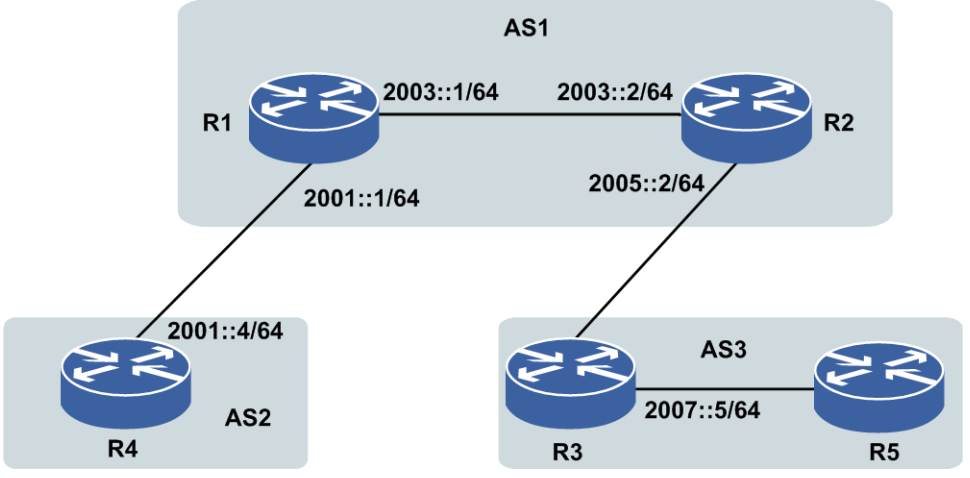
12.7.4 BGP4+综合配置实例

配置说明

下面是一个BGP4+综合实例，其中涉及到IBGP和EBGP建立邻居，路由策略，路由的再分配，MD5加密等BGP4+功能的实际应用。

如*图 12-18*所示，R4和R1建立EBGP，R1和R2建立IBGP，R2和R5建立多跳EBGP。其中，R2与R5之间通过R3建立EBGP多跳关系，此时在配置BGP之前需要保证该两台路由器建立邻居的地址能够互通（提供配置IGP来配置，这部分配置省略）。

图 12-18 BGP4+综合配置实例拓扑图



配置思路

1.对各接口开启IPv6，配置IPv6地址。

2.创建一个BGP4+实例。

3.配置BGP4+邻居，配置路由策略。

4.配置重分发命令，邻居通告路由。

配置过程

本实例接口IPv6地址配置省略，具体配置可以参考“BGP4+路由负荷分担配置实例”。

R4上的配置如下：

```
R4(config)#router bgp 2
R4(config-bgp)#neighbor 2001::1 remote-as 1
R4(config-bgp)#address-family ipv6
R4(config-bgp-af-ipv6)#neighbor 2001::1 activate
R4(config-bgp-af-ipv6)#redistribute static   /*配置重分发静态路由*/
R4(config-bgp-af-ipv6)#end
```

R1上的配置如下：

```
R1(config)#router bgp 1
R1(config-bgp)#neighbor 2003::2  remote-as 1
R1(config-bgp)#neighbor 2001::4  remote-as 2
R1(config-bgp)#address-family ipv6
R1(config-bgp-af-ipv6)#neighbor 2001::4 activate
R1(config-bgp-af-ipv6)#neighbor 2003::2 activate
R1(config-bgp-af-ipv6)#end
```

R2上的配置如下：

```
R2(config)#router bgp 1
R2(config-bgp)#neighbor 2003::1 remote-as 1
R2(config-bgp)#neighbor 2007::5 remote-as 3
R2(config-bgp)#neighbor 2007::5 ebgp-multihop  /*配置多跳*/
R2(config-bgp)#neighbor 2007::5 password hello  /*配置认证*/
R2(config-bgp)#address-family ipv6
R2(config-bgp-af-ipv6)#neighbor 2003::1 activate
R2(config-bgp-af-ipv6)#neighbor 2007::5 activate
R2(config-bgp-af-ipv6)#end
```

R5上的配置如下：

```
R5(config)#router bgp 3
R5(config-bgp)#neighbor 2005::2 remote-as 1
R5(config-bgp)#neighbor 2005::2 ebgp-multihop
R5(config-bgp)#neighbor 2005::2 password hello
R5(config-bgp)#address-family ipv6
R5(config-bgp-af-ipv6)#neighbor 2005::2 activate
R5(config-bgp-af-ipv6)#end
```

配置验证

R1上用命令**show bgp ipv6 unicast summary**查看邻居关系：

```
R1(config)#show bgp ipv6 unicast summary
Neighbor    Ver  As    MsgRcvd    MsgSend    Up/Down    State/PfxRcd
2003::2      4   1     12         12         00:25:34     0
2001::4      4   2     14         14         00:28:06     4
```

R1上用命令**show bgp ipv6 unicast**查看路由表：

```
R1(config)#show bgp ipv6 unicast
Status codes: * valid, > best, i - internal, s - stale
Origin codes: i-IGP, e-EGP, ?-incomplete
   Network          Next Hop     Metric   LocPrf   RtPrf  Path
*> 2004:1::/64    2001::4/64                           2 ?
*> 2004:2::/64    2001::4/64                           2 ?
*> 2004:3::/64    2001::4/64                           2 ?
*> 2004:4::/64    2001::4/64                           2 ?
```

R2上用命令**show bgp ipv6 unicast summary**查看邻居关系：

```
R2(config)#show bgp ipv6 unicast summary
Neighbor     Ver  As     MsgRcvd    MsgSend    Up/Down     State/PfxRcd
2003::1       4    1      12         12       00:25:34     4
2007::5       4    3      15         15       00:32:30     0
```

R2上用命令**show bgp ipv6 unicast**查看路由表：

```
R2(config)#show bgp ipv6 unicast
Status codes: * valid, > best, i - internal, s - stale
Origin codes: i-IGP, e-EGP, ?-incomplete
   Network          Next Hop     Metric    LocPrf  RtPrf   Path
*> 2004:1::/64    2003::1/64              100           2 ?
*> 2004:2::/64    2003::1/64              100           2 ?
*> 2004:3::/64    2003::1/64              100           2 ?
*> 2004:4::/64    2003::1/64              100           2 ?
```

R4上用命令**show bgp ipv6 unicast summary**查看邻居关系：

```
R4(config)#show bgp ipv6 unicast summary
Neighbor     Ver  As     MsgRcvd    MsgSend     Up/Down     State/PfxRcd
2001: : 1     4    1     14         14         00:28:06     0
```

R4上用命令**show bgp ipv6 unicast**查看路由表：

```
R4(config)#show bgp ipv6 unicast
Status codes: * valid, > best, i - internal, s - stale
Origin codes: i-IGP, e-EGP, ?-incomplete
   Network       Next Hop       Metric    LocPrf  RtPrf   Path
*> 2004:1::/64    ::                                  2 ?
*> 2004:2::/64    ::                                  2 ?
*> 2004:3::/64    ::                                  2 ?
*> 2004:4::/64    ::                                  2 ?
```

R5上用命令**show bgp ipv6 unicast summary**查看邻居关系：

```
R5(config)#show bgp ipv6 unicast summary
Neighbor     Ver  As     MsgRcvd    MsgSend    Up/Down      State/PfxRcd
2005::2       4    1     15         15         00:32:30     4
```

R5上用命令**show bgp ipv6 unicast**查看路由表：

```
R5(config)#show bgp ipv6 unicast
Status codes: * valid, > best, i - internal, s - stale
Origin codes: i-IGP, e-EGP, ?-incomplete
   Network       Next Hop       Metric    LocPrf  RtPrf   Path
*> 2004:1::/64    2005::2/64                          1 2 ?
*> 2004:2::/64    2005::2/64                          1 2 ?
*> 2004:3::/64    2005::2/64                          1 2 ?
*> 2004:4::/64    2005::2/64                          1 2 ?
```

12.8 IPv6 Route-Map 策略配置

IPv6 Router-Map是在原IPv4 Router-Map的基础上，增加支持了IPv6的功能，具体功能

同IPv4 Router-Map。

12.8.1 配置 IPv6 路由策略

配置IPv6路由策略的相关属性和功能，包括基本属性、路由属性以及路由策略调用。

1.在路由映射模式下，配置IPv6路由策略的基本属性参数。

步骤	命令	功能
1	inspur(config)#**route-map** <*route-map-name*>[**permit** | **deny**][<*sequence-number*>	创建用于路由策略的route-map，并且进入路由映射配置模式
2	inspur(config-route-map)#**match ipv6 address *(**<*access-list-name*>**)**	在路由映射配置模式下配置match项，匹配类型为IPv6路由条目的目的网段/目的地址，选择使用ACL进行匹配
	inspur(config-route-map)#**match ipv6 metric *(**<*metric-value*>**)**	匹配路由的ipv6 metric值，可根据需要连配多个，取值范围为0~4294967295
	inspur(config-route-map)#**match ipv6 tag *(**<*tag-value*>**)**	匹配路由的ipv6 tag值，OSPF和static路由带此属性，可根据需要连配多个，取值范围为0~4294967295
	inspur(config-route-map)#**match as-path *(**<*as-path list number*>**)**	匹配BGP协议路由as-path的属性，可根据需要连配多个，取值范围为1~199
	inspur(config-route-map)#**match community-list *(**<*community-list-number*>**)**	匹配BGP协议路由的community属性，可根据需要连配多个，取值范围为1~499
	inspur(config-route-map)#**match extcommunity-list *(**<*community-list-number*>**)**	匹配BGP/VPN路由的extcommunity属性，可根据需要连配多个，取值范围为1~500
	inspur(config-route-map)#**match route-type** {**external** [**type-1** | **type-2**]| **internal** | **level-1** | **level-2** | **local**}	匹配路由类型为route-type，根据需要选择路由类型，不能连配，但是可以配置多条此类型的match项。

<*route-map-name*>：路由映射的名称，长度为1~31个字符。

permit | **deny**：一个route-map当中可以有一个或多个sequence，各个序列的属性可以灵活配置为**permit**或**deny**。**permit**表示匹配后执行路由策略；**deny**表示无论是否匹配，都不执行任何动作。

<*sequence-number*>：route-map的序列号，每个route-map支持一至多个序列，在进行匹配时，所有路由按照序列号由小到大的顺序进行匹配，一旦匹配上，根据当前sequence的属性决定是否执行路由策略。

2.配置路由策略中的路由属性参数。

命令	功能
inspur(config-route-map)#**set as-path prepend *(**<*as-number*>**)**	配置路由策略中的路由属性，配置类型为BGP协议独有的as-path属性，可根据需要连配多个
inspur(config-route-map)#**set community**	BGP协议独有，设置团体属性

命令	功能
{**none** | **additive*{no-advertise** | **no-export** | **no-export-subconfed** | **internet** |<*0-65535*>**:**<*0-65535*>|<*1-4294967295*>})}	
inspur(config-route-map)#**set extcommunity rt-trans** {{**remove** | **additive** ***{<*0-65535*>**:**<*0-4294967295*>|<*1-65535*>**.**<*0-65535*>**:**<*0-65535*>| **A.B.C.D:**<*0-65535*>}}|{<*0-65535*>**:**<*0-4294967295*>|<*1-65535*>**.**<*0-65535*>**:**<*0-65535*>| **A.B.C.D:**<*0-65535*>})}	BGP协议独有，设置扩展团体属性
inspur(config-route-map)#**set extcommulity soo-trans** {<*0-65535*>**:**<*0-4294967295*>|<*1-65535*>**.**<*0-65535*>**:**<*0-65535*>| **A.B.C.D:**<*0-65535*>| **remove**}	BGP协议独有，设置扩展团体属性
inspur(config-route-map)#**set dampening** <*half-life*><*reuse*><*suppress*><*max-suppress-time*>	BGP协议独有，设置路由的阻尼参数
inspur(config-route-map)#**set local-preference** <*value*>	BGP协议独有，设置路由的local-preference属性
inspur(config-route-map)#**set origin** {**igp** | **egp** | **incomplete**}	BGP协议独有，设置路由起源属性
inspur(config-route-map)#**set level** <*level-value*>	IS-IS协议中使用，设置IS-IS路由属性
inspur(config-route-map)#**set next-hop** <*ip-address*>[**...**<*ip-address*>]	在路由策略中设置路由的下一跳
inspur(config-route-map)#**set ipv6 metric** [+|-]<*metric-value*>	设置路由的metric值
inspur(config-route-map)#**set ipv6 next-hop ***(<*ipv6-address*>)	设置下一跳地址为IPv6的路由 ***(<*ipv6-address*>)** 下一跳IPv6地址，十六进制点分形式，最多支持10个IPv6地址
inspur(config-route-map)#**set ipv6 precedence** {<*precedence-value*>|<*precedence-value*>}	设置IPv6报头优先级 <*precedence-value*> 在IP报头中设置优先值的编号，范围0~7
inspur(config-route-map)#**set ipv6 traffic-class** <*traffic-value*>	设置IPv6路由的traffic等级，使用**no**命令取消设置 <*traffic-value*> IPv6路由traffic等级值，范围0~255
inspur(config-route-map)#**set ipv6 path interface** <*interface*> **next-hop** <*nexthop*>	当数据包符合用于策略路由时，使用本命令把数据包路由到指定的以太接口及下一跳
inspur(config-route-map)#**set ipv6 metric-type** {**internal** | **external** | **type-1** | **type-2**}	设置路由选择协议的尺度类型
inspur(config-route-map)#**set ipv6 tag** <*tag-value*>	OSPF和静态路由使用的属性

<*half-life*>：改变路由阻尼因素的半衰期，范围为1~45。

<*reuse*>：改变路由阻尼因素的重新使用值，范围为1~20000。

<*suppress*>：改变路由阻尼因素的路由抑制值，范围为1~20000。

<*max-suppress-time*>：改变路由阻尼因素的最大抑制时间，通常路由抑制时间到达该值以后，惩罚值不再增加，范围为1~255。

3.配置RIPng调用路由策略。

步骤	命令	功能
1	inspur(config)#**ipv6 router rip**	进入RIPng配置模式
2	inspur(config-rip)#**redistribute** <*protocol*>[**process-id**][**metric** <*metric-value*>][**route-map** <*prefix-list-name*>]	配置重分发协议路由

<*protocol*>：重分配的协议名称，可以是bgp、connected、isis、ospf、static、aftr、sf-nat64、sl-nat64、subscriber-host。

<*metric-value*>：重分配该协议的度量值，范围为1~16。

<*route-map-name*>：重分配该协议所使用的路由图，范围为1~31。

4.配置IS-ISv6调用路由策略。

步骤	命令	功能
1	inspur(config)#**router isis** <*process-id*>[**vrf** <*vrf-name*>]	进入IS-IS路由配置模式功能
2	inspur(config-isis-id)#**address-family ipv6**	进入IS-ISv6地址簇配置模式
3	inspur(config-isis-id-af)#**redistribute** <*protocol*>[**process-id**][**level-1**][**level-1-2**][**level-2**][**metric-type** <*metric-type*>][**metric** <*metric-value*>][**route-map** <*route-map-name*>]	配置重分发协议路由
4	inspur(config-isis-id-af)#**route-leak level-2 into level-1 route-map** <*route-map-name*>	配置路由泄漏

<*protocol*>：路由来源，可以为connect、static、rip、is-is、ospf、bgp，这是必选项；若重分配IS-IS或OSPF路由，则需要指定相应的实例号。

level-1：设置重分发的路由信息进入Level-1。

level-1-2：设置重分发的路由信息同时进入Level-1和Level-2。

level-2：设置重分发的路由信息进入Level-2。

<*metric-type*>：设置重分发的路由是携带external还是internal的metric值。

<*metric-value*>：metric值，范围0~4261412864。

5.配置OSPFv3调用路由策略。

步骤	命令	功能
1	inspur(config-ospfv3-id)#**redistribute bgp route-map** <*route-map-name*>	按照route-map名字为name的方法重分发BGP路由
2	inspur(config-ospfv3-id)#**redistribute connected route-map** <*route-map-name*>	按照route-map名字为name的方法重分发直连路由
3	inspur(config-ospfv3-id)#**redistribute isis** <*process-id*> **route-map** <*route-map-name*>	按照route-map名字为name的方法重分发IS-IS路由
4	inspur(config-ospfv3-id)#**redistribute rip route-map** <*route-map-name*>	按照route-map名字为name的方法重分发RIP路由
5	inspur(config-ospfv3-id)#**redistribute static route-map** <*route-map-name*>	按照route-map名字为name的方法重分发静态路由

6.配置BGP4+调用路由策略。

步骤	命令	功能
1	inspur(config)#**router bgp** {<*1~65535*>|<*1~65535*>**.**<*0~65535*>}	进入BGP路由配置模式
2	inspur(config-bgp)#**bgp dampening** [**route-map** <*route-map-name*>]	使BGP路由阻尼有效或修改各种BGP路由阻尼因素
3	inspur(config-bgp)#**neighbor** [<*ipv6-address*>|<*peer-group-name*>] **route-map** <*route-map-name*>{**in** | **out**}	对邻居/邻居对等体组通告来的路由，或通告给邻居/邻居对等体组的路由进行过滤，或设置路由的优先级；其中**in** | **out**分别表示应用于输入或输出路由
4	inspur(config-bgp)#**address-family ipv6**	进入BGP4+地址簇配置模式
5	inspur(config-bgp-af)#**redistribute** <*protocol*>[**process-id**][**route-map** <*route-map-name*>]	配置将其他协议类型的路由重分发到BGP中，其中<*protocol*>表示协议类型，如果是OSPF或者ISIS，还需要给出实例号

7.配置VRF调用路由策略。

步骤	命令	功能
1	inspur(config)#**ip vrf** <*vrf-name*>	创建VRF
2	inspur(config-vrf-name)#**rd** <*route-distinguisher*>	配置RD
3	inspur(config-vrf-name)#**route-target** [**import** | **export** | **both**]<*extended-community*>	创建与VRF关联的route-target扩展团体属性

步骤	命令	功能
4	inspur(config-vrf-name)#**address-family ipv6**	进入地址族配置模式
5	inspur(config-vrf-name-af-ipv6)#**import map** <*route-map-name*>	配置与VRF关联的导入路由映射
	inspur(config-vrf-name-af-ipv6)#**export map** <*route-map-name*>	配置与VRF关联的导出路由映射

8.验证配置结果。

命令	功能
inspur(config)#**show running-config ripng**	查看各路由协议当中是否使用了路由策略（显示RIPng协议的配置）
inspur(config)#**show running-config isis**	查看各路由协议当中是否使用了路由策略（显示IS-IS协议的配置）
inspur(config)#**show running-config ospfv3**	查看各路由协议当中是否使用了路由策略（显示OSPF协议的配置）
inspur(config)#**show running-config bgp**	查看各路由协议当中是否使用了路由策略（显示BGP协议的配置）
inspur(config)#**show running-config vrf**	查看各路由协议当中是否使用了路由策略（显示VRF路由的配置）
inspur(config)#**show ip vrf detail** [<*vrf-name*>]	查看VRF的具体配置信息，可指定查看某个目标VRF实例的配置
inspur(config)#**show route-map** [<*route-map-name*>]	查看具体的route-map模板的配置

12.8.2 配置 IPv6 策略路由

本节介绍IPv6策略路由的配置步骤和命令。

1.配置IPv6策略路由。

IPv6策略路由的配置命令和IPv4策略路由的配置命令类似，只是地址可以是IPv6形式的。具体配置命令参考“配置指导 （策略模板）”中“配置策略路由”内容。

2.验证配置结果。

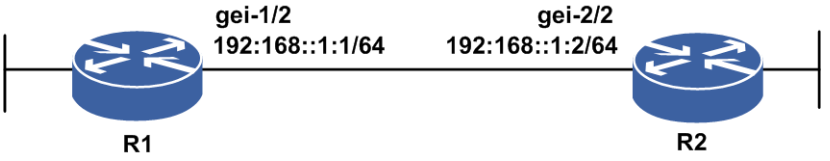
命令	功能
inspur(config)#**show running-config pbr**	显示数据库中存在的策略路由配置信息

12.8.3 RIPng 重分配路由策略配置实例

配置说明

如*图 12-19*所示，在R1和R2上运行RIPng，通告各自的RIPng路由，可重分发其他路由，以重分发静态路由为例。

图 12-19 RIPng 重分配路由策略配置实例示意图



配置思路

1.对各接口使能IPv6，配置IPv6地址。

2.在接口上启用RIPng协议相关配置。

3.重分发其他路由，配置重分发命令。

4.为重分发命令关联route-map名称。

5.配置route-map策略。

6.查看配置结果，确认两台设备分别能够学到对端通告的路由。

配置过程

R1上的配置如下：

```
R1(config)#interface  gei-1/2
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#ipv6 enable
R1(config-if-gei-1/2)#ipv6 address 192:168::1:1/64
R1(config-if-gei-1/2)#exit

R1(config)#route-map www permit 10
R1(config-route-map)#set ipv6 metric 10
R1(config-route-map)#exit

R1(config)#ipv6 router rip
R1(config-ripng)#interface gei-1/2
R1(config-ripng-if-gei-1/2)#ipv6 rip enable
R1(config-ripng-if-gei-1/2)#exit
R1(config-ripng)#redistribute static route-map www
R1(config-ripng)#exit

R1(config)#ipv6 route 1:2:3::0/64  192:168::1:2
```

R2的配置如下：

```
R2(config)#interface gei-2/2
R2(config-if-gei-2/2)#no shutdown
R2(config-if-gei-2/2)#ipv6 enable
R2(config-if-gei-2/2)#ipv6 address 192:168::1:2/64
```

```
R2(config-if-gei-2/2)#exit

R2(config)#ipv6 router rip
R2(config-ripng)#interface gei-2/2
R2(config-ripng-if-gei-2/2)#ipv6 rip enable
R2(config-ripng-if-gei-2/2)#end
```

配置验证

在R1和R2上利用**show**命令来查看RIP、route-map和静态路由的配置信息，以及RIP的路由表和路由信息。

R1上的路由信息如下：

```
R1#show running-config ripng
!<ripng>
ipv6 router rip
  redistribute static route-map www
  interface gei-1/2
    ipv6 rip enable
  $
$
!</ripng>

R1#show running-config ipv6-static-route
!<ipv6-static-route>
ipv6 route 1:2:3::/64 192:168::1:2
!</ipv6-static-route>

R1#show  running-config route-map
!<route-map>
route-map www permit 10
set ip metric 10
$
!</route-map>

R1#show ipv6 rip database
 1:2:3::/64
    nexthop: ::, via: gei-1/2
    metric:   10, tag:   0
 192:168::/64
    nexthop: ::, via: gei-1/2
    metric:   1, tag:   0
```

R2上的路由信息如下：

```
R2#show running-config ripng
!<ripng>
ipv6 router rip
  interface gei-2/2
    ipv6 rip enable
  $
$
!</ripng>

R2#show ipv6 rip database
 1:2:3::/64
    nexthop: fe80::221:1dff:fe1d:1100, via: gei-2/2
    metric:   11, tag:   0, time: 00:13
 192:168::/64
    nexthop: ::, via: gei-2/2
    metric:   1, tag:   0

R2#show ipv6 protocol routing
IPv6 Routing Table
Codes: D - Direct, A - Address, S - Static, R - RIP, UI - USER_IPADDR,
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS static,
```

```
      O - OSPF intra, OI - OSPF inter, E1 - OSPF ext 1, E2 - OSPF ext 2, N -
ND,
      B - BGP, IB - IBGP, EB - EBGP, AG - BGP AGG, V - VRRP, P - PPP, D6 - DHCPv6,
      SFN - Stateful NAT64, SLN - Stateless NAT64, AF - AFTR
Time: The time of last modified!

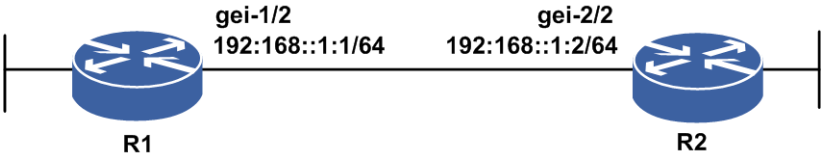
R  1:2:3::/64 [120/11]
    via fe80::221:1dff:fe1d:1100, gei-2/2, 06h39m58s
  D   192:168::/64
    via  , gei-2/2, 03h42m55s
  A   192:168::1:2/128
    via  , gei-2/2, 03h42m55s
```

12.8.4 IS-ISv6 路由策略配置实例

配置说明

如*图 12-20*所示，R1和R2建立ISISv6邻居，状态为up。在R1上配置静态路由，在IS-ISv6中重分发静态路由带route-map参数。

图 12-20 IS-ISv6 路由策略配置实例示意图



配置思路

1.对各接口使能IPv6，配置IPv6地址。

2.R1和R2配置IS-ISv6协议，建立邻居。

3.在R1上配置**route-map testisisv6**。

4.在R1上配置静态路由。

5.在R1上重分发静态路由带route-map参数。

配置过程

1.R1和R2配置IS-ISv6协议，建立邻居。

在R1上配置IS-ISv6：

```
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#ipv6 enable
R1(config-if-gei-1/2)#ipv6 address 192:168::1:1/64
R1(config-if-gei-1/2)#exit

R1(config)#router isis 44
R1(config-isis-44)#system-id 5555.5555.5555
R1(config-isis-44)#area 44
R1(config-isis-44)#is-type level-1-2
```

```
R1(config-isis-44)#metric-style wide
R1(config-isis-44)#interface gei-1/2
R1(config-isis-44-if-gei-1/2)#ipv6 router isis
R1(config-isis-44-if-gei-1/2)#exit
R1(config-isis-44)#address-family ipv6
R1(config-isis-44-af)#multi-topology
```

在R2上配置IS-ISv6：

```
R2(config)#interface gei-2/2
R2(config-if-gei-2/2)#no shutdown
R2(config-if-gei-2/2)#ipv6 enable
R2(config-if-gei-2/2)#ipv6 address 192:168::1:2/64
R2(config-if-gei-2/2)#exit

R2(config)#router isis 44
R2(config-isis-44)#system-id 2222.2222.2222
R2(config-isis-44)#area 44
R2(config-isis-44)#is-type level-1-2
R2(config-isis-44)#metric-style wide
R2(config-isis-44)#interface gei-2/2
R2(config-isis-44-if-gei-2/2)#ipv6 router isis
R2(config-isis-44-if-gei-2/2)exit
R2(config-isis-44)#address-family ipv6
R2(config-isis-44-af)#multi-topology
```

2.在R1上配置**route-map testisisv6**：

```
R1(config)#route-map testisisv6 permit 10
R1(config-route-map)#set ipv6 metric 10
R1(config-route-map)#exit
```

3.在R1上配置静态路由：

```
R1(config)#ipv6 route 1:2:3::/64 192:168::1:2
```

4.在R1上重分发静态路由带route-map参数：

```
R1(config)#router isis 44
R1(config-isis-44)#address-family ipv6
R1(config-isis-44-af)#redistribute static route-map testisisv6
R1(config-isis-44)#exit
```

配置验证

IS-ISv6配置结果：

```
R1(config)#show running-config isis
!<isis>
router isis 44
  area 44
  system-id 5555.5555.5555
  is-type level-1-2
  metric-style wide
  address-family ipv6
    multi-topology
    redistribute static route-map testisisv6
  $
  interface gei-1/2
    ipv6 router isis
  $
$
!</isis>
R2(config)#show running-config isis
!<isis>
router isis 44
  area 44
  system-id 2222.2222.2222
```

```
  is-type level-1-2
  metric-style wide
  address-family ipv6
    multi-topology
  $
  interface gei-2/2
    ipv6 router isis
  $
$
!</isis>
```

Route-Map配置结果：

```
R1(config)#show route-map testisisv6
[route-map testisisv6] IP type: IPv6
route-map testisisv6 permit 10
set ipv6 metric 10
```

静态路由配置结果：

```
R1(config)#show ipv6 forwarding route static
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                              Owner    Metric
  Interface      Pri  Gw
1:2:3::/64                         S        0
  gei-1/2        1    192:168::1:2
```

在R2上查看R1通告过来的IS-ISv6路由信息：

```
R2(config)#show ipv6 protocol routing isis
IPv6 Routing Table
Codes: D - Direct, A - Address, S - Static, R - RIP, UI - USER_IPADDR,
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS static,
       O - OSPF intra, OI - OSPF inter, E1 - OSPF ext 1, E2 - OSPF ext 2, N -
ND,
       B - BGP, IB - IBGP, EB - EBGP, AG - BGP AGG, V - VRRP, P - PPP, D6 - DHCPv6,
       SFN - Stateful NAT64, SLN - Stateless NAT64, AF - AFTR
       M - Multicast
        * - FIB route
       > - selected route, p - stale info
Time: The time of last modified!

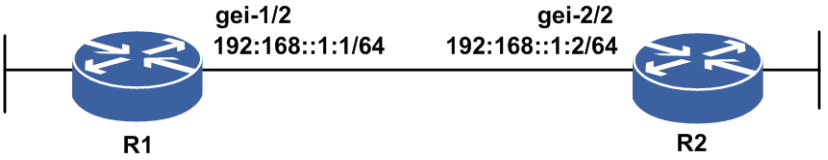
 I2  1:2:3::/64 [115/20]
     via fe80::221:1dff:fe1d:1100, gei-2/2, 06h06m18s
 I1  192:168::/64 [115/20]
     via fe80::221:1dff:fe1d:1100, gei-2/2, 01h46m35s
```

12.8.5 OSPFv3 路由策略配置实例

配置说明

如*图 12-21*所示，R1上的接口放入OSPFv3区域1中，R2上的接口放入OSPFv3区域1中，R1和R2建立OSPFv3邻居，状态为full。在R1上配置1条静态路由，把静态路由在OSPFv3中带route-map参数重分发。

图 12-21 OSPFv3 路由策略配置实例示意图



配置思路

1.对各接口使能IPv6，配置IPv6地址。

2.R1和R2在区域1建立邻居。

3.在R1上配置route-map。

4.在R1上配置1条静态路由。

5.R1上配置OSPFv3重分发静态路由带route-map参数。

配置过程

1.R1和R2直连接口配置同网段地址，用于建立OSPFv3邻居：

```
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#ipv6 enable
R1(config-if-gei-1/2)#ipv6 address 192:168::1:1/64
R1(config-if-gei-1/2)#exit
R1(config)#ipv6 router ospf 1026
R1(config-ospfv3-1026)#router-id 11.11.11.11
R1(config-ospfv3-1026)#area 1
R1(config-ospfv3-1026-area-1)#interface  gei-1/2
R1(config-ospfv3-1026-area-1-if-gei-1/2)#exit
R1(config-ospfv3-1026-area-1)#exit

R2(config)#interface gei-2/2
R2(config-if-gei-2/2)#no shutdown
R2(config-if-gei-2/2)#ipv6 enable
R2(config-if-gei-2/2)#ipv6 address 192:168::1:2/64
R2(config-if-gei-2/2)#exit
R2(config)#ipv6 router ospf 1026
R2(config-ospfv3-1026)#router-id 22.22.22.22
R2(config-ospfv3-1026)#area 1
R2(config-ospfv3-1026-area-1)#interface gei-2/2
R2(config-ospfv3-1026-area-1-if-gei-2/2)#exit
```

2.在R1上配置route-map：

```
R1(config)#route-map ff
R1(config-route-map)#match ipv6 metric 0
R1(config-route-map)#set ipv6 metric 50
R1(config-route-map)#set ipv6 metric-type type-1
R1(config-route-map)#set ipv6 tag 100
```

3.在R1上配置静态路由：

```
R1(config)#ipv6 route 1:2:3::/64 192:168::1:2
```

4.在R1上配置OSPF中重分配静态路由带route-map参数：

```
R1(config)#ipv6 router ospf 1026
R1(config-ospfv3-1026)#redistribute static route-map ff
```

```
  R1(config-ospfv3-1026)#end
```

配置验证

查看R1上的配置结果，以及R1上的静态、OSPF路由：

```
R1#show route-map ff

[route-map ff] IP type: IPv6
route-map ff permit 10
match ipv6 metric 0
set ipv6 metric-type type-1
set ipv6 metric 50
set ipv6 tag 100

R1#show ipv6 forwarding route static
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                Owner    Metric
  Interface       Pri  Gw
1:2:3::/64                           S       0
  gei-1/2         1    192:168::1:2

R1#show running-config  | begin ipv6 router ospf 1026
ipv6 router ospf 1026
  router-id 11.11.11.11
  redistribute static route-map ff
 area 0.0.0.1
    interface gei-1/2
    $
  $
$
!</ospfv3>
R1#show ipv6 ospf database process 1026

          OSPFv3 Router with ID (11.11.11.11) (Process ID 1026)

              Router Link States (Area 0.0.0.1)

ADV Router      Age       Seq#       Link count        Bits
11.11.11.11     997       0x80000006          1     -|-|E|-
22.22.22.22    1246       0x80000005          1     -|-|-|-

              Net Link States (Area 0.0.0.1)

ADV Router      Age       Seq#          Link ID    Rtr count
22.22.22.22     997       0x80000006         22           2

              Intra Area Prefix Link States (Area 0.0.0.1)

ADV Router      Age       Seq#          Link ID    Ref-lstype  Ref-LSID
22.22.22.22    1248       0x80000004          2        0x2002  22

              Link (Type-8) Link States (Area 0.0.0.1)

ADV Router      Age       Seq#         Link ID    Interface
11.11.11.11    1643       0x80000004        22    gei-1/2
22.22.22.22    1256       0x80000004        27    gei-1/2

              Type-5 AS External Link States

ADV Router      Age       Seq#       Prefix
11.11.11.11     996       0x80000001  1:2:3::/64
```

```
/*查看tag的设置*/

R1#show  ipv6  ospf  database  external

          OSPFv3 Router with ID (11.11.11.11) (Process ID 1026)
              Type-5 AS External Link States
LS  age:  109
LS  Type:  AS-external-LSA
Link  State  ID:  0.0.0.13
Advertising  Router:  11.11.11.11
LS  Seq  Number:  0x80000001
Checksum:  0xD1E9
Length:  48
Metric  Type:  1  (Larger  than  any  link  state  path)
Metric:  50
Prefix:  1234::1/128
Prefix  Options:  0  (-|-|-|-)
External  Route  Tag:  100
```

在R2上查看OSPFv3路由的属性：

```
R2#show ipv6 protocol routing ospf
IPv6 Routing Table
Codes: D - Direct, A - Address, S - Static, R - RIP, UI - USER_IPADDR,
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS static,
      O - OSPF intra, OI - OSPF inter, E1 - OSPF ext 1, E2 - OSPF ext 2, N -
ND,
      B - BGP, IB - IBGP, EB - EBGP, AG - BGP AGG, V - VRRP, P - PPP, D6 - DHCPv6,
      SFN - Stateful NAT64, SLN - Stateless NAT64, AF - AFTR
      M - Multicast
       * - FIB route
      > - selected route, p - stale info
Time: The time of last modified!

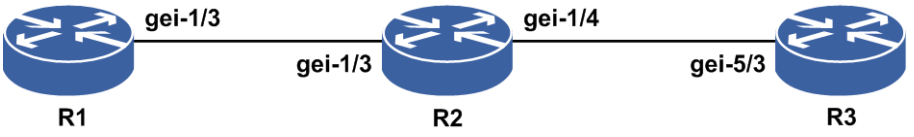
 E1  1:2:3::/64 [110/51]
     via fe80::221:1dff:fe1d:1100, gei-2/2, 08h53m18s
  O  192:168::/64 [110/1]
     via ::, gei-2/2, 07h19m08s
```

12.8.6 BGP4+路由策略配置实例

配置说明

如*图 12-22*所示，R1和R2建立EBGP邻居，R2和R3建立IBGP邻居，R1向R2通告路由。在R2上配置route-map test1，应用在R2连接R1的in方向上，在R2上配置route-map test2，应用在R2连接R3的out方向上。

图 12-22 BGP4+路由策略配置实例



配置思路

1.对各接口使能IPv6，配置IPv6地址。

2.R1和R2建立EBGP邻居，R2和R3建立IBGP邻居。

3.R1向R2通告若干BGP4+路由，R2及R3应正常学习到。

4.R2上配置ipv6-access-list 1、ipv6-access-list 2、route-map test1、route-map test2。

5.R2上将route-map test1应用在R2连接R1邻居的in方向上，将route-map test2应用在R2连接R3邻居的out方向上。

提示：

Route-map分别应用在入接口和出接口时，除了设置下一跳不生效外，其余属性均生效。

Route-map 中 BGP4+ 协 议 的 专 用 选 项 有 （ set： community-list 、 dampening 、 local-preference、origin、as-path、next-hop, Match： as-path、community-list)。

配置过程

1.将三台路由器之间直连接口配置同网段地址，配置EBGP邻居：

R1上的配置如下：

```
R1(config)#interface gei-1/3
R1(config-if-gei-1/3)#no shutdown
R1(config-if-gei-1/3)#ipv6 enable
R1(config-if-gei-1/3)#ipv6 address 1:2::1/64
R1(config-if-gei-1/3)#exit
R1(config)#router bgp 1011
R1(config-bgp)#neighbor 1:2::2 remote-as 200
R1(config-bgp)#address-family ipv6
R1(config-bgp-af-ipv6)#neighbor 1:2::2 activate
R1(config-bgp-af-ipv6)#exit
R1(config-bgp)#exit
```

R2上的配置如下：

```
R2(config)#interface gei-1/3
R2(config-if-gei-1/3)#no shutdown
R2(config-if-gei-1/3)#ipv6 enable
R2(config-if-gei-1/3)#ipv6 address 1:2::2/64
R2(config-if-gei-1/3)#exit

R2(config)#interface gei-1/4
R2(config-if-gei-1/4)#no shutdown
R2(config-if-gei-1/4)#ipv6 enable
R2(config-if-gei-1/4)#ipv6 address 2:3::2/64
R2(config-if-gei-1/4)#exit

R2(config)#router bgp 200
R2(config-bgp)#neighbor 1:2::1 remote-as 1011
R2(config-bgp)#neighbor 2:3::3 remote-as 200
R2(config-bgp)#address-family ipv6
R2(config-bgp-af-ipv6)#neighbor 1:2::1 activate
R2(config-bgp-af-ipv6)#neighbor 2:3::3 activate
R2(config-bgp-af-ipv6)#exit
R2(config-bgp)#exit
```

R3上的配置如下：

```
R3(config)#interface gei-5/3
R3(config-if-gei-5/3)#no shutdown
R2(config-if-gei-5/3)#ipv6 enable
R3(config-if-gei-5/3)#ipv6 address 2:3::3/64
R3(config-if-gei-5/3)#exit

R3(config)#router bgp 200
R3(config-bgp)#neighbor 2:3::2 remote-as 200
```

```
R3(config-bgp)#address-family ipv6
R3(config-bgp-af-ipv6)#neighbor 2:3::2 activate
R3(config-bgp-af-ipv6)#exit
R3(config-bgp)#exit
```

2.R1向R2通告5个BGP路由：

```
R1(config)#router bgp 1011
R1(config-bgp)#address-family ipv6
R1(config-bgp-af-ipv6)#network 4:4::4/64
R1(config-bgp-af-ipv6)#network 5:5::5/64
R1(config-bgp-af-ipv6)#network 6:6::6/64
R1(config-bgp-af-ipv6)#network 7:7::7/64
R1(config-bgp-af-ipv6)#network 8:8::8/64
R1(config-bgp-af-ipv6)#exit
R1(config-bgp)#exit
```

3.R2上配置route-map test1及其中嵌套使用的ACL列表：

```
R2(config)#ipv6-access-list 1
R2(config-ipv6-acl)#rule 1 permit ipv6 4:4::/64 any
R2(config-ipv6-acl)#exit
R2(config)#ipv6-access-list 2
R2(config-ipv6-acl)#rule 1 permit ipv6 7:7::/64 any
R2(config-ipv6-acl)#exit

R2(config)#route-map test1 permit 10
R2(config-route-map)#match ipv6 address 1
R2(config-route-map)#match ipv6 address 2
R2(config-route-map)# set local-preference 30000
R2(config-route-map)#exit
R2(config)#route-map test2 permit 10
R2(config-route-map)#match ipv6 address 1
R2(config-route-map)#match ipv6 metric 5
R2(config-route-map)#match as-path 1
R2(config-route-map)#match community-list 1
R2(config-route-map)#exit
R2(config)#route-map test2 permit 20
R2(config-route-map)#match ipv6 address 2
R2(config-route-map)#set as-path prepend 2
R2(config-route-map)#set local-preference 200
R2(config-route-map)#set origin incomplete
R2(config-route-map)#exit
```

4.R2上将route-map test1应用在连接R1邻居的in方向上，将route-map test2应用在R2连接R3邻居的out方向上：

```
R2(config)#router bgp 200
R2(config-bgp)#address-family ipv6
R2(config-bgp-af-ipv6)#neighbor 1:2::1 route-map test1 in
R2(config-bgp-af-ipv6)#neighbor 2:3::3 route-map test2 out
R2(config-bgp-af-ipv6)#exit
```

配置验证

在步骤2，通告路由后，R2和R3上皆应该能学到5条路由：

```
R2#show bgp ipv6 unicast
Status codes: * valid, > best, i - internal, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop      Metric     LocPrf     RtPrf  Path
*> 4:4::/64         1:2::1                               20     1011 i
*> 5:5::/64         1:2::1                               20     1011 i
*> 6:6::/64         1:2::1                               20     1011 i
*> 7:7::/64         1:2::1                               20     1011 i
*> 8:8::/64         1:2::1                               20     1011 i
```

```
R3#show bgp ipv6 unicast
Status codes: * valid, > best, i - internal, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop       Metric     LocPrf     RtPrf  Path
  i4:4::/64         1:2::1                    100        200    1011 i
  i5:5::/64         1:2::1                    100        200    1011 i
  i6:6::/64         1:2::1                    100        200    1011 i
  i7:7::/64         1:2::1                    100        200    1011 i
  i8:8::/64         1:2::1                    100        200    1011 i
```

步骤4，R2上绑定了路由策略后，R2上仅能学到匹配route-map test1当中嵌套的match项的路由4:4:::/64和7:7::/64，未匹配到的路由学不到。

对应同一条路由策略下，使用多个**match**项时，**macth**项之间是与关系，所以**route-map test2 permit 10**没有匹配到，所以4:4:::/64这条路由不会通告给R3。

使用BGP路由策略后的效果：

```
R2(config)#show bgp ipv6 unicast   /*R2从R1上学习到了2条BGP路由*/
Status codes: * valid, > best, i - internal, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop      Metric     LocPrf     RtPrf  Path
*> 4:4::/64       1:2::1                   30000      20     1011 i
*> 7:7::/64       1:2::1                   30000      20     1011 i
```

2条BGP路由的详细信息如下：

```
R2#show bgp ipv6 unicast detail 4:4::/64
BGP routing table entry for 4:4::/64
  08:50:07 received from 1:2::1 (11.1.1.1)
   origin i, global nexthop 1:2::1, link-local nexthop FE80::220:23FF:FE1D:E0E,
localpref 30000 rtpref 20
   as path [1011]
   as4 path
R2#show bgp ipv6 unicast detail 7:7::/64
BGP routing table entry for 7:7::/64
  08:50:07 received from 1:2::1 (11.1.1.1)
   origin i, global nexthop 1:2::1, link-local nexthop FE80::220:23FF:FE1D:E0E,
localpref 30000 rtpref 20
   as path [1011]
   as4 path
  08:41:38 advertised to 2:3::3 (1.1.1.1)
   origin ?, global nexthop 1:2::1, localpref 200
   as path [2 1011]
   as4 path
```

12.8.7 6VPE 路由策略配置实例

配置说明

6VPE路由策略配置实例组网如*图 12-23*所示，在此网络中建立L3VPN基本组网，PE1和PE2在相同的AS，建立MP-IBGP邻居。PE1上有VRF test1，其中通告了本地Loopback地址生成的Address路由，和对接CE1的直连路由。PE2上有VRF test1，其中通告了本地Loopback地址生成的Address路由，和对接CE2的直连路由。两个PE上VRF test1路由表当中有本地和远端的路由。

PE1上配置VRF test1当中采用route-map路由策略：

•对入向的网段路由进行如下策略是，允许从VPN邻居导入路由。

•对出向的网段进行如下策略是，允许向VPN邻居通告路由。

配置后路由策略生效结果验证。

图 12-23 6VPE 路由策略配置实例示意图



配置实例地址规划表如下。

设备	接口名	IP地址
CE1	gei-1/1	1001::20:2/120
PE1	gei-1/2	1001::20:1/120
	gei-1/3	10.10.12.1/24
PE2	gei-1/6	10.10.12.2/24
	gei-1/7.10	2002::20:2/120
CE2	gei-1/8.10	2002::20:1/120

配置思路

1.配置CE1–PE1–PE2–CE2的L3VPN基本组网环境，对各接口使能IPv6，配置IPv6地址。

2.两台PE的私网路由表内能学到配置说明中规划的所有路由。

3.在PE1上配置route-map，其中定义将要实施路由策略的路由信息的特征，即定义一组匹配规则。可以以路由信息中的不同属性作为匹配依据进行设置，如目的地址、发布路由信息的路由器地址等。

4.PE1上配置VRF实例中应用route-map，实现对路由的导入/导出、路由发布接收和引入时的策略。

配置过程

1.在PE1和PE2上配置L3VPN基本组网。

PE1的配置如下：

```
PE1(config)#ip vrf test1
PE1(config-vrf-test1)#rd 100:1
PE1(config-vrf-test1)#address-family ipv6
PE1(config-vrf-test1-af-ipv6)#route-target import 100:1
PE1(config-vrf-test1-af-ipv6)#route-target export 100:1
PE1(config-vrf-test1-af-ipv6)#exit
PE1(config-vrf-test1)#exit

PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 10.10.1.1 255.255.255.255
PE1(config-if-loopback1)#exit
PE1(config)#interface gei-1/3
PE1(config-if-gei-1/3)#no shutdown
PE1(config-if-gei-1/3)#ip address 10.10.12.1 255.255.255.0
PE1(config-if-gei-1/3)#exit
PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#route-id loopback1
```

```
PE1(config-ldp-1)#interface gei-1/3
PE1(config-ldp-1-if-gei-1/3)#exit
PE1(config-ldp-1)#exit

PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#no shutdown
PE1(config-if-gei-1/2)#ip vrf forwarding test1
PE1(config-if-gei-1/2)#ipv6 enable
PE1(config-if-gei-1/2)#ipv6 address 1001::20:1/120
PE1(config-if-gei-1/2)#exit

PE1(config)#router ospf 1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 10.0.0.0 0.255.255.255
PE1(config-ospf-1-area-0)#exit
PE1(config)#ipv6 router ospf 1 vrf test1
PE1(config-ospfv3-1)#router-id 10.10.1.1
PE1(config-ospfv3-1)#area 0
PE1(config-ospfv3-1-area-0)#interface gei-1/2
PE1(config-ospfv3-1-area-0-if-gei-1/2)#exit
PE1(config-ospfv3-1-area-0)#exit

PE1(config-ospfv3-1)#redistribute bgp
PE1(config-ospfv3-1)#exit

PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 10.10.3.3 remote-as 100
PE1(config-bgp)#neighbor 10.10.3.3 update-source loopback1
PE1(config-bgp)#address-family ipv6 vrf test1
PE1(config-bgp-af-ipv6-vrf)#redistribute connected
PE1(config-bgp-af-ipv6-vrf)#exit
PE1(config-bgp)#address-family vpnv6
PE1(config-bgp-af-vpnv6)#neighbor 10.10.3.3 activate
PE1(config-bgp-af-vpnv6)#exit
PE1(config-bgp)#exit
PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#interface gei-1/3
PE1(config-ldp-1-if-gei-1/3)#exit
PE1(config-ldp-1)#exit
```

PE2的配置如下：

```
PE2(config)#ip vrf test1
PE2(config-vrf-test1)#rd 100:1
PE2(config-vrf-test1)#address-family ipv6
PE2(config-vrf-test1-af-ipv6)#route-target import 100:1
PE2(config-vrf-test1-af-ipv6)#route-target export 100:1
PE2(config-vrf-test1-af-ipv6)#exit
PE2(config-vrf-test1)#exit

PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 10.10.3.3 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#interface gei-1/6
PE2(config-if-gei-1/6)#no shutdown
PE2(config-if-gei-1/6)#ip address 10.10.12.2 255.255.255.0
PE2(config-if-gei-1/6)#exit
PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#interface gei-1/6
PE2(config-ldp-1-if-gei-1/6)#exit
PE2(config-ldp-1)#exit

PE2(config)#interface gei-1/7
PE2(config-if-gei-1/7)#no shutdown
PE2(config-if-gei-1/7)#exit

PE2(config)#interface gei-1/7.10
PE2(config-if-gei-1/7.10)#exit
```

```
PE2(config)#vlan-configuration
PE2(config-vlan)#interface gei-1/7.10
PE2(config-vlan-if-gei-1/7.10)#encapsulation-dot1q 10
PE2(config-vlan-if-gei-1/7.10)#exit
PE2(config-vlan)#exit
PE2(config)#interface gei-1/7.10
PE2(config- if-gei-1/7.10)#ip vrf forwarding test1
PE2(config- if-gei-1/7.10)#ipv6 enable
PE2(config- if-gei-1/7.10)#ipv6 address 2002::20:2/120
PE2(config- if-gei-1/7.10)#exit

PE2(config)#router ospf 1
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 10.0.0.0 0.255.255.255
PE2(config-ospf-1-area-0)#exit
PE2(config)#ipv6 router ospf 1 vrf  test1
PE2(config-ospfv3-1)#router-id 2.2.2.2
PE2(config-ospfv3-1)area 0
PE2(config-ospfv3-1-area-0)#interface gei-1/7.10
PE2(config-ospfv3-1-area-0-gei-1/7.10)#exit
PE2(config-ospfv3-1-area-0)#exit

PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 10.10.1.1 remote-as 100
PE2(config-bgp)#neighbor 10.10.1.1 update-source loopback1
PE2(config-bgp)#address-family ipv6 vrf test1
PE2(config-bgp-af-ipv6-vrf)#redistribute ospf-int 1
PE2(config-bgp-af-ipv6-vrf)#redistribute connected
PE2(config-bgp-af-ipv6-vrf)#exit
PE2(config-bgp)#address-family vpnv6
PE2(config-bgp-af-vpnv6)#neighbor 10.10.1.1 activate
PE2(config-bgp-af-vpnv6)#exit
PE2(config-bgp-vpnv6)#exit
```

2.检查PE1、PE2上的VRF路由。

PE1上显示如下：

```
PE1#show ipv6 protocol routing vrf test1
Vrf test1 IPv6 Routing Table
Codes: D - Direct, A - Address, S - Static, R - RIP, UI - USER_IPADDR,
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS static,
       O - OSPF intra, OI - OSPF inter, E1 - OSPF ext 1, E2 - OSPF ext 2, N
- ND,
       B - BGP, IB - IBGP, EB - EBGP, AG - BGP AGG, V - VRRP, P - PPP, D6 -
DHCPv6,
       SFN - Stateful NAT64, SLN - Stateless NAT64, AF - AFTR
Time: The time of last modified!

IB   22::/64 [200/0]
     via ::ffff:10.10.3.3, loopback1, IPv6-mpls, 09h03m49s
  D   33::/64
     via ::, loopback33, 07h10m49s
  A   33::33/128
     via ::, loopback33, 07h10m49s
  D   1001::20:0/120
     via ::, loopback44, 08h47m18s
  A   1001::20:2/128
     via ::, loopback44, 08h47m18s
 IB   2002::20:0/120 [200/0]
     via ::ffff:10.10.3.3, loopback1, IPv6-mpls, 08h33h41s
```

PE2上显示如下：

```
PE2#show ipv6 protocol routing vrf test1
Vrf test1 IPv6 Routing Table
Codes: D - Direct, A - Address, S - Static, R - RIP, UI - USER_IPADDR,
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS static,
       O - OSPF intra, OI - OSPF inter, E1 - OSPF ext 1, E2 - OSPF ext 2, N
- ND,
```

```
      B - BGP, IB - IBGP, EB - EBGP, AG - BGP AGG, V - VRRP, P - PPP, D6 -
DHCPv6,
      SFN - Stateful NAT64, SLN - Stateless NAT64, AF - AFTR
Time: The time of last modified!

D   22::/64
    via ::, loopback22, 21h02m55s
 A   22::1/128
    via ::, loopback22, 21h02m55s
IB   33::/64 [200/0]
    via ::ffff:10.10.1.1, loopback1, IPv6-mpls, 08h33m39s
IB   1001::20:0/120 [200/0]
    via ::ffff:10.10.1.1, loopback1, IPv6-mpls, 08h47m18s
 D   2002::20:0/120
    via ::, gei-1/10.1, 06h22m11s
 A   2002::20:2/128
    via ::, gei-1/10.1, 06h22m11s
```

3.在PE1上配置route-map，并应用到VRF当中。

配置route-map test1，用于限制export方向的路由通告：

```
PE1(config)#ipv6-access-list test1
PE1(config-ipv6-acl)#rule 1 permit ipv6 1001::20:0/120 any
PE1(config-ipv6-acl)#exit
PE1(config)#route-map test1
PE1(config-route-map)#match ipv6 address test1
PE1(config-route-map)#exit
```

配置route-map test2，用于限制import方向的路由通告：

```
PE1(config)#ipv6-access-list test2
PE1(config-ipv6-acl)#rule 1 permit ipv6 2002::20:0/120 any
PE1(config-ipv6-acl)#exit
PE1(config)#route-map test2
PE1(config-route-map)#match ipv6 address test2
PE1(config-route-map)#exit
```

在vrf test1当中应用route-amap：

```
PE1(config)#ip vrf test1
PE1(config-vrf-test1)#address-family ipv6
PE1(config-vrf-test1-af-ipv6)#export map test1
PE1(config-vrf-test1-af-ipv6)#import map test2
```

4.在PE1、PE2上检查VRF路由表，看VRF路由策略是否生效。

PE1上查看：

```
PE1#show ipv6 protocol routing vrf test1
Vrf test1 IPv6 Routing Table
Codes: D - Direct, A - Address, S - Static, R - RIP, UI - USER_IPADDR,
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS static,
      O - OSPF intra, OI - OSPF inter, E1 - OSPF ext 1, E2 - OSPF ext 2, N
- ND,
      B - BGP, IB - IBGP, EB - EBGP, AG - BGP AGG, V - VRRP, P - PPP, D6 -
DHCPv6,
      SFN - Stateful NAT64, SLN - Stateless NAT64, AF - AFTR
Time: The time of last modified!

 D   33::/64
    via ::, loopback33, 00h04m47s
 A   33::33/128
    via ::, loopback33, 00h04m47s
 D   1001::20:0/120
    via ::, loopback44, 00h04m47s
 A   1001::20:2/128
    via ::, loopback44, 00h04m47s
IB   2002::20:0/120 [200/0]
    via ::ffff:10.10.3.3, loopback1, IPv6-mpls, 21h23m00s
```

PE2上查看：

```
PE2#show ipv6 protocol routing vrf test1
Vrf test1 IPv6 Routing Table
Codes: D - Direct, A - Address, S - Static, R - RIP, UI - USER_IPADDR,
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS static,
       O - OSPF intra, OI - OSPF inter, E1 - OSPF ext 1, E2 - OSPF ext 2, N
- ND,
       B - BGP, IB - IBGP, EB - EBGP, AG - BGP AGG, V - VRRP, P - PPP, D6 -
DHCPv6,
       SFN - Stateful NAT64, SLN - Stateless NAT64, AF - AFTR
Time: The time of last modified!

  D   22::/64
      via ::, loopback22, 21h02m55s
  A   22::1/128
      via ::, loopback22, 21h02m55s
 IB   1001::20:0/120 [200/0]
      via ::ffff:10.10.1.1, loopback1, IPv6-mpls, 22h43m00s
  D   2002::20:0/120
      via ::, gei-1/10.1, 00h22m27s
  A   2002::20:2/128
      via ::, gei-1/10.1, 00h22m27s
```

配置验证

PE1上配置成功，使用命令**show running-config**时应有如下配置：

```
PE1#show running-config bgp
!<bgp>
router bgp 100
  synchronization disable
  neighbor 10.10.3.3 remote-as 100
  neighbor 10.10.3.3 activate
  neighbor 10.10.3.3 update-source loopback1

  ……
  address-family ipv6 vrf test1
    redistribute connected
  $

  address-family vpnv6
    neighbor 10.10.3.3 activate
  $
  ……
$
!</bgp>

PE1#show  running-config vrf
!<vrf>
ip vrf test1
  rd 100:1
  address-family ipv6
    route-target import 100:1
    route-target export 100:1
    import map test2
    export map test1
  $
$
!</vrf>

PE1#show route-map test1

[route-map test1] IP type: IPv6
route-map test1 permit 10
match ipv6 address test1
```

```
PE1#show route-map test2

[route-map test2] IP type: IPv6
route-map test2 permit 10
match ipv6 address test2

PE1#show ipv6-access-lists name test1
ipv6-access-list test1
 1/1 (showed/total)
   1 permit ipv6 1001::20:0/120 any

PE1#show ipv6-access-lists name test2
ipv6-access-list test2
 1/1 (showed/total)
   1 permit ipv6 2002::20:0/120 any
```

从export方向上（路由导入），PE1上的vrf test1路由表应该从使用VRF路由策略前的：

```
PE1#show ipv6 protocol routing vrf test1
Vrf test1 IPv6 Routing Table
Codes: D - Direct, A - Address, S - Static, R - RIP, UI - USER_IPADDR,
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS static,
       O - OSPF intra, OI - OSPF inter, E1 - OSPF ext 1, E2 - OSPF ext 2, N -
ND,
       B - BGP, IB - IBGP, EB - EBGP, AG - BGP AGG, V - VRRP, P - PPP, D6 - DHCPv6,
       SFN - Stateful NAT64, SLN - Stateless NAT64, AF - AFTR
Time: The time of last modified!

IB   22::/64 [200/0]
     via ::ffff:10.10.3.3, loopback1, IPv6-mpls, 09h03m49s
  D   33::/64
     via ::, loopback33, 07h10m49s
  A   33::33/128
     via ::, loopback33, 07h10m49s
  D   1001::20:0/120
     via ::, loopback44, 08h47m18s
  A   1001::20:2/128
     via ::, loopback44, 08h47m18s
 IB   2002::20:0/120 [200/0]
     via ::ffff:10.10.3.3, loopback1, IPv6-mpls, 08h33m41s
```

变更为使用之后的：

```
PE1#show ipv6 protocol routing vrf test1
Vrf test1 IPv6 Routing Table
Codes: D - Direct, A - Address, S - Static, R - RIP, UI - USER_IPADDR,
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS static,
       O - OSPF intra, OI - OSPF inter, E1 - OSPF ext 1, E2 - OSPF ext 2, N -
ND,
       B - BGP, IB - IBGP, EB - EBGP, AG - BGP AGG, V - VRRP, P - PPP, D6 - DHCPv6,
       SFN - Stateful NAT64, SLN - Stateless NAT64, AF - AFTR
Time: The time of last modified!

  D   33::/64
     via ::, loopback33, 00h04m47
  A   33::33/128
     via ::, loopback33, 00h04m47
  D   1001::20:0/120
     via ::, loopback44, 00h04m47
  A   1001::20:2/128
     via ::, loopback44, 00h04m47
 IB   2002::20:0/120 [200/0]
     via ::ffff:10.10.3.3, loopback1, IPv6-mpls, 21h23m00
```

其中路由导入（import方向）的路由策略test2，过滤了从对端PE2通告过来的路由：

```
IB   22::/64 [200/0]
     via ::ffff:10.10.3.3, loopback1, IPv6-mpls, 09h03m49s
```

因为在route-map test2当中指定了匹配**rule 1 permit ipv6 2002::20:0/120**

any的路由才进行学习，即：

```
IB   2002::20:0/120 [200/0]
     via ::ffff:10.10.3.3, loopback1, IPv6-mpls, 08h33m41s
```

PE1上使用路由导出（export方向）的路由策略test1，对出向路由通告进行了策略，所以该策略使用后，在PE2上vrf test1路由表应该从原先的：

```
PE2#show ipv6 protocol routing vrf test1
Vrf test1 IPv6 Routing Table
Codes: D - Direct, A - Address, S - Static, R - RIP, UI - USER_IPADDR,
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS static,
       O - OSPF intra, OI - OSPF inter, E1 - OSPF ext 1, E2 - OSPF ext 2, N -
ND,
       B - BGP, IB - IBGP, EB - EBGP, AG - BGP AGG, V - VRRP, P - PPP, D6 - DHCPv6,
       SFN - Stateful NAT64, SLN - Stateless NAT64, AF - AFTR
Time: The time of last modified!

D   22::/64
     via ::, loopback22, 21h02m55s
  A   22::1/128
     via ::, loopback22, 21h02m55s
 IB   33::/64 [200/0]
     via ::ffff:10.10.1.1, loopback1, IPv6-mpls, 08h33m39s
 IB   1001::20:0/120 [200/0]
     via ::ffff:10.10.1.1, loopback1, IPv6-mpls, 08h47m18s
  D   2002::20:0/120
     via ::, gei-1/10.1, 06h2211s
  A   2002::20:2/128
     via ::, gei-1/10.1, 06h22m11s
```

变化为：

```
PE2#show ipv6 protocol routing vrf test1
Vrf test1 IPv6 Routing Table
Codes: D - Direct, A - Address, S - Static, R - RIP, UI - USER_IPADDR,
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS static,
       O - OSPF intra, OI - OSPF inter, E1 - OSPF ext 1, E2 - OSPF ext 2, N -
ND,
       B - BGP, IB - IBGP, EB - EBGP, AG - BGP AGG, V - VRRP, P - PPP, D6 - DHCPv6,
       SFN - Stateful NAT64, SLN - Stateless NAT64, AF - AFTR
Time: The time of last modified!

  D   22::/64
     via ::, loopback22, 21h02m55s
  A   22::1/128
     via ::, loopback22, 21h02m55s
 IB   1001::20:0/120 [200/0]
     via ::ffff:10.10.1.1, loopback1, IPv6-mpls, 22h43m00s
  D   2002::20:0/120
     via ::, gei-1/10.1, 00h22m27s
  A   2002::20:2/128
     via ::, gei-1/10.1, 00h22m27s
```

可以看到从远端学习到的路由仅有一条：

```
IB   1001::20:0/120 [200/0]
     via ::ffff:10.10.1.1, loopback1, IPv6-mpls, 22h43m00s
```

这一条是匹配route-map test1当中定义的match条件**rule 1 permit ipv6 1001::20:0/120 any**的，匹配不上的路由被过滤掉：

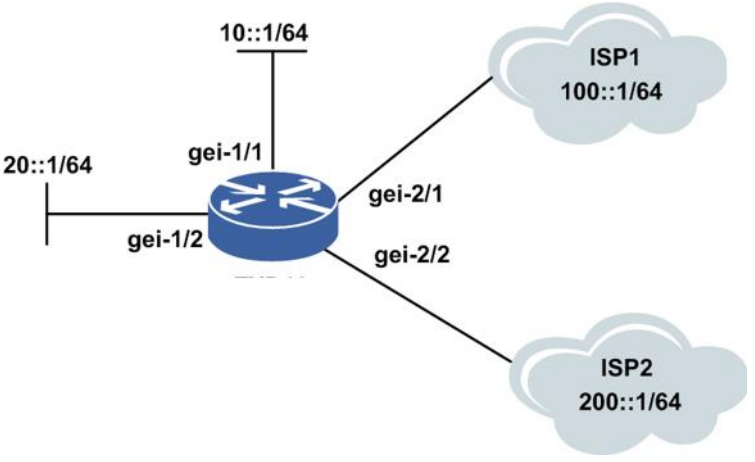
```
IB   33::/64 [200/0]
     via ::ffff:10.10.1.1, loopback1, IPv6-mpls, 08h33m39s
```

12.8.8 IPv6 策略路由配置实例

配置说明

如*图 12-24*所示，路由器通过不同的接口接入两个子网的用户，而且有两个ISP出口可供使用，要求根据用户的IP地址选择不同的出口，IP地址属于10::1/64子网的用户业务使用ISP1出口，而IP地址属于20::1/64子网的用户业务使用ISP2出口。

图 12-24 IPv6 策略路由配置实例



配置思路

1.对各接口使能IPv6，配置IPv6地址。

2.建立ACL定义要控制的流量。

3.创建route-map，关联ACL并定义动作。

4.将route-map关联至相应的接口上。

配置过程

IR12000上的接口配置如下：

```
inspur(config)#interface gei-1/1
inspur(config-if-gei-1/1)#no shutdown
inspur(config-if-gei-1/1)#description To User1
inspur(config-if-gei-1/1)#ipv6 enable
inspur(config-if-gei-1/1)#ipv6 address 10::2/64
inspur(config-if-gei-1/1)#exit
inspur(config)#show running-config-interface gei-1/1
!<if-intf>
interface gei-1/1
  no shutdown
  description To User1
  ipv6 enable
  ipv6 address 10::2/64
$
!</if-intf>
inspur(config)#interface gei-1/2
```

```
inspur(config-if-gei-1/2)#no shutdown
inspur(config-if-gei-1/2)#description To User2
inspur(config-if-gei-1/2)#ipv6 enable
inspur(config-if-gei-1/2)#ipv6 address 20::2/64
inspur(config-if-gei-1/2)#exit
inspur(config)#show running-config-interface gei-1/1
!<if-intf>
interface gei-1/2
  no shutdown
  description To User2
  ipv6 enable
  ipv6 address 20::2/64
$
!</if-intf>
inspur(config)#interface gei-2/1
inspur(config-if-gei-2/1)#no shutdown
inspur(config-if-gei-2/1)#description To ISP1
inspur(config-if-gei-2/1)#ipv6 enable
inspur(config-if-gei-2/1)#ipv6 address 100::2/64
inspur(config-if-gei-2/1)#exit
inspur(config)#show running-config-interface gei-2/1
!<if-intf>
interface gei-2/1
  no shutdown
  description To ISP1
  ipv6 enable
  ipv6 address 100::2/64
$
!</if-intf>
inspur(config)#interface gei-2/2
inspur(config-if-gei-2/2)#no shutdown
inspur(config-if-gei-2/2)#description To ISP2
inspur(config-if-gei-2/2)#ipv6 enable
inspur(config-if-gei-2/2)#ipv6 address 200::2/64
inspur(config-if-gei-2/2)#exit
inspur(config)#show running-config-interface gei-2/2
!<if-intf>
interface gei-2/2
  no shutdown
  description To ISP2
  ipv6 enable
  ipv6 address 200::2/64
$
!</if-intf>
```

配置默认路由：

```
inspur(config)#ipv6 route 0:0::0:0/0 100::1
```

配置route-map的过程：

```
/*配置route-map中应用的ACL列表信息*/
inspur(config)#ipv6-access-list 1
inspur(config-ipv6-acl)#rule 1 permit ipv6 10::1/64 any
inspur(config-ipv6-acl)#exit
inspur(config)#show ipv6-access-lists name 1
ipv6-access-list 1
 1/1 (showed/total)
   1 permit ipv6 10::1/64 any
inspur(config)#ipv6-access-list 2
inspur(config-ipv6-acl)#rule 1 permit ipv6 20::1/64 any
inspur(config-ipv6-acl)#exit
inspur(config)#show ipv6-access-lists name 2
ipv6-access-list 2
 1/1 (showed/total)
   1 permit ipv6 20::1/64 any
/*配置Route-map信息，Sequence号分别为10、20*/
inspur(config)#route-map v6-pbr permit 10
inspur(config-route-map)#match ipv6 address 1
inspur(config-route-map)#set ipv6 next-hop 100::1
```

```
inspur(config-route-map)#exit
inspur(config)#route-map v6-pbr permit 20
inspur(config-route-map)#match ipv6 address 2
inspur(config-route-map)#set ipv6 next-hop 200::1
inspur(config-route-map)#exit
inspur(config)#show route-map v6-pbr
[route-map v6-pbr] IP type: IPv6
route-map v6-pbr permit 10
match ipv6 address 1
set ipv6 next-hop 100:0:0:0:0:0:0:1
route-map v6-pbr permit 20
match ipv6 address 2
set ipv6 next-hop 200:0:0:0:0:0:0:1
```

配置将Route-map应用于接口：

```
inspur(config)#ipv6 policy interface gei-1/1 route-map v6-pbr
inspur(config)#show running-config pbr
!<pbr>
ipv6 policy interface gei-1/1 route-map v6-pbr
!</pbr>
inspur(config)#ipv6 policy interface gei-1/2 route-map v6-pbr
inspur(config)#show running-config pbr
!<pbr>
ipv6 policy interface gei-1/2 route-map v6-pbr
!</pbr>
```

在本案例中，会出现以下三种情况：

- 当ISP1和ISP2出口均正常时，10::1/64和20::1/64子网的用户业务分别走ISP1、ISP2出口。
- 当ISP1正常、ISP2出口异常时，两个子网的用户业务都走ISP1出口，此时10::1/64子网的用户业务利用的是默认路由。
- 当ISP1异常、ISP2出口正常时，20::1/64子网的用户业务正常，而10::1/64子网的用户业务中断。

配置验证

查看route-map配置信息：

```
inspur(config)#show route-map v6-pbr
[route-map v6-pbr] IP type: IPv6
route-map v6-pbr permit 10
match ipv6 address 1
set ipv6 next-hop 100:0:0:0:0:0:0:1
route-map v6-pbr permit 20
match ipv6 address 2
set ipv6 next-hop 200:0:0:0:0:0:0:1
```

查看接口pbr的绑定信息：

```
inspur(config)#show running-config pbr
!<pbr>
ipv6 policy interface gei-1/1 route-map v6-pbr
ipv6 policy interface gei-1/2 route-map v6-pbr
!</pbr>
```

12.9 IPv6 组播

作为IPv4协议的替代，IPv6协议使用128位的地址结构解决了IP地址不足的问题，同时对一些特性进行了优化处理。IPv4的组播技术，有效解决了单点发送、多点接收的问题，实现了网络中点到多点的高效数据传送，能够大量节约网络带宽、降低网络负载。

IPv6组播继承了IPv4组播的有点，区别在于IPv6组播地址机制极其丰富，其它如组成员管理、组播报文转发以及组播路由建立等与IPv4组播基本相同。

静态组播是一种特殊的组播路由协议，提供用户直接配置组播路由表的出接口和入接口，并根据用户的这种配置形成组播转发表。如果同时存在静态组播路由和动态组播路由，静态组播路由优先。静态组播的逻辑地位同PIM-SM和PIM-DM。

IPv6的静态组播原理同IPv4组播。

12.9.1 配置公共组播

本节介绍公共组播的配置步骤和命令。

1.配置启用组播。

步骤	命令	功能
1	inspur(config)#**ipv6 multicast-routing**	启用IPv6组播路由功能
2	inspur(config-mcast-ipv6)#**router pim**	启用IPv6 PIM组播

2.配置组播转发表项限制参数。

命令	功能
inspur(config-mcast-ipv6)#**mroute6-limit** <*limit*>	配置对组播转发表中的表项数量进行限制，缺省情况下，采用系统允许的最大值

3.配置组播damping。

步骤	命令	功能
1	inspur(config-mcast-ipv6)#**damping-enable**	使能damping
2	inspur(config-mcast-ipv6)#**damping-threshold** <*threshold*>	对路由下发次数的阈值限制，超过阈值路由下发将启动damping功能，抑制下发，最少等10s最多等60秒下发

4. 配置组播负荷分担。

命令	功能

命令	功能
inspur(config-mcast-ipv6)#**multipath**	启用负荷分担，使用基于源地址的哈希算法
inspur(config-mcast-ipv6)#**multipath s-g-hash basic**	启用负荷分担，使用基于源地址、组播地址的哈希算法
inspur(config-mcast-ipv6)#**multipath s-g-hash next-hop-based**	启用负荷分担，使用基于下一跳的哈希算法

5.验证配置结果。

命令	功能
inspur#**show ipv6 mroute** [**group** <*group-address*>][**source** <*source-address*>]	显示IPv6组播路由表的内容
inspur#**show ipv6 mroute summary**	显示IPv6组播路由表的具体数目
inspur#**show ipv6 mroute brief**	显示IPv6组播路由表的内容

6.维护公共组播。

命令	功能
inspur#**clear ipv6 mroute** [**group-address** <*group-address*>][**source-address** <*source-address*>]	清除组播路由

12.9.2 配置 IPv6 静态组播

本节介绍IPv6静态组播功能的配置和验证。

1.配置静态组播。

步骤	命令	功能
1	inspur(config-mcast-ipv6)#**ipv6 multicast-static-start**	启用MSTATIC
2	inspur(config-mcast-ipv6)#**ipv6 multicast-static-limit xg** <*xg-limit*> **sg** <*sg-limit*>	配置静态组播路由条目数最大值
3	inspur(config-mcast-ipv6)#**ipv6 multicast-static-route** <*source-address*><*group-address*>[{[**iif** <*iif-name*>],[**oif** <*oif-index*>]}]	配置静态组播路由条目
4	inspur(config-mcast-ipv6)#**ipv6 multicast-static-interface index** <*index*> **interface** <*interface-name*>	配置静态组播出接口集合

<*xg-limit*>：允许配置的静态组播(*,G)路由条目数，默认允许配置的静态组播(*,G)路由条目数为0。

<*sg-limit*>：允许配置的静态组播(S,G)路由条目数，默认允许配置的静态组播(S,G)路由条目数为0。

<*source-address*>：指定的组播源地址。

<*group-address*>：指定的组播组地址。

<*iif-name*>：组播路由条目入接口名称。

<*oif-index*>：组播路由条目出接口集合序号。

<*index*>：配置出接口集合的序号。

<*interface-name*>：加入出接口集合的接口名。

2.验证配置结果。

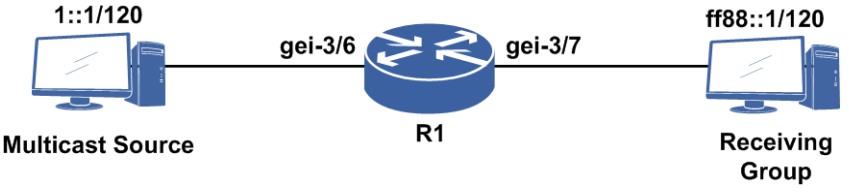
命令	功能
inspur#**show ipv6 multicast-static-interface** [**index** <*index*>]	显示出接口集合中有效的接口
inspur#**show ipv6 multicast-static-route** [**group** <*group-address*>|[**source** <*source-address*>]]|[**source** <*source-address*>]	显示静态组播路由表内容
inspur#**show ipv6 multicast-static-route summary**	显示静态组播路由表的内容统计计数

12.9.3 IPv6 静态组播配置实例

配置说明

如*图 12-25*所示，配置一条源为1::1，目的为ff88::1的静态组播路由，使组播流可以正常转发。

图 12-25 IPv6 静态组播配置实例组网图



配置思路

1. 配置接口IP地址。

2. 进入组播模式。

3.启动静态组播

4.配置静态组播（*,G）、(S,G)最大条目数。

5.配置静态组播出接口列表。

6.配置具体静态组播路由。

配置过程

R1的配置如下：

```
R1(config)#ipv6 multicast-routing
R1(config-mcast-ipv6)#ipv6 multicast-static-start
R1(config-mcast-ipv6)#ipv6 multicast-static-limit xg 1024 sg 1024
R1(config-mcast-ipv6)#ipv6 multicast-static-interface index 2 interface
 gei-3/7
R1(config-mcast-ipv6)#ipv6 multicast-static-route 1::1 ff88::1 iif
 gei-3/6 oif 2
R1(config-mcast-ipv6)#end
```

配置验证

在R1上通过**show ipv6 multicast-static-interface**命令查看端口静态组播信息：

```
R1(config)#show ipv6 multicast-static-interface
STATIC-MULTICAST OUT PORT INDEX 2:
Outgoing Interface:
               gei-3/7
R1(config)#show ipv6 multicast-static-route
The Capability of Static Multicast6 Route
(*, g) 1024, (s, g) 1024
(1::1, ff88::1)
Incoming interface: gei-3/6  A
Outgoing interface list:
          gei-3/7  F
R1(config)#show ipv6 mroute
IPv6 Multicast Routing Table
Flags:NS:SPT upsend,RT:Reg upsend,F:Forward,
NTP:NTP join,DPU:Damping enable,DPD:Damping del,
(1::1, ff88::1), TYPE: STATIC, FLAGS:
   Incoming interface: gei-3/6, flags:
   Outgoing interface list:
     gei-3/7, flags: F
```

12.10 MLD

MLD协议源自IGMP协议。与IGMP协议采用IP协议号为2的报文类型不同，MLD协议采用ICMPv6（IP协议号为58）的报文类型，包括MLD查询报文（类型值130）、MLDv1报告报文（类型值131）、MLDv1离开报文（类型值132）和MLDv2报告报文（类型值143）。MLD协议与IGMP协议除报文格式不同外，协议行为完全相同。

目前MLD有两个版本：

·MLDv1相当于IGMPv2，增加了组成员快速离开等机制

·MLDv2相当于IGMPv3，增加的主要功能是成员可以指定接收或拒绝来自某些组播源的报文，以实现对SSM模型的支持。

12.10.1 配置 MLD

配置MLD的基础功能，包括版本信息、加入/离开组功能以及定时器相关属性参数。

1.配置版本信息。

MLD有v1和v2两种版本，缺省为v2，可以根据情况使用**version** <*version*>命令调整。基于安全考虑，IR12000智能路由器设备要求同一网段上的网元都是MLDv1或者v2。MLD版本的配置可以基于实例也可以基于接口，接口优先，不同的接口可以配置为不同的版本。

步骤	命令	功能
1	inspur(config-mcast-ipv6)#**router mld**	进入MLD配置模式
2	inspur(config-mcast-ipv6-mld)#**version**{**1**|**2**}	配置MLD实例下协议版本号
3	inspur(config-mcast-ipv6-mld)#**interface** <*interface-name*>	进入MLD接口配置模式
4	inspur(config-mcast-ipv6-mld-if-interface-name)#**version** {**1**|**2**}	配置MLD接口下协议版本号

2.配置MLD查询者规避。

命令	功能
inspur(config-mcast-ipv6-mld-if-interface-name)#**querier-election disable**	配置不进行查询者选举，即路由器认为自己就是查询者

3.配置Require-Alert-Option选项。

命令	功能
inspur(config-mcast-ipv6-mld)#**require-alert-options**	只接收IPv6头中包含Router Alert options选项的报文，否则丢弃

4.配置SSM-Mapping。

命令	功能
inspur(config-mcast-ipv6-mld)#**ssm-map static** {**default** | **group-list** |<*access-list-name*>}<*source-address*>	配置ssm-mapping映射功能，实现MLDv1的指定组源加入，default组范围是FF3*/32

5.配置允许丢包的限制。

可以在实例下配置也可以在接口下配置，接口下优先。

命令	功能
inspur(config-mcast-ipv6-mld)#**robustness-count** *<times>*	允许丢包的限制，范围：2~7，默认值为2
inspur(config-mcast-ipv6-mld-if-interface-name)#**robustness-count** *<times>*	允许丢包的限制，范围：2~7，默认值为2，接口下优先

6.配置接口上的MLD组功能。

步骤	命令	功能
1	inspur(config)#**ipv6 multicast-routing**	进入组播配置模式
2	inspur(config-mcast-ipv6)#**router mld**	进入MLD配置模式
3	inspur(config-mcast-ipv6-mld)#**interface** *<interface-name>*	进入MLD接口配置模式
4	inspur(config-mcast-ipv6-mld-if-interface-name)#**access-group** *<access-list-number>*	允许MLD加入的组范围
5	inspur(config-mcast-ipv6-mld-if-interface-name)#**join-group** *<group-address>*	配置MLD接口上的静态组成员，要发送report报文
6	inspur(config-mcast-ipv6-mld-if-interface-name)#**static-group** *<group-address>*[**source** {*<source-address>*[{**include** | **exclude**}]| **ssm-map**}]	配置MLD协议接口上的静态组成员
7	inspur(config-mcast-ipv6-mld-if-interface-name)#**immediate-leave** {**all** | **group-list** *<access-list-name>*}	配置允许MLD立即离开的组范围 缺省收到MLD离开消息后，经过（last member query interval*2）秒时间没有收到report消息后，组成员离开。该命令如果没有选项，则对所有组播组有效

7.配置MLD定时器功能。

在连接共享网段的组播路由器接口上启用MLD后，选举出一个最优的充当该网段上的查询者（querier），负责发送查询消息来获取组成员的信息。

查询者发送出问询消息后，会在一段时间内等待接收主机成员的报告，时长为发送问询消息时携带的最大响应时间（max response time）值，缺省为10秒。

网段上的主机成员在收到问询消息后，会在最大响应时间的基础上减去一个随机偏差值，将结果作为自己的响应时间。在此期间若收到其他主机成员的报告则取消，若没有则到时发出主机报告。所以提高最大响应时间则相应增加了网段上组成员的等待机会，可以减少网段上多个主机报告的突发率。

根据网络实际情况，可以适当调整与查询者相关的几个定时器的参数值。

步骤	命令	功能
1	inspur(config-mcast-ipv6-mld)#**query-interval** <*seconds*>	配置实例下MLD普通查询时间间隔，范围1~65535，缺省为125，单位：秒
	inspur(config-mcast-ipv6-mld-if-interface-name)#**query-interval** <*seconds*>	配置接口下MLD普通查询时间间隔，接口优先，范围1~65535，缺省为125，单位：秒
2	inspur(config-mcast-ipv6-mld)#**query-max-response-time** <*seconds*>	配置实例下MLD协议发送查询消息时携带的最大响应时间，范围1~25，缺省为10，单位：秒
	inspur(config-mcast-ipv6-mld-if-interface-name)#**query-max-response-time** <*seconds*>	配置接口下MLD协议发送查询消息时携带的最大响应时间，接口优先，范围1~25，缺省为10，单位：秒
3	inspur(config-mcast-ipv6-mld)#**querier-timeout** <*seconds*>	配置实例下MLD查询器超时时间，范围60~300，单位：秒
	inspur(config-mcast-ipv6-mld-if-interface-name)#**querier-timeout** <*seconds*>	配置接口下MLD查询器超时时间，接口优先，范围60~300，单位：秒
4	inspur(config-mcast-ipv6-mld)#**last-member-query-interval** <*seconds*>	配置实例下MLD特定组查询间隔，范围1~25，缺省为1，单位：秒
	inspur(config-mcast-ipv6-mld-if-interface-name)#**last-member-query-interval** <*seconds*>	配置接口下MLD特定组查询间隔，接口优先，范围1~25，缺省为1，单位：秒

8.验证配置结果。

命令	功能
inspur#**show ipv6 mld interface** [<*interface-name*>]	查看接口上MLD配置情况
inspur#**show ipv6 mld groups** [{[<*interface-name*>],[<*group-address*>]}][**detail**]	显示通过MLD协议学习到和路由器直连的组播组加入情况
inspur#**show ipv6 mld packet-count** [<*interface-name*>]	查看MLD协议报文接收和发送的统计计数

9.维护MLD。

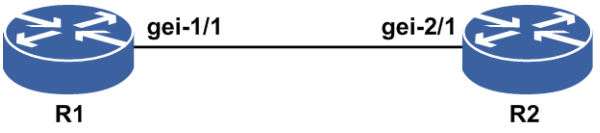
命令	功能
inspur#**clear ipv6 mld groups** [<*interface-name*>]	删除动态加入的组播组
inspur#**clear ipv6 mld packet-count**[<*interface-name*>]	清除MLD接收和发送的报文统计计数

12.10.2 MLD 查询路由器选举配置实例

配置说明

如*图 12-26*所示，R1和R2上启用PIM-SM协议，最低link-local地址的MLD路由器成为查询路由器。

图 12-26 MLD 查询路由器选举配置实例



配置思路

1.接口模式下，配置两台路由器接口地址，使R1的link-local地址小于R2的link-local地址。

2.打开组播模块的总开关ipv6 multicast-routing。

3.进入PIM路由模式，再进入所要配置的接口。

4.接口模式下，开启PIM-SM协议。

配置过程

R1的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ipv6 enable
R1(config-if-gei-1/1)#ipv6 address link-local fe80::1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#ipv6 multicast-routing
R1(config-mcast-ipv6)#router pim
R1(config-mcast-ipv6-pim)#interface gei-1/1
R1(config-mcast-ipv6-pim-if-gei-1/1)#pimsm
R1(config-mcast-ipv6-pim-if-gei-1/1)#end
```

R2的配置如下：

```
R2(config)#interface gei-2/1
R2(config-if-gei-2/1)#ipv6 enable
R2(config-if-gei-2/1)#ipv6 address link-local fe80::2
R2(config-if-gei-2/1)#no shutdown
R2(config-if-gei-2/1)#exit
R2(config)#ipv6 multicast-routing
R2(config-mcast-ipv6)#router pim
R2(config-mcast-ipv6-pim)#interface gei-2/1
R2(config-mcast-ipv6-pim-if-gei-2/1)#pimsm
R2(config-mcast-ipv6-pim-if-gei-2/1)#end
```

配置验证

在R1上查看配置的有效性：

```
R1#show ipv6 mld interface gei-1/1
gei-1/1
  Internet address is fe80::1
  MLD is enabled on interface
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD last member query interval is 1 seconds
  MLD query max response time is 10 seconds
  MLD querier timeout period is 255 seconds
  MLD robustness variable is 2
  MLD querier is fe80::1, never expire
  Inbound MLD access group is not set
  MLD immediate leave control is not set
```

在R2上查看配置的有效性：

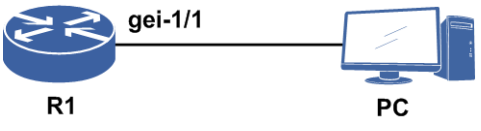
```
R2#show ipv6 mld interface gei-2/1
gei-2/1
  Internet address is fe80::2
  MLD is enabled on interface
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD last member query interval is 1 seconds
  MLD query max response time is 10 seconds
  MLD querier timeout period is 255 seconds
  MLD robustness variable is 2
  MLD querier is fe80::2, expire timer: 00:03:33
  Inbound MLD access group is not set
  MLD immediate leave control is not set
```

12.10.3 MLD 动态组、静态组加入配置实例

配置说明

如*图 12-27*所示，R1上启用PIM-SM协议，MLD协议版本默认为v2，在R1上配置静态组加入ffee::1，并通过PC配置动态组加入ffee::2。

图 12-27 MLD 动态组、静态组加入配置实例图



配置思路

1.接口模式下，配置路由器接口地址。

2.打开组播模块的总开关ipv6 multicast-routing。

3.进入PIM路由模式，再进入所要配置的接口。

4.接口模式下，开启PIM-SM协议。

5.组播模式下，进入MLD路由模式，再进入所要配置的接口。

6.在R1的gei-1/1接口上配置静态组加入。

7.在PC上向R1发送MLD组加入报文。

配置过程

R1的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ipv6 enable
R1(config-if-gei-1/1)#ipv6 address 100::1/64
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#ipv6 multicast-routing
R1(config-mcast-ipv6)#router pim
R1(config-mcast-ipv6-pim)#interface gei-1/1
R1(config-mcast-ipv6-pim-if-gei-1/1)#pimsm
R1(config-mcast-ipv6-pim-if-gei-1/1)#end
R1#configure terminal
R1(config)#ipv6 multicast-routing
R1(config-mcast-ipv6)#router mld
R1(config-mcast-ipv6-mld)#interface gei-1/1
R1(config-mcast-ipv6-mld-if-gei-1/1)#static-group ffee::1 source 200::1
R1(config-mcast-ipv6-mld-if-gei-1/1)#end
```

配置验证

在R1上查看接口信息：

```
R1#show ipv6 mld interface gei-1/1
gei-1/1
  Internet address is fe80::2d0:d0ff:fe06:606
  MLD is enabled on interface
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD last member query interval is 1 seconds
  MLD query max response time is 10 seconds
  MLD querier timeout period is 255 seconds
  MLD robustness variable is 2
  MLD querier is fe80::2d0:d0ff:fe06:606, never expire
  Inbound MLD access group is not set
  MLD immediate leave control is not set
```

在R1上查看对应接口组的详细信息：

```
R1#show ipv6 mld groups gei-1/1 detail
Flags: S - Static Group, SSM - SSM Group, M - MDT Group
Interface:      gei-1/1
Group:         ffee::1
Flags:
Uptime:        01:06:51
Group mode:     INCLUDE
Last reporter:  fe80::2d0:e0ff:fe10:201f
Group source list: (M - SSM Mapping, S - Static, R - Report)
  Source addr                           Present   Expires   Fwd  Flag
  200::1                               01:06:51  Never     Yes  S
```

PC申请加入组播组，在R1上查看：

```
R1(config-mcast-ipv6)#show ipv6 mld groups
Total: 2 groups
Group Address : ffee::2
Last Reporter : fe80::200:65ff:fe03:102
    Interface : gei-1/1
```

```
      Uptime : 00:01:44
     Expires : 00:03:44
Group Address : ffee::1
Last Reporter : fe80::2d0:d0ff:fe06:606
    Interface : gei-1/1
      Uptime : 00:03:11
     Expires : never
```

12.11 PIM-DM

PIM-DM协议适用于密集模式，即网络中组播接收者较多的应用场景。PIM-DM协议机制相对较为简单，采用PUSH方式，将组播流量周期性扩散到网络中所有设备，建立和维护SPT转发树。

12.11.1 配置 IPv6 PIM-DM

本节介绍IPv6 PIM-DM的配置步骤和命令。

1.配置IPv6 PIM-DM。

步骤	命令	功能
1	inspur(config)#**ipv6 multicast-routing**	启动IPv6组播
2	inspur(config-mcast-ipv6)#**router pim**	启用IPv6组播PIM协议
3	inspur(config-mcast-ipv6-pim)#**interface** <*interface-name*>	进入IPv6 PIM接口配置模式
4	inspur(config-mcast-ipv6-pim-if-interface-name)#**pimdm**	接口启用IPv6组播路由协议PIM-DM

2.验证配置结果。

命令	功能
inspur#**show ipv6 pim interface** [<*interface-name*>]	查看配置的IPv6 PIM接口情况
inspur#**show ipv6 pim mroute** [[**group** <*group-address*>[**source** <*source-address*>]][[**summary**]]	显示IPv6 PIM组播路由表的内容
inspur#**show ipv6 pim neighbor** [[<*interface-name*>][**detail**]]	查看IPv6 PIM接口的邻居情况

3.维护PIM-DM。

命令	功能
inspur#**debug ipv6 pim data-info**	跟踪显示IPv6 PIM收到数据报文的调试信息

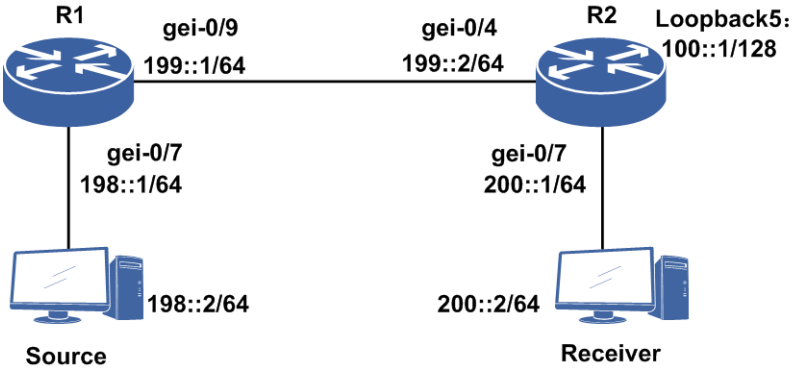
命令	功能
inspur#**debug ipv6 pim packet-send**	跟踪显示IPv6 PIM发送协议报文的调试信息
inspur#**debug ipv6 pim packet-recv**	跟踪显示IPv6 PIM收到协议报文的调试信息
inspur#**debug ipv6 pim mrt**	跟踪显示IPv6 PIM路由的调试信息
inspur#**debug ipv6 pim ast**	跟踪显示IPv6 PIM断言的调试信息
inspur#**debug ipv6 pim**	跟踪显示IPv6 PIM的调试信息
inspur#**debug ipv6 pim all**	跟踪显示IPv6 PIM的所有调试信息

12.11.2 IPv6 PIM-DM 配置实例

配置说明

如图 12-28所示，要在R1和R2之间建立PIM-DM邻居。

图 12-28 PIM-DM 配置实例示意图



配置思路

1.配置相应接口地址。

2.进入组播模式。

3.进入IPv6 PIM模式。

4.在相应接口下使能PIM-DM。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-0/9
R1(config-if-gei-0/9)#ipv6 enable
R1(config-if-gei-0/9)#ipv6 address 199::1/64
R1(config-if-gei-0/9)#no shutdown
R1(config-if-gei-0/9)#exit
R1(config)#interface gei-0/7
R1(config-if-gei-0/7)#ipv6 enable
R1(config-if-gei-0/7)#ipv6 address 198::1/64
R1(config-if-gei-0/7)#no shutdown
R1(config-if-gei-0/7)#exit

R1(config)#ipv6 multicast-routing
R1(config-mcast-ipv6)#router pim
R1(config-mcast-ipv6-pim)#interface gei-0/9
R1(config-mcast-ipv6-pim-if-gei-0/9)#pimdm
R1(config-mcast-ipv6-pim-if-gei-0/9)#exit
R1(config-mcast-ipv6-pim)#interface gei-0/7
R1(config-mcast-ipv6-pim-if-gei-0/7)#pimdm
R1(config-mcast-ipv6-pim-if-gei-0/7)#end
```

R2上的配置如下：

```
R2(config)#interface gei-0/4
R2(config-if-gei-0/4)#ipv6 enable
R2(config-if-gei-0/4)#ipv6 address 199::2/64
R2(config-if-gei-0/4)#no shutdown
R2(config-if-gei-0/4)#exit
R2(config)#interface gei-0/7
R2(config-if-gei-0/7)#ipv6 enable
R2(config-if-gei-0/7)#ipv6 address 200::1/64
R2(config-if-gei-0/7)#no shutdown
R2(config-if-gei-0/7)#exit

R2(config)#ipv6 multicast-routing
R2(config-mcast-ipv6)#router pim
R2(config-mcast-ipv6-pim)#interface gei-0/4
R2(config-mcast-ipv6-pim-if-gei-0/4)#pimdm
R2(config-mcast-ipv6-pim-if-gei-0/4)#exit
R2(config-mcast-ipv6-pim)#interface gei-0/7
R2(config-mcast-ipv6-pim-if-gei-0/7)#pimdm
R2(config-mcast-ipv6-pim-if-gei-0/7)#end

R2#configure terminal
R2(config)#ipv6 route 198::/64 199::1  /*到源的单播路由*/
```

配置验证

在R1上使用命令**show ipv6 pim neighbor**查看邻居状态：

```
R1(config)#show ipv6 pim neighbor
Neighbor Address         Interface     Uptime    Expires   DR Pri
fe80::2d0:d0ff:fe06:600   gei-0/9       00:09:12  00:00:26  1
```

在R1上使用命令**show ipv6 pim interface**查看接口状态：

```
R1(config)#show ipv6 pim interface
Interface       State  Nbr    Hello   DR        PIM Silent  Mode
                       Count  Period  Priority
gei-0/7         Up     0      30      1         Disabled    D
   Address: fe80::2d0:d0ff:fe06:606
DR     : fe80::2d0:d0ff:fe06:606
gei-0/9         Up     1      30      1         Disabled    D
```

```
   Address: fe80::2d0:d0ff:fe06:606
DR     : fe80::2d0:d0ff:fe06:606
```

在R1上使用命令**show ipv6 pim mroute**查看IPv6组播路由表状态：

```
R1(config)#show ipv6 pim mroute
IPv6 PIM Multicast Routing Table
Flags: T- SPT-bit set,A- Forward,J- Join SPT,U- Upsend,S- PIM-SM,D- PIM-DM,
Macro state: Ind- Pim Include Macro,Exd- Pim Exclude Macro,
     Jns- Pim Joins Macro,LAst- Pim Lost_assert Macro,
     Imo- Pim Immediate_olist Macro,Ino- Pim Inherited_olist Macro,
     Lcd- Pim Local_receiver_include Macro
Timers:Uptime/Expires(Upstream State)
(198::2, ff88::1), 00:07:20/00:00:00(JOINED)/00:03:25,
 Reg:NO INFO; RP:0::0; RT:NULL;
  Ind:0/Exd:0/Jns:1/LAst:0/Imo:1/Ino:1
  Iif: gei-0/7, RPF nbr:0::0(S); AT
      RPF nbr:0::0(D); 00:00:00(FORWARD);
  Oif:
    gei-0/9,   JoinsSG  /  InoSG  /  DenseOlist
```

12.12 PIM-SM

PIM-SM主要适用于组成员分布相对分散、范围较广、网络带宽资源有限的应用场景，不依赖于特定的单播路由协议。

PIM-SM通过设置RP向所有支持PIM-SM的路由器通告组播信息。在PIM-SM中，路由器显式地加入和退出组播组，可以减少数据报文和控制报文占用的网络带宽。

12.12.1 配置 IPv6 组播 PIM-SM

配置IPv6组播PIM-SM的基本属性和功能，包括基本信息、全局参数以及策略控制功能。

1.配置启用IPv6 PIM-SM协议。

步骤	命令	功能
1	inspur(config-mcast-ipv6)#**router pim**	启用PIM协议
2	inspur(config-mcast-ipv6-pim)#**interface** <*interface-name*>	接口上启动组播路由协议PIM-SM时，会自动在该接口上启动MLD，缺省时接口不启动组播路由协议PIM-SM
3	inspur(config-mcast-ipv6-pim-if-interface-name)#**pimsm**	

2.配置静态RP。

命令	功能
inspur(config-mcast-ipv6-pim)#**static-rp** <*ipv6-address*>[{[**group-list** <*prefix-list-name*>],[**priority** <*priority*>]}]	配置静态RP，缺省没有静态RP

<*ip-address*>：静态RP地址，为X:X::X:X形式。

<*priority*>：优先级，范围0~255，缺省为192。

静态RP的使用说明如下：

- 静态RP配置后即进入RP集参加选择，即使这个路由器没有收到任何BSR的RP信息通告。
- 如果命令不带<*prifix-list-name*>参数，静态RP适用于所有组播组。

配置静态RP示例：为所有的组配置静态RP 2001::1。

```
inspur(config-mcast-ipv6-pim)#static-rp 2001::1
```

3.配置候选BSR。

命令	功能
inspur(config-mcast-ipv6-pim)#**bsr-candidate** <*ipv6-address*>[{[**hash-mask-length** <*hash-mask-length*>],[**priority** <*priority*>]}]	配置候选BSR

<*hash-mask-length*>：哈希掩码长度，范围0~128。

<*priority*>：优先级，范围0~255，缺省为0。

如果不使用静态RP机制，则每个组播域必须在一个以上的组播路由器上配置备选BSR，并选举出一个BSR。

BSR周期性地发送启动（BSR）消息来通告RP的情况，运行PIM-SM的路由器根据最新的通告消息更新RP的状态。BSR发送的启动（bootstrap）消息也用于在候选BSR中选举出正式的BSR。

候选BSR的缺省优先级为0，具有较高优先级的候选BSR成为正式BSR。如果多个路由器的BSR优先级一样，则比较IP地址，具有较大地址的候选BSR成为正式BSR。

4.配置候选RP。

命令	功能
inspur(config-mcast-ipv6-pim)#**rp-candidate** <*ipv6-address*>[{[**group-list** <*prefix-list-name*>],[**priority** <*priority*>]}]	配置候选RP <*priority*>：候选RP优先级，范围0~255，缺省值为192

在PIM-SM中，RP即为共享组播树的根，负责沿共享树向下游发送组播包到组播接收成员。每一个组播组只能有一个正式的RP。

候选RP使用说明：

- 如果该命令不带<*prefix-list-name*>参数，表明该候选RP为所有组服务。
- 候选RP的缺省优先级为192，优先级数值较小的候选RP优先；如果优先级数值相同，则比较hash值，hash值大的RP优先；如果hash值相同，则比较IP地址，IP地址大的RP优先。
- 推荐用户将候选RP配置在loopback接口上，从而减少由于物理接口up/down造成的网络震荡。

5.配置IPv6 PIM-SM全局参数。

运行IPv6 PIM-SM协议时，不同的参数都有其缺省值，可以设置这些参数来优化网络。

步骤	命令	功能
1	inspur(config-mcast-ipv6-pim)#**spt-threshold infinity**	源最短路径树切换，**infinity**表示配置从共享RP树到SPT树为永不切换
2	inspur(config-mcast-ipv6-pim-if-interface-name)#**dr-priority** <*priority*>	设置PIM接口的DR优先级，范围0~4294967295，缺省为1
3	inspur(config-mcast-ipv6-pim-if-interface-name)#**bsr-border**	配置接口使其成为PIM-SM域边界
4	inspur(config-mcast-ipv6-pim-if-interface-name)#**hello-interval** <*seconds*>	设置HELLO报文的发送间隔

缺省情况下，从共享树切换到源最短路径树的阈值为0。只有最末跳DR和RP可以主动切换到源最短路径树。

缺省情况下，当RP收到第一个注册消息时即开始切换。而对于最末跳DR，可以以单个组播组为控制粒度，配置源最短路径树切换阈值策略。如果配置一个组的切换阈值为**infinity**，则不发生切换。默认为只要有流量就发生切换。

在一个共享（或多路访问）网段上必须选举出一个DR。优先级最高的路由器将赢得选举，若优先级都相同，则选择IP地址最大的路由器为DR。

在连接组播数据源的共享网段上，只有DR能够向RP发送注册消息；在连接接收者的共享网段上，只有DR才能响应MLD加入、离开消息，向上游发送PIM加入/剪枝消息。设备的优先级包含在同邻居交换的hello消息中，缺省值为1。

在路由器接口gei-1/1上配置DR优先级：

```
inspur(config)#ipv6 multicast-routing
inspur(config-mcast-ipv6)#router pim
inspur(config-mcast-ipv6-pim)#interface gei-1/1
inspur(config-mcast-ipv6-pim-if-gei-1/1)#dr-priority 20
inspur(config-mcast-ipv6-pim-if-gei-1/1)#exit
```

缺省情况下接口不是PIM域边界。当在接口上配置该命令时，没有引导报文能在任一方向上通过该边界。该命令有效地将网络划分成使用不同引导报文的区域。其他PIM报文可以通过域边界。

在路由器接口gei-1/1上配置PIM域边界：

```
inspur(config-mcast-ipv6)#router pim
inspur(config-mcast-ipv6-pim)#interface gei-1/1
inspur(config-mcast-ipv6-pim-if-gei-1/1)#bsr-border
inspur(config-mcast-ipv6-pim-if-gei-1/1)#exit
```

根据网络的实际情况，可以适当的调整PIM-SM邻居发送hello消息的时间间隔。

在设备接口gei-1/1上配置PIM hello报文发送间隔：

```
inspur(config-mcast-ipv6)#router pim
inspur(config-mcast-ipv6-pim)#interface gei-1/1
inspur(config-mcast-ipv6-pim-if-gei-1/1)#hello-interval 25
inspur(config-mcast-ipv6-pim-if-gei-1/1)#exit
```

6.配置IPv6 PIM-SM的策略控制。

步骤	命令	功能
1	inspur(config-mcast-ipv6-pim)#**accept-register** < *access-list-name* >	对接收到的register报文中封装的组播数据报文进行过滤
2	inspur(config-mcast-ipv6-pim)#**accept-rp** <*access-list-name*>	对BSR消息中通告的候选RP地址进行过滤

7.验证配置结果。

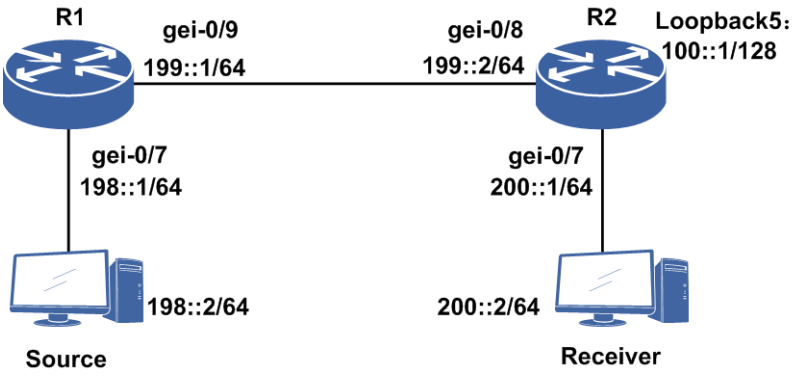
命令	功能
inspur(config)#**show ipv6 pim mroute** [**group** <*group-address*>][**source** <*source-address*>]	显示IPv6组播PIM路由表的内容
inspur(config)#**show ipv6 pim mroute summary**	显示IPv6组播PIM路由表的内容统计信息
inspur(config)#**show ipv6 pim bsr**	显示引导路由器（BSR）的信息
inspur(config)#**show ipv6 pim rp mapping** [{**bsr** | **default** | **embedded** | **static**}]	显示路由器上通告的RP集信息
inspur(config)#**show ipv6 pim rp hash** <*group-address*>	显示特定组播组选择的RP信息
inspur(config)#**show ipv6 pim interface** [<*interface-name*>]	查看配置的PIM接口情况
inspur(config)#**show ipv6 pim neighbor** [<*interface-name*>]	查看IPv6 PIM接口的邻居情况
inspur(config)#**show ipv6 pim nexthop** [**dest-address** <*ipv6-address*>]	查看IPv6 PIM下一跳的信息
inspur(config)#**show ipv6 pim traffic** [<*interface-name*>]	显示IPv6 PIM协议流量统计信息

12.12.2 IPv6 PIM-SM 配置实例

配置说明

如*图 12-29*所示，R2端PIM-SM组加入，R1端组播源加入，配置BSR和CRP。

图 12-29 PIM-SM 配置实例示意图



配置思路

1.配置相应接口地址。

2.进入组播配置模式。

3.进入PIM配置模式。

4.配置R2的loopback5接口为CRP和BSR。

5.进入接口启动PIM-SM。

6.在R1上配置到RP的单播路由，在R2上配置到组播源的单播路由（本例使用静态路由配置也可以使用IGP动态路由配置来打通路由）。

配置过程

R1的配置如下：

```
R1(config)#interface gei-0/9
R1(config-if-gei-0/9)#ipv6 enable
R1(config-if-gei-0/9)#ipv6 address 199::1/64
R1(config-if-gei-0/9)#no shutdown
R1(config-if-gei-0/9)#exit
R1(config)#interface gei-0/7
R1(config-if-gei-0/7)#ipv6 enable
R1(config-if-gei-0/7)#ipv6 address 198::1/64
R1(config-if-gei-0/7)#no shutdown
R1(config-if-gei-0/7)#exit
R1(config)#ipv6 multicast-routing
R1(config-mcast-ipv6)#router pim
R1(config-mcast-ipv6-pim)#interface gei-0/9
R1(config-mcast-ipv6-pim-if-gei-0/9)#pimsm
R1(config-mcast-ipv6-pim-if-gei-0/9)#exit
R1(config-mcast-ipv6-pim)#interface gei-0/7
R1(config-mcast-ipv6-pim-if-gei-0/7)#pimsm
R1(config-mcast-ipv6-pim-if-gei-0/7)#dr-priority 20
R1(config)#ipv6 route 100::1/128 199::2
```

R2的配置如下：

```
R2(config)#interface gei-0/8
R2(config-if-gei-0/8)#ipv6 enable
R2(config-if-gei-0/8)#ipv6 address 199::2/64
R2(config-if-gei-0/8)#no shutdown
R2(config-if-gei-0/8)#exit
```

```
R2(config)#interface gei-0/7
R2(config-if-gei-0/7)#ipv6 enable
R2(config-if-gei-0/7)#ipv6 address 200::1/64
R2(config-if-gei-0/7)#no shutdown
R2(config-if-gei-0/7)#exit
R2(config)#interface loopback5
R2(config-if-loopback5)#ipv6 enable
R2(config-if-loopback5)#ipv6 address 100::1/128
R2(config-if-loopback5)#exit
R2(config)#ipv6 multicast-routing
R2(config-mcast-ipv6)#router pim
R2(config-mcast-ipv6-pim)#rp-candidate 100::1
R2(config-mcast-ipv6-pim)#bsr-candidate 100::1
R2(config-mcast-ipv6-pim)#interface gei-0/8
R2(config-mcast-ipv6-pim-if-gei-0/8)#pimsm
R2(config-mcast-ipv6-pim-if gei-0/8)#exit
R2(config-mcast-ipv6-pim)#interface gei-0/7
R2(config-mcast-ipv6-pim-if-gei-0/7)#pimsm
R2(config-mcast-ipv6-pim-if-gei-0/7)#dr-priority 20
R2(config-mcast-ipv6-pim-if-gei-0/7)#end
R2#configure terminal
R2(config)#ipv6 route 198::/64 199::1
```

配置验证

在R1上通过**show ipv6 pim interface**查看接口状态：

```
R1(config)#show ipv6 pim interface
Interface      State Nbr   Hello  DR        PIM       Mode
                     Count Period Priority   Silent
gei-0/7        Up    0     30     20        Disabled   S

   Address: fe80::2d0:d0ff:fe06:606
   DR     : fe80::2d0:d0ff:fe06:606
gei-0/9        Up    1     30     1         Disabled   S

   Address: fe80::2d0:d0ff:fe06:606
   DR     : fe80::2d0:d0ff:fe06:606
```

在R1上通过**show ipv6 pim neighbor**查看邻居状态：

```
R1(config)#show ipv6 pim neighbor
Neighbor Address(es)      Interface       Uptime    Expires    DR Pri
fe80::211:12ff:fe51:ea12   gei-0/9         01:02:30   00:01:19   1
```

在R1上通过**show ipv6 pim bsr**查看BSR状态：

```
R1(config)#show ipv6 pim bsr

BSR address: 100::1
Uptime: 00:17:48, BSR Priority :0, Hash mask length:126
Expires:00:01:22
No candidate RP information!
```

在R1上通过**show ipv6 mroute**查看路由表：

```
R1#show ipv6 mroute
IPv6 Multicast Routing Table
Flags:NS:SPT upsend,RT:Reg upsend,F:Forward,
NTP:NTP join,DPU:Damping enable,DPD:Damping del,
(198::2, ff1e::1), TYPE: DYNAMIC, FLAGS:
  Incoming interface: gei-0/7, flags:
  Outgoing interface list:
    gei-0/9, flags: F
```

12.13 PIM-SSM

PIM-SSM具有PIM–SM协议的所有优点，只是不建立共享树，只建立基于源的最短路径树。在收到某个特定的源到组的成员关系报告消息时直接建立最短路径树。

PIM-SSM是PIM-SM的一个子集，PIM-SSM适合于well known源，在域内和域间都有效。PIM-SM使用域间组播路由协议MSDP，而PIM-SSM不需要使用。

12.13.1 配置 PIM-SSM

本节介绍IPv6 PIM-SSM协议的配置步骤和命令。

1.配置IPv6 PIM-SSM。

命令	功能
inspur(config-mcast-ipv6-pim)#**ssm range** | **default** [**group-list** < *access-list-name* >]	配置IPv6 SSM组地址范围或者使用默认组地址范围。 缺省情况不带**group-list**时，默认配置的组范围是FF3X::/32。

2.验证配置结果。

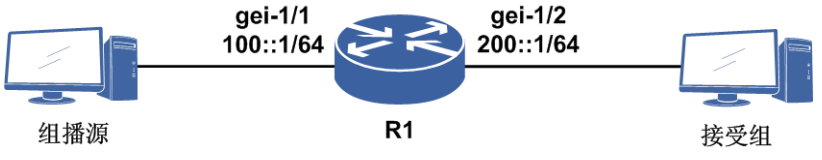
命令	功能
inspur#**show ipv6 pim mroute** [**group** <*group-address*>][**source** <*source-address*>]	显示组播IPv6 PIM路由表的内容

12.13.2 IPv6 PIM-SSM 配置实例

配置说明

如*图 12-30*所示，R1上启用PIM-SM协议，并且使能SSM，配置SSM组的范围，MLD协议版本启用v2。组播源向多个指定源的组播组发流，只有源地址和组播组地址都匹配的流量能通。

图 12-30 PIM-SSM 配置实例示意图



配置思路

1.接口模式下，配置路由器gei-1/1和gei-1/2的接口地址。

2.打开组播模块的总开关**ipv6 multicast-routing**。

3.进入IPv6 PIM路由模式，配置SSM组地址范围。

4.进入接口gei-1/1和gei-1/2，开启PIM-SM协议。

5.进入MLD路由模式，再进入所要配置的接口，在接口下启用v2。

6.在接受组上发送指定源的动态组加入。

配置过程

R1的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ipv6 enable
R1(config-if-gei-1/1)#ipv6 address 100::1/64
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ipv6 enable
R1(config-if-gei-1/2)#ipv6 address 200::1/64
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#exit

R1(config)#ipv6 multicast-routing
R1(config-mcast-ipv6)#router pim
R1(config-mcast-ipv6-pim)#interface gei-1/1
R1(config-mcast-ipv6-pim-if-gei-1/1)#pimsm
R1(config-mcast-ipv6-pim-if-gei-1/1)#exit
R1(config-mcast-ipv6-pim)#interface gei-1/2
R1(config-mcast-ipv6-pim-if-gei-1/2)#pimsm
R1(config-mcast-ipv6-pim-if-gei-1/2)#exit
R1(config-mcast-ipv6-pim)#ssm range default
R1(config-mcast-ipv6-pim)#exit
```

配置验证

R1上查看配置信息：

```
R1#show running-config multicast6
!<multicast6>
ipv6 multicast-routing
  router pim
    ssm range default
    interface gei-1/2
      pimsm
    $
    interface gei-1/1
      pimsm
    $
  $
  router mld
    interface gei-1/1
    $
    interface gei-1/2
    $
  $
$
!</multicast6>
```

在R1上查看路由生效情况：

```
R1#show ipv6 mroute
```

```
IPv6 Multicast Routing Table
Flags:NS:SPT upsend,RT:Reg upsend,F:Forward,
NTP:NTP join,DPU:Damping enable,DPD:Damping del,
(100::2, ff3a::aaaa:1), TYPE: DYNAMIC, FLAGS:
   Incoming interface: gei-1/1, flags:
   Outgoing interface list:
     gei-1/2, flags: F
```

12.14 IPv6 隧道

隧道是一种封装技术，即利用一种网络传输协议，将其他协议产生的数据报文封装在自己的报文中并在网络中传输。

IPv6 over IPv4隧道机制是在IPv6数据报文前封装上IPv4的报文头，通过隧道（Tunnel）使IPv6报文穿越IPv4网络，实现隔离的IPv6网络的互通。

IPv4或IPv6 over IPv6隧道是对IPv4或者IPv6的数据报文进行封装，使这些被封装的数据报文能够在另一个IPv6网络中传输，封装后的数据报文即IPv6隧道报文。

DS-lite隧道主要完成IPv4用户穿越纯IPv6网络访问IPv4 Internet ，以及通过IPv4-IPv4 NAT实现运营级IPv4的地址复用，在转发面进行隧道的封装和解封装。

12.14.1 配置 IPv6 隧道

配置IPv6隧道功能，隧道类型包括6in4隧道、6to4隧道和4in6隧道。

1.创建IPv6隧道接口并进入接口配置模式。

步骤	命令	功能
1	inspur(config)#**interface v6_tunnel**<*tunnel-no*>	创建IPv6隧道接口，IPv6隧道号范围为1~3000
2	inspur(config)#**ipv6-tunnel-config**	进入IPv6隧道配置模式
3	inspur(config-ipv6-tunnel)#**interface** {**byname** <*interface-byname*>|<*interface-name*>}	进入IPv6隧道接口配置模式，接口别名和接口名称最长32字符

2.配置6in4隧道。

步骤	命令	功能
1	inspur(config-ipv6-tunnel-if-v6_tunnel)# **tunnel mode ipv6ip 6in4**	配置当前隧道模式为6in4
2	inspur(config-ipv6-tunnel-if-v6_tunnel)# **tunnel source ipv4** <*src-address*>	配置隧道源地址，地址格式为IPv4地址
3	inspur(config-ipv6-tunnel-if-v6_tunnel)# **tunnel destination ipv4** <*dst-address*>	配置隧道目的地址，地址格式为IPv4地址

3.配置6to4隧道。

步骤	命令	功能
1	inspur(config-ipv6-tunnel-if-v6_tunnel)# **tunnel mode ipv6ip 6to4**	配置当前隧道模式为6to4
2	inspur(config-ipv6-tunnel-if-v6_tunnel)# **tunnel source ipv4** *<src-address>*	配置隧道源地址，地址格式为IPv4地址

4.配置4in6隧道。

步骤	命令	功能
1	inspur(config-ipv6-tunnel-if-v6_tunnel)# **tunnel mode ipipv6 4in6**	配置当前隧道模式为4in6
2	inspur(config-ipv6-tunnel-if-v6_tunnel)# **tunnel source ipv6** *<src-address>*	配置隧道源地址，地址格式为IPv6地址
3	inspur(config-ipv6-tunnel-if-v6_tunnel)# **tunnel destination ipv6** *<dst-address>*	配置隧道目的地址，地址格式为IPv6地址

5.维护IPv6隧道。

命令	功能
inspur#**debug ipv6-tunnel**	打开IPv6隧道debug开关，查看封装及解封装相关信息
inspur#**show debug ipv6-tunnel**	查看IPv6隧道debug开关是否打开

12.14.2 6in4 隧道配置实例

配置说明

如*图 12-31*所示，假设R1、R2为双栈路由器，PC1、PC2为IPv6主机，配置6in4隧道。

图 12-31 6in4 隧道配置实例拓扑图



配置思路

6in4隧道是v6性质的，需要使能IPv6，隧道源地址为本路由器上的v4地址，目的地址为对端路由器上的v4地址。隧道的源和目的地址间必须有路由可以互通（依赖v4路由协议，静态路由等）。

1.创建6in4隧道接口，使能IPv6。

2.全局模式下进入隧道配置模式，再进入所要配置6in4隧道接口。

3.配置隧道模式以及源和目的地址。

配置过程

R1上的配置如下：

```
R1(config)#interface v6_tunnel3
R1(config-if-v6_tunnel3)#ipv6 enable
R1(config-if-v6_tunnel3)#ipv6 address 3172::27/64
R1(config-if-v6_tunnel3)#exit
R1(config)#ipv6-tunnel-config
R1(config-ipv6-tunnel)#interface v6_tunnel3
R1(config-ipv6-tunnel-if-v6_tunnel3)#tunnel mode ipv6ip 6in4
R1(config-ipv6-tunnel-if-v6_tunnel3)#tunnel destination ipv4 33.1.1.28
R1(config-ipv6-tunnel-if-v6_tunnel3)#tunnel source ipv4 33.1.1.27
R1(config-ipv6-tunnel-if-v6_tunnel3)#exit
R1(config-ipv6-tunnel)#exit

R1(config)#interface gei-2/4
R1(config-if-gei-2/4)#no shutdown
R1(config-if-gei-2/4)#ip address 33.1.1.27 255.255.0.0
R1(config-if-gei-2/4)#exit
R1(config)#interface gei-2/3
R1(config-if-gei-2/3)#no shutdown
R1(config-if-gei-2/3)#ipv6 enable
R1(config-if-gei-2/3)#ipv6 address 2700::1/64
R1(config-if-gei-2/3)#exit
```

R2的配置如下：

```
R2(config)#interface v6_tunnel3
R2(config-if-v6_tunnel3)#ipv6 enable
R2(config-if-v6_tunnel3)#ipv6 address 3172::28/64
R2(config-if-v6_tunnel3)#exit
```

```
R2(config)#ipv6-tunnel-config
R2(config-ipv6-tunnel)#interface v6_tunnel3
R2(config-ipv6-tunnel-if-v6_tunnel3)#tunnel mode ipv6ip 6in4
R2(config-ipv6-tunnel-if-v6_tunnel3)#tunnel destination ipv4 33.1.1.27
R2(config-ipv6-tunnel-if-v6_tunnel3)#tunnel source ipv4 33.1.1.28
R2(config-ipv6-tunnel-if-v6_tunnel3)#exit
R2(config-ipv6-tunnel)#exit

R2(config)#interface gei-3/4
R2(config-if-gei-3/4)#no shutdown
R2(config-if-gei-3/4)#ip address 33.1.1.28 255.255.0.0
R2(config-if-gei-3/4)#exit
R2(config)#interface gei-3/3
R2(config-if-gei-3/3)#no shutdown
R2(config-if-gei-3/3)#ipv6 enable
R2(config-if-gei-3/3)#ipv6 address 2800::1/64
R2(config-if-gei-3/3)#exit
```

配置验证

查看R1的隧道配置和生效情况：

```
R1(config)#show running-config-interface v6_tunnel3
!<if-intf>
interface v6_tunnel3
  ipv6 enable
  ipv6 address 3172::27/64
$
!</if-intf>
!<ipv6-tunnel>
ipv6-tunnel-config
  interface v6_tunnel3
    tunnel mode ipv6ip 6in4
    tunnel source ipv4 33.1.1.27
    tunnel destination ipv4 33.1.1.28
  $
$
!</ipv6-tunnel>

R1(config)#show ip interface gei-2/4
gei-2/4 AdminStatus is up, PhyStatus is up, line protocol is up
  Internet address is 33.1.1.27/16
  Broadcast address is 255.255.255.255
  IP MTU is 1500 bytes

R1(config)#show ipv6 interface brief
v6_tunnel3                          [up/up]
   fe80::2101:11b
   3172::27/64
```

12.14.3 4in6 隧道配置实例

配置说明

如*图 12-32*所示，假设R1、R2为双栈路由器，PC1、PC2为IPv4主机，配置4in6隧道。

图 12-32 4in6 隧道配置实例拓扑图



配置思路

4in6隧道是v4性质的，隧道源地址为本路由器上的v6地址，目的地址为对端路由器上的v6地址。隧道的源和目的地址间必须有路由可以互通（依赖v6路由协议，静态路由等）。

1.创建4in6隧道，配置IPv4地址

2.全局模式下进入隧道配置模式，再进入所要配置4in6隧道接口。

3.配置隧道模式以及源和目的地址。

配置过程

R1上的配置如下：

```
R1(config)#interface v6_tunnel2
R1(config-if-v6_tunnel2)#ip address 27.0.1.1 255.255.0.0
R1(config-if-v6_tunnel2)#exit
R1(config)#ipv6-tunnel-config
R1(config-ipv6-tunnel)#interface v6_tunnel2
R1(config-ipv6-tunnel-if-v6_tunnel2)#tunnel mode ipipv6 4in6
R1(config-ipv6-tunnel-if-v6_tunnel2)#tunnel destination ipv6 2078::28
R1(config-ipv6-tunnel-if-v6_tunnel2)#tunnel source ipv6 2078::27
R1(config-ipv6-tunnel-if-v6_tunnel2)#exit
R1(config-ipv6-tunnel)#exit

R1(config)#interface gei-2/4
R1(config-if-gei-2/4)#no shutdown
R1(config-if-gei-2/4)#ipv6 address 2078::27/64
R1(config-if-gei-2/4)#ipv6 enable
R1(config-if-gei-2/4)#exit
R1(config)#interface gei-2/3
R1(config-if-gei-2/3)#no shutdown
R1(config-if-gei-2/3)#ip address 150.23.1.1 255.255.0.0
R1(config-if-gei-2/3)#exit
```

R2上的配置如下：

```
R2(config)#interface v6_tunnel2
R2(config-if-v6_tunnel2)#ip address 27.0.1.2 255.255.0.0
R2(config-if-v6_tunnel2)#exit
R2(config)#ipv6-tunnel-config
R2(config-ipv6-tunnel)#interface v6_tunnel2
R2(config-ipv6-tunnel-if-v6_tunnel2)#tunnel mode ipipv6 4in6
```

```
R2(config-ipv6-tunnel-if-v6_tunnel2)#tunnel destination ipv6 2078::27
R2(config-ipv6-tunnel-if-v6_tunnel2)#tunnel source ipv6 2078::28
R2(config-ipv6-tunnel-if-v6_tunnel2)#exit
R2(config-ipv6-tunnel)#exit

R2(config)#interface gei-3/4
R2(config-if-gei-3/4)#no shutdown
R2(config-if-gei-3/4)#ipv6 address 2078::28/64
R2(config-if-gei-3/4)#ipv6 enable
R2(config-if-gei-3/4)#exit
R2(config)#interface gei-3/3
R2(config-if-gei-3/3)#no shutdown
R2(config-if-gei-3/3)#ip address 191.15.1.1 255.255.0.0
R2(config-if-gei-3/3)#exit
```

配置验证

查看R1的隧道配置和生效情况：

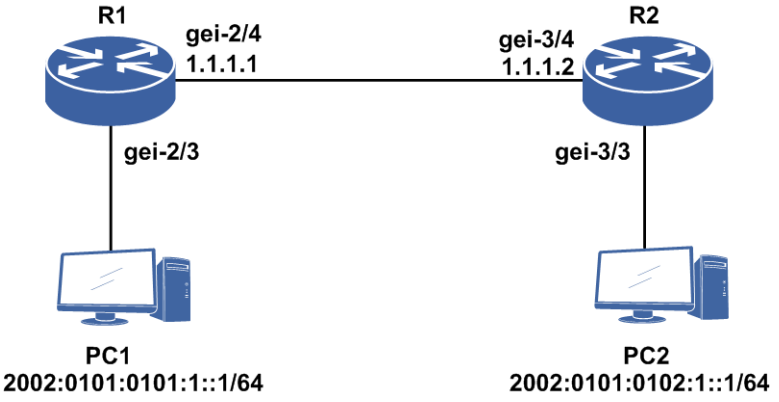
```
R1(config)#show running-config-interface v6_tunnel2
!<if-intf>
interface v6_tunnel2
  ip address 27.0.1.1 255.255.0.0
$
!</if-intf>
!<ipv6-tunnel>
ipv6-tunnel-config
  interface v6_tunnel2
    tunnel mode ipipv6  4in6
    tunnel source ipv6 2078::27
    tunnel destination ipv6 2078::28
  $
$
!</ipv6-tunnel>
R1(config)#show ip interface v6_tunnel2
v6_tunnel2 AdminStatus is up, PhyStatus is up, line protocol is up
  Internet address is 27.0.1.1/16
  Broadcast address is 255.255.255.255
  IP MTU is 1460 bytes
```

12.14.4 6to4 隧道配置实例

配置说明

如*图 12-33*所示，假设R1、R2为双栈路由器，PC1、PC2为IPv6主机，配置6to4隧道。

图 12-33 6to4 隧道配置拓扑图



配置思路

6to4隧道是v6性质的，需要使能IPv6，用于连接前缀为2002::/16的6to4节点。隧道源端绑定本路由器的v4地址，无须配置目的地址。隧道的地址必须使用2002::/16前缀。

1.创建6to4隧道，配置IPv6地址，使能IPv6。隧道和6to4站点前48位前缀模式固定且是根据隧道的源v4地址生成的，过程如下：将隧道的源v4地址x.x.x.x转换成16进制形式yyyy:yyyy，再加上2002::/16就可以得到前48位前缀2002:yyyy:yyyy::/48。

2.全局模式下进入隧道配置模式，再进入所要配置6to4隧道接口。

3.配置隧道模式以及源地址。

4.通告隧道路由：通过静态或者BGP4+来通告隧道路由。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/4
R1(config-if-gei-2/4)#no shutdown
R1(config-if-gei-2/4)#ip address 1.1.1.1 255.255.255.0
R1(config-if-gei-2/4)#exit

R1(config)#interface v6_tunnel2
R1(config-if-v6_tunnel2)#ipv6 address 2002:0101:0101:1::1/64
R1(config-if-v6_tunnel2)#ipv6 enable
R1(config-if-v6_tunnel2)#exit
R1(config)#ipv6-tunnel-config
R1(config-ipv6-tunnel)#interface v6_tunnel2
R1(config-ipv6-tunnel-if-v6_tunnel2)#tunnel mode ipv6ip 6to4
R1(config-ipv6-tunnel-if-v6_tunnel2)#tunnel source ipv4 1.1.1.1
R1(config-ipv6-tunnel-if-v6_tunnel2)#exit
R1(config-ipv6-tunnel)#exit

R1(config)#ipv6 route 2002::/16 v6_tunnel2
```

R2上的配置如下：

```
R2(config)#interface gei-3/4
R2(config-if-gei-3/4)#no shutdown
R2(config-if-gei-3/4)#ip address 1.1.1.2 255.255.255.0
R2(config-if-gei-3/4)#exit
```

```
R2(config)#interface v6_tunnel2
R2(config-if-v6_tunnel2)#ipv6 address 2002:0101:0102:1::1/64
R2(config-if-v6_tunnel2)#ipv6 enable
R2(config-if-v6_tunnel2)#exit

R2(config)#ipv6-tunnel-config
R2(config-ipv6-tunnel)#interface v6_tunnel2
R2(config-ipv6-tunnel-if-v6_tunnel2)#tunnel mode ipv6ip 6to4
R2(config-ipv6-tunnel-if-v6_tunnel2)#tunnel source ipv4 1.1.1.2
R2(config-ipv6-tunnel-if-v6_tunnel2)#exit
R2(config-ipv6-tunnel)#exit

R2(config)#ipv6 route 2002::/16 v6_tunnel2
```

配置验证

查看R1的隧道配置和生效情况：

```
R1(config)#show running-config-interface v6_tunnel2
!<if-intf>
interface v6_tunnel2
  ipv6 enable
  ipv6 address 2002:101:101:1::1/64
$
!</if-intf>
!<ipv6-tunnel>
ipv6-tunnel-config
  interface v6_tunnel2
    tunnel mode ipv6ip 6to4
    tunnel source ipv4 1.1.1.1
  $
$
!</ipv6-tunnel>
R1(config)#show ipv6 interface brief
v6_tunnel2                        [up/up]
   fe80::101:101
   2002:101:101:1::1/64
```

12.15 ISATAP 隧道

随着 IPv6技术的推广，现有的IPv4 网络中将会出现越来越多的IPv6主机，ISATAP隧道技术为这种应用提供了一个较好的解决方案，通过在IPv6报文的目的地址中嵌入的IPv4 地址，可以自动获取隧道的终点。

使用ISATAP隧道时，IPv6 报文的目的地址和隧道接口的IPv6地址都要采用特殊的ISATAP地址。ISATAP地址格式为：Prefix(64bit):0:5EFE:ip-address。其中，64位的Prefix为任何合法的IPv6单播地址前缀，ip-address为32位IPv4 源地址，形式为a.b.c.d或abcd:efgh。通过这个嵌入的IPv4地址就可以自动建立隧道，完成IPv6报文的传送。

ISATAP隧道主要用于在IPv4网络中IPv6路由器-IPv6路由器、IPv6主机-IPv6路由器的连接。

12.15.1 配置 ISATAP 隧道

本节介绍ISATAP隧道的配置步骤和命令。

1.配置ISATAP隧道。

步骤	命令	功能
1	inspur(config)#**interface v6_tunnel1**<*tunnel_no*>	创建IPv6隧道接口
2	inspur(config-if-v6_tunnel)#**ipv6 enable**	启用IPv6功能
3	inspur(config-if-v6_tunnel)#**ipv6 address** <*addrprefix / prefix-len*> **eui-64**	ISATAP隧道需在接口上配置eui-64地址
4	inspur(config)#**ipv6-tunnel-config**	进入IPv6隧道配置模式
5	inspur(config-v6_tunnel)#**interface** {**byname** <*interface-byname*>|<*interface-name*>}	进入IPv6隧道接口配置模式，接口别名和接口名称最长32字符
6	inspur(config-ipv6-tunnel-if-v6_tunnel)# **tunnel mode ipv6ip isatap**	配置当前隧道模式为**isatap**
7	inspur(config-ipv6-tunnel-if-v6_tunnel)# **tunnel source ipv4** <*src-addr*>	配置隧道源地址，只需指定到IPv4一级，不用指定具体源地址

<*tunnel_no*>：隧道号，指的是可以创建的隧道接口，个数为1~3000。

<*src-addr*>：表示隧道实际出接口源地址。

<*addrprefix /prefix-len*>：配置IPv6地址前缀以及前缀长度。

2.维护ISATAP隧道。

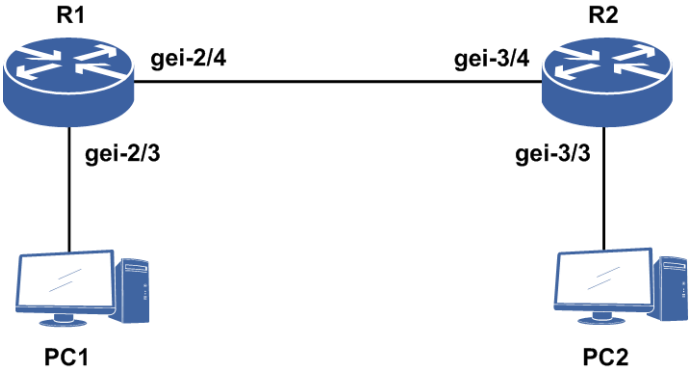
命令	功能
inspur#**debug ipv6-tunnel**	打开IPv6隧道debug开关，查看封装及解封装相关信息
inspur#**show debug ipv6-tunnel**	查看IPv6隧道debug开关是否打开

12.15.2 ISATAP 配置实例

配置说明

如*图 12-34*所示，假设R1、R2为双栈路由器，PC1、PC2为IPv6主机，配置ISATAP隧道。

图 12-34 ISATAP 配置实例图



配置思路

ISATAP隧道是v6性质的，需要使能IPv6。隧道源端绑定本路由器的v4地址，无须配置目的地址。配置步骤如下：

1.创建ISATAP隧道，配置IPv6地址且使能IPv6。ISATAP隧道口IPv6地址采用eui的方式配置。

2.全局模式下进入隧道配置模式，再进入所要配置ISATAP隧道接口。

3.配置隧道模式以及源地址。

4.通过静态或者BGP4+来通告隧道路由。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/4
R1(config-if-gei-2/4)#no shutdown
R1(config-if-gei-2/4)#ip add 1.1.1.1 255.255.255.0
R1(config-if-gei-2/4)#exit
R1(config)#interface v6_tunnel2
R1(config-if-v6_tunnel2)#ipv6 add 82::/64 eui-64
R1(config-if-v6_tunnel2)#ipv6 enable
R1(config-if-v6_tunnel2)#exit

R1(config)#ipv6-tunnel-config
R1(config-ipv6-tunnel)#interface v6_tunnel2
R1(config-ipv6-tunnel-if-v6_tunnel2)#tunnel mode ipv6ip isatap
R1(config-ipv6-tunnel-if-v6_tunnel2)#tunnel source ipv4 1.1.1.1
R1(config-ipv6-tunnel-if-v6_tunnel2)#exit
R1(config-ipv6-tunnel)#exit

R1(config)#ipv6 route 81::/16 v6_tunnel2
```

R2上的配置如下：

```
R2(config)#interface gei-3/4
R2(config-if-gei-3/4)#no shutdown
R2(config-if-gei-3/4)#ip add 1.1.1.2 255.255.255.0
R2(config-if-gei-3/4)#exit
R2(config)#interface v6_tunnel2
R2(config-if-v6_tunnel2)#ipv6 add 81::/64 eui-64
R2(config-if-v6_tunnel2)#ipv6 enable
```

```
R2(config-if-v6_tunnel2)#exit

R2(config)#ipv6-tunnel-config
R2(config-ipv6-tunnel)#interface v6_tunnel2
R2(config-ipv6-tunnel-if-v6_tunnel2)#tunnel mode ipv6ip isatap
R2(config-ipv6-tunnel-if-v6_tunnel2)#tunnel source ipv4 1.1.1.2
R2(config-ipv6-tunnel-if-v6_tunnel2)#exit
R2(config-ipv6-tunnel)#exit

R2(config)#ipv6 route 82::/16 v6_tunnel2
```

配置验证

在R1上查看ISATAP配置情况：

```
R1(config)#show running-config-interface v6_tunnel2
!<if-intf>
interface v6_tunnel2
  ipv6 enable
  ipv6 address 82::/64 eui-64
$
!</if-intf>
!<ipv6-tunnel>
ipv6-tunnel-config
  interface v6_tunnel2
    tunnel mode ipv6ip isatap
    tunnel source ipv4 1.1.1.1
  $
$
!</ipv6-tunnel>
!<ipv6-static-route>
ipv6 route 81::/16 v6_tunnel2
!</ipv6-static-route>
```

在R1上通过**show ipv6 interface brief v6_tunnel2**查看隧道的接口情况：

```
R1(config)#show ipv6 interface brief v6_tunnel2
v6_tunnel2              [up/up]
   fe80::5efe:101:101
   82::5efe:101:101/64   [EUI]
```

12.16 DS-Lite B4

DS-Lite技术是IPv6过渡的关键技术之一，其结合IPv4 in IPv6隧道和IPv4 NAT技术，由AFTR和B4（Base Bridge Broadband element，通常为用户终端 ）两个模块协作实施。B4和AFTR设备之间建立DS-Lite隧道，并在AFTR设备上配置NAT，可实现IPv4用户穿越IPv6网络访问IPv4网络，同时NAT技术实现运营商级别IPv4地址复用，减少地址开销。

12.16.1 配置 DS-Lite 隧道

本节介绍DS-Lite隧道的配置步骤和命令。

1.在B4上配置DS-Lite隧道。

步骤	命令	功能
1	inspur(config)#**ipv6-tunnel-config**	进入IPv6隧道配置模式
2	inspur(config-ipv6-tunnel)#**interface v6_tunnelnum**	进入指定IPv6隧道
3	inspur(config-ipv6-tunnel-if-v6_tunnelnum)#**tunnel mode ipipv6 ds-lite-b4**	配置隧道模式
4	inspur(config-ipv6-tunnel-if-v6_tunnelnum)#**tunnel source** {**ipv4** *<ipv4-address>*|**ipv6** *<ipv6-address>*}	配置隧道的源地址
5	inspur(config-ipv6-tunnel-if-v6_tunnelnum)#**tunnel destination** {**ipv4** *<ipv4-address>*|**ipv6** *<ipv6-address>*| **dhcp-interface** *<interface-name>*|**domain** *<domain-name>*}	配置隧道的目地地址或参数

2.维护DS-Lite隧道。

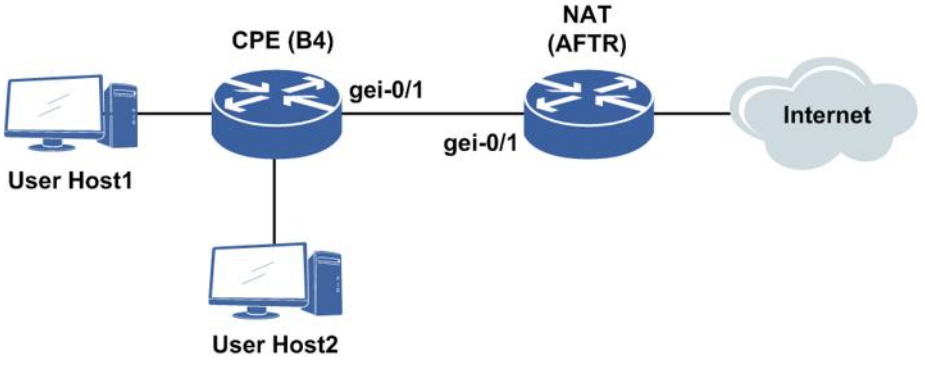
命令	功能
inspur#**debug ipv6-tunnel**	打开IPv6隧道debug功能
inspur#**show debug ipv6-tunnel**	查看IPv6隧道debug开关是否打开

12.16.2 手工配置 AFTR 地址配置实例

配置说明

如*图 12-35*所示，用户主机使用私有网络的IPv4地址，通过CPE和NAT设备组成的IPv6网络来访问外部的IPv4网络，本节B4设备通过手工配置AFTR地址建立DS-Lite隧道。AFTR上隧道以及DS-Lite配置以IR12000智能路由器系列路由器的静态NAT配置为例。

图 12-35 手工配置 AFTR 地址配置实例图



配置思路

CPE（IR12000）设备：

1.配置v6_tunnel。

2.隧道目地地址直接配置AFTR地址。

DS-Lite（IR12000）设备：

1.配置v6_tunnel和ACL。

2.配置NAT地址池和NAT模式。

3.配置域并在域中配置静态NAT转换规则。

4.配置软线和用户。

配置过程

在CPE（IR12000）设备上配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 2017:1::1:1/96
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#ip address 100.1.1.1/24
inspur(config-if-v6_tunnel1)#exit
inspur(config)#ipv6-tunnel-config
inspur(config-ipv6-tunnel)#interface v6_tunnel1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipipv6 ds-lite-b4
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv6 2017:1::1:1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel destination ipv6 2017:1::1:2
inspur(config-ipv6-tunnel-if-v6_tunnel1)#exit
inspur(config-ipv6-tunnel)#exit
```

在DS-Lite（IR12000）设备上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 2017:1::1:2/96
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit

/*配置v6_tunnel*/
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#ipv6 enable
inspur(config-if-v6_tunnel1)#ip address 100.1.1.2/24
inspur(config-if-v6_tunnel1)#exit
inspur(config)#ipv6-tunnel-config
inspur(config-ipv6-tunnel)#interface v6_tunnel1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipipv6 ds-lite static
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv6 2017:1::1:2
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel destination ipv6 2017:1::1:1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#exit
inspur(config-ipv6-tunnel)#exit


/*配置ACL*/
inspur(config)#ipv4-access-list dslite
inspur(config-ipv4-acl)#rule 10 permit any
inspur(config-ipv4-acl)#exit
```

```
inspur(config)#cgn
inspur(config-cgn)#cgn-pool dslite poolid 2 mode nat  /*配置地址池,类型为nat*/
inspur(config-cgn-natpool)#section 1 99.1.1.1 99.1.1.10
inspur(config-cgn-natpool)#exit
inspur(config-cgn)#domain 10 10 type standalone ipv6-issued
inspur(config-cgn-domain)#static source rule-id 1 softwire 2017:1::1:1
2017:1::1:2 192.85.1.2 99.1.1.1
/* 192.85.1.2是用户主机地址，上述命令配置的是静态规则，也可以配置动态规则*/
inspur(config-cgn-domain)#exit

/*配置软线和用户*/
inspur(config-cgn)#softwire-domain dslite
inspur(config-cgn-sw-domain-dslite)#bind nat-domain 10
inspur(config-cgn-sw-domain-dslite)#aftr interface v6_tunnel1
inspur(config-cgn-sw-domain-dslite)#exit
inspur(config-cgn)#subscriber ipv6 prefix 2017:1::1:1/128 softwire-domain
dslite
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
```

配置验证

在CPE上查看DS-Lite隧道配置情况。

```
inspur(config)#show running-config-interface v6_tunnel1
!<if-intf>
interface v6_tunnel1
  ip address 100.1.1.1 255.255.255.0
$
!</if-intf>
!<ipv6-tunnel>
ipv6-tunnel-config
  interface v6_tunnel1
    tunnel mode ipipv6 ds-lite-b4
    tunnel source ipv6 2017:1::1:1
    tunnel destination ipv6 2017:1::1:2
  $
$
!</ipv6-tunnel>
```

在CPE上通过**show ipv6 interface brief v6_tunnel1**查看隧道的接口情况。

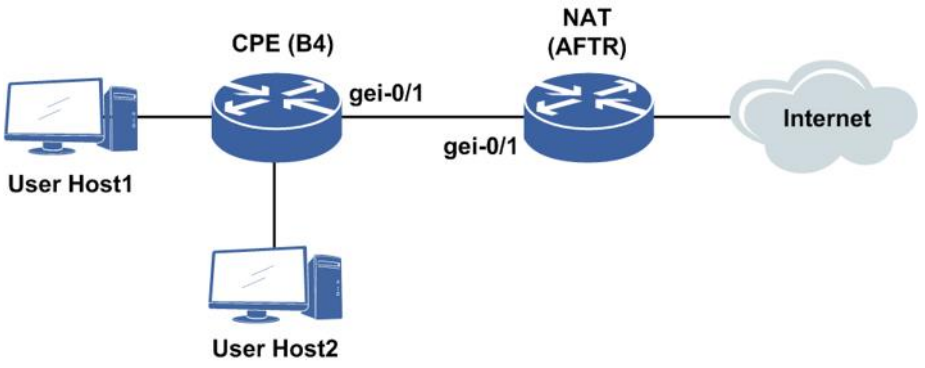
```
inspur(config)#show ipv6 interface brief v6_tunnel1
v6_tunnel1              [up/up]
```

12.16.3 DNS 获取 AFTR 地址配置实例

配置说明

如*图 12-36*所示，用户主机使用私有网络的IPv4地址，通过CPE和NAT设备组成的IPv6网络来访问外部的IPv4网络，本节B4设备通过DNS域名配置获取AFTR地址建立DS-Lite隧道，示例的DNS查询在CPE设备上完成。AFTR上隧道以及DS-Lite配置以IR12000智能路由器系列路由器的静态PAT为例。

图 12-36 DNS 获取 AFTR 地址配置实例图



配置思路

CPE（IR12000）设备：

1.配置v6_tunnel。

2.隧道目地地址配置domain name。

3.配置DNS。

DS-Lite（IR12000）设备：

1.配置v6_tunnel和ACL。

2.配置NAT地址池和NAT模式。

3.配置域并在域中配置静态PAT转换规则。

4.配置软线和用户。

配置过程

在CPE（IR2000）设备上配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 2017:1::1:1/96
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#ip address 100.1.1.1/24
inspur(config-if-v6_tunnel1)#exit
inspur(config)#ipv6-tunnel-config
inspur(config-ipv6-tunnel)#interface v6_tunnel1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipipv6 ds-lite-b4
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv6 2017:1::1:1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel destination domain
a.inspur.com.cn
inspur(config-ipv6-tunnel-if-v6_tunnel1)#exit
inspur(config-ipv6-tunnel)#exit


/*配置DNS*/
inspur(config)#ip domain lookup
inspur(config)#ip domain resolve-type static
inspur(config)#ip domain hostname a.inspur.com.cn ipv6-address 2017:1::1:2
```

在DS-Lite（IR12000）设备上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 2017:1::1:2/96
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit

/*配置v6_tunnel*/
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#ipv6 enable
inspur(config-if-v6_tunnel1)#ip address 100.1.1.2/24
inspur(config-if-v6_tunnel1)#exit
inspur(config)#ipv6-tunnel-config
inspur(config-ipv6-tunnel)#interface v6_tunnel1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipipv6 ds-lite static
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv6 2017:1::1:2
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel destination ipv6 2017:1::1:1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#exit
inspur(config-ipv6-tunnel)#exit


/*配置ACL*/
inspur(config)#ipv4-access-list dslite
inspur(config-ipv4-acl)#rule 10 permit any
inspur(config-ipv4-acl)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool dslite poolid 2 mode pat  /*配置地址池，类型为pat*/
inspur(config-cgn-natpool)#section 1 99.1.1.1 99.1.1.10
inspur(config-cgn-natpool)#exit
inspur(config-cgn)#domain 10 10 type standalone ipv6-issued
inspur(config-cgn-domain)#static source rule-id 1 softwire 2017:1::1:1
2017:1::1:2 192.85.1.2 1024 99.1.1.1 1024 udp
/* 192.85.1.2是用户主机地址，1024是用户端口，协议配置为udp*/
inspur(config-cgn-domain)#exit

/*配置软线和用户*/
inspur(config-cgn)#softwire-domain dslite
inspur(config-cgn-sw-domain-dslite)#bind nat-domain 10
inspur(config-cgn-sw-domain-dslite)#aftr interface v6_tunnel1
inspur(config-cgn-sw-domain-dslite)#exit
inspur(config-cgn)#subscriber ipv6 prefix 2017:1::1:1/128 softwire-domain
dslite
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
```

配置验证

在CPE上查看DS-Lite隧道配置情况。

```
inspur(config)#show running-config-interface v6_tunnel1
!<if-intf>
interface v6_tunnel1
  ip address 100.1.1.1 255.255.255.0
$
!</if-intf>
!<ipv6-tunnel>
ipv6-tunnel-config
  interface v6_tunnel1
    tunnel mode ipipv6 ds-lite-b4
    tunnel source ipv6 2017:1::1:1
    tunnel destination domain a.inspur.com.cn
```

```
  $
$
!</ipv6-tunnel>
```

在CPE上通过**show ipv6 interface brief v6_tunnel1**查看隧道的接口情况。

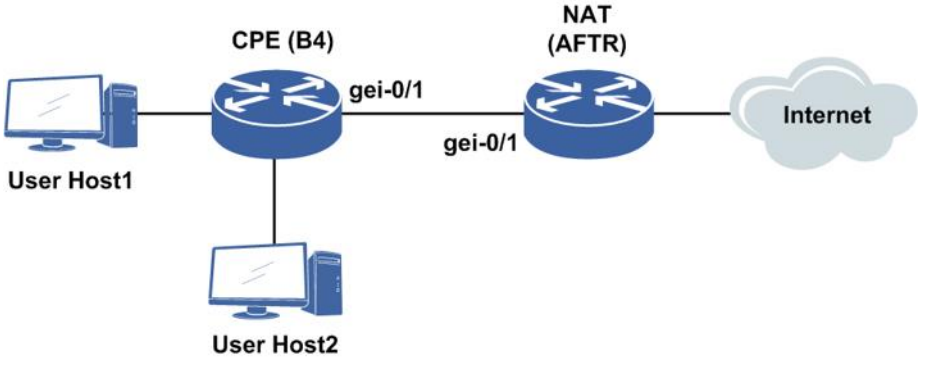
```
inspur(config)#show ipv6 interface brief v6_tunnel1
v6_tunnel1              [up/up]
```

12.16.4 DHCPv6 获取 AFTR 地址配置实例

配置说明

如*图 12-37*所示，用户主机使用私有网络的IPv4地址，通过CPE和NAT设备组成的IPv6网络来访问外部的IPv4网络，本节B4的AFTR地址通过动态参数获取，从DHCPv6获取的AFTR-Name选项中获取AFTR name，再经过DNS获取AFTR地址建立DS-Lite隧道。AFTR上隧道以及DS-Lite配置以IR12000智能路由器系列路由器动态PAT为例。

图 12-37 DHCPv6 获取 AFTR 地址配置实例图



配置思路

CPE（IR12000）设备：

1.配置接口开启DHCPv6 Client。

2.配置v6_tunnel。

3.隧道目地地址配置dhcp-interface。

4.配置DNS。

DS-Lite（IR12000）设备：

1.配置DHCPv6 Server。

2.配置v6_tunnel和ACL。

3.配置NAT地址池和NAT模式。

4.配置域并在域中配置动态PAT转换规则。

5.配置软线和用户。

配置过程

在CPE（IR12000）设备上配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 2017:1::1:1/96
inspur(config-if-gei-0/1)#ipv6 dhcp client address /*配置DHCPv6*/
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#ip address 100.1.1.1/24
inspur(config-if-v6_tunnel1)#exit
inspur(config)#ipv6-tunnel-config
inspur(config-ipv6-tunnel)#interface v6_tunnel1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipipv6 ds-lite-b4
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv6 2017:1::1:1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel destination dhcp-interface
gei-0/1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#exit
inspur(config-ipv6-tunnel)#exit


/*配置DNS*/
inspur(config)#ip domain lookup
inspur(config)#ip domain resolve-type static
inspur(config)#ip domain hostname a.inspur.com.cn ipv6-address 2017:1::1:2
```

在DS-Lite（IR12000）设备上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 2017:1::1:2/96
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit

inspur(config)#ipv6 addr-pool inspur
inspur(config-ipv6-addr-pool)#addr-range 2017:1::1:3 2017:1::1:10
inspur(config-ipv6-addr-pool)#exit

inspur(config)#dhcp ipv6
inspur(config-dhcpv6)#policy inspur 1
inspur(config-dhcpv6-policy)#dhcpv6-pool inspur
inspur(config-dhcpv6-policy)#exit
inspur(config-dhcpv6)#pool inspur
inspur(config-dhcpv6-pool)#address-pool inspur
inspur(config-dhcpv6-pool)#aftr fqdn a.inspur.com.cn
inspur(config-dhcpv6)#interface gei-0/1
inspur(config-dhcpv6-if-gei-10/7)#mode server
inspur(config-dhcpv6-if-gei-10/7)#server policy inspur
inspur(config-dhcpv6-if-gei-10/7)#exit
inspur(config-dhcpv6)#enable
inspur(config-dhcpv6)#exit

/*配置v6_tunnel*/
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#ipv6 enable
inspur(config-if-v6_tunnel1)#ip address 100.1.1.2/24
inspur(config-if-v6_tunnel1)#exit
inspur(config)#ipv6-tunnel-config
inspur(config-ipv6-tunnel)#interface v6_tunnel1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipipv6 ds-lite static
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv6 2017:1::1:2
```

```
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel destination ipv6 2017:1::1:1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#exit
inspur(config-ipv6-tunnel)#exit

/*配置ACL*/
inspur(config)#ipv4-access-list dslite
inspur(config-ipv4-acl)#rule 10 permit any
inspur(config-ipv4-acl)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool dslite poolid 2 mode pat  /*配置地址池，类型为pat*/
inspur(config-cgn-natpool)#section 1 99.1.1.1 99.1.1.10
inspur(config-cgn-natpool)#exit
inspur(config-cgn)#domain 10 10 type standalone ipv6-issued
inspur(config-cgn-domain)# dynamic source rule-id 1 ipv4-list dslite permit
 pool dslite  /*配置动态ACL规则，也可以配置静态规则*/
inspur(config-cgn-domain)#exit

/*配置软线和用户*/
inspur(config-cgn)#softwire-domain dslite
inspur(config-cgn-sw-domain-dslite)#bind nat-domain 10
inspur(config-cgn-sw-domain-dslite)#aftr interface v6_tunnel1
inspur(config-cgn-sw-domain-dslite)#exit
inspur(config-cgn)#subscriber ipv6 prefix 2017:1::/64 softwire-domain dslite
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
```

配置验证

在CPE上查看DS-Lite隧道配置情况。

```
inspur(config)#show running-config-interface v6_tunnel1
!<if-intf>
interface v6_tunnel1
  ip address 100.1.1.1 255.255.255.0
$
!</if-intf>
!<ipv6-tunnel>
ipv6-tunnel-config
  interface v6_tunnel1
    tunnel mode ipipv6 ds-lite-b4
    tunnel source ipv6 2017:1::1:1 dhcp-interface gei-0/1
    tunnel destination
  $
$
!</ipv6-tunnel>
```

在CPE上通过**show ipv6 interface brief v6_tunnel1**查看隧道的接口情况。

```
inspur(config)#show ipv6 interface brief v6_tunnel1
v6_tunnel1              [up/up]
```

12.17 6RD

6RD是IPv6快速部署（IPv6 Rapid Deployment）的简称，是在6to4技术基础上发展起来的一种IPv6网络过渡技术方案。6RD通过在现有IPv4网络中增加6RD BR，给愿意使用IPv6的用户提供IPv6接入，在IPv6用户的家庭网关和6RD网关之间建立6in4隧道，从而实现在IPv4网络提供IPv6服务的能力。

6RD是隧道技术中自动隧道的一种，隧道技术使隧道的两端不感知中间网络类型，是连接IPv6孤岛的有效方法。6RD技术使服务提供者能够快速部署IPv6单播服务给IPv4站点，因此适合IPv4到IPv6演进过程的初期。

12.17.1 配置 6RD

本节介绍6RD隧道的配置步骤和命令。

1.配置6RD隧道功能。

步骤	命令	功能
1	inspur(config)#**interface v6_tunnel** <*tunnel_no*>	创建IPv6隧道接口
2	inspur(config)#**ipv6-tunnel-config**	进入IPv6隧道模式
3	inspur(config-ipv6-tunnel)#**interface** {**byname** <*interface-byname*>|<*interface-name*>}	进入IPv6隧道接口配置模式，接口别名和接口名称最长32字符
4	inspur(config-ipv6-tunnel-if-interface-name)#**tunnel mode ipv6ip 6rd**	配置隧道模式为6RD
5	inspur(config-ipv6-tunnel-if-interface-name)#**tunnel source ipv4** <*src-addr*>	配置隧道源地址，地址格式为IPv4地址
6	inspur(config-ipv6-tunnel-if-interface-name)#**tunnel 6rd-prefix** <*ipv6-address-mask*>	配置6RD隧道的IPv6前缀，前缀长度范围为0~128
7	inspur(config-ipv6-tunnel-if-interface-name)#**tunnel 6rd-ipv4-mask-length** <*lenth*>	配置6RD隧道IPv4掩码，即为6RD隧道配置IPv4前缀长度，范围为0~32

<*tunnel_no*>：隧道号，指的是可以创建的隧道接口，个数为1~3000。

<*ipv6-address-mask*>：为6RD隧道配置IPv6前缀，其中前缀长度的范围为0~128。

<*lenth*>：为6RD隧道配置IPv4掩码长度，范围为0~32。

2.维护6RD隧道。

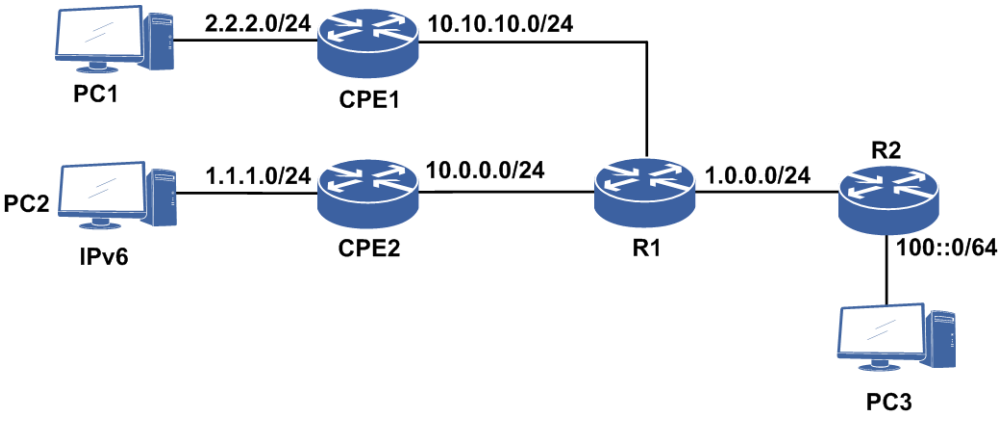
命令	功能
inspur#**debug ipv6-tunnel**	打开IPv6隧道的debug功能
inspur#**show debug ipv6-tunnel**	查看IPv6隧道debug开关是否打开

12.17.2 6RD 配置实例

配置说明

以如*图 12-38*所示组网环境为例，进行6RD的配置，其中R1和R2是IR12000智能路由器，支持做6RD BR（Border Relays）。

图 12-38 6RD 配置实例组网图



配置思路

1.CPE设备和R2之间建立6RD隧道，下面配置为CPE2与R2之间建立6RD隧道。

2.在R2上创建v6_tunnel接口，并使能IPv6功能。

3.创建v6_tunnel隧道模式为6RD，并配置相应的6RD参数。

4.在v6_tunnel接口配置符合6RD规则的域内IPv6地址。

5.R1配置v4路由，使R2与CE之间有v4路由（R1只起到v4转发的功能）。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#ip address 1.0.0.2 255.255.255.0
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#exit
R1(config)#interface gei-1/2
R1(config-if-gei-1/2)#ip address 10.0.0.1 255.255.255.0
R1(config-if-gei-1/2)#no shutdown
R1(config-if-gei-1/2)#exit
/*配置v4路由，使CPE2设备10.0.0.2地址与R2的gei-1/1接口有v4路由可达，此处省略。*/
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#ip address 1.0.0.1 255.255.255.0
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#exit
R2(config)#interface v6_tunnel1
```

```
R2(config-if-v6_tunnel1)#ipv6 enable
R2(config-if-v6_tunnel1)#ipv6 address 3000:0:100:1::1/32
R2(config-if-v6_tunnel1)#exit
R2(config)#ipv6-tunnel-config
R2(config-ipv6-tunnel)#interface v6_tunnel1
R2(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipv6ip 6RD
R2(config-ipv6-tunnel-if-v6_tunnel1)#tunnel 6RD-ipv4-mask-length 0
/*要先配置tunnel mode ipv6ip 6RD，才能配置6RD-ipv4-mask-length等，
否则会有提示信息“%Code 130024: 6RD mode needs config first!”*/
R2(config-ipv6-tunnel-if-v6_tunnel1)#tunnel 6RD-prefix 3000::1/32
R2(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv4 1.0.0.1
R2(config-ipv6-tunnel-if-v6_tunnel1)#exit
R2(config-ipv6-tunnel)#exit
/*配置到CPE2设备10.0.0.2地址的v4路由，此处省略。*/
```

配置验证

打开**debug ipv6-tunnel**功能，R2上执行ping6命令，显示如下：

```
R2#ping6 3000:0:a00:2::1
 sending 5,100-byte ICMP echo(es) to 3000:0:A00:2:0:0:0:1,timeout is 2
second(s).
R2 MPFU-8/0 2012-10-25 15:54:19 v6_tunnel1: Ipv6/Ip(6rd) packet to be
 encapsulated: 3000:0:100:1::1-->3000:0:a00:2::1 (len=100 ttl=64)

R2 MPFU-8/0 2012-10-25 15:54:19 v6_tunnel1: Ipv6/Ip(6rd) packet encapsulated:
 1.0.0.1-->10.0.0.2 (len=120 ttl=255)
```

由以上信息可知R2上解析出正确的v4目的地址。

12.18 6PE

6PE（IPv6 Provider Edge，IPv6提供商边缘）是指在启动MPLS的IPv4骨干网上传输IPv6数据包，使IPv6孤岛CE路由设备通过IPv4 PE路由设备进行通信。

6PE在实现上，是将IPv6路由通过IPv4 MPLS分配标签，再通过MP-BGP通告出去。就BGP而言，需要IPv4地址激活IPv6能力。

12.18.1 配置 6PE

本节介绍6PE的配置步骤和命令。

1.配置6PE。

步骤	命令	功能
1	inspur(config)#**router bgp** <*as-number*>	进入BGP配置模式
2	inspur(config-bgp)#**address-family ipv6**	进入IPv6的单播地址族配置模式
3	inspur(config-bgp-af-ipv6)#**neighbor** {<*ipv4-address*>|<*peer-group-name*>} **activate**	激活IPv4邻居的IPv6能力

步骤	命令	功能
4	inspur(config-bgp-af-ipv6)#**neighbor** {*<ipv4-address>*|*<peer-group-name>*} **send-label**	激活邻居的通告标签的能力

2.验证配置结果。

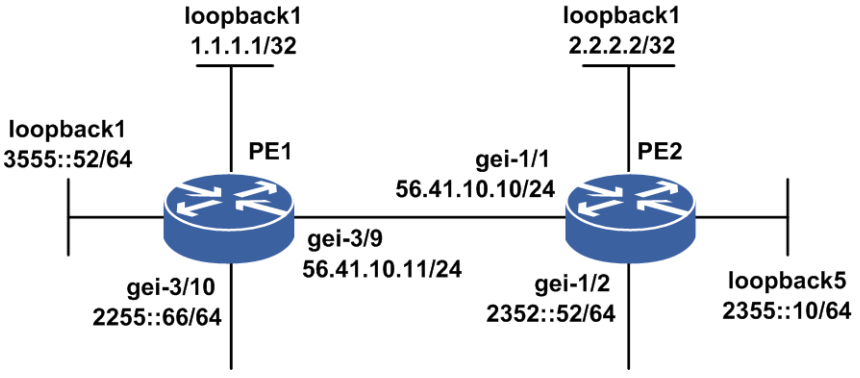
命令	功能
inspur(config)#**show bgp ipv6 unicast neighbor** *<ipv4-address>*	显示IPv6邻居的详细信息
inspur(config)#**show bgp ipv6 unicast labels**	显示IPv6地址族学到的路由分配标签的情况

12.18.2 6PE 配置实例

配置说明

如*图 12-39*所示，PE1和PE2分别配置6PE，在PE1和PE2直连接口起LDP邻居和OSPF邻居，通告各自的loopback1地址，PE1和PE2通过loopback1建立MP-BGP，通告各自的IPv6网段，并重分发直连IPv6路由。

图 12-39 6PE 配置实例拓扑图



配置思路

1.PE1和PE2直连接口配置IPv4地址，各设备分别配置回环接口，配置IPv4地址；对IPv6接口使能IPv6，配置IPv6地址，并配置回环接口，使能IPv6，配置IPv6地址。

2.PE1和PE2直连接口建立LDP邻居。

3.PE1和PE2直连接口建立OSPF邻居，通告各自的loopback1接口地址。

4.PE1和PE2通过loopback1建立MP-BGP邻居，通告各自的IPv6网段，并重分发直连IPv6路由。

5.配置完成后，测试配置结果，确认两台设备正确建立LDP、OSPF、BGP邻居，在设备上可查看到IPv6标签路由，并生成路由。

配置过程

PE1上的配置如下：

```
PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 1.1.1.1 255.255.255.255
PE1(config-if-loopback1)#exit
PE1(config)#interface gei-3/9
PE1(config-if-gei-3/9)#ip address 56.41.10.11 255.255.255.0
PE1(config-if-gei-3/9)#no shutdown
PE1(config-if-gei-3/9)#exit
PE1(config)#interface gei-3/10
PE1(config-if-gei-3/10)#ipv6 enable
PE1(config-if-gei-3/10)#ipv6 address  2255::66/64
PE1(config-if-gei-3/10)#no shutdown
PE1(config-if-gei-3/10)#exit
PE1(config)#interface loopback5
PE1(config-if-loopback5)#ipv6 enable
PE1(config-if-loopback5)#ipv6 address  3555::52/64
PE1(config-if-loopback5)#exit

PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#interface gei-3/9
PE1(config-ldp-1-if-gei-3/9)#discovery transport-address interface
PE1(config-ldp-1-if-gei-3/9)#exit
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#exit

PE1(config)#router ospf 1
PE1(config-ospf-1)#router-id 1.1.1.1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 56.41.10.0 0.0.0.255
PE1(config-ospf-1-area-0)#network 1.1.1.1 0.0.0.0
PE1(config-ospf-1-area-0)#exit

PE1(config)#router bgp 100
PE1(config-bgp)#no synchronization
PE1(config-bgp)#neighbor 2.2.2.2 remote-as 100
PE1(config-bgp)#neighbor 2.2.2.2 activate
PE1(config-bgp)#neighbor 2.2.2.2 update-source loopback1

PE1(config-bgp)#address-family ipv6
PE1(config-bgp-af-ipv6)#redistribute connected
PE1(config-bgp-af-ipv6)#neighbor 2.2.2.2 activate
PE1(config-bgp-af-ipv6)#neighbor 2.2.2.2 send-label
PE1(config-bgp-af-ipv6)#network 2255::/64
PE1(config-bgp-af-ipv6)#exit
```

PE2上的配置如下：

```
PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 2.2.2.2 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#interface gei-1/1
PE2(config-if-gei-1/1)#ip address 56.41.10.10 255.255.255.0
PE2(config-if-gei-1/1)#no shutdown
PE2(config-if-gei-1/1)#exit
PE2(config)#interface gei-1/2
PE2(config-if-gei-1/2)#ipv6 enable
PE2(config-if-gei-1/2)#ipv6 address  2352::52/64
PE2(config-if-gei-1/2)#no shutdown
PE2(config-if-gei-1/2)#exit
PE2(config)#interface loopback5
```

```
PE2(config-if-loopback5)#ipv6 enable
PE2(config-if-loopback5)#ipv6 address  2355::10/64
PE2(config-if-loopback5)#exit

PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#interface gei-1/1
PE2(config-ldp-1-if-gei-1/1)#discovery transport-address interface
PE2(config-ldp-1-if-gei-1/1)#exit
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#exit

PE2(config)#router ospf 1
PE2(config-ospf-1)#router-id 2.2.2.2
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 56.41.10.0 0.0.0.255
PE2(config-ospf-1-area-0)#network 2.2.2.2 0.0.0.0
PE2(config-ospf-1-area-0)#exit

PE2(config)#router bgp 100
PE2(config-bgp)#no synchronization
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.1 activate
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback1
PE2(config-bgp)#address-family ipv6
PE2(config-bgp-af-ipv6)#neighbor 1.1.1.1 activate
PE2(config-bgp-af-ipv6)#neighbor 1.1.1.1 send-label
PE2(config-bgp-af-ipv6)#network 2352::/64
PE2(config-bgp-af-ipv6)#redistribute connected
PE2(config-bgp-af-ipv6)#end
```

配置验证

通过命令**show running-config ospfv2**和**show running-config bgp**命令可以查看设备的OSPF和BGP的配置情况。

在PE1上查看配置：

```
PE1#show running-config ospfv2
!<ospfv2>
router ospf 1
  router-id 1.1.1.1
  area 0
  network 56.41.10.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
 $
$
!</ospfv2>

PE1#show running-config bgp
!<bgp>
router bgp 100
  synchronization disable
  neighbor 2.2.2.2 remote-as 100
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 update-source loopback1
  address-family ipv4 multicast
  $
  address-family l2vpn vpls
  $
  address-family vpnv4
  $
  address-family vpnv4 mcast
  $
  address-family vpnv4 multicast
  $
  address-family ipv6
```

```
   network 2255::/64
   redistribute connected
   neighbor 2.2.2.2 activate
   neighbor 2.2.2.2 send-label
  $
  address-family ipv6 multicast
  $
  address-family vpnv6
  $
  address-family route-target
  $
$
!</bgp>
```

通过命令**show ip ospf neighbor**可以查看设备的OSPF邻居建立情况，State项为FULL就表示邻居已经建立：

```
PE1#show ip ospf neighbor
          OSPF Router with ID (1.1.1.1) (Process ID 1)
Neighbor ID  Pri State    DeadTime  Address        Interface
2.2.2.2      1   FULL/DR  00:00:35  56.41.10.10    gei-3/9
```

查看OSPF邻居已经通告loopback1路由：

```
PE1#show ip forwarding route ospf
IPv4 Routing Table:
Dest          Gw           Interface      Owner     Pri Metric
2.2.2.2/32    56.41.10.10   gei-3/9    o        110 2
```

通过**show ip bgp summary**命令可以查看设备的BGP邻居建立情况：

```
PE1#show ip bgp summary
Neighbor   Ver  As    MsgRcvd  MsgSend  Up/Down      State/PfxRcd
2.2.2.2    4    100     32       35     00:17:00          0
```

可以查看BGP邻居通告的IPv6路由：

```
PE1(config-bgp-af)#show ipv6 forwarding route bgp
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
        D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
        S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                      Owner  Metric
  Interface        Pri     Gw
2352::/64                                  B      0
  gei-3/9       200     ::ffff:2.2.2.2
2355::/64                                  B      0
  gei-3/9       200     ::ffff:2.2.2.2
```

查看IPv6路由的标签：

```
PE1#show bgp ipv6 unicast labels
Network         Next Hop            In Label/Out Label
2255::/64        2255::66           212997/notag
2352::/64        ::ffff:2.2.2.2      213031/212998
2355::/64        ::ffff:2.2.2.2      213024/212999
3555::/64        3555::52           213020/notag
```

同样在PE2上的查看配置情况：

```
PE2#show running-config ospfv2
!<ospfv2>
router ospf 1
  router-id 2.2.2.2
 area 0
  network 56.41.10.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
 $
$
!</ospfv2>
PE2#show running-config bgp
```

```
!</bgp>
  router bgp 100
  synchronization disable
  neighbor 1.1.1.1 remote-as 100
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 update-source loopback1
  address-family ipv4 multicast
  $
  address-family l2vpn vpls

  $
  address-family vpnv4
  $
  address-family vpnv4 mcast
  $
  address-family vpnv4 multicast
  $
  address-family ipv6
    network 2352::/64
    redistribute connected
    neighbor 1.1.1.1 activate
    neighbor 1.1.1.1 send-label
  $
  address-family ipv6 multicast
  $
  address-family vpnv6
  $
  address-family route-target
  $
$
!<bgp>

PE2#show ip ospf neighbor
          OSPF Router with ID (56.41.41.10) (Process ID 1)

Neighbor ID  Pri State     DeadTime  Address        Interface
1.1.1.1      1  FULL/BDR  00:00:35  56.41.10.11    gei-1/1

PE2#show ip forwarding route ospf
IPv4 Routing Table:
Dest          Gw          Interface       Owner    Pri Metric
1.1.1.1/32   56.41.10.11    gei-1/1      o       110 2

PE2#show ip bgp summary
Neighbor  Ver   As   MsgRcvd   MsgSend   Up/Down       State/PfxRcd
1.1.1.1   4    100     31      30      00:15:51          0

PE2(config-bgp-af)#show ipv6 forwarding route bgp
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
        D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
        S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                    Owner  Metric
 Interface        Pri     Gw
2255::/64                                B      0
  gei-1/1         200     ::ffff:2.2.2.2
3555::/64                                B      0
  gei-1/1         200     ::ffff:2.2.2.2

PE2#show bgp ipv6 unicast labels
Network         Next Hop          In Label/Out Label
2255::/64       ::ffff:1.1.1.1     212994/212997
2352::/64       2352::52          212998/notag
2355::/64       2355::10          212999/notag
3555::/64       ::ffff:1.1.1.1     213027/213020
```

12.19 6VPE

6VPE（IPv6 VPN Provider Edge）是一种为IPv6用户网络提供BGP MPLS VPN服务的技术。其技术原理和实现方式与MPLS L3VPN相似，6VPE使用了双栈技术，在用户网络（CE所在子网）采用的地址族可以是IPv4也可以是IPv6，骨干网可以是IPv4网络也可以是IPv6网络。

6VPE是对IPv4 BGP MPLS VPN的一种扩展，采用6VPE技术不会危及服务提供商现有的IPv4骨干网和用户网络，对于IPv4 VPN用户来说，IPv6 VPN服务和IPv4的MPLS VPN一样。

12.19.1 配置 6VPE

在MPLS VPN网络中的PE和CE设备上配置6VPE功能，为IPv6用户提供VPN服务。

1.在PE设备上创建VRF并激活IPv6地址簇。

步骤	命令	功能
1	inspur(config)#**ip vrf** < *vrf-name*>	配置一个VPN实例
2	inspur(config-vrf-vrf-name)#**rd** <*route-distinguisher*>	定义VRF的路由标识符，有三种格式： ▸<0-65535>:<0-4294967295> ▸<1-65535>.<0-65535>:<0-65535> ▸A.B.C.D:<0-65535>
3	inspur(config-vrf-vrf-name)#**address-family ipv6**	激活IPv6地址族
4	inspur(config-vrf-vrf-name-af-ipv6)#**route-target** [**import**|**export** | **both**]<*extended-community*>	创建IPv6地址族下与VRF关联的route-target扩展团体属性

import：根据route-target扩展团体属性导入路由到VRF。

export：导出VRF路由携带route-target扩展团体属性。

both：等同于同时配置import和export。

<*extended-community*>：route-target扩展团体属性，有三种格式：<0~65535>:<0~4294967295> 或 A.B.C.D:<0~65535> 或 <1-65535>.<0-65535>:<0-65535>。

2.配置接口关联VRF并配置接口IPv6地址。

步骤	命令	功能
1	inspur(config)#**interface** <*interface-name*>	进入接口配置模式

步骤	命令	功能
2	inspur(config-if-interface-name)#**ip vrf forwarding** <*vrf-name*>	将接口与VRF关联，如果该接口预先配置了IP地址，必须删除已经配置的IP地址，重新配置该命令
3	inspur(config-if-interface-name)#**ipv6 enable**	接口上启用IPv6功能
4	inspur(config-if-interface-name)#**ipv6 address** {**X:X::X:X/**<*1-128*>[**anycast** | **eui-64**]| **link-local** <*X:X::X:X*>}	配置IPv6接口地址 **anycast**，任播地址 **eui-64**，eui64前缀地址

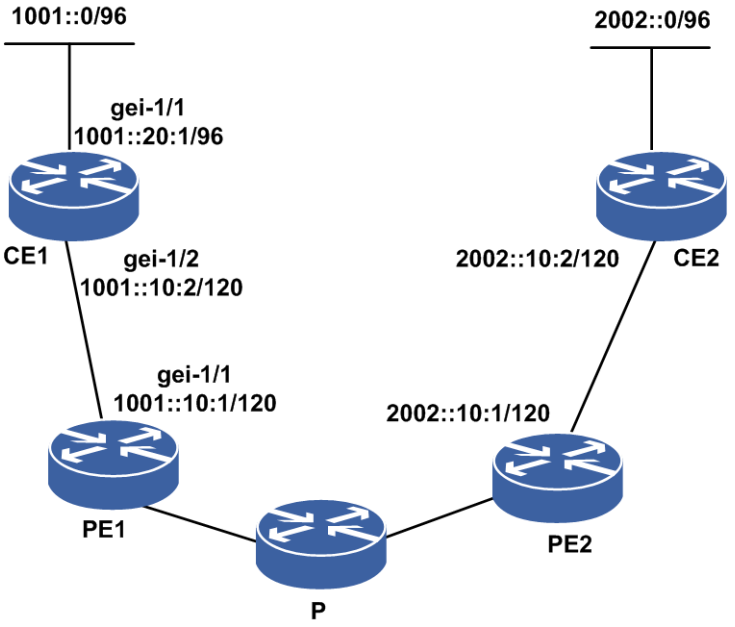
3.在PE与CE上配置IPv6静态路由。

在CE与PE之间运行IPv6静态路由时，需要在PE上配置一条到CE的IPv6静态路由，并将该静态路由分发到BGP中。

步骤	命令	功能
1	inspur(config)#**ipv6 route vrf**< *vrf-name*>< *prefix of destination ipaddress*>< *network mask*>< *next hop address*>	在PE上配置一条到CE的静态路由，在配置时，需要指定该静态路由所属的VRF
2	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
3	inspur(config-bgp)#**address-family ipv6 vrf** <*vrf-name*>	进入相应VRF的地址族配置模式
4	inspur(config-bgp-af-ipv6-vrf)#**redistribute static** [**metric** <*metric-value*>],[**route-map** <*map-tag*>]	重分发静态路由

配置CE与PE之间IPv6静态路由协议举例如下。如*图 12-40*所示，在CE1和PE1之间运行静态路由，需要分别在CE1和PE1上配置静态路由。

图 12-40 CE 与 PE 之间运行 IPv6 静态路由协议拓扑图



CE1上的配置：

```
CE1(config)#interface gei-1/1
CE1(config-if-gei-1/1)#ipv6 enable
CE1(config-if-gei-1/1)#ipv6 address 1001::20:1/96
CE1(config-if-gei-1/1)#exit
CE1(config)#interface gei-1/2
CE1(config-if-gei-1/2)#ipv6 enable
CE1(config-if-gei-1/2)#ipv6 address 1001::10:2/120
CE1(config-if-gei-1/2)#exit
CE1(config)#ipv6 route 2002::0/96 1001::10:1
```

PE1上的配置：

```
PE1(config)#ipv6 route vrf vpn_a 1001::0/96 1001::10:2
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6 vrf vpn_a
PE1(config-bgp-af-ipv6-vrf)#redistribute static
PE1(config-bgp-af-ipv6-vrf)#exit
```

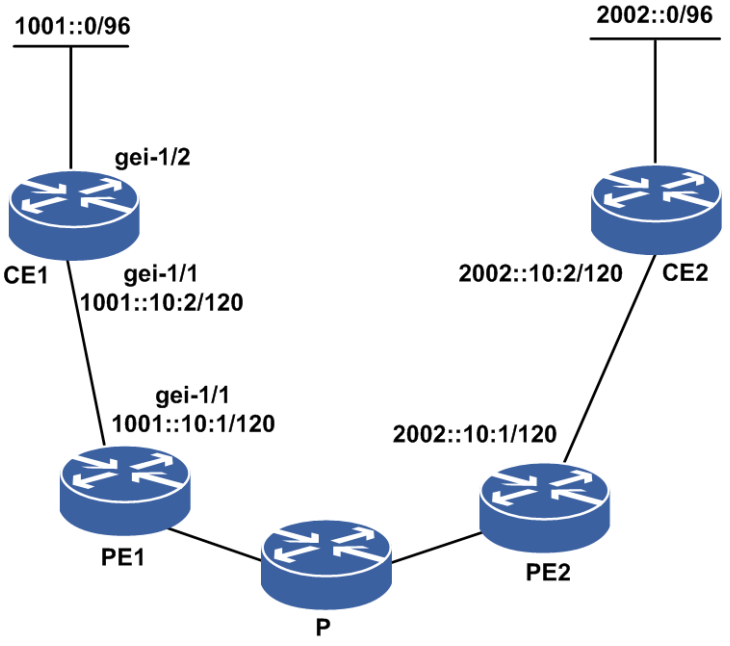
4.在PE与CE上配置RIPng协议。

步骤	命令	功能
1	inspur(config)#**ipv6 router rip vrf** <*vrf-name*>	启动并进入RIPng配置模式
2	inspur(config-ripng-vrf-vrf-name)#**redistribute bgp** [**metric** <*metric-value*>],[**route-map** <*map-tag*>]	重分发BGP到RIP中
3	inspur(config-ripng-vrf-vrf-name)#**interface** <*interface-name*>	进入RIPng接口模式，此接口为绑定VRF的接口
	inspur(config-ripng-vrf-vrf-name)#**ipv6 rip enable**	在接口上使能RIPng
4	inspur(config)#**router bgp** <*as-number*>	进入BGP路由配置模式
5	inspur(config-bgp)#**address-family ipv6 vrf**	进入相应VRF的地址族配置

步骤	命令	功能
	< *vrf- name*>	模式
	inspur(config-bgp-af-ipv6-vrf)#**redistribute rip** [**metric** <*metric-value*>],[**route-map** <*map-tag*>]	重分发RIP路由

配置CE与PE之间运行RIPng协议举例如下。如*图 12-41*所示，在CE1和PE1之间运行RIPng协议，需要在CE1和PE1上分别启用RIPng协议，互相分发路由信息。

图 12-41 CE 和 PE 之间运行 RIPng 协议拓扑图



CE1上的配置如下：

```
CE1(config)#ipv6 router rip
CE1(config-ripng)#interface gei-1/1
CE1(config-ripng-if-gei-1/1)#ipv6 rip enable
CE1(config-ripng-if-gei-1/1)#exit
```

PE1上的配置如下：

```
PE1(config)#ipv6 router rip vrf vpn_a
PE1(config-ripng-vrf-vpn_a)#redistribute bgp
PE1(config-ripng-vrf-vpn_a)#interface gei-1/1
PE1(config-ripng-vrf-vpn_a-if-gei-1/1)#ipv6 rip enable
PE1(config-ripng-vrf-vpn_a-if-gei-1/1)#exit
PE1(config-ripng-vrf-vpn_a)#exit

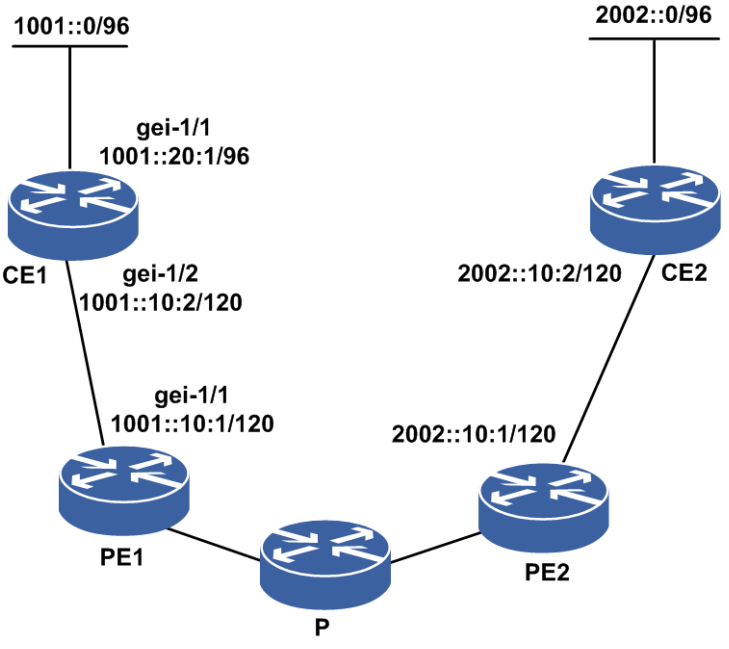
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6 vrf vpn_a
PE1(config-bgp-af-ipv6-vrf)#redistribute rip
PE1(config-bgp-af-ipv6-vrf)#redistribute connected
PE1(config-bgp-af-ipv6-vrf)#exit
```

5.在PE与CE上配置OSPFv3协议。

步骤	命令	功能
1	inspur(config)#**ipv6 router ospf** <*process-id*>[**vrf** < *vrf-name*>]	启动并进入OSPF VRF配置模式
	inspur(config-ospfv3-process-id)#**router-id** <*router-id*>	配置OSPFv3的Router-ID
	inspur(config-ospfv3-process-id)#**area** <*area-id*>	配置OSPFv3的区域
	inspur(config-ospfv3-process-id-area-id)#**interface** <*interface-name*>[**instance** <*instance-id*>]	定义OSPFv3协议运行的接口
2	inspur(config-ospfv3-process-id)#**redistribute bgp** [{[**tag** <*tag-value*>],[**metric** <*metric-value*>],[**metric-type** {**ext-2**	**ext-1**}],[**route-map** <*routemap*>]}]	重分发BGP路由
3	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
4	inspur(config-bgp)#**address-family ipv6 vrf** < *vrf-name*>	进入相应VRF的地址簇配置模式
5	inspur(config-bgp-af-ipv6-vrf)#**redistribute** {**ospf-int**	**ospf-ext**}<*process-id*>[**metric** <*metric-value*>],[**route-map** <*map-tag*>]	重分发OSPFv3路由

CE与PE之间运行OSPFv3协议举例如下。如*图 12-42*所示，在CE1和PE1上分别启用OSPFv3协议，互相分发路由信息。

图 12-42 CE 与 PE 之间运行 OSPFv3 协议拓扑图



CE1上的配置如下：

```
CE1(config)#ipv6 router ospf 1
CE1(config-ospfv3-1)#router-id 1.1.1.1
```

```
CE1(config-ospfv3-1)#area 0
CE1(config-ospfv3-1-area-0)#interface gei-1/1
```

PE1上的配置如下：

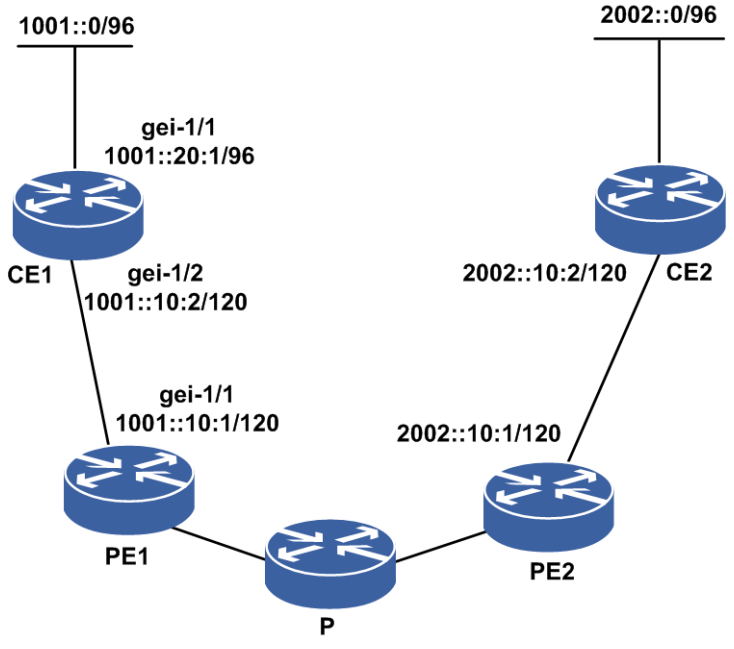
```
PE1(config)#ipv6 router ospf 2 vrf vpn_a
PE1(config-ospfv3-2)#router-id 2.2.2.2
PE1(config-ospfv3-2)#area 0
PE1(config-ospfv3-2-area-0)#interface gei-1/1
PE1(config-ospfv3-2-area-0-if-gei-1/1)#exit
PE1(config-ospfv3-2-area-0)#exit
PE1(config-ospfv3-2)#redistribute bgp
PE1(config-ospfv3-2)#exit
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6 vrf vpn_a
PE1(config-bgp-af-ipv6-vrf)#redistribute ospf-int 2
PE1(config-bgp-af-ipv6-vrf)#redistribute connected
PE1(config-bgp-af-ipv6-vrf)#exit
```

6.在PE与CE上配置EBGP协议。

步骤	命令	功能
1	inspur(config)#**router bgp** < *as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**address-family ipv6 vrf** < *vrf-name*>	进入相应VRF的地址族配置模式
3	inspur(config-bgp-af-ipv6-vrf)#**neighbor** < *ipv6-address*> **remote-as** <*as-number*>	配置一个EBGP邻居或配置一个邻居对等体组的自治系统号

配置CE与PE之间运行EBGP协议举例如下。如*图 12-43*所示，在CE1和PE1之间运行EBGP协议，需要分别在CE1和PE1上配置BGP协议，互相分发路由信息。

图 12-43 CE 和 PE 之间运行 EBGP 协议拓扑图



CE1上的配置：

```
CE1(config)#router bgp 65001
```

```
CE1(config-bgp)#neighbor 1001::10:1 remote-as 100
CE1(config-bgp)#neighbor 1001::10:1 activate
CE1(config-bgp)#redistribute connected
CE1(config-bgp)#exit
```

PE1上的配置：

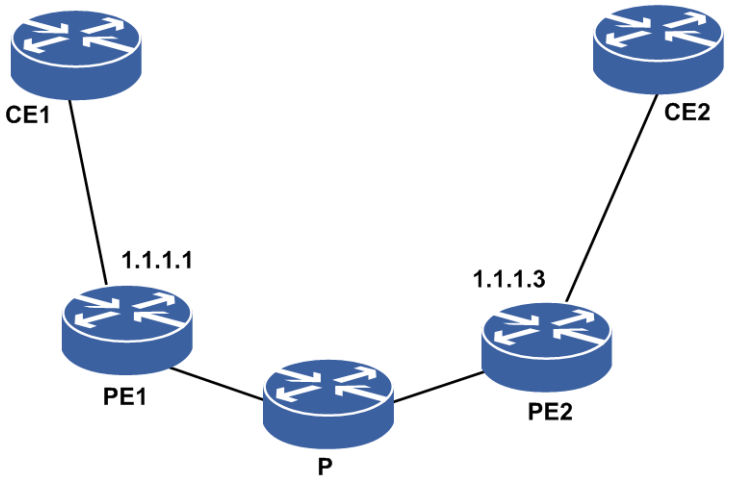
```
PE1(config)#router bgp 100
PE1(config-bgp)#address-family ipv6 vrf vpn_a
PE1(config-bgp-af-ipv6-vrf)#neighbor 1001::10:2 remote-as 65001
PE1(config-bgp-af-ipv6-vrf)#neighbor 1001::10:2 activate
PE1(config-bgp-af-ipv6-vrf)#redistribute connected
PE1(config-bgp-af-ipv6-vrf)#exit
```

7.在PE1与PE2上配置MPBGP协议。

步骤	命令	功能
1	inspur(config)#**router bgp** <*as-number*>	进入BGP路由配置模式
2	inspur(config-bgp)#**neighbor** {<*ipv4-address*>|<*peer-group-name*>} **remote-as** <*as-number*>	配置BGP邻居
3	inspur(config-bgp)#**neighbor** {<*ipv4-address*>|<*peer-group-name*>} **update-source** <*interface-name*>	指定路由更新的源地址为自己的MPBGP建链使用的接口地址
4	inspur(config-bgp)#**address-family vpnv6**	进入VPNv6地址族配置模式
5	inspur(config-bgp-af-vpnv6)#**neighbor** {<*ipv4-address*>|<*peer-group-name*>} **activate**	激活邻居的VPNv6功能

在PE1与PE2上配置MPBGP协议，如*图 12-44*所示，在PE1和PE2之间运行MPBGP协议。

图 12-44 MPBGP 协议配置拓扑图



配置前，需要确保PE1和PE2的loopback地址能够相互ping通。

PE1上的配置如下：

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 1.1.1.3 remote-as 100
PE1(config-bgp)#neighbor 1.1.1.3 activate
PE1(config-bgp)#neighbor 1.1.1.3 update-source loopback1
```

```
PE1(config-bgp)#address-family vpnv6
PE1(config-bgp-af-vpnv6)#neighbor 1.1.1.3 activate
PE1(config-bgp-af-vpnv6)#exit
```

PE2上的配置如下：

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.1 activate
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback1
PE2(config-bgp)#address-family vpnv6
PE2(config-bgp-af-vpnv6)#neighbor 1.1.1.1 activate
PE2(config-bgp-af-vpnv6)#exit
```

8.配置AS覆盖功能。

当PE和CE之间运行BGP时，有时在不同的站点内需要重用AS号。为了提供CE1和CE2之间的连通性，可以实施一种叫AS覆盖的新方法。当在PE上配置了AS覆盖后，PE在向CE发送路由更新之前，会把整个AS_PATH中每一个直连的CE设备AS号替换成自己的AS号，但保留AS_PATH的长度。

步骤	命令	功能
1	inspur(config)#**router bgp** *<as-number>*	进入BGP路由配置模式
2	inspur(config-bgp)#**address-family ipv6 vrf** *<vrf-name>*	进入IPv6 VRF地址簇配置模式
3	inspur(config-bgp-af-ipv6-vrf)#**neighbor** *<neighbor-address>* **as-override**	把整个AS_PATH中每一个直连的CE设备AS号替换成自己的AS号

9.配置Export Map和Import Map。

Export Map和Import Map的含义如下：

- Import Map：通过对导入VRF的路由进行**import map**过滤，使VRF中可以只存储自己关心的路由前缀。
- Export Map：通过**export map**给路由前缀设置不同的RT值，使不同的VRF可以选择接受不同RT的前缀。

步骤	命令	功能
1	inspur(config)#**ip vrf** *<vrf-name>*	配置一个VPN实例，并进入VPN实例配置模式
2	inspur(config-vrf-vrf-name)#**address-family ipv6**	激活IPv6地址族
3	inspur(config-vrf-vrf-name-af-ipv6)#**export map** *< route-map-name>*	配置与VRF关联的导出路由映射，路由映射名称长度为1~31个字符
	inspur(config-vrf-vrf-name-af-ipv6)#**import map** *< route-map-name>*	配置与VRF关联的导入路由映射，路由映射名称长度为1~31个字符

10.验证配置结果。

命令	功能
inspur#**ping6** [**vrf** <*vrf-name*>]{<*ipv6-address*>| **domain** <*domain-name*>}{[**limit** {**0** |<*limit-num*>}], [**repeat** <*repeat-count*>],[**size** <*datagram-size*>],[**timeout** <*timeout*>],[**interface** <*interface-name*>],[**source** <*source-address*>]}	检查网络连通性
inspur#**show ip vrf** [[[**brief** | **detail**][< *vrf-name*>]]| **summary**]	查看VRF的信息
inspur#**show ipv6 protocol routing vrf** <*vrf-name*>[[**network** <*ipv6-address*>[**/**<*mask_len*>]]|<*protocol*>| **database**]	查看VRF路由表

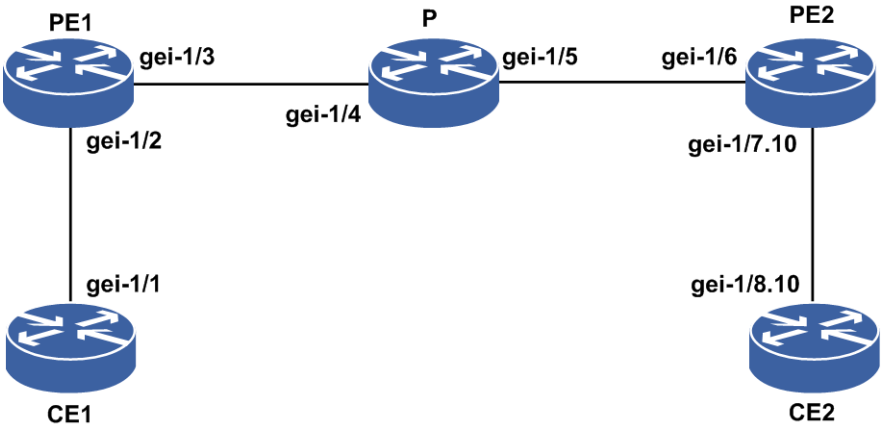
12.19.2 6VPE 配置实例

配置说明

如*图 12-45*所示，CE1和CE2在同一个VPN中，CE1的loopback为1001::10:1/112，CE2的loopback地址为2002::10:1/112。

要求进行适当的VPN配置，通过路由协议OSPFv3，使得CE1和CE2能够互相学习到对端的网络路由。CE1与PE1之间运行BGP协议，CE2与PE2之间运行OSPFv3协议，使得CE1与CE2能够互相学到对方的路由，可以ping通。

图 12-45 6VPE 配置实例拓扑图



6VPE配置实例中各个接口的地址规划如表*表 12-1*所示。

表 12-1 6VPE 配置实例地址规划表

设备	接口名	IP地址
CE1	gei-1/1	1001::20:2/120
PE1	gei-1/2	1001::20:1/120
	gei-1/3	10.10.12.1/24

设备	接口名	IP地址
P	gei-1/4	10.10.12.2/24
	gei-1/5	10.10.23.2/24
PE2	gei-1/6	10.10.23.3/24
	gei-1/7.10	2002::20:2/120
CE2	gei-1/8.10	2002::20:1/120

配置思路

1.在CE1上配置loopback1接口，与PE1建立激活IPv6能力的EBGP邻居，并将loopback1接口在BGP中通告。

2.在PE1上配置loopback1、gei-1/3的IP地址，配置vrf test1，将gei-1/2绑定在vrf test1中并配置IP地址。PE1上要配置OSPF，通告10.10.0.0/16这个网段；与PE2起MPBGP邻居，并使能VPNv6的能力；与CE1建立EBGP邻居，另外接口gei-1/3起LDP。

3.在P上配置gei-1/4和gei-1/5的IP地址；并配置OSPF，通告10.10.0.0/16这个网段，同时接口gei-1/4和gei-1/5起LDP协议。

4.在PE2上配置loopback1、gei-1/6的地址，配置vrf test1，将gei-1/7.10绑定在vrf test1中并配置IP地址。PE2上要配置OSPF，通告10.10.0.0/16这个网段；与PE1起MPBGP邻居，并使能VPNv6的能力；与CE2建立OSPF邻居，接口gei-1/6起LDP协议。

5.在CE2上配置loopback1和子接口gei-1/8.10的IP地址，配置OSPF，并在OSPF中通告IP地址。

配置过程

CE1上的配置如下：

```
CE1(config)#interface loopback1
CE1(config-if-loopback1)#ipv6 enable
CE1(config-if-loopback1)#ipv6 address 1001::10:1/112
CE1(config-if-loopback1)#exit
CE1(config)#interface gei-1/1
CE1(config-if-gei-1/1)#ipv6 enable
CE1(config-if-gei-1/1)#ipv6 address 1001::20:2/120
CE1(config-if-gei-1/1)#no shutdown
CE1(config-if-gei-1/1)#exit

CE1(config)#router bgp 200
CE1(config-bgp)#neighbor 1001::20:1 remote-as 100
CE1(config-bgp)#address-family ipv6
CE1(config-bgp-af-ipv6)#neighbor 1001::20:1 activate
CE1(config-bgp-af-ipv6)#exit
```

PE1上的配置如下：

```
PE1(config)#ip vrf test1
PE1(config-vrf-test1)#rd 100:1
PE1(config-vrf-test1)#address-family ipv6
PE1(config-vrf-test1-af-ipv6)#route-target import 100:1
PE1(config-vrf-test1-af-ipv6)#route-target export 100:1
PE1(config-vrf-test1-af-ipv6)#exit
```

```
PE1(config-vrf-test1)#exit

PE1(config)#interface loopback1
PE1(config-if-loopback1)#ip address 10.10.1.1 255.255.255.255
PE1(config-if-loopback1)#exit
PE1(config)#interface gei-1/3
PE1(config-if-gei-1/3)#ip address 10.10.12.1 255.255.255.0
PE1(config-if-gei-1/3)#no shutdown
PE1(config-if-gei-1/3)#exit

PE1(config)#mpls ldp instance 1
PE1(config-ldp-1)#router-id loopback1
PE1(config-ldp-1)#interface gei-1/3
PE1(config-ldp-1-if-gei-1/3)#exit
PE1(config-ldp-1)#exit

PE1(config)#interface gei-1/2
PE1(config-if-gei-1/2)#ip vrf forwarding test1
PE1(config-if-gei-1/2)#ipv6 enable
PE1(config-if-gei-1/2)#ipv6 address 1001::20:1/120
PE1(config-if-gei-1/2)#no shutdown
PE1(config-if-gei-1/2)#exit

PE1(config)#router ospf 1
PE1(config-ospf-1)#area 0
PE1(config-ospf-1-area-0)#network 10.10.0.0 0.0.255.255
PE1(config-ospf-1-area-0)#exit

PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 10.10.3.3 remote-as 100
PE1(config-bgp)#neighbor 10.10.3.3 update-source loopback1
PE1(config-bgp)#address-family ipv6 vrf test1
PE1(config-bgp-af-ipv6-vrf)#redistribute connected
PE1(config-bgp-af-ipv6-vrf)#neighbor 1001::20:2 remote-as 200
PE1(config-bgp-af-ipv6-vrf)#exit
PE1(config-bgp)#address-family vpnv6
PE1(config-bgp-af-vpnv6)#neighbor 10.10.3.3 activate
PE1(config-bgp-af-vpnv6)#exit
PE1(config-bgp)#exit
```

P上的配置如下：

```
P(config)#interface gei-1/4
P(config-if-gei-1/4)#ip address 10.10.12.2 255.255.255.0
P(config-if-gei-1/4)#no shutdown
P(config-if-gei-1/4)#exit

P(config)#interface gei-1/5
P(config-if-gei-1/5)#ip address 10.10.23.2 255.255.255.0
P(config-if-gei-1/4)#no shutdown
P(config-if-gei-1/5)#exit

P(config)#interface loopback1
P(config-if-loopback1)#ip address 10.10.2.2 255.255.255.255
P(config-if-loopback1)#exit

P(config)#router ospf 1
P(config-ospf-1)#area 0
P(config-ospf-1-area-0)#network 10.10.0.0 0.0.255.255
P(config-ospf-1-area-0)#exit

P(config)#mpls ldp instance 1
P(config-ldp-1)#router-id loopback1
P(config-ldp-1)#interface gei-1/4
P(config-ldp-1-if-gei-1/4)#exit
P(config-ldp-1)#interface gei-1/5
P(config-ldp-1-if-gei-1/5)#exit
P(config-ldp-1)#exit
```

PE2上的配置（这里使用了以太网子接口与CE2连接）：

```
PE2(config)#ip vrf test1
PE2(config-vrf-test1)#rd 100:1
PE2(config-vrf-test1)#address-family ipv6
PE2(config-vrf-test1-af-ipv6)#route-target import 100:1
PE2(config-vrf-test1-af-ipv6)#route-target export 100:1
PE2(config-vrf-test1-af-ipv6)#exit
PE2(config-vrf-test1)#exit

PE2(config)#interface loopback1
PE2(config-if-loopback1)#ip address 10.10.3.3 255.255.255.255
PE2(config-if-loopback1)#exit
PE2(config)#interface gei-1/6
PE2(config-if-gei-1/6)#ip address 10.10.23.3 255.255.255.0
PE2(config-if-gei-1/6)#no shutdown
PE2(config-if-gei-1/6)#exit

PE2(config)#interface gei-1/7.10
PE2(config-if-gei-1/7.10)#exit
PE2(config)#vlan-configuration
PE2(config-vlan)#interface gei-1/7.10
PE2(config-vlan-if-gei-1/7.10)#encapsulation-dot1q 10
PE2(config-vlan-if-gei-1/7.10)#exit
PE2(config-vlan)#exit

PE2(config)#interface gei-1/7.10
PE2(config-if-gei-1/7.10)#ip vrf forwarding test1
PE2(config-if-gei-1/7.10)#ipv6 enable
PE2(config-if-gei-1/7.10)#ipv6 address 2002::20:2/120
PE2(config-if-gei-1/7.10)#exit

PE2(config)#router ospf 1
PE2(config-ospf-1)#area 0
PE2(config-ospf-1-area-0)#network 10.10.0.0 0.0.255.255
PE2(config-ospf-1-area-0)#exit

PE2(config)#ipv6 router ospf 2 vrf test1
PE2(config-ospfv3-2)#router-id 2.2.2.2
PE2(config-ospfv3-2)#area 0
PE2(config-ospfv3-2-area-0)#interface gei-1/7.10
PE2(config-ospfv3-2-area-0-if-gei-1/7.10)#exit

PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 10.10.1.1 remote-as 100
PE2(config-bgp)#neighbor 10.10.1.1 update-source loopback1
PE2(config-bgp)#address-family ipv6 vrf test1
PE2(config-bgp-af-ipv6-vrf)#redistribute ospf-int 1
PE2(config-bgp-af-ipv6-vrf)#redistribute connected
PE2(config-bgp-af-ipv6-vrf)#exit
PE2(config-bgp)#address-family vpnv6
PE2(config-bgp-af-vpnv6)#neighbor 10.10.1.1 activate
PE2(config-bgp-af-vpnv6)#exit
PE2(config-bgp)#exit

PE2(config)#mpls ldp instance 1
PE2(config-ldp-1)#router-id loopback1
PE2(config-ldp-1)#interface gei-1/6
PE2(config-ldp-1-if-gei-1/6)#exit
PE2(config-ldp-1)#exit
```

CE2上的配置如下：

```
CE2(config)#interface loopback1
CE2(config-if-loopback1)#ipv6 enable
CE2(config-if-loopback1)#ipv6 address 2002::10:1/112
CE2(config-if-loopback1)#exit
CE2(config)#interface gei-1/8.10
CE2(config-if-gei-1/8.10)#exit

CE2(config)#vlan-configuration
CE2(config-vlan)#interface gei-2/8.10
```

```
CE2(config-vlan-if-gei-2/8.10)#encapsulation-dot1q 10
CE2(config-vlan-if-gei-2/8.10)#exit
CE2(config-vlan)#exit

CE2(config)#interface gei-2/8.10
CE2(config-if-gei-2/8.10)#ipv6 enable
CE2(config-if-gei-2/8.10)#ipv6 address 2002::20:1/120
CE2(config-if-gei-2/8.10)#no shutdown
CE2(config-if-gei-2/8.10)#exit

CE2(config)#ipv6 router ospf 3
CE2(config-ospfv3-3)#router-id 3.3.3.3
CE2(config-ospfv3-3)#area 0
CE2(config-ospfv3-3-area-0)#interface gei-1/8.10
CE2(config-ospfv3-3-area-0-if-gei-1/8.10)#end
```

配置验证

可以查看PE1的BGP邻居建立情况：

```
PE1#show bgp vpnv6 unicast summary
Neighbor     Ver    As     MsgRcvd  MsgSend   Up/Down   State/PfxRcd
10.10.3.3    4      100    29       112       03:38:29     1
```

可以查看BGP邻居通告的IPv6路由：

```
PE1#show ipv6 forwarding route vrf test1 bgp
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                Owner Metric
  Interface    Pri   Gw
2002::20:0/120                        B     0
  gei-1/3  200   ::ffff:10.10.3.3
```

查看IPv6路由的标签：

```
PE1#show bgp vpnv6 unicast labels
Network         Next Hop          In Label/Out Label
Route Distinguisher: 666:666 (default for vrf test1)
2002::20:0/120  ::ffff:10.10.3.3   212994/212997
1001::20:0/120  1001::20:1         212999/notag
```

可ping通对端设备的IPv6地址：

```
PE1#ping6 vrf test1 2002::20:2
sending 5,100-byte ICMP echoes to 2002::20:2,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 0/0/0 ms.
```

同样的PE2上也可以进行以下验证：

```
PE2#show bgp vpnv6 unicast summary
Neighbor     Ver    As     MsgRcvd  MsgSend   Up/Down    State/PfxRcd
10.10.1.1    4      100    27       109       03:35:22     1

PE2#show ipv6 forwarding route vrf test1 bgp
IPv6 Routing Table:
Headers: Dest: Destination, Gw: Gateway, Pri: Priority;
Codes  : K: kernel, I1: isis-l1, SFN: sf-nat64, R: ripng, AF: aftr, B: bgp,
         D: direct, I2: isis-l2, SLN: sl-nat64, O: ospfv3, D6: dhcp, P: ppp,
         S: static, N: nd, V: vrrp, A: address, M: multicast, UI: user-ipaddr;
Dest                                Owner Metric
  Interface    Pri   Gw
1001::20:0/120                        B     0
  gei-1/6  200   ::ffff:10.10.1.1
```

```
PE2#show bgp vpnv6 unicast labels
Network        Next Hop          In Label/Out Label
Route Distinguisher: 100:1  (default for vrf test1)
1001::20:0/120  ::ffff:10.10.1.1   212997/212999
2002::20:0/120  2002::20:2        212997/notag

PE2#ping6 vrf test1 1001::20:1
sending 5,100-byte ICMP echoes to 1001::20:1,timeout is 2 seconds.
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max= 0/0/0 ms.
```

12.20 IPv6 ACL

ACL是一种对流量进行分类的策略，使用该策略可以实现诸如port-ACL、URPF、策略路由等功能。

IPv6 ACL主要依据IPv6报文中的字段对报文进行筛选过滤。

一张IPv6 ACL列表可以有多条规则，每条规则都描述了一定的匹配条件，对于给定的报文，从第一条规则开始顺序匹配，一旦匹配则返回规则内的设定的动作（permit/deny）。

IPv6 ACL原理同IPv4 ACL。

12.20.1 配置 IPv6 ACL

本节介绍IPv6 ACL规则策略的配置步骤和配置命令。

1.进入IPv6 ACL配置模式，配置IPv6 ACL规则。

步骤	命令	功能
1	inspur(config)#**ipv6-access-list** <*acl-name*>	配置IPv6 ACL列表，进入IPv6 ACL配置模式
2	inspur(config-ipv6-acl)#**rule** [<*rule-id*>]{**permit** | **deny**}[**flowlabel** <*flowlabel-value*>]{<*0-255*>| **ipv6** |<*protocol-type*>}{[<*source-ipv6-address*>| **any**}{<*destination-ipv6-address*>| **any**}[**dscp** <*dscp-value*>][{[**routing**],[**authen**],[**destopts**],[**fragments**],[**hop-by-hop**],[**esp**]}][**time-range** <*time-range-name*>]	配置扩展的IPv6 ACL规则
	inspur(config-ipv6-acl)#**rule** [<*rule-id*>]{**permit**|**deny**}[**flowlabel** <*flowlabel-value*>] **tcp** {<*source-ipv6-address*>| **any**}[{<*operator*>{<*0-65535*>|<*source-porttype*>}| **range** <*0-65535*>**-**<*0-65535*>}]{<*destination-ipv6-address*>| **any**}[{<*operator*>{<*0-65535*>|<*destination-porttype*>}| **range** <*0-65535*>**-**<*0-65535*>}][{[**established**],[**rst**<*rst*>],[**ack**<*ack*>],[**fin**<*fin*>],[**syn**<*syn*>],[**urg**<*urg*>],[**psh**<*psh*>]}][**dscp**<*dscp-value*>][{[**routing**],[**authen**],[**de**	配置基于TCP协议的IPv6 ACL规则

步骤	命令	功能
	stopts],[**fragments**],[**hop-by-hop**],[**esp**]}][**time-range** <*time-range-name*>]	
	inspur(config-ipv6-acl)#**rule** [<*rule-id*>]{**permit** | **deny**}[**flowlabel** <*flowlabel-value*>] **udp** {<*source-ipv6-address*>| **any**}[<*oper*><*source-port*>]{<*destination-ipv6-address*>| **any**}[<*oper*><*destination-port*>][**dscp** <*dscp-value*>][{[**routing**],[**authen**],[**destopts**],[**fragments**],[**hop-by-hop**],[**esp**]}][**time-range** <*time-range-name*>]	配置基于UDP协议的IPv6 ACL规则
	inspur(config-ipv6-acl)#**rule** [<*rule-id*>]{**permit** | **deny**}[**flowlabel** <*flowlabel-value*>] **icmp** {<*source-ipv6-address*>| **any**}{<*destination-ipv6-address*>| **any**}[{<*icmp-type*>|<*icmp-type-value*>}[<*icmp-code*>]][**dscp** <*dscp-value*>][{[**routing**],[**authen**],[**destopts**],[**fragments**],[**hop-by-hop**],[**esp**]}][**time-range** <*time-range-name*>]	配置基于ICMP协议的IPv6 ACL规则
3	inspur(config)#**resequence-access-list ipv6** <*acl-name*>[<*base*>[<*increment*>]]	对指定ACL列表的规则进行重新编号

<*rule-id*>：规则在IPv6 ACL表中的唯一标识，该ID决定了规则在表中的顺序，范围：1~2147483644。如不指定rule-id，系统默认插入表的末位，并按默认base（基值）和increment（步进）来分配rule-id。

<*0-255*>| **ipv6** |<*protocol-type*>：要匹配的协议类型，可以是关键字TCP、UDP、IP之一，或者代表IP协议号的范围为0~255，IPv6代表匹配任意协议类型。

<*icmp-type*>：ICMP报文类型字段，可以是关键字destination-unreachable、packet-too-big、time-exceeded、parameter-problem、echo-request、echo-reply、mld-query、mld-report、mld-reduction、router-solicitation、router-advertisment、nd-ns、nd-na、redirect、router-renumbering中的一个。

<*icmp-type-value*>：ICMP报文类型字段，范围0~255。

<*icmp-code*>：ICMP消息类型，范围0~255。

<*protocol-type*>：IP协议类型，可以是关键字gre、ospf、pim、vrrp中的一个。

<*operator*>：针对端口的操作类型，可以是关键字eq、ge、le中的一个。

<*source-porttype*>：源端口类型，可以是关键字ftp、telnet、smtp、domain、finger、www、pop2、pop3、bgp、login中的一个。

<*destination-porttype*>：目的端口类型，可以是关键字ftp、telnet、smtp、domain、finger、www、pop2、pop3、bgp、login中的一个。

range：针对端口的操作类型，需要指定2个port操作数，范围是0-65535。

dscp <*value*>：DSCP字段，值范围0~63。

established：TCP建链关键字，仅对TCP可用。

<*rst*><*ack*><*fin*><*syn*><*psh*><*urg*>：TCP头部URG、ACK、PSH、RST、SYN、FIN等标志的组合。

routing、authen、destopts 、fragments、hop-by-hop、esp：路由选项（routing header），认证选项（authentication header）、目的选项（destination option header），分片包头（fragment header），逐跳选项（Hop-by-Hop Options Header）和封装安全载荷头（ESP Header）。

<*base*>：rule-id的基值，重新编号成功后第一个规则的编号，默认为10，取值范围：1~2147483644。

<*increment*>：rule-id的步进值，重新编号成功后每个规则rule-id之间的差值，默认为10，取值范围：1~2147483644。

2.配置接口上绑定IPv6 ACL。

步骤	命令	功能
1	inspur(config)#**ipv6-access-group interface** <*interface-name*>{**ingress** | **egress**}<*acl-name*>	在接口上绑定的IPv6 ACL
2	inspur(config)#**interface** <*interface-name*>	进入接口配置模式
	inspur(config-if-interface-name)#**ipv6-access-group** {**ingress** | **egress**}<*acl-name*>	接口配置模式下绑定IPv6 ACL，**ingress**表示绑定在接口的入方向上；**egress**表示绑定在接口的出方向上

3.验证配置结果。

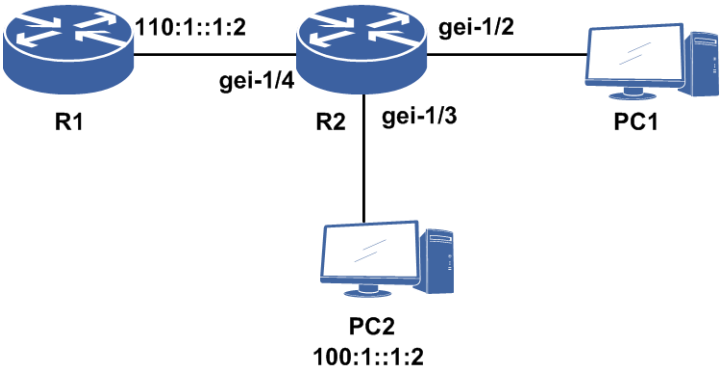
命令	功能
inspur(config)#**show ipv6-access-lists** [{**config** | **brief** [**name** <*acl-name*>]| **name** <*acl-name*>[**from** <*from-id*> **to** <*to-id*>]}][|<*match-type*><*LINE*>]	显示IPv6 ACL列表/简要信息
inspur(config)#**show ipv6-access-groups** [{[**by-access-list** <*acl-name*>],[**by-direction** {**ingress** | **egress**}],[**by-interface** <*interface-name*>]}]	显示IPv6 ACL绑定信息，可根据选项过滤显示
inspur(config)#**show running-config ipv6-acl** [**all**][|{**begin** |**exclude** |**include**}<*key_words*>]	显示IPv6 ACL列表所有信息
inspur(config)#**show running-config port-acl**[**all**][|{**begin** |**exclude** |**include**}<*key_words*>]	显示IPv6 ACL所有绑定信息，若有绑定IPv4 ACL则一并进行显示

12.20.2 IPv6 ACL 配置实例

配置说明

在如*图 12-46*所示的网络中，假设PC1和PC2都通过R2发送telnet请求给R1，如果R1希望只接收PC1的登录请求，而不接收PC2的登录请求。那么可以在gei-1/3的入方向上绑定ACL来过滤掉PC2来的telent报文（也可以绑定在gei-1/4的出方向上）。

图 12-46 IPv6 ACL 配置实例拓扑图



这时只需要创建一个ACL，给这个ACL添加规则：要求对匹配PC2的IP地址，协议类型是TCP，端口类型是telnet的报文做deny处理。ACL创建完成后，将这个ACL绑定到gei-1/3的入方向或者gei-1/4的出方向即可。

这样配置后，PC2获不到R1的telnet用户名和密码，发出的请求也不会到达R1，报文在到达R2后就被丢弃。同时R1和PC2的其他通信不受影响。

配置思路

1.对各接口使能IPv6，配置IPv6地址。

2.创建一个ipv6-access-list，用户在创建时可以给这个list赋予一个自定义的名称，注意名称长度最长支持31个字符。

3.创建列表后就进入了IPv6 ACl配置模式，在这里添加rule，每个rule可以指定一种报文类型，并且规定此种报文的是被permit或deny。

4.根据流量过滤的需要，将定制的ipv6-access-list绑定在需要过滤流量的接口的入方向或者出方向。

配置过程

本范例接口地址配置省略。

R2上的配置如下：

```
R2(config)#ipv6-access-list test
R2(config-ipv6-acl)#rule deny tcp 100:1::1:2/128 eq 23 110:1::1:2/128
R2(config-ipv6-acl)#rule permit ip any any
R2(config-ipv6-acl)#exit
R2(config)#ipv6-access-group interface gei-1/3 ingress test
```

配置验证

查看配置的ACL，提供了三种方式查看配置的ACL：

```
/*查看设备上所有ACL，显示出ACL名称和各ACL rule的数量*/
R2(config)#show ipv6-access-lists brief
No.     ACL                             RuleSum
-------------------------------------------------------
```

```
1       test                              2
/*查看指定名称的ACL信息，可以查看指定ACL中规则的条目信息*/
R2(config)#show ipv6-access-lists name test
ipv6-access-list test
 2/2 (showed/total)
   10 deny tcp 100:1::1:2/128 eq telnet 110:1::1:2/128
   20 permit ip any any
/*查看设备上所有ACL的详细信息，可以查看到所有ACL的规则条目信息*/
R2(config)#show ipv6-access-lists
ipv6-access-list test
 2/2 (showed/total)
   10 deny tcp 100:1::1:2/128 eq telnet 110:1::1:2/128
   20 permit ipv6 any any
```

查看ACL绑定接口的情况，提供三种方式查看ACL与接口的绑定关系：

```
/*查看设备上所有IPv6 ACL与接口的绑定关系*/
R2(config)#show ipv6-access-groups
Interface name|vlan             Direction  ACL name
------------------------------------------------------
gei-1/3                     Ingress    test
/*查看设备上所有ACL与接口的绑定关系，包括IPv4 ACL和IPv6 ACL*/
R2(config)#show running-config port-acl
!<port-acl>
interface gei-0/8 /*设备上绑定IPv4 ACL的其他接口*/
  ipv4-access-group ingress 1K
$
interface gei-1/3
  ipv6-access-group ingress test
$
!</port-acl>
```

12.21 URPF

URPF的主要功能是用于防止基于源地址欺骗的网络攻击行为。

URPF通过检查数据包中源IP地址以及根据接收到数据包的接口和路由表中是否存在源地址路由信息条目，来确定流量是否真实有效，并选择数据包是转发或丢弃。

URPF有以下三种工作模式：

•严格URPF

•松散URPF

•忽略缺省路由的URPF

IPv6 URPF原理同IPv4 URPF。

12.21.1 配置 IPv6 URPF

本节介绍IPv6 URPF功能的配置步骤和命令。

1.在接口上配置IPv6 URPF功能。

步骤	命令	功能
1	inspur(config)#**ipv6 verify unicast source**	开启接口IPv6 URPF功能

步骤	命令	功能
	reachable-via {**rx interface** <*interface-name*>[**acl-name** <*acl-name*>]| **any interface** <*interface-name*>[**acl-name** <*acl-name*>][**ignore-default-route**]}	
2	`inspur(config)#`**interface** <*interface-name*>	进入接口配置模式
3	`inspur(config-if-interface-name)#`**ipv6 verify unicast source reachable-via** {**rx** [**acl-name** <*acl-name*>]| **any** [**acl-name** <*acl-name*>][**ignore-default-route**]}	在接口配置模式开启端口IPv6 URPF功能

rx：严格模式。

any：松散模式。

interface <*interface-name*>：配置IPv6 URPF的接口名称。

ignore-default-route：忽略默认路由选项，仅适用于松散模式。

2.验证配置结果。

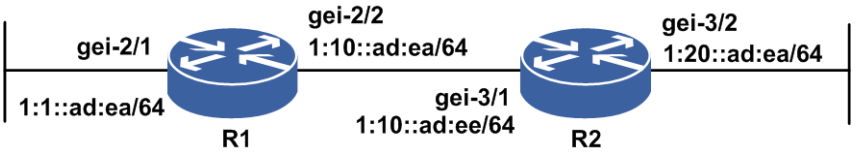
命令	功能
`inspur#`**show running-config urpf** [**all**]	查看所有IPv6 URPF配置
`inspur#`**show running-config-interface** <*interface-name*>[**all**]	查看某个接口下的IPv6 URPF配置

12.21.2 严格 IPv6 URPF 配置实例

配置说明

如*图* **12-47**所示，在路由器R1的gei-2/1接口上配置严格URPF，防止来自1:1::ad:ea/64前面的网络用户恶意攻击R1后面的网络，同时允许来自源地址是1:11::ad:ea/64网段的数据流通过URPF检查。

图 12-47 严格 IPv6 URPF 配置实例拓扑图



配置思路

1.为接口配置IPv6地址。

2.创建ACL，添加符合需求的ACL规则，如允许源地址为1:11::ad:ea/64网段的数据流通过。

3.接口绑定带有ACL列表的严格URPF。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/1
R1(config-if-gei-2/1)#no shutdown
R1(config-if-gei-2/1)#ipv6 enable
R1(config-if-gei-2/1)#ipv6 address 1:1::ad:ea/64
R1(config-if-gei-2/1)#exit
R1(config)#ipv6-access-list acl
R1(config-ipv6-acl)#rule permit ipv6 1:11::ad:ea/64 any
R1(config-ipv6-acl)#exit
R1(config)#ipv6 verify unicast source reachable-via rx interface
gei-2/1 acl-name acl
```

配置验证

查看配置结果：

```
R1(config)#show running-config urpf
!<urpf>
interface gei-2/1
  ipv6 verify unicast source reachable-via rx acl-name acl
$
!</urpf>

R1(config)#show running-config-interface gei-2/1
!<if-intf>
interface gei-2/1
  no shutdown
  ipv6 enable
  ipv6 address 1:1::ad:ea/64
$
!</if-intf>
!<urpf>
interface gei-2/1
  ipv6 verify unicast source reachable-via rx acl-name acl
$
!</urpf>

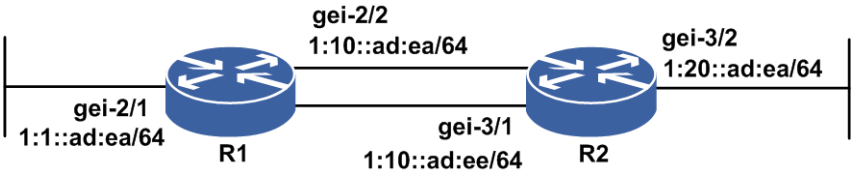
R1(config)#show ipv6-access-lists name acl
ipv6-access-list acl
1/1 (showed/total)
  10 permit ipv6 1:11::ad:ea/64 any
```

12.21.3 松散 IPv6 URPF 配置实例

配置说明

如*图 12-48*所示，举例松散IPv6 URPF配置。

图 12-48 松散 IPv6 URPF 配置实例拓扑图



配置思路

1.按*图 12-48*所示搭建环境，R1和R2之间增加一条子接口链路，配置各个接口IPv6地址。

2.R1和R2之间配置OSPFv3，使得单播互通。

3.R2的入口gei-3/1配置松散URPF，并且配置ACL。

4.发流源是3ff1::1，从R1到R2。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-2/1
R1(config-if-gei-2/1)#no shutdown
R1(config-if-gei-2/1)#ipv6 enable
R1(config-if-gei-2/1)#ipv6 address 1:1:ad::ea/64
R1(config-if-gei-2/1)#exit
R1(config)#interface gei-2/2
R1(config-if-gei-2/2)#no shutdown
R1(config-if-gei-2/2)#ipv6 enable
R1(config-if-gei-2/2)#ipv6 address 1:10::ad:ea/64
R1(config-if-gei-2/2)#exit
R1(config)#interface gei-2/2.1
R1(config-if-gei-2/2.1)#exit
R1(config)#vlan-configuration
R1(config-vlan)#interface gei-2/2.1
R1(config-vlan-if-gei-2/2.1)#encapsulation-dot1q 100
  /*配置子接口，建立另一条链路*/
R1(config-vlan-if-gei-2/2.1)#exit
R1(config-vlan)#exit
R1(config)#interface gei-2/2.1
R1(config-if-gei-2/2.1)#ipv6 enable
R1(config-if-gei-2/2.1)#ipv6 address 200::1/64
R1(config-if-gei-2/2.1)#exit

R1(config)#ipv6 router ospf 1
R1(config-ospfv3-1)#area 0
R1(config-ospfv3-1-area-0)#interface gei-2/1
R1(config-ospfv3-1-area-0-if-gei-2/1)#exit
R1(config-ospfv3-1-area-0)#interface gei-2/2
R1(config-ospfv3-1-area-0-if-gei-2/2)#exit
R1(config-ospfv3-1-area-0)#exit
R1(config-ospfv3-1)#router-id 2.2.2.10
R1(config-ospfv3-1)#exit
```

R2上配置松散URPF功能如下：

```
R2(config)#interface gei-3/1
R2(config-if-gei-3/1)#no shutdown
R2(config-if-gei-3/1)#ipv6 verify unicast source reachable-via any acl-name
```

```
wd
/*接口绑松散URPF*/
R2(config-if-gei-3/1)#exit
R2(config-ipv6-acl)#exit
R2(config)#ipv6 route 3ff1::/64 200::1
/*配置静态路由指定到源的路由出接口和流的入口是不相同的*/
```

R2上其余的配置和R1类似。

配置验证

满足URPF配置的流量可以正常转发。

12.22 IPv6 QoS

IPv6 QoS的是在原IPv4 QoS的基础上，增加支持了IPv6的功能。

IPv6 QoS原理同IPv4 QoS。

12.22.1 配置 IPv6 QoS

IPv6 QoS的配置命令和IPv4 QoS的配置命令类似，只是使用了IPv6的地址来完成配置。具体配置命令请参考“QoS”。

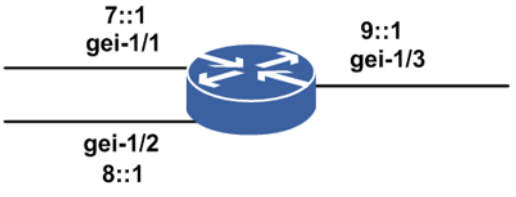
12.22.2 IPv6 优先级调度配置实例

配置说明

如*图 12-49*所示，gei-1/1和gei-1/2接入4个用户：user1、user2、user3和user4，分别要求如下：

- user1优先通过，最大带宽500M。
- user2保证300M，可以大于300M。
- user3保证速率100M，突发速率150M。
- user4保证速率100M，突发速率150M。

图 12-49 IPv6 优先级调度配置实例拓扑图



配置思路

1.在gei-1/3下行配置H-QoS，这样当端口拥塞时可以保证每个用户的带宽

2.四个用户的DSCP分别为1、2 、3 和4，配置四个class进行分类

3.User1为LLQ队列，并限速500Mbps

4.User2为WFQ队列，bandwidth限制为端口带宽的30%

5.User3和user4为WFQ队列，bandwidth限制为端口带宽的20%

6.User3和user4的class中配置下一层policy进行限速

7.在第二层policy中，两个用户的cir＝100M；pir＝150M

配置过程

1.配置IR12000的接口：

```
inspur(config)#interface gei-1/1
inspur(config-if-gei-1/1)#ipv6 enable
inspur(config-if-gei-1/1)#ipv6 address 7::1/64
inspur(config-if-gei-1/1)#exit
inspur(config)#interface gei-1/2
inspur(config-if-gei-1/2)#ipv6 enable
inspur(config-if-gei-1/2)#ipv6 address 8::1/64
inspur(config-if-gei-1/2)#exit
inspur(config)#interface gei-1/3
inspur(config-if-gei-1/3)#ipv6 enable
inspur(config-if-gei-1/3)#ipv6 address 9::1/64
inspur(config-if-gei-1/3)#exit
```

2.配置class分类：

```
inspur(config)#class-map dscp1  match-all ipv6
inspur(config-cmap)#match dscp 1
inspur(config-cmap)#exit
inspur(config)#class-map dscp2  match-all ipv6
inspur(config-cmap)#match dscp 2
inspur(config-cmap)#exit
inspur(config)#class-map dscp3  match-all ipv6
inspur(config-cmap)#match dscp 3
inspur(config-cmap)#exit
inspur(config)#class-map dscp4  match-all ipv6
inspur(config-cmap)#match dscp 4
inspur(config-cmap)#exit
inspur(config)#class-map dscp34  match-all ipv6
inspur(config-cmap)#match dscp 3,4
inspur(config-cmap)#exit
```

3.配置第二层的policy：

```
inspur(config)#policy-map car1
inspur(config-pmap)#class dscp3
inspur(config-pmap-c)#police cir 100000 cbs 100 pir 150000 pbs 150
conform-action transmit exceed-action transmit violate-action drop
inspur(config-pmap-c)#exit
inspur(config-pmap)#class dscp4
inspur(config-pmap-c)#police cir 100000 cbs 100 pir 150000 pbs 150
conform-action transmit exceed-action transmit violate-action drop
inspur(config-pmap-c)#exit
inspur(config-pmap)#exit
```

4.配置第一层的policy：

```
inspur(config)#policy-map test
inspur(config-pmap)#class dscp1
inspur(config-pmap-c)#priority-llq
inspur(config-pmap-c)#police cir 500000 cbs 500 conform-action transmit
exceed-action drop
inspur(config-pmap-c)#exit
inspur(config-pmap)#class dscp2
inspur(config-pmap-c)#bandwidth percent 30
inspur(config-pmap-c)#exit
inspur(config-pmap)#class dscp34
inspur(config-pmap-c)#bandwidth percent 20
inspur(config-pmap-c)#service-policy car1
inspur(config-pmap-c)#exit
inspur(config-pmap)#exit
```

5.将策略绑定到接口：

```
inspur(config)#service-policy gei-1/3 output test
```

配置验证

用**show policy-map**命令验证策略配置是否正确：

```
inspur(config)#show policy-map
policy-map test
class dscp1
priority-llq
police cir 500000 cbs 500 conform-action transmit exceed-action drop
class dscp2
bandwidth percent 30
class dscp34
service-policy car1
bandwidth percent 20
policy-map car1
class dscp3
police cir 100000 cbs 100 pir 150000 pbs 150 conform-action transmit
exceed-action transmit violate-action drop
class dscp4
police cir 100000 cbs 100 pir 150000 pbs 150 conform-action transmit
exceed-action transmit violate-action drop
```

用**show service-policy**验证绑定接口是否正确：

```
inspur#show service-policy
 service-policy gei-1/3 output test
```

12.22.3 IPv6 WRED 配置实例

配置说明

在路由器接口的上行配置WRED策略，使得不同的优先级报文在发生拥塞时有不同的丢弃策略。需要达成以下目标：

- 优先级为0的队列最低丢弃门限为30kb，最高丢弃门限为100kb，丢弃概率为90%，平均队列长度的指数为8。
- 优先级为1的队列最低丢弃门限为120kb，最高丢弃门限为200kb，丢弃概率为80%，平均队列长度的指数为8。
- 优先级为2的队列最低丢弃门限为220kb，最高丢弃门限为300kb，丢弃概率为70%，平均队列长度的指数为8。

配置思路

1.建立一个新的class-map，匹配precedence 0-2。

2.建立一个新的policy-map，在策略中加入新建的匹配precedence 0-2的 class类，在类中将不同的优先级队列加入到wred中。

3.将第2步中的policy-map策略绑在接口的出方向。

配置过程

1.配置class分类：

```
inspur(config)#class-map pre0-2 match-all ipv6
inspur(config-cmap)#match precedence 0-2
inspur(config-cmap)#exit
```

2.配置policy策略：

```
inspur(config)#policy-map wred
inspur(config-pmap)#class pre0-2
inspur(config-pmap-c)#random-detect enable
inspur(config-pmap-c)#random-detect weight 8
inspur(config-pmap-c)#random-detect precedence 0 30 100 90
inspur(config-pmap-c)#random-detect precedence 1 120 200 80
inspur(config-pmap-c)#random-detect precedence 2 220 300 70
inspur(config-pmap-c)#exit
inspur(config-pmap)#exit
```

3.将策略绑定到接口：

```
inspur(config)#service-policy gei-0/7 output wred
```

配置验证

在流量的入接口上流量拥塞，在流量的出接口可以通过抓包看到，不同优先级队列的报文，丢弃概率和配置说明的一致。

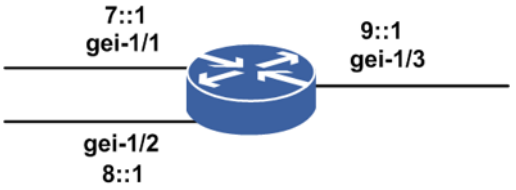
12.22.4 IPv6 CAR 配置实例

配置说明

如*图 12-50*所示，user1、user2分别从gei-1/1和gei-1/2接入，DSCP分别为1和2，从gei-1/3出去。

要求从gei-1/3出去的两个用户的DSCP值为7，保证带宽为100M，最大带宽150M。

图 12-50 IPv6 CAR 配置实例拓扑图



配置思路

在gei-1/3下行配置两个CAR，分别匹配DSCP值1和2，并将通过的流量的DSCP设为7，为每个用户设置保证带宽为100M，最大带宽150M。

配置过程

1.进入CAR配置模式：

```
inspur(config)#qos
inspur(config-qos)#
```

2.进入接口配置模式：

```
inspur(config-qos)#interface gei-1/3
inspur(config-qos-if-gei-1/3)#
```

3.配置CAR命令：

```
inspur(config-qos-if-gei-1/3)#rate-limit output ipv6 dscp 1 cir 100000 cbs
200000 pir 150000 pbs 300000 conform-action set-dscp-transmit 7
exceed-action set-dscp-transmit 7 violate-action drop
inspur(config-qos-if)#rate-limit output ipv6  dscp 2 cir 100000 cbs 200000
pir 150000 pbs 300000 conform-action set-dscp-transmit 7
exceed-action set-dscp-transmit 7 violate-action drop
```

配置验证

通过**show running-config carset**查看接口配置的CAR：

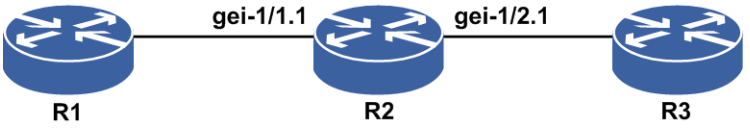
```
inspur(config)#show running-config car
!<car>
qos
  interface gei-8/1
    rate-limit output ipv6 dscp 1 cir 100000 cbs 200000 pir 150000 pbs 300000
conform-action set-dscp-transmit 7 exceed-action set-dscp-transmit 7 violate-
action drop
    rate-limit output ipv6 dscp 2 cir 100000 cbs 200000 pir 150000 pbs 300000
conform-action set-dscp-transmit 7 exceed-action set-dscp-transmit 7 violate-
action drop
  $
$
!</car>
```

12.22.5 IPv6 优先级继承配置实例

配置说明

如*图 12-51*所示，要求R2上从VLAN子接口（gei-1/1.1）入的流转发出去时，实现入接口流的802.1p到出接口流的IPP的映射。

图 12-51 IPv6 优先级继承配置实例拓扑图



配置思路

1.创建VLAN子接口，配置VLAN子接口的IP地址。

2.配置子接口的VLAN ID。

3.配置802.1p继承策略。

配置过程

R2上的配置如下：

```
R2(config)#interface gei-1/1.1
R2(config-if-gei-1/1.1)#ipv6 enable
R2(config-if-gei-1/1.1)#ipv6 address 7::1/64
R2(config-if-gei-1/1.1)#exit
R2(config)#interface gei-1/2.1
R2(config-if-gei-1/2.1)#ipv6 enable
R2(config-if-gei-1/2.1)#ipv6 address 8::1/64
R2(config-if-gei-1/2.1)#exit

R2(config)#vlan-configuration
R2(config-vlan)#interface gei-1/1.1
R2(config-vlan-if-gei-1/1.1)#encapsulation-dot1q 100
R2(config-vlan-if-gei-1/1.1)#exit
R2(config-vlan)#interface gei-1/2.1
R2(config-vlan-if-gei-1/2.1)#encapsulation-dot1q 200
R2(config-vlan-if-gei-1/2.1)#exit
R2(config-vlan)#exit

R2(config)#class-map 802.1p match-all ipv6
R2(config-cmap)#match child
R2(config-cmap)#exit
R2(config)#policy-map 802.1p
R2(config-pmap)#class 802.1p
R2(config-pmap-c)#set precedence inherit-from 8021p
R2(config-pmap-c)#exit
R2(config-pmap)#exit
R2(config)#service-policy gei-1/1.1 input 802.1p
```

R1和R3上只需要配置VLAN子接口和IP地址，具体配置省略。

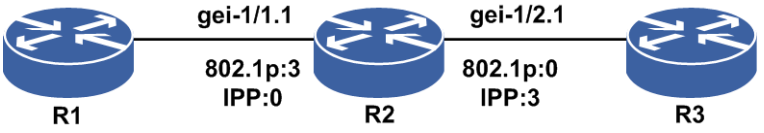
配置验证

在R2上查看配置结果：

```
R2(config)#show class-map 802.1p
class-map 802.1p match-all ipv6
  match child
R2(config)#show policy-map 802.1p
 policy-map 802.1p
  class 802.1p
    set precedence inherit-from 8021p
R2(config)#show service-policy gei-1/1.1
service-policy gei-1/1.1 input 802.1p
```

入接口的802.1p到出接口的IPP的继承关系如*图 12-52*所示。

图 12-52 802.1p 到 IPP 的继承关系字段变化示意图



12.23 IPv6 VRRP

IPv6 VRRP的功能与IPv4 VRRP相同，为具有多播能力的局域网提供路由器的冗余备份功能，只是网络中运行了IPv6协议并配置了IPv6地址。IPv6 VRRP工作在运行了IPv6协议的网络中，将一组路由设备组织成一个虚拟的路由设备，对外提供虚拟IP地址给用户做网关，实现对网关的冗余备份，避免了因单个路由设备故障而引起整个网络的通信故障。

12.23.1 配置 IPv6 VRRP

配置IPv6 VRRP的基本属性和功能，包括版本号、报文发送模式、接口属性参数等。

1.配置IPv6 VRRP的基本属性参数。

步骤	命令	功能
1	`inspur(config)#`**vrrp**	进入VRRP配置模式
2	`inspur(config-vrrp)#`**vrrp** *<vrid>* **version** {**2**|**3**}	配置VRRP协议版本号，VRRP默认协议版本号为3
	`inspur(config-vrrp)#`**vrrp** *<vrid>* **send-mode** {**all**|**rotation**}	配置VRRP报文发送模式，默认发送模式为**all**
	`inspur(config-vrrp)#`**vrrp** *<vrid>* **reload-delay** *<reload-delay>*	配置VRRP组接口状态机延迟启动时间

all ：报文向所有的出接口发送。

rotation：报文向每个出接口轮流发送。

<*reload-delay*> 配置接口状态机延迟启动时间，范围：0~65535，单位：秒，默认延迟时间为0秒。

2.配置IPv6 VRRP的接口属性可选参数。

步骤	命令	功能
1	inspur(config-vrrp)#**interface** <*interface-name*>	进入VRRP接口配置模式
2	inspur(config-vrrp-if-interface-name)# **vrrp** <*vrid*>**ipv6**<*ipv6-address*>[**secondary**]	配置VRRP的虚拟IPv6地址，<*vrid*>，虚拟路由器的ID，范围：1~255
	inspur(config-vrrp-if-interface-name)# **vrrp** <*vrid*> **priority** <*level*>	配置VRRP优先级，优先级取值范围1~254，缺省优先级为100
	inspur(config-vrrp-if-interface-name)# **vrrp** <*vrid*> **preempt** {[**delay** <*delay-time*>][{**disable**}]}	配置VRRP组是否抢占，默认为抢占模式，抢占延迟为0秒
	inspur(config-vrrp-if-interface-name)# **vrrp** <*vrid*> **timers advertise** {<*1-40*>|**msec** <*50-40000*>}	配置发送VRRP通告的时间间隔，缺省通告时间间隔为1秒。 参数<*1-40*>的单位为秒；参数<*50-40000*>的单位为毫秒 **msec**：将时间间隔的单位从秒变为毫秒（可选）
	inspur(config-vrrp-if-interface-name)# **vrrp** <*vrid*> **timers** {**advertise** {<*adver-time-in-seconds*>|**msec** <*adver-time-in-milliseconds*>}| **learn** [**disable**]}	配置VRRP是否从通告报文中学习发送时间间隔，缺省为不学习方式
	inspur(config-vrrp-if-interface-name)# **vrrp** <*vrid*> **track interface** <*interface-name*>[**priority-decrement** <*1-254*>| **rapid-down**]	配置VRRP跟踪接口，如不指定降低的优先级数值，则默认下降优先级10，缺省不跟踪任何链路状态
	inspur(config-vrrp-if-interface-name)# **vrrp** <*vrid*> **out-interface** <*interface-name*>	配置VRRP报文发送出接口（心跳线）
	inspur(config-vrrp-if-interface-name)# **vrrp** <*vrid*> **track** { **group** | **object**}<*string*>{ **link-type** | **peer-type** | **priority-decrement** <*1-254*>}	配置VRRP跟踪的检测组或检测对象及其策略类型
	inspur(config-vrrp-if-interface-name)# **vrrp** <*vrid*> **accept** [**disable**]	配置accept功能，默认开启
	inspur(config-vrrp-if-interface-name)# **vrrp** <*vrid*> **check-ttl** [**disable**]	配置check-ttl功能，默认开启
	inspur(config-vrrp-if-interface-name)# **vrrp** <*vrid*> **admin-group** { **owner** | **interface** <*interface-name*> **vrid** <*1-255*>}	配置VRRP管理组功能 **owner**：VRRP组配置为管理组，负责收发报文和状态管理

group ：检测组。

object：检测对象。

string：检测组或检测对象名称

link-type ： 指定link类型，跟踪本端设备链路状态时用该策略。

peer-type ： 指定peer类型，跟踪对端设备链路状态时用该策略。

priority-decrement <*1-254*>：配置指定降低优先级策略，指定降低的数值。

3.验证配置结果。

命令	功能
inspur#**show vrrp ipv6 brief**	查看路由器上所有IPv6 VRRP组简要信息
inspur#**show vrrp ipv6 brief interface** <*interface-name*>	简要查看路由器上指定接口下的所有IPv6 VRRP组信息
inspur#**show vrrp interface** <*interface-name*>[**vrid** <*1-255*>]	查看指定接口下的所有或指定VRRP组详细信息

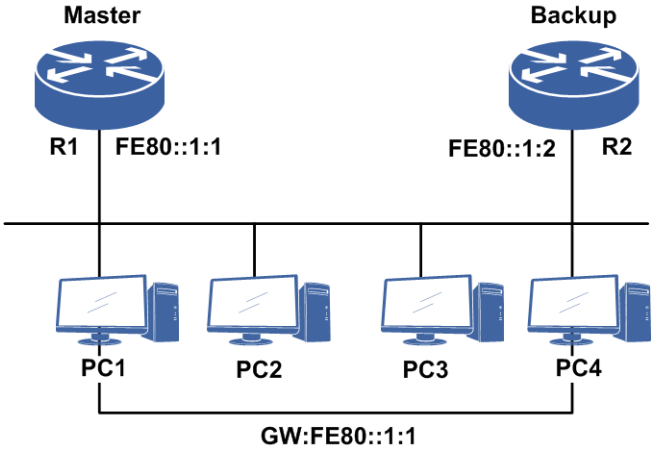
12.23.2 基本 VRRP 配置实例

配置说明

如*图 12-53*所示，R1和R2之间运行IPv6 VRRP协议。R1的接口地址配置为FE80::1:1，R2的接口地址配置为FE80::1:2。在R1和R2的接口上配置相同的VRRP组号和虚拟地址，虚拟地址配置为FE80::1:1，此时的R1虚拟地址和接口实际IP地址相同，被称为IP地址拥有者，拥有最高优先级255，R1将作为主用路由器。

当然VRRP虚拟地址也可以配置其他的Link-local地址（注意配置的主虚拟地址必须用link-local地址，以FE80::为前缀的），R1上配置较高优先级，使其成为主用路由器。

图 12-53 基本 VRRP 配置



配置思路

1.进入要配置VRRP的接口，开启IPv6功能，并为其配置网络IPv6地址。

2.全局模式下进入VRRP配置模式，再进入要配置VRRP的接口。

3.分别为R1和R2配置相同的VRRP组号及虚拟地址。为使R1作为主用路由器，可以在R1设备上配置较高的优先级，或者直接配成IP地址拥有者（用R1的接口IP地址做虚拟地址，此时R1拥有最高优先级255），也可先在R1上按照以上配置步骤执行，因为相同优先级（默认100）情况下，先配置VRRP并使其生效、开始发布报文的路由器会作为组内的主用路由器。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ipv6 enable
R1(config-if-gei-1/1)#ipv6 address link-local fe80::1:1
R1(config-if-gei-1/1)#exit
R1(config)#vrrp
R1(config-vrrp)#interface gei-1/1
R1(config-vrrp-if-gei-1/1)#vrrp 1 ipv6 fe80::1:1
/*对于VRRP v3中的IPv6地址配置，虚拟主IP地址必须是Link-local地址，即FE80开头的地址，
如：vrrp 1 ipv6 fe80::1。如果此处配置的地址为global地址，只能作为VRRP的虚拟辅IP地址，
如：vrrp 1 ipv6 1::2 secondary*/
R1(config-vrrp-if-gei-1/1)#end
```

R2上的配置如下：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ipv6 enable
R2(config-if-gei-1/1)#ipv6 address link-local fe80::1:2
R2(config-if-gei-1/1)#exit
R2(config)#vrrp
R2(config-vrrp)#interface gei-1/1
R2(config-vrrp-if-gei-1/1)#vrrp 1 ipv6 fe80::1:1
R2(config-vrrp-if-gei-1/1)#end
```

配置验证

查看R1的VRRP配置和生效情况：

```
R1(config)#show vrrp ipv6 brief
Interface      vrID Pri Time   A P L State  Master addr     VRouter addr
gei-1/1        1    255 1000   A P   Master FE80:0:0:0:0:0: FE80:0:0:0:0:0:1
                                          1:1            :1
/*A：是否Owner。P：是否抢占。L：是否学习MASTER的VRRP报文发送时间间隔*/

R1(config)#show vrrp interface gei-1/1 vrid 1
gei-1/1 - vrID 1
  Vrrp configure info:  /*VRRP配置信息*/
    IP version 6, VRRP version 3
    Virtual IP address is FE80:0:0:0:0:0:1:1
    Virtual MAC address is 0000.5e00.0201  /*IPv4物理地址为0000.5e00.01XX*/
    Advertise time is 1.000 sec
    Configured priority is 100
    Preemption enable, delay 0(s)
```

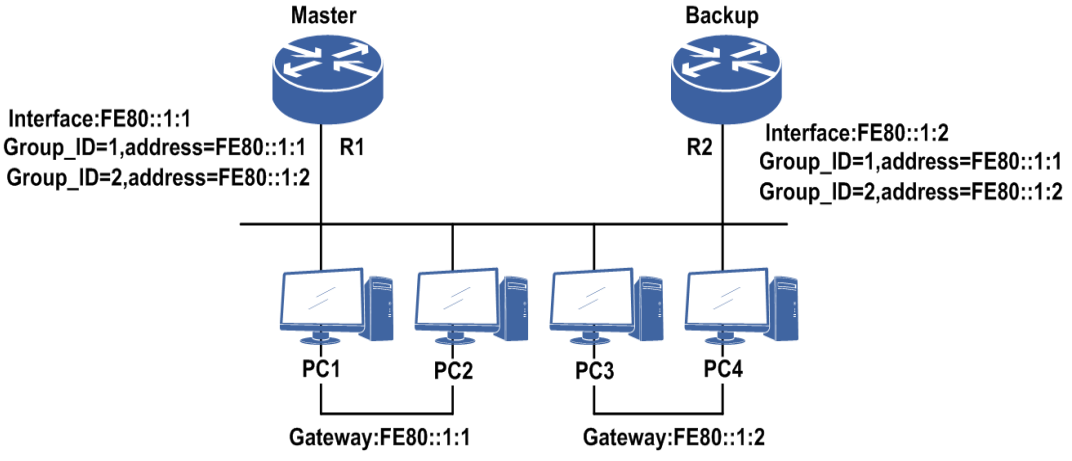
```
    Reload delay 0 (s)
    No authentication data
    Check ttl enable
    Vrrp accept mode enable
    Out-interface send-mode is all
    Tracked interface items: 0
        Interface        State    Decrement-Priority
    Tracked detect items: 0
Admin-group is None
/*VRRP在当前接口的运行信息*/
  Vrrp run info:
State is Master
/*VRRP运行状态*/
     1 state changes, last state change 01:19:21
/*切换次数与上次切换时系统已经运行的时间*/
Current priority is 255
/*当前优先级，Owner状态优先级为最高255*/
    Master router is local
      Master router address is FE80:0:0:0:0:0:1:1
      Master router priority is 255
      Master Advertisement interval is 1.000 sec
      Master Down interval is 3.003 sec, no learn
```

12.23.3 对称 VRRP 配置实例

配置说明

如*图 12-54*所示，对称VRRP即为支持负载分担的组网应用，本例中启动了两个VRRP组，其中PC1和PC2使用组1的虚拟路由器作为默认网关，地址为FE80::1:1，PC3和PC4则使用组2的虚拟路由器作为默认网关，地址为FE80::1:2。路由器R1和R2互为备份，只有当两个路由器全部失效时四台主机与外界的通信才会中断。

图 12-54 对称 VRRP 配置



配置思路

1.进入要配置VRRP的接口，开启IPv6功能，并为其配置网络IPv6地址。

2.全局模式下进入VRRP配置模式，再进入要配置VRRP的接口。

3.在R1，R2上分别配置VRRP组1，组2及相应的虚拟地址，R1上的VRRP组1配置为较

高优先级，R2上的VRRP组2配置为较高优先级，这样R1成为组1的主用路由器，同时成为组2的备用路由器。R2成为组2的主用路由器，同时成为组1的备用路由器，R1和R2互为备份。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-1/1
R1(config-if-gei-1/1)#no shutdown
R1(config-if-gei-1/1)#ipv6 enable
R1(config-if-gei-1/1)#ipv6 address link-local fe80::1:1
R1(config-if-gei-1/1)#exit
R1(config)#vrrp
R1(config-vrrp)#interface gei-1/1
R1(config-vrrp-if-gei-1/1)#vrrp 1 ipv6 fe80::1:1
R1(config-vrrp-if-gei-1/1)#vrrp 2 ipv6 fe80::1:2
R1(config-vrrp-if-gei-1/1)#end
```

R2的配置：

```
R2(config)#interface gei-1/1
R2(config-if-gei-1/1)#no shutdown
R2(config-if-gei-1/1)#ipv6 enable
R2(config-if-gei-1/1)#ipv6 address link-local fe80::1:2
R2(config-if-gei-1/1)#exit
R2(config)#vrrp
R2(config-vrrp)#interface gei-1/1
R2(config-vrrp-if-gei-1/1)#vrrp 1 ipv6 fe80::1:1
R2(config-vrrp-if-gei-1/1)#vrrp 2 ipv6 fe80::1:2
R2(config-vrrp-if-gei-1/1)#end
```

配置验证

查看R1的VRRP配置和生效情况：

```
R1#show vrrp ipv6 brief
Interface    vrID Pri Time   A P L State  Master addr     VRouter addr
gei-1/1      1    255 1000   A P   Master FE80:0:0:0:0:0: FE80:0:0:0:0:0:1
                                      1:1           :1
gei-1/1      2    100 1000     P   Backup FE80:0:0:0:0:0: FE80:0:0:0:0:0:1
                                      1:1           :2
/* A：是否Owner。P：是否抢占。L：是否自学习MASTER的VRRP报文发送时间间隔*/
R1#show vrrp interface gei-1/1
gei-1/1 - vrID 1
  Vrrp configure info:
    IP version 6, VRRP version 3
    Virtual IP address is FE80:0:0:0:0:0:1:1
    Virtual MAC address is 0000.5e00.0201
    Advertise time is 1.000 (s)
    Configured priority is 100
    Preemption enable, delay 0 (s)
    Reload delay 5 (s)
    No authentication data
    Check ttl enable
    Vrrp accept mode enable
    Out-interface send-mode is all
    Tracked interface items: 0
       Interface        State  Policy        Reduce-Priority
    Tracked detect items: 0
    Admin-group is None
  Vrrp run info:
    State is Master
```

```
    5 state changes, last state change 17:05:34 1 day(s)
  Current priority is 255
  Master router is local
    Master router address is FE80:0:0:0:0:0:1:1
    Master router priority is 255
    Master Advertisement interval is 1.000 (s)
    Master Down interval is 3.003 (s), no learn

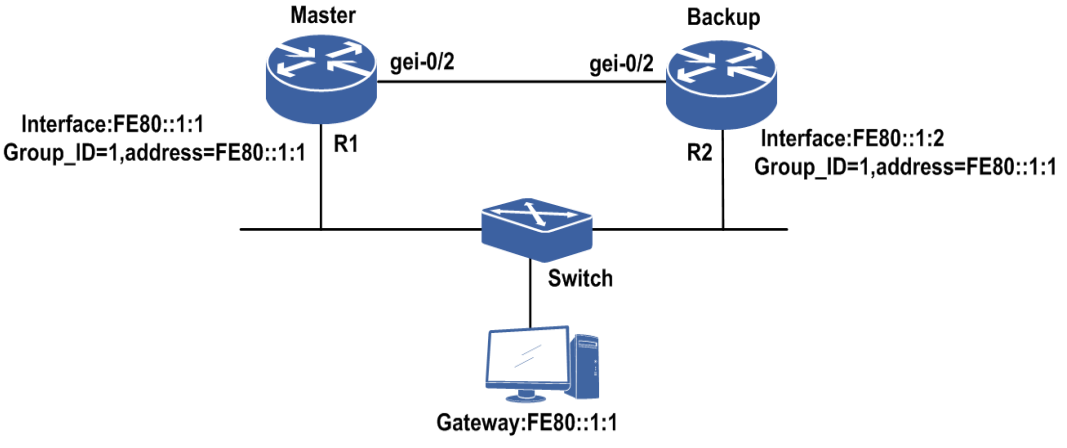
gei-1/1 - vrID 2
 Vrrp configure info:
  IP version 6, VRRP version 3
  Virtual IP address is FE80:0:0:0:0:0:1:2
  Virtual MAC address is 0000.5e00.0202
  Advertise time is 1.000 (s)
  Configured priority is 100
  Preemption enable, delay 0 (s)
  Reload delay 5 (s)
  No authentication data
  Check ttl enable
  Vrrp accept mode enable
  Out-interface send-mode is all
  Tracked interface items: 0
     Interface        State  Policy        Reduce-Priority
  Tracked detect items: 0
  Admin-group is None
 Vrrp run info:
  State is Backup
    6 state changes, last state change 17:05:34 1 day(s)
  Current priority is 100
  Master router is remote
    Master router address is FE80:0:0:0:0:0:1:2
    Master router priority is 255
    Master Advertisement interval is 1.000 (s)
    Master Down interval is 3.609 (s), no learn
```

12.23.4 VRRP 心跳线配置实例

配置说明

如*图 12-55*所示，本例中R1和R2之间运行VRRP协议。VRRP虚拟地址选用R1的接口地址FE80::1:1，R1将作为主用路由器。

图 12-55 VRRP 心跳线（IPv6）配置



配置思路

1.进入要配置VRRP的接口，开启IPv6功能，并为其配置网络IPv6地址。

2.全局模式下进入VRRP配置模式，再进入要配置VRRP的接口。

3.分别为R1，R2配置相同的VRRP组号及虚拟地址。为使R1作为主用路由器，可在R1设备上配置较高的优先级，或直接配成IP地址拥有者（用R1的接口IP地址做虚拟地址，此时R1拥有最高优先级255）。

4.在R1，R2的VRRP接口配置模式下，分别为VRRP组配置报文出接口，要保证报文在这一对出接口上是可以互相收发的。

配置过程

R1上的配置如下：

```
R1(config)#interface gei-0/2
R1(config-if-gei-0/2)#no shutdown
R1(config-if-gei-0/2)#ipv6 enable
R1(config-if-gei-0/2)#ipv6 address link-local fe80::1:1
R1(config-if-gei-0/2)#exit
R1(config)#vrrp
R1(config-vrrp)#interface gei-0/2
R1(config-vrrp-if-gei-0/2)#vrrp 1 ipv6 fe80::1:1
R1(config-vrrp-if-gei-0/2)#vrrp 1 out-interface gei-0/1
R1(config-vrrp-if-gei-0/2)#end
```

R2上的配置如下：

```
R2(config)#interface gei-0/2
R2(config-if-gei-0/2)#no shutdown
R2(config-if-gei-0/2)#ipv6 enable
R2(config-if-gei-0/2)#ipv6 address link-local fe80::1:2
R2(config-if-gei-0/2)#exit
R2(config)#vrrp
R2(config-vrrp)#interface gei-0/2
R2(config-vrrp-if-gei-0/2)#vrrp 1 ipv6 fe80::1:1
R2(config-vrrp-if-gei-0/2)#vrrp 1 out-interface gei-0/1
R2(config-vrrp-if-gei-0/2)#end
```

配置验证

查看R1的VRRP配置和生效情况：

```
R1#show vrrp ipv6 brief
Interface      vrID Pri Time   A P L State  Master addr     VRouter addr
gei-0/2        1    255 1000   A P   Master FE80:0:0:0:0:0: FE80:0:0:0:0:0:1
                                        1:1            :1
/*A：是否Owner。P：是否抢占。L：是否自学习MASTER的VRRP报文发送时间间隔*/

R1#show vrrp interface gei-0/2
gei-0/2 - vrID 1
  Vrrp configure info:      /*VRRP配置信息*/
    IP version 6, VRRP version 3
    Virtual IP address is FE80:0:0:0:0:0:1:1
    Virtual MAC address is 0000.5e00.0201
    Advertise time is 1.000 sec
    Configured priority is 100
    Preemption enable, delay 0(s)
    Reload delay 0 (s)
```

```
  No authentication data
  Check ttl enable
  Vrrp accept mode enable
  Out-interface send-mode is all
  Out-interface(heartbeat line) is gei-0/2
  Tracked interface items: 0
     Interface        State    Decrement-Priority
  Tracked detect items: 0
  Admin-group is None
Vrrp run info:          /*VRRP在当前接口的运行信息*/
  State is Master       /*VRRP运行状态*/
    3 state changes, last state change 03:38:35    /*切换次数与时间*/
  Current priority is 255     /*当前优先级，Owner状态优先级为最高255*/
  Master router is local
    Master router address is FE80:0:0:0:0:0:1:1
    Master router priority is 255
    Master Advertisement interval is 1.000 sec
    Master Down interval is 3.003 sec, no learn
```

12.24 DHCPv6

DHCPv6协议是IETF定义的IPv6网络中的有状态地址自动配置协议。通过DHCPv6协议，IPv6中的网络节点可以向DHCPv6服务器端（DHCPv6 Server）请求其需要的IPv6地址，以及其它的一些配置参数。

IPv6网络中，DHCPv6客户端（DHCPv6 Client）通过使用一个保留的、链路内有效的多播地址来定位DHCPv6 Server，因此要求Client和Server在同一个链路之上。但是在某些场景下，Client可以和不在同一链路上的Server通信，通过DHCPv6中继（DHCPv6 Relay）来实现。DHCPv6 Relay可以中继来自Client或者来自其它Relay的接入请求。

DHCPv6协议采用UDP来传输协议报文，客户端侦听的端口是546，而服务器端与中继侦听的端口都是547。

12.24.1 配置 DHCPv6 Server

本节介绍DHCPv6 Server的配置步骤和命令。

1. 开启DHCPv6功能，配置接口的DHCPv6模式为DHCPv6 Server。

步骤	命令	功能
1	inspur(config)#**dhcp ipv6**	进入DHCPv6配置模式
2	inspur(config-dhcpv6)#**enable**	启用DHCPv6功能
3	inspur(config-dhcpv6)#**interface** <*interface-name*>	进入DHCPv6的接口配置模式
4	inspur(config-dhcpv6-if-interface-name)#**mode** {**server** | **relay**}	启用接口的DHCPv6工作模式，选择**server**配置为DHCPv6 Server工作模式

2.配置IPv6地址池。

步骤	命令	功能
1	inspur(config)#**ipv6 addr-pool** <*pool-name*>	进入IPv6地址池配置模式
2	inspur(config-ipv6-addr-pool)#**addr-range** <*start-ipv6*><*end-ipv6*>[**vrf-instance** <*vrf-name*>]	配置IPv6地址池范围
3	inspur(config-ipv6-addr-pool)#**exclude-range** <*start-ipv6*><*end-ipv6*>[**vrf-instance** <*vrf-name*>]	配置IPv6保留的地址
4	inspur(config-ipv6-addr-pool)#**conflict-time** <*timeout*>	配置IPv6地址池的冲突地址释放时间，单位：分钟，范围：1~18000，默认30分钟
5	inspur(config-ipv6-addr-pool)#**lock**	锁定该IPv6地址池，默认不锁定
6	inspur(config-ipv6-addr-pool)#**threshold** <*percent*>	配置IPv6地址池的告警阈值，范围50~100，默认阈值为100%

3.配置IPv6 prefix-pool。

步骤	命令	功能
1	inspur(config)#**ipv6 prefix-pool** <*pool-name*>	进入IPv6 prefix-pool配置模式
2	inspur(config-ipv6-prefix-pool)#**lock**	锁定该IPv6 prefix-pool，默认不锁定
3	inspur(config-ipv6-prefix-pool)#**prefix-delegation** <*ipv6 prefix-delegation*><*prefix-length*>[**vrf-instance** <*vrf-name*>]	配置IPv6 prefix-delegation
4	inspur(config-ipv6-prefix-pool)#**exclude-prefix** <*ipv6-prefix-delegation*><*1-128*>[**vrf-instance** <*vrf-name*>]	配置IPv6保留前缀块
5	inspur(config-ipv6-addr-pool)#**threshold** <*percent*>	配置IPv6 prefix-pool的告警阈值，默认阈值为100%

4.配置DHCPv6 Pool。

步骤	命令	功能
1	inspur(config-dhcpv6)#**pool** <*pool-name*>	在DHCPv6配置模式下进入DHCPv6地址池配置模式
2	inspur(config-dhcpv6-pool)#**prefix-pool** <*pool-name*>	绑定指定的prefix-pool到DHCPv6 pool
3	inspur(config-dhcpv6-pool)#**prefix-lifeti**	指定地址前缀的生命期（有效时

步骤	命令	功能
	me {<*valid-lifetime1*>| **infinite**}{<*preferred-lifetime1*>| **infinite**}	间和首选时间）
4	inspur(config-dhcpv6-pool)#**aftr** {**address** <*xx:xx::xx:xx*>| **fqdn** <*word*>}[**option-code-value** <*1-65535*>]	在DHCPv6 pool模式下，配置aftr选项命令。aftr有两个类型，2005年之前草案定义的是地址，2006年及之后的草案定义的是域名，这里两个参数为可配置的选项，一次只能配置其中一个
5	inspur(config-dhcpv6-pool)#**address-pool** <*pool-name*>	绑定指定的IPv6 address-pool到DHCPv6 pool
6	inspur(config-dhcpv6-pool)#**address-lifetime** {<*valid-lifetime2*>| **infinite**}{<*preferred-lifetime2*>| **infinite**}	指定地址的生命期（有效时间和首选时间）
7	inspur(config-dhcpv6-pool)#**dns-server** <*server-number*><*server-ipv6*>	配置IPv6 DNS服务器地址
8	inspur(config-dhcpv6-pool)#**domain-name** <*domain-name-number*><*domain-name*>	配置IPv6 DNS服务器域名
9	inspur(config-dhcpv6-pool)#**preference** <*preference-value*>	配置Server的preference，范围：1~255
10	inspur(config-dhcpv6-pool)#**server-unicast-address** <*ipv6-address*>	配置Server的单播地址

<*valid-lifetime1*>，配置分配的前缀的有效时间，单位：秒，可配范围：60~4294967295，缺省：3600。

<*preferred-lifetime1*>，配置分配的前缀的首选时间，单位：秒，可配范围：60~4294967295，缺省：3600。

infinite，配置分配的前缀的有效时间/首选时间为永久。

<*valid-lifetime2*>，配置分配的地址的有效时间，单位：秒，可配范围：60~4294967295，缺省：3600。

<*preferred-lifetime2*>，配置分配的地址的首选时间，单位：秒，可配范围：60~4294967295，缺省：3600。

<*server-number*>，配置DNS的号码，可配范围：1~2。

5.配置DHCPv6 Policy。

步骤	命令	功能
1	inspur(config-dhcpv6)#**policy** <*policy-name*><*priority*>	在DHCPv6模式下进入DHCPv6策略配置模式，并配置该策略的优先级，可配范围：1~5
2	inspur(config-dhcpv6-policy)#**dhcpv6-pool** <*pool-name*>	将DHCPv6策略与DHCPv6地址池绑定

步骤	命令	功能
3	inspur(config-dhcpv6-policy)#**link-address** <*ipv6-address*>	配置DHCPv6 policy link-address

6.配置DHCPv6 Server接口。

步骤	命令	功能
1	inspur(config-dhcpv6)#**interface** <*interface-name*>	进入DHCPv6的接口配置模式
2	inspur(config-dhcpv6-if)#**server policy** <*policy-name*>	配置接口的DHCPv6 Server策略
3	inspur(config-dhcpv6-if)#**enable server-unicast**	使能DHCPv6接口单播标记

7.验证配置结果。

命令	功能
inspur#**show ipv6 dhcp server user** [**interface** <*interface-name*>][**summary**]	显示DHCPv6 Server上的客户端信息

8.维护DHCPv6。

命令	功能
inspur#**debug dhcpv6 server**	开启DHCPv6 Server的debug功能
inspur#**kick-off ipv6 dhcp server user** [[**interface** <*interface-name*>][**prefix** <*IPv6 prefix*>[**vrf-instance** <*vrf-name*>]][**address** <*IPv6 address*>[**vrf-instance** <*vrf-name*>]]	按照指定属性（接口/IPv6前缀/IPv6地址）踢掉Server上在线的用户

12.24.2 配置 DHCPv6 Relay

本节介绍DHCPv6 Relay的配置步骤和命令。

1.开启DHCPv6功能。

步骤	命令	功能
1	inspur(config)#**dhcp ipv6**	进入DHCPv6配置模式
2	inspur(config-dhcpv6)#**enable**	启用DHCPv6功能

2.配置DHCPv6 Relay Server Group。

步骤	命令	功能
1	inspur(config-dhcpv6)#**relay server group** <*number*>	在DHCPv6模式下进入DHCPv6 Relay Server Group配置模式
2	inspur(config-dhcpv6r-server-group)#**algorithm** {**normal** | **first** | **round-robin**}	配置DHCPv6 Relay Server使用策略，默认为**normal**方式转发
3	inspur(config-dhcpv6r-server-group)#**server** <*server-no*><*server-ipv6*>[**interface** <*interface-name*>][**master**]	配置DHCPv6 Relay Server相关信息
4	inspur(config-dhcpv6r-server-group)#**deadtime** <*time*>	配置DHCPv6 Relay Server在发送失败后，处于不可用状态的时间
5	inspur(config-dhcpv6r-server-group)#**description** <*descript-string*>	配置DHCP Relay Server描述内容
6	inspur(config-dhcpv6r-server-group)#**max-retry** <*limit-value*>	配置DHCPv6 Relay Server Group向外部DHCPv6 Server申请地址时发起重试的次数，默认10次

normal：表示向所有Server转发。

first：为主备方式。

round-robin：为负载均衡方式。

<*server-no*>：Server的编号，可配置范围：1~5。

[**master**]：配置主服务器。

3.配置DHCPv6 Relay Policy。

步骤	命令	功能
1	inspur(config-dhcpv6)#**relay policy** <*policy-name*>	在DHCPv6模式下进入DHCPv6 Relay Policy配置模式
2	inspur(config-dhcpv6r-policy-group)#**default server-group** <*server-group-number*>	配置DHCPv6 Relay Policy组默认绑定的DHCPv6 Relay Server Group

4.配置DHCPv6 Relay参数。

步骤	命令	功能
1	inspur(config-dhcpv6)#**relay intfid-format** {**china-tel** | **dsl-forum** | **user-configuration**}	配置DHCPv6 Relay的interface-id格式，缺省情况下直接取三层接口索引
2	inspur(config-dhcpv6)#**relay remote-id** <*enterprise-number*><*remote-id*>	配置Relay全局remote-id，可以不配，默认为没有该值

china-tel：中国电信格式。

dsl-forum：DSL论坛格式。

user-configuration：用户可配置模式的格式。

<*enterprise-number*>：企业号，可配置范围：0~4294967295。

<*remote-id*>：Remote-id字符串，长度：1~32个字符。

5.配置DHCPv6 Relay接口。

步骤	命令	功能
1	inspur(config-dhcpv6)#**interface** <*interface-name*>	进入DHCPv6的接口配置模式
2	inspur(config-dhcpv6-if-interface-name)#**relay agent** <*ipv6-address*>	配置接口的DHCPv6代理IP地址
3	inspur(config-dhcpv6-if-interface-name)#**relay interface-id** <*interface-id*>	配置接口的DHCPv6 Relay的interface-id，在格式为用户配置时有效 接口ID字符串，长度为1~16个字符，缺省为保持原有82选项，即透传
4	inspur(config-dhcpv6-if-interface-name)#**relay policy** <*policy-name*>	配置接口的DHCPv6 Relay策略

6.验证配置结果。

命令	功能
inspur#**show ipv6 dhcp relay user** [**interface** <*interface-name*>][**summary**]	显示DHCPv6 Relay上的客户端信息

7.维护DHCPv6。

命令	功能
inspur#**debug dhcpv6 relay**	开启DHCPv6 Relay的debug功能
inspur#**kick-off ipv6 dhcp relay user** [[**interface** <*interface-name*>][**prefix** <*IPv6 prefix*>[**vrf-instance** <*vrf-name*>]][**address** <*IPv6 address*>[**vrf-instance** <*vrf-name*>]]	按照指定属性（接口/IPv6前缀/IPv6地址）踢掉Relay上在线的用户

12.24.3 配置 DHCPv6 Client

本节介绍DHCPv6 Client的配置步骤和命令。

配置DHCPv6 Client。

步骤	命令	功能
1	inspur(config-interface-name)#**ipv6 dhcp client address** [<*rapid-commit*>]	获取IPv6地址
2	inspur(config-interface-name)#**ipv6 dhcp address** <*name*> **X:X::X:X/**<*1-128*>	配置DHCPv6 Client前缀
3	inspur(config-interface-name)#**ipv6 dhcp client pd** <*name*>[<*rapid-commit*>]	DHCPv6获取前缀功能

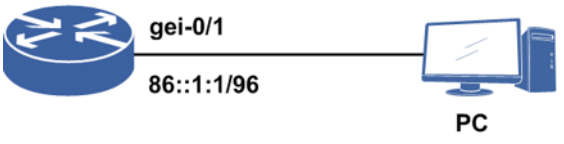
<*rapid-commit*>：快速协商。

12.24.4 DHCPv6 Server 配置实例

配置说明

如*图 12-56*所示，IR12000作为DHCPv6 Server使用，同时充当默认网关，PC通过DHCP动态获取IPv6地址接入网络。

图 12-56 DHCPv6 Server 配置实例拓扑图



IR12000全局下需要配置：IPv6 Addr-pool、DHCPv6 Pool、DHCPv6 Policy、打开DHCPv6功能开关；IR12000接口下需要配置IPv6地址、绑定DHCP Policy、DHCP Server模式。

配置思路

1.配置接口开启IPv6功能并配置v6地址。

2.配置IPv6地址池，IPv6地址池配置的是地址池范围等相关选项，地址池的范围要限制在一个网段内。

3.配置全局使能DHCPv6。

4.配置DHCPv6 POOL，DHCPv6 Pool需要绑定一个IPv6地址池，管理DNS、lease-time等设置。

5.配置DHCPv6 Policy，DHCPv6 Policy是策略选项，同一个名字下支持多个优先级别，用于策略管理。

6.配置DHCPv6 Server，在DHCPv6接口模式下配置为Server功能模式，并绑定刚配置的Policy。

配置过程

在IR12000上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 86::1:1/96
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit

/*配置IPv6地址池*/
inspur(config)#ipv6 addr-pool inspur
inspur(config-ipv6-addr-pool)#addr-range 86::1:2 86::1:10
inspur(config-ipv6-addr-pool)#exit

/*使能DHCPv6*/
inspur(config)#dhcp ipv6
inspur(config-dhcpv6)#enable

/*把IPv6地址池和DHCPv6 POOL绑定*/
inspur(config-dhcpv6)#pool inspur
inspur(config-dhcpv6-pool)#address-pool inspur
inspur(config-dhcpv6-pool)#exit

/*把DHCPv6 POOL和DHCPv6 POLICY绑定*/
inspur(config-dhcpv6)#policy inspur 1
inspur(config-dhcpv6-policy)#dhcpv6-pool inspur
inspur(config-dhcpv6-policy)#exit

/*接口下配置Server模式以及选定POLICY*/
inspur(config-dhcpv6)#interface gei-0/1
inspur(config-dhcpv6-if-gei-0/1)#mode server
inspur(config-dhcpv6-if-gei-0/1)#server policy inspur
inspur(config-dhcpv6-if-gei-0/1)#exit
```

配置验证

在IR12000上查看IPv6地址池的配置：

```
inspur#show ipv6 addr-pool configure inspur
PoolName     Lock  Begin     End       Vrf    Used     Free
inspur         no    86::1:2    86::1:10          0      15
RangeTotal:1
```

在IR12000上查看DHCP的配置：

```
inspur#show running-config dhcpv6
!<dhcpv6>
dhcp ipv6
  policy inspur 1
    dhcpv6-pool inspur
  $
  pool inspur
    address-pool inspur
  $
  interface gei-0/1
    mode server
    server policy inspur
  $
  enable
$
!</dhcpv6>
```

当PC用户通过DHCPv6申请到地址以后，可以在IR12000上查看用户信息：

```
inspur#show ipv6 dhcp server user
```

```
Client DUID: 000100014CFBF3DB001094000001
  IA NA: IA ID 0, T1 50000, T2 80000
    Address: 86::1:2
       preferred lifetime 1000, valid lifetime 1000
       expires at 11:08:10 12/07/2010 (994 seconds)
```

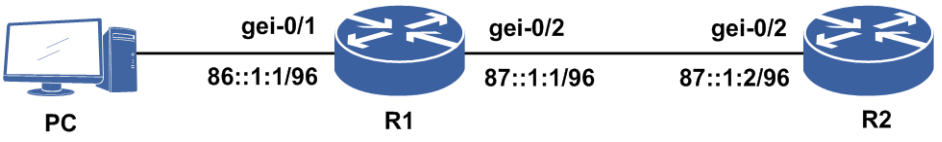
12.24.5 DHCPv6 Relay 配置实例

配置说明

当DHCPv6客户机和服务器不在同一网络中时，需要直连用户端的路由器充当DHCPv6中继。

如*图 12-57*所示，R1上启用DHCPv6中继功能，由一台单独的服务器R2提供DHCPv6服务器的功能。在需要DHCPv6服务的主机比较多的情况下通常采用这种做法。

图 12-57 DHCPv6 Relay 配置实例拓扑图



R1接口下需要配置：IPv6地址、DHCPv6 Server地址、DHCPv6 Relay模式；

R2接口下需要配置：IPv6地址、绑定DHCPv6 Policy、DHCPv6 Server模式；

R2全局下需要配置：使能DHCPv6、IPv6地址池、DHCPv6 Pool、DHCPv6 Policy，指向R1接口网段的路由。

配置思路

1.Relay接口上配置IPv6地址并使能DHCPv6。

2.Relay上配置Relay Server Group，在Relay Policy中绑定此Group。

3.Relay和PC相连接口上配置模式和Relay Agent。

4.Server上配置基本和之前配置Server组网中类似，只是需要在DHCPv6 Policy中指定Relay接口的IPv6地址。

5.Server上需要配置一条到Relay接口网段的静态路由。

配置过程

R1上的配置如下：

```
/*配置接口*/
R1(config)#interface gei-0/1
R1(config-if-gei-0/1)#ipv6 enable
R1(config-if-gei-0/1)#ipv6 address 86::1:1/96
R1(config-if-gei-0/1)#no shutdown
R1(config-if-gei-0/1)#exit
R1(config)#interface gei-0/2
```

```
R1(config-if-gei-0/2)#ipv6 enable
R1(config-if-gei-0/2)#ipv6 address 87::1:1/96
R1(config-if-gei-0/2)#no shutdown
R1(config-if-gei-0/2)#exit

/*使能DHCPv6功能*/
R1(config)#dhcp ipv6
R1(config-dhcpv6)#enable

/*指定Server*/
R1(config-dhcpv6)#relay server group 1
R1(config-dhcpv6-server-group)#server 1 87::1:2
R1(config-dhcpv6-server-group)#exit

/*配置Relay Policy*/
R1(config-dhcpv6)#relay policy 1
R1(config-dhcpv6-policy-group)#default server-group 1
R1(config-dhcpv6-policy-group)#exit

/*配置接口的DHCP模式和其他属性/*
R1(config-dhcpv6)#interface gei-0/1
R1(config-dhcpv6-if-gei-0/1)#mode relay
R1(config-dhcpv6-if-gei-0/1)#relay agent 86::1:1
R1(config-dhcpv6-if-gei-0/1)#relay policy 1
R1(config-dhcpv6-if-gei-0/1)#exit
R1(config-dhcpv6)#exit
```

R2上的配置如下：

```
/*配置接口*/
R2(config)#interface gei-0/2
R2(config-if-gei-0/2)#ipv6 enable
R2(config-if-gei-0/2)#ipv6 address 87::1:2/96
R2(config-if-gei-0/2)#no shutdown
R2(config-if-gei-0/2)#exit

/*配置IPv6地址池*/
R2(config)#ipv6 addr-pool inspur1
R2(config-ipv6-addr-pool)#addr-range 86::1:10 86::1:50
R2(config-ipv6-addr-pool)#exit

/*使能DHCPv6*/
R2(config)#dhcp ipv6
R2(config-dhcpv6)#enable

/*把IPv6地址池和DHCP POOL绑定*/
R2(config-dhcpv6)#pool inspur1
R2(config-dhcpv6-pool)#address-pool inspur1
R2(config-dhcpv6-pool)#exit

/*把DHCP POOL和DHCP POLICY绑定*/
R2(config-dhcpv6)#policy inspur1 1
R2(config-dhcpv6-policy)#dhcpv6-pool inspur1
R2(config-dhcpv6-policy)#link-address 86::1:1
R2(config-dhcpv6-policy)#exit

/*配置接口的DHCP模式*/
R2(config-dhcpv6)#interface gei-0/2
R2(config-dhcpv6-if-gei-0/2)#mode server
R2(config-dhcpv6-if-gei-0/2)#server policy inspur1
R2(config-dhcpv6-if-gei-0/2)#exit

/*配置静态路由*/
R2(config)#ipv6 route 86::/96 87::1:1
```

配置验证

在R1上查看DHCPv6配置：

```
R1#show running-config dhcpv6
!<dhcpv6>
dhcp ipv6
  relay policy 1
    default server-group 1
  $
  relay server group 1
    server 1 87::1:2
  $
  interface gei-0/1
    mode relay
    relay agent 86::1:1
    relay policy 1
  $
  enable
$
!</dhcpv6>
```

在R2上查看IPv6地址池的配置：

```
R2#show ipv6 addr-pool configure inspur1
PoolName      Lock  Begin      End         Vrf    Used    Free
inspur1         no    86::1:10   86::1:50           0       65
RangeTotal:1
```

在R2上查看DHCPv6配置：

```
R2#show running-config dhcpv6
!<dhcpv6>
dhcp ipv6
  policy inspur1 1
  dhcpv6-pool inspur1
  link-address 86::1:1
  $
  pool inspur1
    address-pool inspur1 lifetime 10000 10000
  $
  interface gei-0/2
    mode server
    server policy inspur1
  $
  enable
$
!</dhcpv6>
```

当PC用户通过DHCPv6申请到地址以后，可以在R2上查看用户信息：

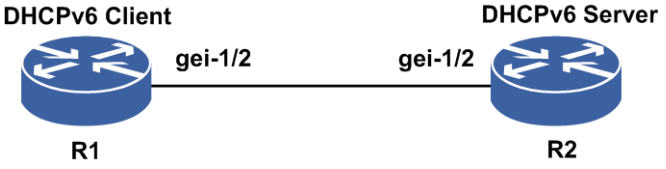
```
R2#show ipv6 dhcp server user
Client DUID: 000100014CFBF3DB001094000001
  IA NA: IA ID 0, T1 50000, T2 80000
    Address: 86::1:10
        preferred lifetime 10000, valid lifetime 10000
        expires at 13:18:21 12/08/2010 (9995 seconds)
Client DUID: 000100014CFBF3DB001094000002
  IA NA: IA ID 0, T1 50000, T2 80000
    Address: 86::1:11
        preferred lifetime 10000, valid lifetime 10000
        expires at 13:18:20 12/08/2010 (9994 seconds)
Client DUID: 000100014CFBF3DB001094000003
  IA NA: IA ID 0, T1 50000, T2 80000
    Address: 86::1:12
        preferred lifetime 10000, valid lifetime 10000
        expires at 13:18:20 12/08/2010 (9994 seconds)
```

12.24.6 DHCPv6 Client 配置实例

配置说明

如*图 12-58*所示，R2作为DHCPv6 Server使用，同时作为默认网关，R1通过DHCP动态获取IPv6地址接入网络。

图 12-58 DHCPv6 Client 配置实例拓扑图



配置思路

1.R2完成DHCPv6 Server的配置。

2.R1开启DHCPv6 Client功能。

配置过程

R2上的配置如下：

```
R2(config)#interface gei-1/2
R2(config-if-gei-1/2 )#no shutdown
R2(config-if-gei-1/2 )#ipv6 enable
R2(config-if-gei-1/2 )#ipv6 address 11:11::1:1/112
R2(config-if-gei-1/2 )#exit
R2(config)#ipv6 prefix-pool inspur1
R2(config-ipv6-prefix-pool)#prefix-delegation 11:11::12:0/112 112
R2(config-ipv6-prefix-pool)#exit

R2(config)#dhcp ipv6
R2(config-dhcpv6)#enable
R2(config-dhcpv6)#pool inspur
R2(config-dhcpv6-pool)#prefix-lifetime 60 60
R2(config-dhcpv6-pool)#prefix-pool inspur1
R2(config-dhcpv6-pool)#exit
R2(config-dhcpv6)#policy inspur 1
R2(config-dhcpv6-policy)#dhcpv6-pool inspur
R2(config-dhcpv6-policy)#exit
R2(config-dhcpv6)#interface gei-1/2
R2(config-dhcpv6-if-gei-1/2 )#mode server
R2(config-dhcpv6-if-gei-1/2 )#server policy inspur
```

R1上的配置如下：

```
R1(config)#interface gei-1/2
R1(config-if-gei-1/2 )#no shutdown
R1(config-if-gei-1/2 )#ipv6 enable
R1(config-if-gei-1/2 )#ipv6 dhcp address inspur ::110/112     /*配置后缀*/
R1(config-if-gei-1/2 )#ipv6 dhcp client pd inspur rapid-commit /*获取IPv6前缀*/
```

配置验证

R1上使用命令**show ipv6 interface**<*interface-name*>查看接口信息：

```
R1(config)#show ipv6 interface gei-1/2
Interface gei-1/2  is up, line protocol is up
  IPv6 is enabled, Hardware is Gigabit Ethernet
  Hardware address is 000d.0d00.000c
  Index 17
  Bandwidth 1000000 Kbits
  IPv6 MTU 1500 bytes
  inet6 fe80::20d:dff:fe00:c/10
  inet6 11:11::12:110/112
  ND DAD is enabled, number of DAD attempts: 3
  ND reachable time is 30000 milliseconds
```

如上所示，客户端已经获取到一个IPv6前缀加自己配置的后缀而成的IPv6地址：11:11::12:110/112。

也可在服务器R2上查看分配出去的IPv6地址和前缀。

```
R2(config)#show ipv6 dhcp server user
Client DUID: 00030001000D0D00000C
  IA PD: IA ID 17, T1 30, T2 48
    Prefix: 11:11::12:0/112
      preferred lifetime 60, valid lifetime 60
      expires at 23:52:49 11/01/2000 (59 seconds)
```

13 NAT

13.1 基本 NAT

NAT是一种地址转换技术，通常用来解决如下几个问题。

•IPv4地址匮乏问题

NAT技术通过将私网地址转换为公网地址，可以较好地解决IPv4的网络地址匮乏问题。

•网络安全问题

NAT技术可以有效地将私网地址对外隐藏，通过在NAT出口路由器上实施安全措施，降低网络安全配置难度，减少来自Internet上的网络攻击。

•私网地址整合

RFC推荐的私网地址方案存在重复使用相同私网IP地址的问题，NAT技术可以在两个重复使用相同私网地址的网络间进行转换，使两个私网网络能互相访问。

•IPv6过渡问题

在IPv6的过渡初期，可解决保持IPv4的后向兼容性问题，使用户能够在IPv6的接入环境中使用IPv4的应用与服务。

13.1.1 配置启用 NAT

本节介绍IR12000智能路由器进入NAT配置模式的命令。

配置NAT配置模式。

命令	功能
`inspur(config)#cgn`	进入NAT配置模式 NAT的相关功能需要在NAT配置模式下配置

13.1.2 配置地址池

本节介绍PAT地址池和NAT地址池的配置步骤和命令。

1.配置PAT地址池。

i.进入NAT配置模式，配置PAT地址池。

步骤	命令	功能
1	inspur(config)#**cgn**	进入NAT配置模式
2	inspur(config-cgn)#**cgn-pool** <*pool-name*> **poolid** <*pool-id*> **mode pat**	配置PAT地址池

<*pool-name*>：地址池名称，范围1~31个字符。

<*pool-id*>：地址池ID，范围0~1999。

ii.配置PAT地址池属性。

命令	功能
inspur(config-cgn-patpool)#**description** <*description*>	配置地址池描述，长度1~63字节
inspur(config-cgn-patpool)#**max-ports-per-address** <*value*>	配置一个公网地址可以使用的端口地址转换数，取值范围1~65535，默认值65535
inspur(config-cgn-patpool)#**allowed-port-range** <*start-port*><*end-port*>	配置允许使用的端口范围
inspur(config-cgn-patpool)#**port-range-enable** <*port-range-size*>	配置开启端口块功能并配置大小，取值范围：[1024~65536] 区间内2的N次方
inspur(config-cgn-patpool)#**bind-vrf** <*vrf-name*>	配置地址池绑定VRF
inspur(config-cgn-patpool)#**section** <*section-num*>{<*start-ip*>[<*end-ip*>]|<*IP/mask*>| **interface** <*interface-name*>}	配置地址池中地址范围
inspur(config-cgn-patpool)#**well-known-port-forbidden** {**enable** [<*start-port*>]|**disable**}	配置禁止地址池中知名端口号是否转换开关，默认disable，<start-port>：使能知名端口禁止后，允许使用的起始端口号，取值范围<64-8912>，必须是64的整数倍

<*section-num*>：用来标识子地址池，配置范围1~64。

iii.配置PAT地址池告警。

命令	功能
inspur(config-cgn-patpool)#**alarm-threshold port-range** <*percent*>	配置端口块中端口使用率的告警阈值，范围1~100，默认值80

2.配置NAT地址池。

i.进入NAT配置模式，配置NAT地址池。

步骤	命令	功能
1	inspur(config)#**cgn**	进入NAT配置模式
2	inspur(config-cgn)#**cgn-pool** <*pool-name*> **poolid** <*pool-id*> **mode nat**	配置NAT地址池

ii.配置NAT地址池属性。

命令	功能
inspur(config-cgn-natpool)#**description** <*description*>	配置地址池描述，长度1~63字节
inspur(config-cgn-natpool)#**bind-vrf** <*vrf-name*>	配置地址池绑定VRF
inspur(config-cgn-natpool)#**section** <*section-num*>{**start-ip** [<*end-ip*>]| **IP/mask**}	配置地址池中地址范围

<*section-num*>：用来标识子地址池，配置范围1~64。

13.1.3 配置域

本节介绍NAT域的配置步骤和命令。

1.进入NAT配置模式，创建域。

步骤	命令	功能
1	inspur(config)#**cgn**	进入NAT配置模式
2	inspur(config-cgn)#**domain** <*domain-name*><*domain-id*> **type** {**standalone**	**sr**	**bras** }{**ipv6-issued**	**ipv4-issued**}	创建并进入域配置模式

type：域类型，产品形态选择**standalone**、**sr**或**bras**，技术形态选择**ipv6-issued**或**ipv4-issued**。

2.配置域属性。

命令	功能
inspur(config-cgn-domain)#**description** <*description*>	配置域描述，长度1~63字节
inspur(config-cgn-domain)#**dynamic source rule-id** <*rule-id*>{**ipv4-list**	**ipv6-list**}<*aclname*>{**deny**	**drop**	**(permit pool** <*pool-name*>[<*interface-name*>]**)**}	配置动态映射规则

命令	功能
inspur(config-cgn-domain)#**max-translations** {**per-ipv4**|**per-softwire**|**per-subscriber**}{**tcp**|**udp**|**icmp**|**nat**|**all**} {[**dynamic** <*max-trans*>]}[**time-range** <*max-trans*>{[**dynamic** <*max-trans*>]}]	配置域下每个IPv4地址/每个软线/每个用户的最大转换条目数
inspur(config-cgn-domain)#**static source rule-id** <*rule-id*>{**softwire** <*cpe-ipv6-address*><*aftr-ipv6-address*><*local-ip*>| **vrf** <*vrf-name*><*local-ip*>| **public** <*local-ip*>| **cpe-ipv6-address** <*cpe-ipv6-address*> **nat64-prefix** <*nat64-prefix-address*>}{<*local-port*><*global-ip*><*global-port*>{**tcp** | **udp**}|<*global-ip*>}[**time-range** <*time-range-name*>]	配置静态映射规则
inspur(config-cgn-domain)#**dns-exclude-session-limit**{**enable**|**disable**}	配置DNS
inspur(config-cgn-domain)#**max-static-rule-num** <*rule-num*>	配置静态规则数

<*rule-id*>：静态NAT规则标识号，取值范围1~2000。

<*cpe-ipv6-address*>：用户CPE（Customer Premise Equipment）IPv6地址。

<*nat64-prefix-address*>：NAT64前缀地址。

<*local-ip*>：私网源IPv4地址。

<*global-ip*>：做NAT转换后的公网IPv4地址，此地址需为地址池里的地址。

<*local-port*>：私网源端口号，若选择端口号则为PAT映射方式，否则为NAT方式，取值范围1~65535。

<*global-port*>：做NAT后的公网端口号，若选择端口号则为PAT映射方式，否则为NAT方式，取值范围1~65535。

13.1.4 配置策略

本节介绍NAT策略的配置步骤和命令。

1.配置用户ICMP策略映射模板。

步骤	命令	功能
1	inspur(config-cgn-domain)#**icmp-policy**	进入ICMP策略配置模式
2	inspur(config-cgn-domain-icmp-policy)#**mapping-mode** {**endpoint-independent** | **address-dependent** }	配置映射模式，缺省值**endpoint-independent**
	inspur(config-cgn-domain-icmp-policy)#**filtering-mode** {**endpoint-independent** | **address-dependent**}	配置过滤模式，缺省值**endpoint-independent**

步骤	命令	功能
3	inspur(config-cgn-domain-icmp-policy)#**refreshing-mode** {**both-bounds**| **outbound**| **inbound**}	配置ICMP条目刷新策略，缺省为**outbound**
4	inspur(config-cgn-domain-icmp-policy)#**timeout** <*aging-time*>	配置ICMP映射条目老化时间，取值范围1~7200，单位：秒，缺省值60秒

address-dependent：地址相关，即NAT映射或过滤取决于内部源地址、内部源端口以及目的地址。

endpoint-independent：端点无关，即NAT映射或过滤只取决于内部源地址和内部源端口。

2.配置用户UDP策略映射模板。

步骤	命令	功能
1	inspur(config-cgn-domian)#**udp-policy**	进入UDP策略配置模式
2	inspur(config-cgn-domian-udp-policy)#**mapping-mode** {**endpoint-independent** | **address-dependent** | **address-and-port-dependent**}	配置映射模式，缺省值**endpoint-independent**
3	inspur(config-cgn-domian-udp-policy)#**filtering-mode** {**endpoint-independent** | **address-dependent** | **address-and-port-dependent**}	配置过滤模式，缺省值**endpoint-independent**
4	inspur(config-cgn-domian-udp-policy)#**timeout unwell-known-port** <*aging-time*>	配置UDP非知名端口映射条目的老化时间，取值范围1~7200，单位：秒，缺省值180秒
	inspur(config-cgn-domian-udp-policy)#**timeout well-known-port** <*aging-time*>	配置UDP知名端口映射条目的老化时间，取值范围1~7200，单位：秒，缺省值180秒
5	inspur(config-cgn-domian-udp-policy)#**refreshing-mode** {**both-bounds** | **outbound** | **inbound** }	配置UDP条目刷新策略，缺省为**outbound**
6	inspur(config-cgn-domian-udp-policy)#**allowed-port-range** <*start-port*> <*end-port*>	配置用户使用的端口范围
7	inspur(config-cgn-domian-udp-policy)#**forbidden-port-range** <*start-port*> <*end-port*>	配置用户禁止使用的端口范围
8	inspur(config-cgn-domian-udp-policy)#**port-parity-preserve** {**enable** | **disable**}	开启/关闭保持端口奇偶性配置，缺省为**disable**
9	inspur(config-cgn-domian-udp-policy)#**port-randomization** {**enable** | **disable**}	开启/关闭端口随机性配置，缺省为**enable**

mapping-mode 命令的参数说明如下：

- **address-and-port-dependent**：映射模式与地址和端点相关，即NAT映射取决于内

部源地址、内部源端口、目的地址以及目的端口。

- **address-dependent**：映射模式与地址相关，即NAT映射取决于内部源地址、内部源端口以及目的地址。
- **endpoint-independent**：映射模式与端点无关，即NAT映射只取决于内部源地址和内部源端口。

filtering-mode 命令的参数说明如下：

- **address-and-port-dependent**：过滤模式与地址和端点相关，即NAT过滤不到内部地址X:x（地址+端口）的报文。
- **address-dependent**：过滤模式与地址相关，即NAT过滤不到内部地址的报文。
- **endpoint-independent**：过滤模式与端点无关，即NAT只过滤不到内部地址和端口的报文。

refreshing-mode 命令的参数说明如下：

- **both-bounds**：Inbound和outbound双向流量均能触发映射条目刷新。
- **outbound**：仅outbound流量能够触发映射条目刷新。
- **inbound**：仅inbound流量能够触发映射条目刷新。

3.配置用户TCP策略映射模板。

步骤	命令	功能
1	inspur(config-cgn-doamin)#**tcp-policy**	进入TCP策略配置模式
2	inspur(config-cgn-doamin-tcp-policy)#**mapping-mode** {**endpoint-independent** | **address-dependent** | **address-and-port-dependent**}	配置映射模式，缺省为**endpoint-independent**
3	inspur(config-cgn-doamin-tcp-policy)#**filtering-mode** {**endpoint-independent** | **address-dependent** | **address-and-port-dependent**}	配置过滤模式，缺省为**endpoint-independent**
4	inspur(config-cgn-doamin-tcp-policy)#**timeout unwell-known-port** {[**tcp** <*tcp-time*>][**tcp-syn** <*tcp-syn-time*>][**tcp-fin-rst** <*tcp-fin-rst-time*>]}	配置TCP非知名端口映射条目的老化时间
	inspur(config-cgn-doamin-tcp-policy)#**timeout well-known-port** {[**tcp** <*tcp-time*>][**tcp-syn**<*tcp-syn-time*>][**tcp-fin-rst** <*tcp-fin-rst-time*>]}	配置TCP知名端口映射条目的老化时间
5	inspur(config-cgn-doamin-tcp-policy)#**refreshing-mode** {**both-bounds**| **outbound**| **inbound**}	配置TCP条目刷新策略，缺省为**outbound**
6	inspur(config-cgn-doamin-tcp-policy)#**allowed-port-range** <*start-port*><*end-port*>	配置用户使用的端口范围
7	inspur(config-cgn-doamin-tcp-policy)#**forbidden-port-range** <*start-port*> <*end-port*>	配置用户禁止使用的端口范围
8	inspur(config-cgn-doamin-tcp-policy)#**po**	开启/关闭保持端口奇偶性配

步骤	命令	功能
	rt-parity-preserve {**enable** | **disable**}	置，缺省为**disable**
9	inspur(config-cgn-doamin-tcp-policy)#**port-randomization** {**enable** | **disable**}	开启/关闭端口随机性配置，缺省为**enable**

<*tcp-time*>：TCP数据报文映射条目超时时间，取值范围1~7200，单位：秒，缺省值120秒。

<*tcp-syn-time*>：TCP-syn报文映射条目超时时间，取值范围1~7200，单位：秒，缺省值60秒。

<*tcp-fin-rst-time*>：TCP-fin报文映射条目超时时间，取值范围1~7200，单位：秒，缺省值120秒。

4.配置用户地址分配策略。

步骤	命令	功能
1	inspur(config-cgn-domain)#**address-policy**	进入地址分配策略配置模式
2	inspur(config-cgn-domain-addr-policy)#**allocate-diff-address** <*diff-address-name*>{**tcp** <*tcp-port*>| **udp** <*udp-port*>| **icmp**}	配置不同地址策略，对于用户的ICMP和DNS请求尽量分配不同的公网地址
3	inspur(config-cgn-domain-addr-policy)#**same-address-allocate**{ **for-same-ipv4**| **for-same-softwire**| **for-same-user**}{**must**| **random**|**try-best**}	配置相同地址策略

5.配置用户NAT策略映射模板。

步骤	命令	功能
1	inspur(config-cgn-domain)#**nat-policy**	进入NAT策略配置模式
2	inspur(config-cgn-domain-nat-policy)#**mapping-mode** {**endpoint-independent** | **address-dependent**}	配置映射模式，缺省为**endpoint-independent**
	inspur(config-cgn-domain-nat-policy)#**filtering-mode** {**endpoint-independent** | **address-dependent**}	配置过滤模式，缺省为**endpoint-independent**
	inspur(config-cgn-domain-nat-policy)#**refreshing-mode** {**both-bounds** | **outbound** | **inbound**}	配置NAT条目刷新策略，缺省为**outbound**
	inspur(config-cgn-domain-nat-policy)#**timeout** <*aging-time*>	配置NAT映射条目老化时间，取值范围1~7200，单位：秒，缺省值120秒

13.1.5 配置高级业务

本节介绍NAT高级业务的配置步骤和命令。

1.进入NAT高级业务配置模式。

步骤	命令	功能
1	inspur(config)#**cgn**	进入NAT配置模式
2	inspur(config-cgn)#**advanced-service**	进入高级业务模式

2.配置NAT高级业务。

步骤	命令	功能
1	inspur(config-cgn-adv-srv)#**enable**	开启高级NAT服务功能
	inspur(config-cgn-adv-srv)#**tcp-mss-clamping** {**disable** | **new-mss-value** {**auto** |<*tcp-mss-value*>}}	配置**tcp-mss-clamping**功能并设置MSS值，取值范围：64~9216，单位：bytes 缺省该功能为**disable**
	inspur(config-cgn-adv-srv)#**tcp-state-tracking** {**enable** | **disable**}	配置**tcp-state-tracking**功能，缺省为**disable**
2	inspur(config-cgn-adv-srv)#**alg** {[**ftp** {**enable** | **disable**}],[**icmp** {**enable** | **disable**}],[**dns** {**enable** | **disable**}],[**rtsp** {**enable** | **disable**}],[**h323** {**enable** | **disable**}],[**sip** {**enable** | **disable**}],[**pptp** {**enable** | **disable**}]}	配置ALG功能，缺省各协议的ALG功能为**disable**
3	inspur(config-cgn-adv-srv)#**protocol-session-timeout** <*description*>{**tcp** | **udp**}<*destination-port*><*timeout-value*>	配置TCP/UDP协议端口号和老化时间： 协议端口号取值范围：1~65535 老化时间取值范围：1~7200，单位：秒

13.1.6 配置日志

本节介绍NAT日志的配置步骤和命令。

1.开启NAT日志功能。

步骤	命令	功能
1	inspur(config-cgn)#**log**	进入NAT日志配置模式

步骤	命令	功能
2	inspur(config-cgn-log)#**enable**	开启日志功能

2.配置NAT日志相关参数。

命令	功能
inspur(config-cgn-log)#**buffer-size** <*size*>	配置日志缓存大小，取值范围为10~64，单位：MB，缺省为16
inspur(config-cgn-log)#**destination** {**local** | **syslog**}	配置日志存储的地点，缺省为**local** **local**：日志存放在设备硬盘中 **syslog**：日志信息上传Syslog服务器
inspur(config-cgn-log)#**resource-exhaust-action** {**stop-cgn-service** | **stop-logging**}	配置资源耗尽时的处理方式，缺省为**stop-logging** **stop-cgn-service**：停止NAT功能 **stop-logging**：停止发送日志功能
inspur(config-cgn-log)#**logging-translation-when** {**created** | **deleted** | **created-and-deleted**}	配置条目转换产生日志的时机 **created**：生成映射条目时产生日志 **deleted**：删除映射条目时产生日志 **created-and-deleted**：生成和删除时都产生日志
inspur(config-cgn-log)#**translation-logging-fields syslog** {[**vrf-name**],[**destination-ip**],[**destination-port**],[**inbound-packets**],[**outbound-packets**],[**inbound-bytes**],[**outbound-bytes**]}	配置生成SYSLOG日志的NAT条目字段，默认关闭所有字段
inspur(config-cgn-log)#**format** {**binary** | **text**}	配置日志格式，缺省为**text**
inspur(config-cgn-log)#**log-style**{**style1**|**style2**}	配置日志规范方式，**style1**为电信方式，**style2**为联通方式
inspur(config-cgn-log)#**logging-portrange-detail** {**disable** | **enable**}	配置开启/关闭portrange明细日志开关，缺省为**disable**
inspur(config-cgn-log)#**logging-portrange-when** {[**created**][**deleted**][**first-session-create**][**last-session-delete**]}	配置portrange用户端口块日志生成的时机

3.维护NAT日志。

命令	功能
inspur(config-cgn-log)#**stop-service-on-err** {**enable** | **disable**}	配置开启/关闭NAT日志通道故障则停止NAT业务，缺省为**disable**

13.1.7 配置告警

本节介绍NAT告警功能的配置步骤和命令。

1.开启NAT告警开关。

步骤	命令	功能
1	inspur(config-cgn)#**alarm**	进入告警配置模式
2	inspur(config-cgn-alarm)#**enable**	开启告警开关

2.配置NAT告警相关参数。

步骤	命令	功能
1	inspur(config-cgn-alarm)#**alarm-threshold translations** <*percent*>	配置单个SP-CPU最大转换条目数的某一百分比则产生告警
	inspur(config-cgn-alarm)#**alarm-threshold resource** <*percent*>	配置单个SP-CPU的IP使用率达到某一百分比则产生告警

13.1.8 配置 NAT 控制面安全

本节介绍NAT控制面安全的配置步骤和命令。

配置NAT控制安全相关参数。

命令	功能
inspur(config)#**control-plane-security**	进入控制面安全配置模式
inspur(config-cps)#**interface** <*interface-name*>	进入控制面安全接口配置模式
inspur(config-cps-if-interface-name)#**flow limit** | **flowtype nat-alg rate-limit** <*speed-value*> **quota-limit** <*speed-value*>	为指定接口的nat-alg报文配置上送速率以及quota值 **rate-limit**<*speed-value*>：端口上送流速率值，范围0~85000，单位pps，开通NAT业务，建议配置85000 **quota-limit**<*speed-value*>：配置quota值，范围0~85000，开通NAT业务，建议配置85000
inspur(config-cps-if-interface-name)#**flow limit** | **flowtype nat-nonat rate-limit** <*speed-value*> **quota-limit** <*speed-value*>	为指定接口的nat-nonat报文配置上送速率以及quota值 **rate-limit**<*speed-value*>：端口上送流速率值，范围0~85000，单位pps，开通NAT业务，建议配置

命令	功能
	85000 **quota-limit**<*speed-value*>：配置quota值，范围0~85000，开通NAT业务，建议配置85000

提示：

NAT业务由于瞬间上送到控制面CPU处理的新建条目数较多，且存在控制面安全策略，会限制新建上送CPU处理的条目数，这样会导致新建NAT条目的报文丢弃，从而影响NAT业务。因此对于开通NAT业务的设备，需要适当放开NAT业务的控制面限制。

13.2 SR NAT44

SR NAT44在SR设备上实现IPv4到IPv4地址的转换。企业不想让外部网络用户知道自己的网络内部结构，可以通过NAT44将内部网络与外部Internet隔离开。一个企业申请的合法公网IP地址很少，而内部网络用户很多，可以通过NAT44功能实现多个用户同时共用一个合法公网IP与外部Internet进行通信。

13.2.1 配置 SR NAT44

本节介绍SR NAT44用户的配置步骤和命令。

1.配置NAT44。

步骤	命令	功能
1	`inspur(config)#`**cgn**	进入NAT配置模式
2	`inspur(config-cgn)#`**subscriber ipv4** {**public** | **vrf** <*vrf-name*>} **subscriber-id** <*subscriber-id*> **nat-domain** <*nat-domain-id*>	配置VRF用户，并进入用户配置模式
3	`inspur(config-cgn-sub)#`**interface** <*interface-name*>	在VRF用户下绑定接入接口

public：配置默认的VRF用户，即VPNID为0的用户。

2.验证配置结果。

查看NAT44相关配置信息：

命令	功能
`inspur#`**show cgn-pool** [**pool-name** <*pool-name*>]	查看地址池配置信息
`inspur#`**show cgn domain** [**domain-name** <*domain-name*>]	查看域配置信息

命令	功能
inspur#**show cgn instance** {**summary**|**verbose**}	查看NAT全部信息

查看NAT条目：

命令	功能
inspur#**show cgn translations all-sessions**	显示所有NAT条目信息
inspur#**show cgn translations protocol**	显示指定协议类型的详细NAT条目信息
inspur#**show cgn translations translation-type**	显示指定转换类型的详细NAT条目信息
inspur#**show cgn translations global-ip**	显示指定公网地址的详细NAT条目信息
inspur#**show cgn translations local-ip**	显示指定私网地址的详细NAT条目信息

3.维护NAT条目。

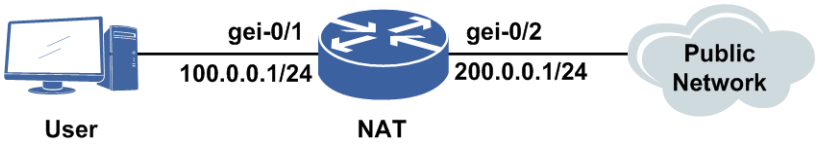
命令	功能
inspur#**clear cgn translations all-sessions**	清除所有转换条目
inspur#**clear cgn translations protocol**	清除指定协议类型的详细NAT条目
inspur#**clear cgn translations translation-type**	清除指定转换类型的详细NAT条目
inspur#**clear cgn translations global-ip**	清除指定公网地址的详细NAT条目
inspur#**clear cgn translations local-ip**	清除指定私网地址的详细NAT条目

13.2.2 静态 NAT 转换 NAT44 配置实例

配置说明

如*图 13-1*所示，PC上配置私网地址，通过IR12000智能路由器进行静态NAT转换后，可以访问Internet。

图 13-1 静态 NAT 转换 NAT44 配置实例组网图



配置思路

1.配置接口地址。

2.配置NAT地址池。

3.配置域并在域中配置静态映射规则。

4.配置用户，将NAT域绑定在和PC相连的接口上。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ip address 100.0.0.1 255.255.255.0
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip address 200.0.0.1 255.255.255.0
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit

inspur(config)#ipv4-access-list test
inspur(config-ipv4-acl)#rule permit any
inspur(config-ipv4-acl)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool test poolid 1 mode nat  /*配置地址池*/
inspur(config-cgn-natpool)#section 1 1.2.3.1 1.2.3.10
inspur(config-cgn-natpool)#exit
inspur(config-cgn)#domain 1 1 type sr ipv4-issued
inspur(config-cgn-domain)#static source rule-id 1 public 100.0.0.2 1.2.3.1
/*配置静态规则*/
inspur(config-cgn-domain)#exit
inspur(config-cgn)#subscriber ipv4 public subscriber-id 1 nat-domain 1
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
inspur(config-cgn)#exit
inspur(config)#ip route 0.0.0.0 0.0.0.0 200.0.0.2
```

配置验证

查看静态NAT条目信息：

```
inspur(config)#show cgn translations all-sessions
================================================================================
Subscriber
    Pro    Type    Inside Local         Inside Global        Destination
================================================================================
     ---   sta     100.0.0.2            1.2.3.1              *:*
```

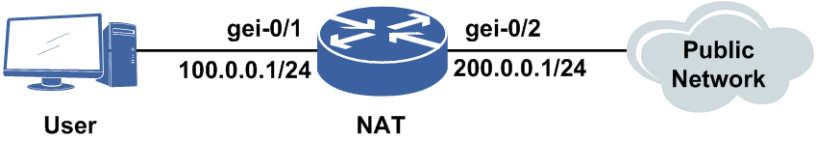
```
--------------------------------------------------------------------------------
Loading data from MPFU-8/0...
================================================================================
```

13.2.3 动态 PAT 转换 NAT44 配置实例

配置说明

如*图 13-2*所示，PC上配置私网地址，通过IR12000智能路由器进行动态PAT转换后，可以访问Internet。

图 13-2 动态 PAT 转换 NAT44 配置实例组网图



配置思路

1.配置接口地址。

2.配置PAT地址池。

3.配置域并在域中配置动态映射规则。

4.配置用户，将NAT域绑定在和PC相连的接口上。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ip address 100.0.0.1 255.255.255.0
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip address 200.0.0.1 255.255.255.0
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit

inspur(config)#ipv4-access-list test
inspur(config-ipv4-acl)#rule permit any
inspur(config-ipv4-acl)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool test poolid 1 mode pat  /*配置地址池*/
inspur(config-cgn-patpool)#section 1 1.2.3.1 1.2.3.10
inspur(config-cgn-patpool)#exit
inspur(config-cgn)#domain 1 1 type sr ipv4-issued
inspur(config-cgn-domain)#dynamic source rule-id 1 ipv4-list test permit
 pool test  /*这里配置的是动态ACL规则，也可以配置静态规则*/
inspur(config-cgn-domain)#exit
inspur(config-cgn)#subscriber ipv4 public subscriber-id 1 nat-domain 1
inspur(config-cgn-sub)#interface gei-0/1
```

```
inspur(config-cgn-sub)#exit
inspur(config)#ip route 0.0.0.0 0.0.0.0 200.0.0.2
```

配置验证

查看动态PAT条目信息：

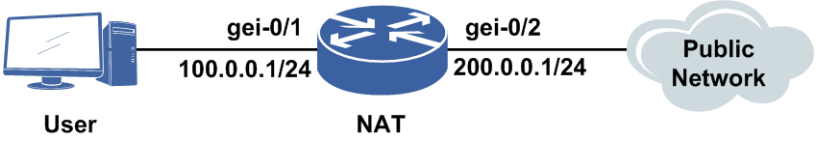
```
inspur(config)#show cgn translations all-sessions
=========================================================================
Subscriber
Pro  Type    Inside Local         Inside Global      Destination
=========================================================================
Loading data from MPFU-8/0...
=========================================================================
UDP  dyn     100.0.0.2:1          1.2.3.1:2112          *:*
-------------------------------------------------------------------------
```

13.2.4 复用出接口 NAT44 配置实例

配置说明

如*图 13-3*所示，用户主机通过私网地址连接到IR12000智能路由器，经过地址转换后访问外部的IPv4网络。转换后的公网地址为出接口gei-0/2的地址，以静态PAT为例。

图 13-3 复用出接口 NAT44 配置实例组网图



配置思路

1.配置接口地址。

2.配置PAT地址池，绑定出接口。

3.配置域并在域中配置静态映射规则。

4.配置用户，将NAT域绑定在和PC相连的接口上。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ip address 100.0.0.1 255.255.255.0
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip address 200.0.0.1 255.255.255.0
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit
```

```
inspur(config)#ipv4-access-list test
inspur(config-ipv4-acl)#rule permit any
inspur(config-ipv4-acl)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool test poolid 1 mode pat      /*配置地址池*/
inspur(config-cgn-natpool)#section 1 interface gei-0/2   /*地址复用出接口*/
inspur(config-cgn-natpool)#exit
inspur(config-cgn)#domain 1 1 type sr ipv4-issued
inspur(config-cgn-domain)#static source rule-id 1 public 100.0.0.2 2000
interface
 gei-0/2 2562 tcp
/*配置复用出接口静态规则*/
inspur(config-cgn-domain)#exit
inspur(config-cgn)#subscriber ipv4 public subscriber-id 1 nat-domain 1
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
inspur(config-cgn)#exit
inspur(config)#ip route 0.0.0.0 0.0.0.0 200.0.0.2
```

配置验证

查看接口复用静态PAT条目信息：

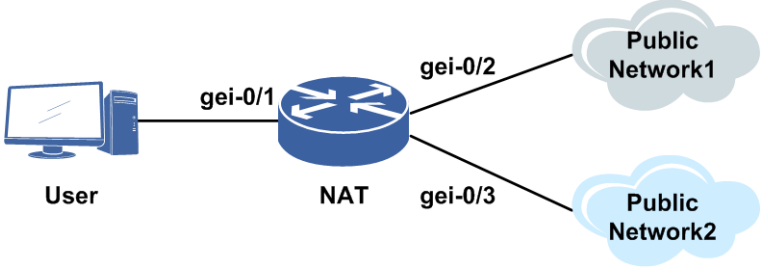
```
inspur(config)#show cgn translations all-sessions
================================================================================
Subscriber
    Pro    Type    Inside Local         Inside Global        Destination
================================================================================
    TCP   sta     100.0.0.2:2000        200.0.0.1:2562            *:*
--------------------------------------------------------------------------------
Loading data from MPFU-8/0...
================================================================================
```

13.2.5 动态多出口 NAT44 配置实例

配置说明

如*图 13-4*所示，PC上配置私网地址，通过IR12000智能路由器动态多出口配置实现访问不同网络时使用不同公网IP。

图 13-4 动态 PAT 转换 NAT44 配置实例组网图



配置思路

1.配置接口地址。

2.配置两个PAT地址池。

3.配置域并在域中配置动态多出口映射规则。

4.配置用户，将NAT域绑定在和PC相连的接口上。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ip address 100.0.0.1 255.255.255.0
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip address 200.0.0.1 255.255.255.0
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit
inspur(config)#interface gei-0/3
inspur(config-if-gei-0/3)#ip address 122.0.0.1 255.255.255.0
inspur(config-if-gei-0/3)#no shutdown
inspur(config-if-gei-0/3)#exit


inspur(config)#ipv4-access-list test
inspur(config-ipv4-acl)#rule permit any
inspur(config-ipv4-acl)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool testA poolid 1 mode pat  /*配置地址池A*/
inspur(config-cgn-patpool)#section 1 1.2.3.1 1.2.3.10
inspur(config-cgn-patpool)#exit
inspur(config-cgn)#cgn-pool testB poolid 2 mode pat  /*配置地址池B*/
inspur(config-cgn-patpool)#section 1 2.2.3.1 2.2.3.10
inspur(config-cgn-patpool)#exit
inspur(config-cgn)#domain 1 1 type sr ipv4-issued
inspur(config-cgn-domain)#dynamic source rule-id 1 ipv4-list test permit
 pool testA gei-0/2
/*这里配置的是流量出口为gei-0/2的动态多出口规则，NAT转换后公网地址地址池testA中的地址
*/
inspur(config-cgn-domain)#dynamic source rule-id 2 ipv4-list test permit
 pool testB gei-0/3
/*这里配置的是流量出口为gei-0/3的动态多出口规则，NAT转换后公网地址地址池testB中的地址
*/
inspur(config-cgn-domain)#exit
inspur(config-cgn)#subscriber ipv4 public subscriber-id 1 nat-domain 1
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
```

配置验证

用户上线以后发送outbound流量，设出口为gei-0/2的流量源IP和Port是<100.0.0.2，1000>，出口为gei-0/3的流量源IP、Port是<100.0.0.2，2000>。

生成条目后，通过命令**show cgn translation all-session**进行查看：

```
inspur(config)#show cgn translations all-sessions
```

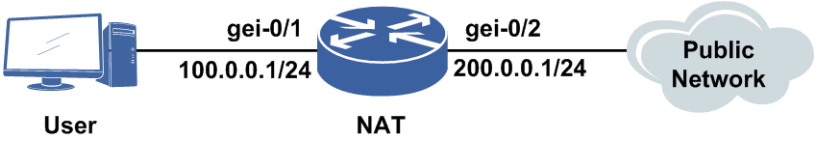
```
=========================================================================
Subscriber
Pro  Type    Inside Local         Inside Global      Destination
=========================================================================
Loading data from MPFU-8/0...
=========================================================================
UDP  dyn     100.0.0.2:1000        1.2.3.1:2112          *:*
-------------------------------------------------------------------------
UDP  dyn     100.0.0.2:2000        2.2.3.1:2112          *:*
-------------------------------------------------------------------------
```

13.2.6 VPN（私网-公网）NAT44 配置实例

配置说明

如*图 13-5*所示，用户主机通过私网地址连接到IR12000智能路由器，经过地址转换后访问外部的IPv4网络。

图 13-5 VPN（私网—公网）NAT44 配置实例组网图



配置思路

1.配置接口地址。

2.配置NAT地址池。

3.配置域并在域中配置动态映射规则。

4.配置用户，将NAT域绑定在和PC相连的接口上。

5.配置到公网的路由（本例采用静态路由配置）。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#ip vrf wd
inspur(config-vrf-wd)#rd 33:33
/*rd：路由标识符，格式为AS:分配号*/
inspur(config-vrf-wd)#route-target import 25:1
inspur(config-vrf-wd)#route-target export 25:1
inspur(config-vrf-wd)#address-family ipv4
inspur(config-vrf-wd-af-ipv4)#exit
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ip vrf forwarding wd
inspur(config-if-gei-0/1)#ip address 100.0.0.1 255.255.255.0
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip address 200.0.0.1 255.255.255.0
```

```
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit

inspur(config)#ipv4-access-list test
inspur(config-ipv4-acl)#rule permit any
inspur(config-ipv4-acl)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool test poolid 1 mode nat  /*配置地址池*/
inspur(config-cgn-natpool)#section 1 1.2.3.1 1.2.3.10
inspur(config-cgn-natpool)#exit
inspur(config-cgn)#domain 1 1 type sr ipv4-issued   /*域类型选择SR*/
inspur(config-cgn-domain)#dynamic source rule-id 1 ipv4-list test permit
 pool test  /*配置动态规则*/
inspur(config-cgn-domain)#exit
inspur(config-cgn)#subscriber ipv4 vrf wd subscriber-id 1 nat-domain 1
/*配置VPN NAT*/
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
inspur(config-cgn)#exit
inspur(config)#ip route vrf wd 0.0.0.0 0.0.0.0 200.0.0.2 global
```

配置验证

查看动态PAT条目信息：

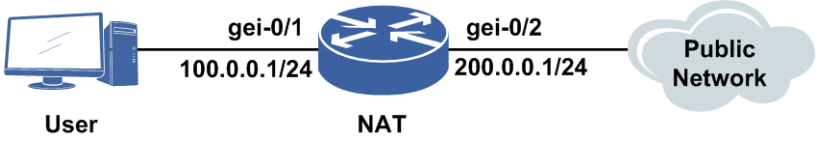
```
inspur(config)#show cgn translations all-sessions
=========================================================================
Subscriber
Pro  Type    Inside Local         Inside Global      Destination
=========================================================================
Loading data from MPFU-8/0...
=========================================================================
VPN name : wd
---   dyn      100.0.0.2           1.2.3.1          *:*
-------------------------------------------------------------------------
```

13.2.7 VPN（私网-相同私网）NAT44 配置实例

配置说明

如*图 13-6*所示，用户主机通过私网地址连接到IR12000智能路由器 ，经过地址转换后访问外部的IPv4网络。

图 13-6 VPN（私网—相同私网）NAT44 配置实例组网图



配置思路

1.配置接口地址。

2.配置NAT地址池。

3.配置域并在域中配置动态映射规则。

4.配置用户，将NAT域绑定在和PC相连的接口上。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#ip vrf wd
inspur(config-vrf-wd)#rd 33:33
/*rd：路由标识符，格式为AS:分配号*/
inspur(config-vrf-wd)#route-target import 25:1
inspur(config-vrf-wd)#route-target export 25:1
inspur(config-vrf-wd)#address-family ipv4
inspur(config-vrf-wd-af-ipv4)#exit
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ip vrf forwarding wd
inspur(config-if-gei-0/1)#ip address 100.0.0.1 255.255.255.0
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip vrf forwarding wd
inspur(config-if-gei-0/2)#ip address 200.0.0.1 255.255.255.0
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit
inspur(config)#ipv4-access-list test
inspur(config-ipv4-acl)#rule permit any
inspur(config-ipv4-acl)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool test poolid 1 mode nat /*配置地址池*/
inspur(config-cgn-natpool)#bind-vrf wd
inspur(config-cgn-natpool)#section 1 1.2.3.1 1.2.3.10
inspur(config-cgn-natpool)#exit
inspur(config-cgn)#domain 1 1 type sr ipv4-issued   /*域类型选择SR*/
inspur(config-cgn-domain)#dynamic source rule-id 1 ipv4-list test permit pool
 test  /*配置动态规则*/
inspur(config-cgn-domain)#exit

inspur(config-cgn)#subscriber ipv4 vrf wd subscriber-id 1 nat-domain 1
/*配置VPN NAT*/
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
```

配置验证

查看动态PAT条目信息：

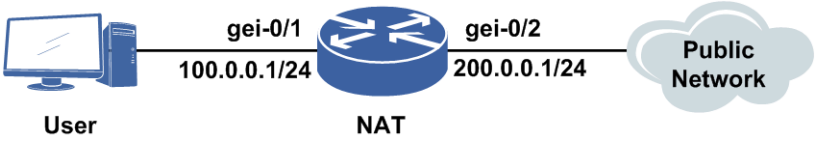
```
show cgn translations  all-sessions
================================================================================
Subscriber
    Pro  Type    Inside Local         Inside Global        Destination
================================================================================
Loading data from MPFU-8/0 ...
================================================================================
VPN name : wd
    ---   dyn    100.0.0.2            1.2.3.1            *:*
--------------------------------------------------------------------------------
```

13.2.8 VPN（私网-不同私网）NAT44 配置实例

配置说明

如*图 13-7*所示，用户主机通过私网地址连接到IR12000智能路由器，经过地址转换后，访问外部的IPv4网络。

图 13-7 VPN（私网—不同私网）NAT44 配置实例组网图



配置思路

1.配置接口地址。

2.配置NAT地址池。

3.配置域并在域中配置动态映射规则。

4.配置用户，将NAT域绑定在和PC相连的接口上。

5.配置策略路由。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#ip vrf wd
inspur(config-vrf-wd)#rd 33:33
/*rd：路由标识符，格式为AS:分配号*/
inspur(config-vrf-wd)#address-family ipv4
inspur(config-vrf-wd)#route-target import 25:12
inspur(config-vrf-wd)#route-target export 25:12
inspur(config-vrf-wd-af)#exit

inspur(config)#ip vrf wd1
inspur(config-vrf-wd1)#rd 55:55
inspur(config-vrf-wd1)#route-target import 25:1
inspur(config-vrf-wd1)#route-target export 25:1
inspur(config-vrf-wd1)#address-family ipv4
inspur(config-vrf-wd1-af-ipv4)#exit

inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ip vrf forwarding wd
inspur(config-if-gei-0/1)#ip address 100.0.0.1 255.255.255.0
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip vrf forwarding wd1
inspur(config-if-gei-0/2)#ip address 200.0.0.1 255.255.255.0
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit

inspur(config)#ipv4-access-list test
```

```
inspur(config-ipv4-acl)#rule permit any
inspur(config-ipv4-acl)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool test poolid 1 mode nat  /*配置地址池*/
inspur(config-cgn-natpool)#bind-vrf wd1
inspur(config-cgn-natpool)#section 1 1.2.3.1 1.2.3.10
inspur(config-cgn)#domain 1 1 type sr ipv4-issued   /*域类型选择SR*/
inspur(config-cgn-domain)#dynamic source rule-id 1 ipv4-list test permit pool
test
 /*配置动态规则*/
inspur(config-cgn-domain)#exit

inspur(config-cgn)#subscriber ipv4 vrf wd subscriber-id 1 nat-domain 1
/*配置VPN NAT*/
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit

inspur(config)#ipv4-access-list hh
inspur(config-ipv4-acl)#rule permit any
inspur(config-ipv4-acl)#exit
inspur(config)#route-map wd permit 10
inspur(config-route-map)#match ip address hh
inspur(config-route-map)#set vrf wd1 ip next-hop 200.0.0.2
inspur(config)#ip policy interface gei-0/1 route-map wd
```

配置验证

查看动态PAT条目信息：

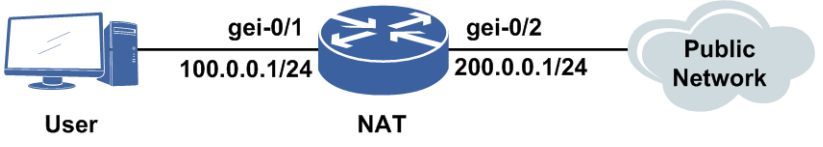
```
inspur(config)#show cgn translations  all-sessions
================================================================================
Subscriber
    Pro  Type    Inside Local         Inside Global        Destination
================================================================================
Loading data from MPFU-8/0 ...
================================================================================
VPN name : wd
    ---  dyn     100.0.0.2            1.2.3.1            *:*
--------------------------------------------------------------------------------
```

13.2.9 VPN（公网-私网）NAT44 配置实例

配置说明

如*图 13-8*所示，用户主机通过私网地址连接到IR12000智能路由器，经过地址转换后，访问外部的IPv4网络。

图 13-8 VPN（公网—私网）NAT44 配置实例组网图



配置思路

1.配置接口地址。

2.配置NAT地址池。

3.配置域并在域中配置动态映射规则。

4.将NAT域绑定在和PC相连的接口上。

5.配置策略路由。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#ip vrf wd
inspur(config-vrf-wd)#rd 33:33
/*rd：路由标识符，格式为AS:分配号*/
inspur(config-vrf-wd)#route-target import 25:1
inspur(config-vrf-wd)#route-target export 25:1
inspur(config-vrf-wd)#address-family ipv4
inspur(config-vrf-wd-af-ipv4)#exit
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ip address 100.0.0.1 255.255.255.0
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip vrf forwarding wd
inspur(config-if-gei-0/2)#ip address 200.0.0.1 255.255.255.0
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit

inspur(config)#ipv4-access-list test
inspur(config-ipv4-acl)#rule permit any
inspur(config-ipv4-acl)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool test poolid 1 mode nat /*配置地址池*/
inspur(config-cgn-natpool)#bind-vrf wd
inspur(config-cgn-natpool)#section 1 1.2.3.1 1.2.3.10
inspur(config-cgn-natpool)#exit
inspur(config-cgn)#domain 1 1 type sr ipv4-issued   /*域类型选择SR*/
inspur(config-cgn-domain)#dynamic source rule-id 1 ipv4-list test permit
 pool test  /*配置动态规则*/
inspur(config-cgn-domain)#exit

inspur(config-cgn)#subscriber ipv4 public subscriber-id 1 nat-domain 1
/*配置VPN NAT*/
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
inspur(config)#ipv4-access-list hh
inspur(config-ipv4-acl)#rule permit any
inspur(config-ipv4-acl)#exit
inspur(config)#route-map wd permit 10
inspur(config-route-map)#match ip address hh
inspur(config-route-map)#set vrf wd ip next-hop 200.0.0.2
inspur(config)#ip policy interface gei-0/1 route-map wd
```

配置验证

查看动态NAT条目信息：

```
inspur(config)#show cgn translations  all-sessions
================================================================================
Subscriber
    Pro  Type    Inside Local         Inside Global        Destination
================================================================================
 Loading data from  MPFU-8/0 ...
================================================================================
   ---    dyn     100.0.0.100           1.2.3.1            *:*
--------------------------------------------------------------------------------
```

13.3 NAT64

NAT64是一种有状态的网络地址与协议转换技术，支持通过IPv6网络侧用户发起连接访问IPv4侧网络资源，满足了IPv6主机与IPv4网络互通的需求。NAT64也支持通过手工配置静态映射关系实现IPv4网络主动发起连接访问IPv6网络的需求。

13.3.1 配置 NAT64

本节介绍NAT64的配置步骤和命令。

相关信息

NAT64分为有状态和无状态两种实现方式，有状态NAT64动态生成映射条目，无状态NAT64手动添加映射条目。

1.配置溯源功能的相关参数。

日志的作用是为了方便用户查询NAT转换前的源地址及源端口信息。

步骤	命令	功能
1	inspur(config)#**syslog-server host** [**vrf** <*vrf-name*>]<*ip-address*>[**fport** <*fport*>][**lport** <*lport*>]{[**alarmlog**], [**braslog**],[**cmdlog**],[**debugmsg**],[**natlog**],[**servicelog**]}	设置日志服务器的参数，包括日志服务器的IP地址和通信双方的端口号
2	inspur(config)#**logging nat ftp** [**vrf** <*vrf-name*>]<*ftp-server*><*username*><*password*>	设置发送NAT日志到FTP服务器

<*ip-address*>：日志服务器的IP地址，支持32位的IPv4地址或者128位的IPv6地址。

<*fport*>：日志服务器的端口号，范围1~65535，缺省为514。

<*lport*>：客户端的端口号，取值范围是514或1024~65535 ，缺省为514。

2.配置软线域。

软线域是用户引用的一个数据组，包含了NAT64前缀地址信息和NAT域信息。

步骤	命令	功能
1	inspur(config)#**cgn**	进入NAT配置模式
2	inspur(config-cgn)#**softwire-domain** <*softwire-domain-name*>	配置软线域名，并进入软线域配置模式
3	inspur(config-cgn-sw-domain-name)#**aftr nat64-prefix** {**stateful** | **stateless**}<*nat64-prefix*>	配置NAT64前缀
4	inspur(config-cgn-sw-domain-name)#**description** <*description*>	配置软线域描述信息
5	inspur(config-cgn-sw-domain-name)#**bind nat-domain** <*nat-domain-id*>	绑定NAT域
6	inspur(config-cgn-sw-domain-name)#**max-softwire-per-subscriber** <*number*>	配置软线域中用户最大软线数，默认不限制

stateful：配置有状态的NAT64前缀。

stateless：配置无状态的NAT64前缀。

3.配置NAT64接入。

步骤	命令	功能
1	inspur(config)#**cgn**	进入NAT配置模式
2	inspur(config-cgn)#**subscriber ipv6 prefix** <*ipv6-prefix*> **softwire-domain** <*domain-name*>	配置有状态NAT64用户，并进入用户配置模式
	inspur(config-cgn-sub)#**interface** <*interface-name*>	配置用户的接入接口
3	inspur(config-cgn)#**subscriber ipv6 stateless-nat64** <*nat64-prefix*> **softwire-domain** <*domain-name*>	配置无状态NAT64用户，并进入用户配置模式
	inspur(config-cgn-sub)#**nat64-ipv4-route** <*ipv4-address*><*ipv4-mask*> **mode** {**1:1** | **1:n divi-q-value** <*value*>}	配置无状态NAT64用户的IPv4路由

1:1：1:1模式（地址映射）。

1:n：1:n模式（地址加端口映射）。

<*value*>：表示一个IPv4地址对应IPv6地址的个数，取值范围1~12。

4.验证配置结果。

显示NAT64的配置信息：

命令	功能
inspur#**show cgn-pool** [**pool-name**	显示地址池配置信息

命令	功能
<*pool-name*>]]	
inspur#**show cgn domain** [**domain-name** <*domain-name*>]	显示域配置信息
inspur#**show cgn instance** {**summary**|**verbose**}	显示NAT全部信息

显示NAT64的条目：

命令	功能
inspur#**show cgn translations all-sessions**	显示所有NAT条目信息
inspur#**show cgn translations subscriber**	显示指定用户的详细NAT条目信息
inspur#**show cgn translations protocol**	显示指定协议类型的详细NAT条目信息
inspur#**show cgn translations translation-type**	显示指定转换类型的详细NAT条目信息
inspur#**show cgn translations cpe-address**	显示指定CPE地址的详细NAT条目信息
inspur#**show aftr softwire** {**all** |<*IPv6 prefix*>|<*IPv6 address*>|<*interface*>|<*soft-domain* >|**summary**}	显示用户软线信息

5.维护NAT64。

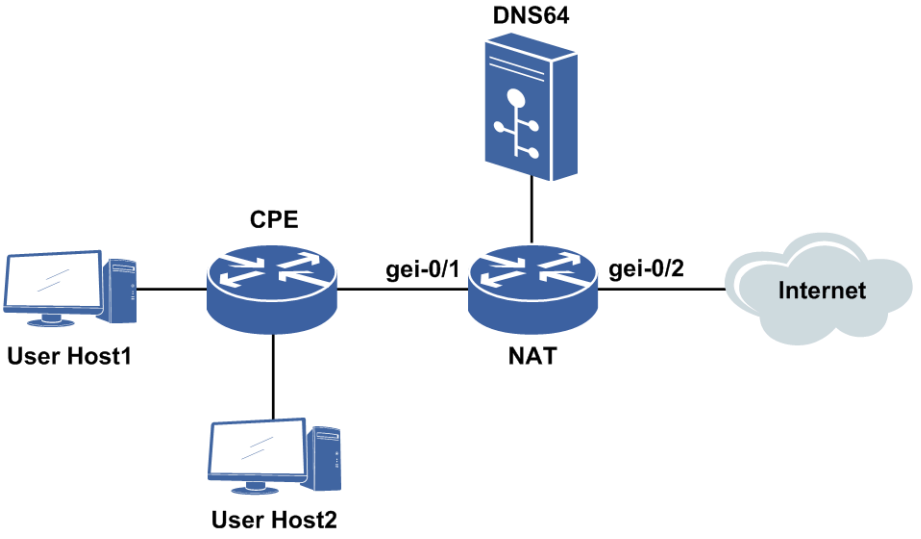
命令	功能
inspur#**clear cgn translations all-sessions**	清除所有转换条目
inspur#**clear cgn translations subscriber**	清除指定用户的转换条目
inspur#**clear cgn translations protocol**	清除指定协议类型的详细NAT条目
inspur#**clear cgn translations translation-type**	清除指定转换类型的详细NAT条目
inspur#**clear cgn translations cpe-address**	清除指定CPE地址的详细NAT条目
inspur#**clear aftr softwire** {**all** |<*IPv6 prefix*>|<*IPv6 address*>}|	踢用户下线

13.3.2 有状态 NAT64 静态 NAT 转换配置实例

配置说明

有状态NAT64的静态NAT转换配置实例如*图 13-9*所示。

图 13-9 有状态 NAT64 静态 NAT 配置实例组网图



实现的功能流程如下：

1.用户主机通过DHCP方式从CPE处获取v6地址。

2.CPE收到用户发送的v6报文后根据路由直接转发。

3.NAT设备收到v6报文后进行判断，如果需要则进行静态NAT转换，转换后用户可以访问Internet。

配置思路

1.配置NAT地址池。

2.配置域并在域中配置静态映射规则。

3.配置软线。

4.配置用户，绑定软线、接口。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 51::1/64
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip address 10.32.20.2 255.255.255.0
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool cgntest poolid 1 mode nat /*配置NAT地址池*/
inspur(config-cgn-natpool)#section 1 200.1.21.10 200.1.21.20
inspur(config-cgn-natpool)#exit
inspur(config-cgn)#domain 1 1 type standalone ipv6-issued
inspur(config-cgn-domain)#static source rule-id 1 cpe-ipv6-address 51::2
```

```
 nat64-prefix 77:88::/96 200.1.21.10     /*配置NAT64*/
inspur(config-cgn-domain)#exit
inspur(config-cgn)#exit

/*配置软线*/
inspur(config-cgn)#softwire-domain wd
inspur(config-cgn-sw-domain)#bind nat-domain 1
inspur(config-cgn-sw-domain)#aftr nat64-prefix stateful 77:88::/96
inspur(config-cgn-sw-domain)#exit
inspur(config-cgn)#subscriber ipv6 prefix 51::2/128 softwire-domain wd
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
```

配置验证

查看NAT条目信息：

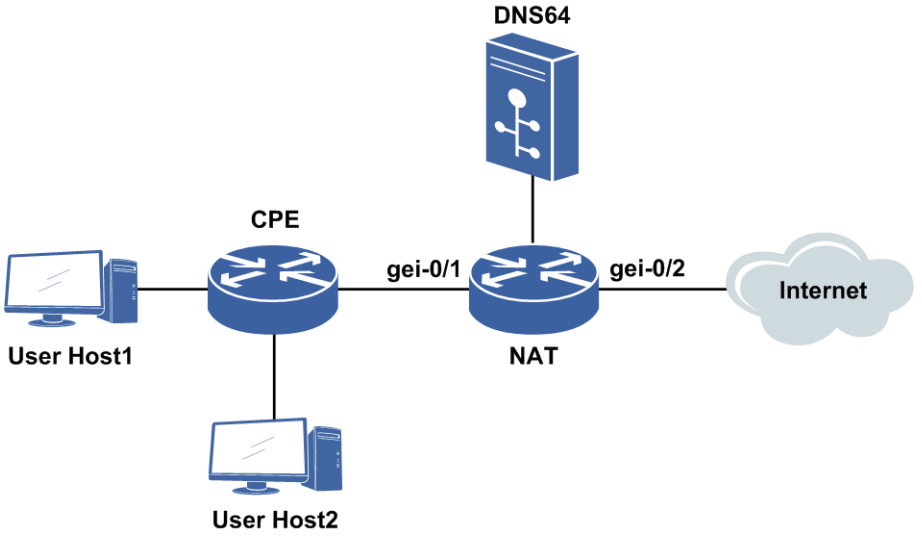
```
inspur#show cgn translations all-sessions
================================================================
Subscriber
    Pro  Type   Inside    Local Inside Global  Destination
================================================================
51::2                              77:88::/96
     ---   sta       ---     200.1.21.10     *
----------------------------------------------------------------
Loading data from MPFU-8/0 ...
================================================================
```

13.3.3 有状态 NAT64 静态 PAT 转换配置实例

配置说明

有状态NAT64的静态PAT转换配置实例如*图 13-10*所示。

图 13-10 有状态 NAT64 静态 PAT 配置实例组网图



实现的功能流程如下：

1.用户主机通过DHCP方式从CPE处获取v6地址。

2.CPE收到用户发送的v6报文后根据路由直接转发。

3.NAT设备收到v6报文后进行判断，如果需要则进行静态PAT转换，转换后用户可以访问Internet。

配置思路

1.配置PAT地址池。

2.配置域并在域中配置静态映射规则。

3.配置软线。

4.配置用户，绑定软线、接口。

配置过程

IR12000智能路由器上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 51::1/64
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip address 10.32.20.2 255.255.255.0
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool cgntest poolid 1 mode pat /*配置PAT地址池*/
inspur(config-cgn-patpool)#section 1 200.1.21.10 200.1.21.20
inspur(config-cgn-patpool)#exit
inspur(config-cgn)#domain 1 1 type standalone ipv6-issued
inspur(config-cgn-domain)#static source rule-id 1 cpe-ipv6-address 51::2
 nat64-prefix 77:88::/9660 200.1.21.10 60 udp    /*配置NAT64*/
inspur(config-cgn-domain)#exit
inspur(config-cgn)#exit

/*配置软线*/
inspur(config-cgn)#softwire-domain wd
inspur(config-cgn-sw-domain)#bind nat-domain 1
inspur(config-cgn-sw-domain)#aftr nat64-prefix stateful 77:88::/96
inspur(config-cgn-sw-domain)#exit
inspur(config-cgn)#subscriber ipv6 prefix 51::2/128 softwire-domain wd
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
```

配置验证

查看NAT条目信息：

```
inspur#show cgn translations all-sessions
================================================================
Subscriber
Pro  Type  Inside Local     Inside Global    Destination
================================================================
51::2                                       77:88::/96
UDP   sta      ---:60          200.1.21.10:60         *:*
```

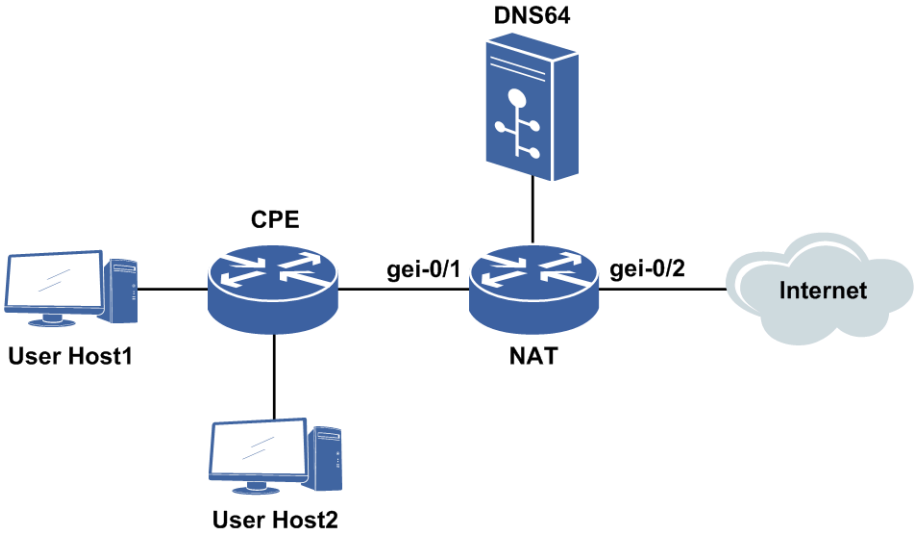
```
------------------------------------------------------------
Loading data from MPFU-8/0 ...
============================================================
```

13.3.4 有状态 NAT64 动态 NAT 转换配置实例

配置说明

有状态NAT64的动态NAT转换配置实例如*图 13-11*所示。

图 13-11 有状态 NAT64 动态 NAT 配置实例组网图



实现的功能流程如下：

1.用户主机通过DHCP方式从CPE处获取v6地址。

2.CPE收到用户的v6报文后根据路由直接转发。

3.NAT设备收到v6报文后进行判断，如果需要则进行动态NAT转换，转换后用户可以访问Internet。

配置思路

1.配置NAT地址池。

2.配置域并在域中配置动态映射规则。

3.配置软线。

4.配置用户，绑定软线、接口。

配置过程

在IR12000智能路由器上的配置如下：

```
inspur(config)#ipv6-access-list cgn
inspur(config-ipv6-acl)#rule 10 permit ipv6 any any
inspur(config-ipv6-acl)#exit

inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 51::1/64
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip address 10.32.20.2 255.255.255.0
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool cgntest poolid 1 mode nat /*配置NAT地址池*/
inspur(config-cgn-natpool)#section 1 200.1.21.10 200.1.21.20
inspur(config-cgn-natpool)#exit
inspur(config-cgn)#domain 1 1 type standalone ipv6-issued
inspur(config-cgn-domain)#dynamic source rule-id 1 ipv6-list cgn permit
 pool cgntest
inspur(config-cgn-domain)#exit
inspur(config-cgn)#exit

/*配置软线*/
inspur(config-cgn)#softwire-domain wd
inspur(config-cgn-sw-domain)#bind nat-domain 1
inspur(config-cgn-sw-domain)#aftr nat64-prefix stateful 77:88::/96
inspur(config-cgn-sw-domain)#exit
inspur(config-cgn)#subscriber ipv6 prefix 51::/64 softwire-domain wd
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
```

配置验证

查看NAT条目信息：

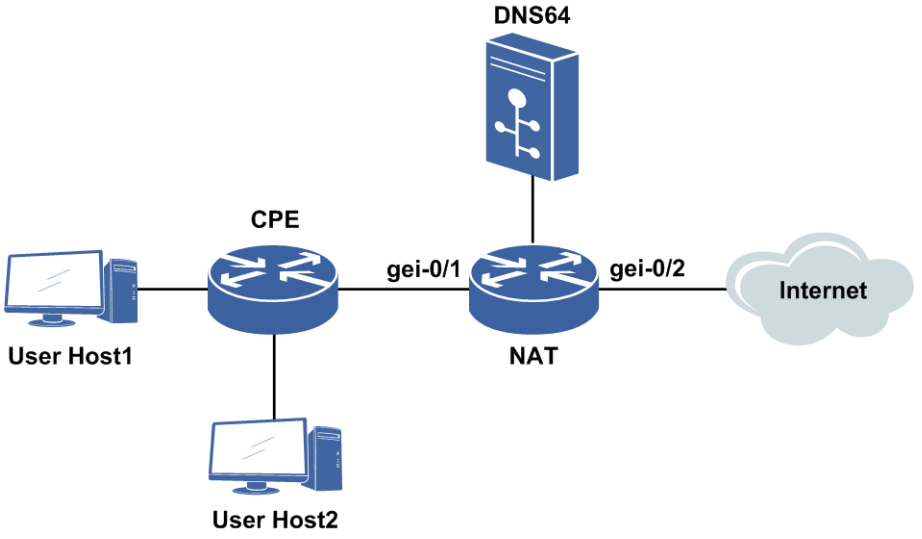
```
NAT#show cgn translations all-sessions
================================================================================
Subscriber
 Pro      Type   Inside Local      Inside Global    Destination
================================================================================
Loading data from MPFU-8/0 ...
================================================================================
51::2                                          77:88::/96
   ---       dyn        ---         200.1.21.10      *
--------------------------------------------------------------------------------
```

13.3.5 有状态 NAT64 动态 PAT 转换配置实例

配置说明

有状态NAT64的动态PAT转换配置实例如*图 13-12*所示。

图 13-12 有状态 NAT64 动态 PAT 转换配置实例组网图



实现的功能流程如下：

1.用户主机上通过DHCP方式从CPE处获取v6地址。

2.CPE收到v6报文后根据路由直接转发。

3.NAT设备收到v6报文后进行判断，如果需要则进行动态PAT转换，转换后用户可以访问Internet。

配置思路

1.配置PAT地址池。

2.配置域并在域中配置动态映射规则。

3.配置软线。

4.配置用户，绑定软线、接口。

配置过程

在IR12000智能路由器上的配置如下：

```
/*配置ACL*/
inspur(config)#ipv6-access-list cgn
inspur(config-ipv6-acl)#rule 10 permit ipv6 any any
inspur(config-ipv6-acl)#exit

inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 51::1/64
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip address 10.32.20.2 255.255.255.0
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit

inspur(config)#cgn
```

```
inspur(config-cgn)#cgn-pool cgntest poolid 1 mode pat /*配置PAT地址池*/
inspur(config-cgn-patpool)#section 1 200.1.21.10 200.1.21.20
inspur(config-cgn-patpool)#exit
inspur(config-cgn)#domain 1 1 type standalone ipv6-issued
inspur(config-cgn-domain)#dynamic source rule-id 1 ipv6-list cgn permit pool
 cgntest  /*配置NAT64*/
inspur(config-cgn-domain)#exit
inspur(config-cgn)#exit

/*配置软线*/
inspur(config-cgn)#softwire-domain wd
inspur(config-cgn-sw-domain)#bind nat-domain 1
inspur(config-cgn-sw-domain)#aftr nat64-prefix stateful 77:88::/96
inspur(config-cgn-sw-domain)#exit
inspur(config-cgn)#subscriber ipv6 prefix 51::/64 softwire-domain wd
inspur(config-cgn-sub)#interface gei-0/1
```

配置验证

查看NAT条目信息：

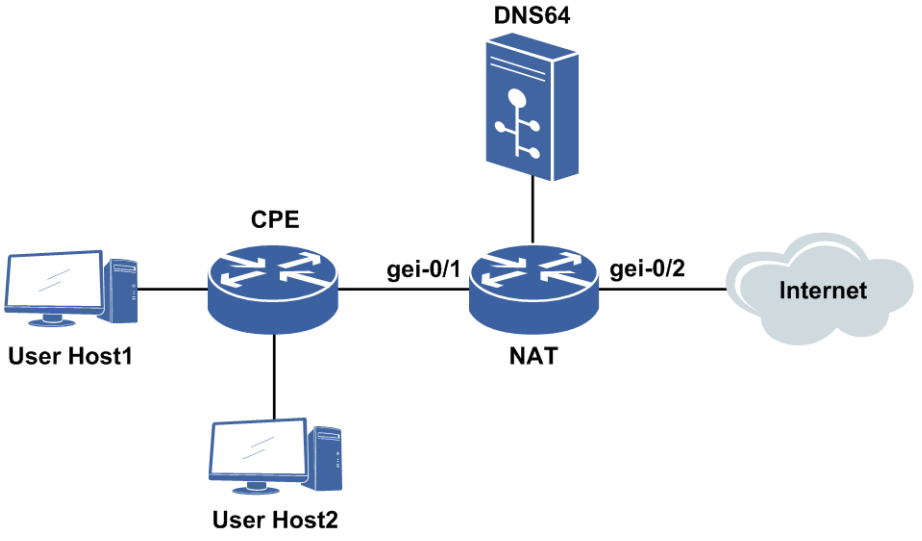
```
inspur#show cgn translations all-sessions
================================================================================
Subscriber
Pro  Type    Inside Local         Inside Global        Destination
================================================================================
Loading data from MPFU-8/0 ...
================================================================================
51::2                                                 77:88::/96
UDP  dyn     ---:10              200.1.21.10:63616    *:*
--------------------------------------------------------------------------------
```

13.3.6 无状态 NAT64 转换配置实例

配置说明

无状态NAT64的转换配置实例如*图 13-13*所示。

图 13-13 无状态 NAT64 转换配置实例组网图



实现的功能流程如下：

1.用户主机通过DHCP方式从CPE处获取v6地址。

2.CPE收到用户发送的v6报文后根据路由直接转发。

3.NAT设备收到v6报文后进行判断，如果需要则进行NAT转换，转换后用户可以访问Internet。

配置思路

1.配置NAT64。

2.配置软线。

3.配置用户，绑定软线，配置NAT64用户的IPv4路由。

配置过程

在IR12000智能路由器上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 51::1/64
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface gei-0/2
inspur(config-if-gei-0/2)#ip address 10.32.20.2 255.255.255.0
inspur(config-if-gei-0/2)#no shutdown
inspur(config-if-gei-0/2)#exit

inspur(config)#cgn

/*配置软线*/
inspur(config-cgn)#softwire-domain wd
inspur(config-cgn-sw-domain)#bind nat-domain 1
inspur(config-cgn-sw-domain)#aftr nat64-prefix stateless 77:88::/96
inspur(config-cgn-sw-domain)#exit
inspur(config-cgn)#subscriber ipv6stateless-nat64 51::/96 softwire-domain wd
inspur(config-cgn-sub)#nat64-ipv4-route 192.0.2.0 255.255.255.0 mode 1:1
/*配置NAT64用户的IPv4路由，这里是1:1的模式，也可以配置1:n模式*/
inspur(config-cgn-sub)#exit
```

配置验证

无状态NAT64不生成映射条目，可以在接收端抓包查看转换情况。

13.4 DS-Lite

双栈隧道电信级NAT（Dual-stack lite Carrier Grade Network Address Translation）技术，简称DS-Lite。DS-Lite通过使用具有双栈功能的设备、4in6隧道以及NAT44技术，使运营商可以先从接入网络逐步地、从小到大地、更加灵活地部署IPv6，降低部署IPv6

的成本，有利于促进运营商尽早开始进行实质性的、有意义的IPv6业务部署。

DS-Lite NAT技术通过将各用户的私网数据包在用户CPE处封装到4in6隧道中，使得不同CPE的用户主机可以共享相同的私网IPv4地址段来发起数据访问。所有的用户主机在DS-Lite NAT设备处共用相同的公网地址池进行外部网络访问，这在一定程度上解决了用户网络IP地址分配的问题。同时在CPE和DS-Lite NAT设备之间的网络部署IPv6技术，可以平滑、逐步地进行网络升级改造。

13.4.1 配置 DS-Lite

本节介绍DS-Lite的配置步骤和命令。

1.配置溯源，log模式下的配置参见配置日志。

步骤	命令	功能
1	inspur(config)#**syslog-server host** [**vrf** <*vrf-name*>][**fport** <*fport*>][**lport** <*lport*>]{[**alarmlog**],[**braslog**],[**cmdlog**],[**debugmsg**],[**natlog**],[**servicelog**]}	设置日志服务器的参数，包括日志服务器的地址和通信双方的端口号
2	inspur(config)#**logging nat ftp** [**vrf** <*vrf-name*>]<*ftp-server*><*username*><*password*>	设置发送NAT日志到FTP服务器

<*ip-address*>：日志服务器的IP地址，支持32位的IPv4地址或者128位的IPv6地址。

<*fport*>：日志服务器的端口号，范围1~65535，缺省为514。

<*lport*>：客户端的端口号，取值范围是514或1024~65535 ，缺省为514。

2.配置软线域。

步骤	命令	功能
1	inspur(config)#**cgn**	进入NAT配置模式
2	inspur(config-cgn)#**softwire-domain** <*softwire-domain-name*>	配置软线域名，并进入软线域配置模式
3	inspur(config-cgn-sw-domain-name)#**aftr interface v6-tunnel**<*id*>	配置软线域的DS-Lite v6隧道接口
4	inspur(config-cgn-sw-domain-name)#**description** <*description*>	配置软线域描述信息
5	inspur(config-cgn-sw-domain-name)#**bind nat-domain** <*nat-domain-id*>	绑定NAT域
6	inspur(config-cgn-sw-domain-name)#**max-softwire-per-subscriber** <*number*>	配置软线域中用户使用的最大软线数，默认不限制

3.配置DS-Lite接入。

步骤	命令	功能
1	inspur(config)#**cgn**	进入NAT配置模式
2	inspur(config-cgn)#**subscriber ipv6** {**prefix** *<ipv6-prefix>*|**mask-length** *<mask-length>*} **softwire-domain** *<domain-name>*	配置DS-Lite用户
3	inspur(config-cgn-sub)#**interface** *<interface-name>*	配置用户的接入接口

4.配置DS-Lite B4。

步骤	命令	功能
1	inspur(config)#**ipv6-tunnel-config**	进入IPv6隧道配置模式
2	inspur(config-ipv6-tunnel)#**interface v6_tunnel***<id>*	进入指定IPv6隧道
3	inspur(config-ipv6-tunnel-if-v6_tunneld)#**tunnel mode** {**ipipv6** {**4in6**|**ds-lite** {**dynamic**|**static**}|**ds-lite-b4**}|**ipv6ip** {**6to4**|**6rd**|**isatap**|**6in4**}}	配置隧道模式
4	inspur(config-ipv6-tunnel-if-v6_tunneld)#**tunnel source** {**ipv4** *<ipv4-address>*||**ipv6** *<ipv6-address>*}	配置隧道的源地址
5	inspur(config-ipv6-tunnel-if-v6_tunneld)#**tunnel destination** {**ipv4** *<ipv4-address>*|**ipv6** *<ipv6-address>*| **dhcp-interface** *<interface-name>*|**domain** *<domain-name>*}	配置隧道的目的地址或参数

5.验证配置结果。

查看DS-Lite的配置信息：

命令	功能
inspur#**show cgn-pool** [**pool-name***<pool-name>*]	显示地址池配置信息
inspur#**show cgn domain** [**domain-name** *<domain-name>*]	显示域配置信息
inspur#**show cgn instance** {**summary**|**verbose**}	显示NAT全部信息

显示DS-Lite的条目：

命令	功能
inspur#**show cgn translations all-sessions**	显示所有NAT条目信息
inspur#**show cgn translations subscriber**	显示指定用户的详细NAT条目信息

命令	功能
inspur#**show cgn translations protocol**	显示指定协议类型的详细NAT条目信息
inspur#**show cgn translations translation-type**	显示指定转换类型的详细NAT条目信息
inspur#**show aftr softwire** {**all** |<*IPv6 prefix*>|<*IPv6 address*>|<*interface*>|<*soft-domain* >|**summary**}	显示用户软线信息

6.维护DS-Lite。

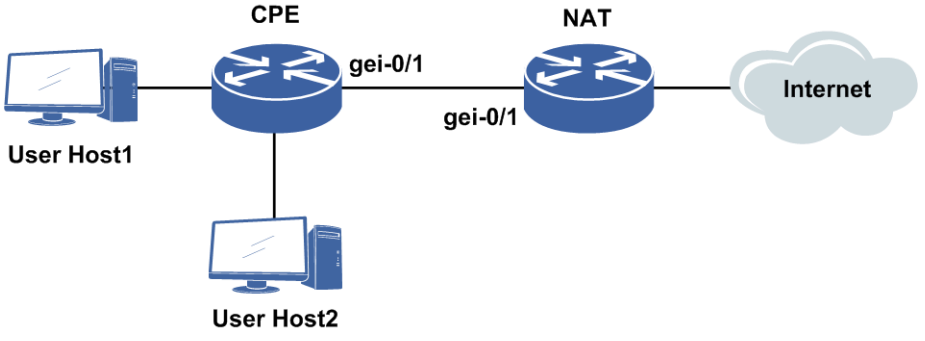
命令	功能
inspur#**clear cgn translations all-sessions**	清除所有转换条目信息
inspur#**clear cgn translations subscriber**	清除指定用户的转换条目信息
inspur#**clear cgn translations protocol**	清除指定协议类型的详细NAT条目信息
inspur#**clear cgn translations translation-type**	清除指定转换类型的详细NAT条目信息
inspur#**clear aftr softwire** {**all** |<*IPv6 prefix*>|<*IPv6 address*>}	踢用户下线

13.4.2 静态 NAT 转换配置实例

配置说明

如*图 13-14*所示，用户主机使用私有网络的IPv4地址，通过CPE和DS-Lite NAT设备组成的IPv6网络来访问外部的IPv4网络，B4设备直接使用AFTR address进行隧道配置。

图 13-14 静态 NAT 转换配置实例组网图



配置思路

Ds-Lite设备：

1.配置v6_tunnel和ACL

2.配置NAT地址池和NAT模式

3.配置域并在域中配置静态NAT转换规则

4.配置软线和用户

CPE设备：

1.配置v6_tunnel

2.隧道目的地址直接配置AFTR地址

配置过程

在CPE设备上配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 2017:1::1:1/96
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#ip address 100.1.1.1/24
inspur(config-if-v6_tunnel1)#exit
inspur(config)#ipv6-tunnel-config
inspur(config-ipv6-tunnel)#interface v6_tunnel1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipipv6 ds-lite-b4
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv4 2017:1::1:1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel destination ipv4 2017:1::1:2
inspur(config-ipv6-tunnel-if-v6_tunnel1)#exit
inspur(config-ipv6-tunnel)#exit
```

在DS-Lite NAT设备上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 2017:1::1:2/96
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit

/*配置v6_tunnel*/
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#ipv6 enable
inspur(config-if-v6_tunnel1)#ip address 100.1.1.2/24
inspur(config-if-v6_tunnel1)#exit
inspur(config)#ipv6-tunnel-config
inspur(config-ipv6-tunnel)#interface v6_tunnel1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipipv6 ds-lite static
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv6 2017:1::1:2
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel destination ipv4 2017:1::1:1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#exit
inspur(config-ipv6-tunnel)#exit

/*配置ACL*/
inspur(config)#ipv4-access-list dslite
inspur(config-ipv4-acl)#rule 10 permit any
inspur(config-ipv4-acl)#exit

inspur(config)#cgn
```

```
inspur(config-cgn)#cgn-pool dslite poolid 2 mode nat  /*配置地址池,类型为nat*/
inspur(config-cgn-natpool)#section 1 99.1.1.1 99.1.1.10
inspur(config-cgn-natpool)#exit
inspur(config-cgn)#domain 10 10 type standalone ipv6-issued
inspur(config-cgn-domain)#static  source  rule-id  1  softwire  2017:1::1:1
2017:1::1:2
192.85.1.2 99.1.1.1
/*192.85.1.2是用户主机地址，上述命令配置的是静态规则，也可以配置动态规则*/
inspur(config-cgn-domain)#exit

/*配置软线和用户*/
inspur(config-cgn)#softwire-domain dslite
inspur(config-cgn-sw-domain-dslite)#bind nat-domain 10
inspur(config-cgn-sw-domain-dslite)#aftr interface v6_tunnel1
inspur(config-cgn-sw-domain-dslite)#exit
inspur(config-cgn)#subscriber  ipv6  prefix  2017:1::1:1/128  softwire-domain
dslite
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
```

配置验证

在NAT设备上查看NAT条目信息：

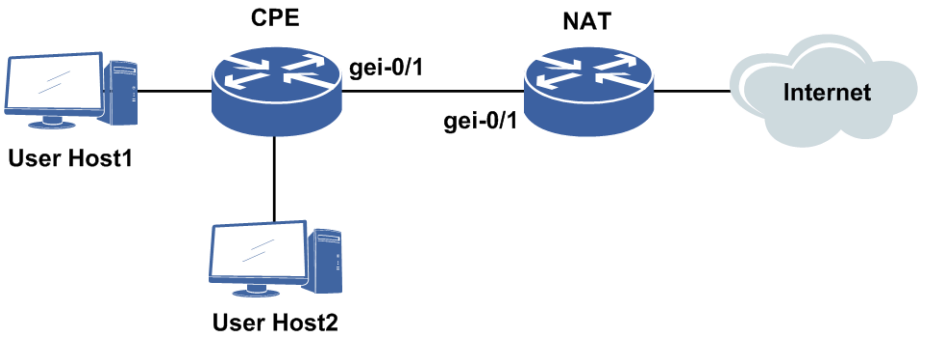
```
inspur#show cgn translations all-sessions
================================================================================
======
Subscriber
    Pro  Type    Inside Local         Inside Global    Destination
================================================================================
======
2017:1::1:1
    ---  sta     192.85.1.2           99.1.1.1         *:*
--------------------------------------------------------------------------------
------
Loading data from MPFU-12/0 ...
================================================================================
======
```

13.4.3 静态 PAT 转换配置实例

配置说明

如*图 13-15*所示，用户主机使用私有网络的IPv4地址，通过CPE和DS-Lite NAT设备组成的IPv6网络来访问外部的IPv4网络，B4设备配置通过DNS获取AFTR地址，DNS查询在CPE设备上完成。

图 13-15 静态 PAT 转换配置实例组网图



配置思路

DS-Lite设备：

1.配置v6_tunnel和ACL

2.配置NAT地址池和NAT模式

3.配置域并在域中配置静态PAT转换规则

4.配置软线和用户

CPE设备：

1.配置v6_tunnel

2.隧道目的地址配置domain name

3.配置DNS

配置过程

在CPE设备上配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 2017:1::1:1/96
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#ip address 100.1.1.1/24
inspur(config-if-v6_tunnel1)#exit
inspur(config)#ipv6-tunnel-config
inspur(config-ipv6-tunnel)#interface v6_tunnel1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipipv6 ds-lite-b4
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv4 2017:1::1:1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel destination domain
a.inspur.com.cn
inspur(config-ipv6-tunnel-if-v6_tunnel1)#exit
inspur(config-ipv6-tunnel)#exit

/*配置DNS*/
inspur(config)#ip domain lookup
inspur(config)#ip domain resolve-type static
inspur(config)#ip domain hostname a.inspur.com.cn ipv6-address 2017:1::1:2
```

DS-Lite NAT设备上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 2017:1::1:2/96
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit

/*配置v6_tunnel*/
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#ipv6 enable
inspur(config-if-v6_tunnel1)#ip address 100.1.1.2/24
inspur(config-if-v6_tunnel1)#exit
inspur(config)#ipv6-tunnel-config
inspur(config-ipv6-tunnel)#interface v6_tunnel1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipipv6 ds-lite static
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv6 2017:1::1:2
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel destination ipv4 2017:1::1:1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#exit
inspur(config-ipv6-tunnel)#exit

/*配置ACL*/
inspur(config)#ipv4-access-list dslite
inspur(config-ipv4-acl)#rule 10 permit any
inspur(config-ipv4-acl)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool dslite poolid 2 mode pat  /*配置地址池，类型为pat*/
inspur(config-cgn-natpool)#section 1 99.1.1.1 99.1.1.10
inspur(config-cgn-natpool)#exit
inspur(config-cgn)#domain 10 10 type standalone ipv6-issued
inspur(config-cgn-domain)#static  source  rule-id  1  softwire  2017:1::1:1
2017:1::1:2
192.85.1.2 1024 99.1.1.1 1024 udp
/* 192.85.1.2是用户主机地址,1024是用户端口，协议配置为udp*/
inspur(config-cgn-domain)#exit

/*配置软线和用户*/
inspur(config-cgn)#softwire-domain dslite
inspur(config-cgn-sw-domain-dslite)#bind nat-domain 10
inspur(config-cgn-sw-domain-dslite)#aftr interface v6_tunnel1
inspur(config-cgn-sw-domain-dslite)#exit
inspur(config-cgn)#subscriber  ipv6  prefix  2017:1::1:1/128  softwire-domain
dslite
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
```

配置验证

在NAT上查看NAT条目信息：

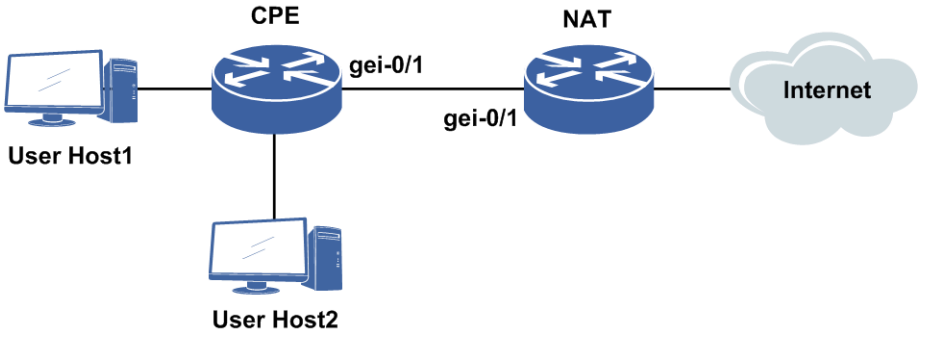
```
inspur#show cgn translations all-sessions
================================================================================
======
Subscriber
   Pro  Type    Inside Local         Inside Global        Destination
================================================================================
======
2017:1::1:1
   UDP  sta     192.85.1.2:1024      99.1.1.1:1024        *:*
--------------------------------------------------------------------------------
------
Loading data from MPFU-12/0 ...
================================================================================
======
```

13.4.4 动态 NAT 转换配置实例

配置说明

如*图 13-16*所示，用户主机使用私有网络的IPv4地址，通过CPE和DS-Lite NAT设备组成的IPv6网络来访问外部的IPv4网络，B4的AFTR地址通过动态参数获取，从DHCPv6获取的AFTR-Name选项中获取AFTR name，再获取AFTR地址。

图 13-16 动态 NAT 转换配置实例组网图



配置思路

DS-Lite设备：

1.配置DHCPv6 server

2.配置v6_tunnel和ACL

3.配置NAT地址池和NAT模式

4.配置域并在域中配置动态NAT转换规则

5.配置软线和用户

CPE设备：

1.配置接口开启DHCPv6 client

2.配置v6_tunnel

3.隧道目的地址配置dhcp-interface

4.配置DNS

配置过程

在CPE设备上配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 2017:1::1:1/96
inspur(config-if-gei-0/1)#ipv6 dhcp client address /*配置DHCPv6*/
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
```

```
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#ip address 100.1.1.1/24
inspur(config-if-v6_tunnel1)#exit
inspur(config)#ipv6-tunnel-config
inspur(config-ipv6-tunnel)#interface v6_tunnel1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipipv6 ds-lite-b4
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv4 2017:1::1:1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel  destination  dhcp-interface
gei-1/7
inspur(config-ipv6-tunnel-if-v6_tunnel1)#exit
inspur(config-ipv6-tunnel)#exit

inspur(config)#ip domain lookup
inspur(config)#ip domain resolve-type static
inspur(config)#ip domain hostname a.inspur.com.cn ipv6-address 2017:1::1:2
```

在DS-Lite NAT设备上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 2017:1::1:2/96
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit

inspur(config)#ipv6 addr-pool inspur
inspur(config-ipv6-addr-pool)#addr-range 2017:1::1:3 2017:1::1:10
inspur(config-ipv6-addr-pool)#exit

inspur(config)#dhcp ipv6
inspur(config-dhcpv6)#policy inspur 1
inspur(config-dhcpv6-policy)#dhcpv6-pool inspur
inspur(config-dhcpv6-policy)#exit
inspur(config-dhcpv6)#pool inspur
inspur(config-dhcpv6-pool)#address-pool inspur
inspur(config-dhcpv6-pool)#aftr fqdn a.inspur.com.cn
inspur(config-dhcpv6)#interface gei-0/1
inspur(config-dhcpv6-if-gei-0/1)#mode server
inspur(config-dhcpv6-if-gei-0/1)#server policy inspur
inspur(config-dhcpv6-if-gei-0/1)#exit
inspur(config-dhcpv6)#enable
inspur(config-dhcpv6)#exit

/*配置v6_tunnel*/
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#ipv6 enable
inspur(config-if-v6_tunnel1)#ip address 100.1.1.2/24
inspur(config-if-v6_tunnel1)#exit
inspur(config)#ipv6-tunnel-config
inspur(config-ipv6-tunnel)#interface v6_tunnel1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipipv6 ds-lite static
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv6 2017:1::1:2
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel destination ipv4 2017:1::1:1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#exit
inspur(config-ipv6-tunnel)#exit

/*配置ACL*/
inspur(config)#ipv4-access-list dslite
inspur(config-ipv4-acl)#rule 10 permit any
inspur(config-ipv4-acl)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool dslite poolid 2 mode nat  /*配置地址池，类型为pat*/
inspur(config-cgn-natpool)#section 1 99.1.1.1 99.1.1.10
inspur(config-cgn-natpool)#exit
inspur(config-cgn)#domain 10 10 type standalone ipv6-issued
inspur(config-cgn-domain)#dynamic source rule-id 1 ipv4-list dslite permit
 pool dslite  /*配置动态ACL规则，也可以配置静态规则*/
inspur(config-cgn-domain)#exit
```

```
/*配置软线和用户*/
inspur(config-cgn)#softwire-domain dslite
inspur(config-cgn-sw-domain-dslite)#bind nat-domain 10
inspur(config-cgn-sw-domain-dslite)#aftr interface v6_tunnel1
inspur(config-cgn-sw-domain-dslite)#exit
inspur(config-cgn)#subscriber ipv6 prefix 2017:1::/64 softwire-domain dslite
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
```

配置验证

在NAT设备上查看NAT条目信息：

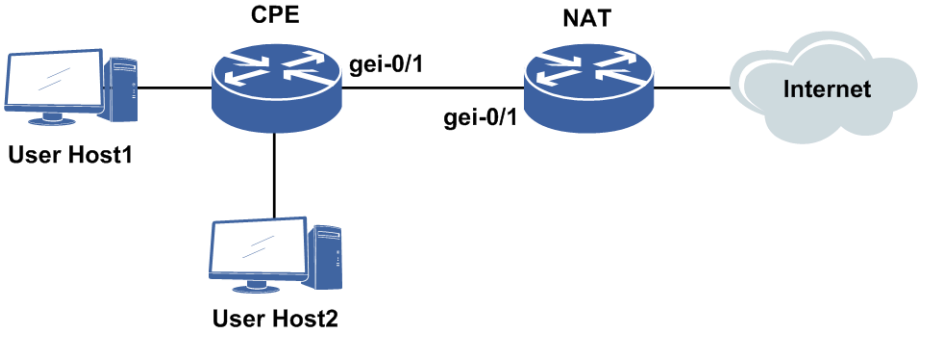
```
inspur#show cgn translations all-sessions
================================================================================
Subscriber
    Pro  Type    Inside Local         Inside Global        Destination
================================================================================
Loading data from MPFU-12/0 ...
================================================================================
 2017:1::1:1
    ---  dyn     192.85.1.2           99.1.1.1             *:*
--------------------------------------------------------------------------------
```

13.4.5 动态 PAT 转换配置实例

配置说明

如*图* **13-17**所示，用户主机使用私有网络的IPv4地址，通过CPE和DS-Lite NAT设备组成的IPv6网络来访问外部的IPv4网络，B4设备配置通过DNS获取AFTR地址，DNS查询在CPE设备上完成。

图 13-17 动态 PAT 转换配置实例组网图



配置思路

DS-Lite设备：

1.配置DHCPv6 server

2.配置v6_tunnel和ACL

3.配置NAT地址池和NAT模式

4.配置域并在域中配置动态PAT转换规则

5.配置软线和用户

CPE设备：

1.配置接口开启DHCPv6 client

2.配置v6_tunnel

3.隧道目的地址配置dhcp-interface

4.配置DNS

配置过程

在CPE设备上配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 2017:1::1:1/96
inspur(config-if-gei-0/1)#ipv6 dhcp client address /*配置DHCPv6*/
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#ip address 100.1.1.1/24
inspur(config-if-v6_tunnel1)#exit
inspur(config)#ipv6-tunnel-config
inspur(config-ipv6-tunnel)#interface v6_tunnel1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipipv6 ds-lite-b4
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv4 2017:1::1:1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel destination dhcp-interface
gei-1/7
inspur(config-ipv6-tunnel-if-v6_tunnel1)#exit
inspur(config-ipv6-tunnel)#exit

inspur(config)#ip domain lookup
inspur(config)#ip domain resolve-type static
inspur(config)#ip domain hostname a.inspur.com.cn ipv6-address 2017:1::1:2
```

在Ds-Lite NAT设备上的配置如下：

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#ipv6 enable
inspur(config-if-gei-0/1)#ipv6 address 2017:1::1:2/96
inspur(config-if-gei-0/1)#no shutdown
inspur(config-if-gei-0/1)#exit

inspur(config)#ipv6 addr-pool inspur
inspur(config-ipv6-addr-pool)#addr-range 2017:1::1:3 2017:1::1:10
inspur(config-ipv6-addr-pool)#exit

inspur(config)#dhcp ipv6
inspur(config-dhcpv6)#policy inspur 1
inspur(config-dhcpv6-policy)#dhcpv6-pool inspur
inspur(config-dhcpv6-policy)#exit
inspur(config-dhcpv6)#pool inspur
inspur(config-dhcpv6-pool)#address-pool inspur
inspur(config-dhcpv6-pool)#aftr fqdn a.inspur.com.cn
inspur(config-dhcpv6)#interface gei-0/1
inspur(config-dhcpv6-if-gei-0/1)#mode server
inspur(config-dhcpv6-if-gei-0/1)#server policy inspur
inspur(config-dhcpv6-if-gei-0/1)#exit
inspur(config-dhcpv6)#enable
inspur(config-dhcpv6)#exit
```

```
/*配置v6_tunnel*/
inspur(config)#interface v6_tunnel1
inspur(config-if-v6_tunnel1)#ipv6 enable
inspur(config-if-v6_tunnel1)#ip address 100.1.1.2/24
inspur(config-if-v6_tunnel1)#exit
inspur(config)#ipv6-tunnel-config
inspur(config-ipv6-tunnel)#interface v6_tunnel1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel mode ipipv6 ds-lite static
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel source ipv6 2017:1::1:2
inspur(config-ipv6-tunnel-if-v6_tunnel1)#tunnel destination ipv4 2017:1::1:1
inspur(config-ipv6-tunnel-if-v6_tunnel1)#exit
inspur(config-ipv6-tunnel)#exit


/*配置ACL*/
inspur(config)#ipv4-access-list dslite
inspur(config-ipv4-acl)#rule 10 permit any
inspur(config-ipv4-acl)#exit

inspur(config)#cgn
inspur(config-cgn)#cgn-pool dslite poolid 2 mode pat  /*配置地址池，类型为pat*/
inspur(config-cgn-natpool)#section 1 99.1.1.1 99.1.1.10
inspur(config-cgn-natpool)#exit
inspur(config-cgn)#domain 10 10 type standalone ipv6-issued
inspur(config-cgn-domain)# dynamic source rule-id 1 ipv4-list dslite permit
 pool dslite  /*配置动态ACL规则，也可以配置静态规则*/
inspur(config-cgn-domain)#exit

/*配置软线和用户*/
inspur(config-cgn)#softwire-domain dslite
inspur(config-cgn-sw-domain-dslite)#bind nat-domain 10
inspur(config-cgn-sw-domain-dslite)#aftr interface v6_tunnel1
inspur(config-cgn-sw-domain-dslite)#exit
inspur(config-cgn)#subscriber ipv6 prefix 2017:1::/64 softwire-domain dslite
inspur(config-cgn-sub)#interface gei-0/1
inspur(config-cgn-sub)#exit
```

配置验证

在NAT设备上查看NAT条目信息：

```
inspur#show cgn translations all-sessions
================================================================================
Subscriber
    Pro  Type    Inside Local         Inside Global        Destination
================================================================================
Loading data from MPFU-12/0 ...
================================================================================
2017:1::1:1
    UDP  dyn     192.85.1.2:1024      99.1.1.1:1024        *:*
--------------------------------------------------------------------------------
```

14 二层交换

14.1 二层交换功能

局域网定义为一个广播域，即一个用户在自己所在的局域网内广播信息时，信息会在局域网内广播，被所有用户收到。可以使用路由器来防止广播信息从局域网扩散，这种方式的缺点是，和交换机对比路由器往往需要更多时间处理接收的报文。

VLAN作为限制广播流量的另一个手段而出现。由于按职能划分工作组的科学性以及移动办公的流行，使VLAN技术成为第二层交换机的重要功能。因此要求在网络的汇聚层（Distribution layer）具有支持VLAN的高速第二层交换功能和快速第三层处理VLAN间的数据功能，以适应新的网络流量模型的要求。

IR12000智能路由器系列路由器既有路由功能又增加了二层交换能力。

14.1.1 配置二层端口

IR12000智能路由器系列路由器默认端口为三层口，使用以下命令可以将三层口切换为二层口。

1.将三层端口切换为二层口。

步骤	命令	功能
1	inspur(config)#**interface** < *interface-name*>	进入以太网接口配置模式
2	inspur(config-if-interface-name)#**switch attribute**{ **enable** | **disable** }	端口二三层切换功能：开启/关闭端口二层功能

2.配置二层端口的三播抑制。

步骤	命令	功能
1	inspur(config-if-interface-name)#**broadcast-limit**{ **percent**< *1-100*>| **pps**< *1-1480*>| **value**< *1-1000*>}	配置二层口的广播抑制
2	inspur(config-if-interface-name)#**unknowncast-limit**{ **percent**< *1-100*>| **pps**< *1-1480*>| **value**< *1-1000*>}	配置二层口的未知单播抑制
3	inspur(config-if-interface-name)#**multicast-limit**{ **percent**< *1-100*>| **pps**< *1-1480*>| **value**< *1-1000*>}	配置二层口的组播抑制
4	inspur(config-if-interface-name)#**mixc**	配置二层口的三播总抑制

步骤	命令	功能
	ast-limit{ **percent**< *1-100*>| **pps**< *1-1480*>| **value**< *1-1000*>}	

3.验证配置结果。

命令	功能
inspur(config)#**show interface brief**	查看二层口的状态

14.1.2 切换二层口配置实例

配置说明

将IR12000智能路由器设备上的以太接口配置成二层口。

配置过程

```
inspur(config)#interface gei-0/1
inspur(config-if-gei-0/1)#switch attribute enable
Would you change the L2/L3 attribute of the interface?[yes/no] :y
```

配置验证

```
inspur(config)#show interface brief
Interface Port attribute Mode BW(Mbits) Admin Phy Prot Description
gei-0/1electric Duplex/full 1000 up up up
```

14.2 VLAN

VLAN是一种将物理网络划分成多个逻辑（虚拟）局域网（LAN）的技术。

利用VLAN技术，网络管理者能够根据实际应用需要，把同一物理局域网中的用户逻辑的划分成不同的广播域（每个广播域即一个VLAN），使具有相同需求的用户处于同一广播域，不同需求的用户处于不同的广播域。每个VLAN在逻辑上就像一个独立的局域网，与物理上形成的LAN有相同的属性。同一个VLAN中的所有广播和单播流量都被限制在该VLAN中，不会转发到其他VLAN中。当不同VLAN的设备要进行通信时，必须经过三层的路由转发。

VLAN的优点主要有：

•减少网络上的广播流量。

•增强网络的安全性。

•简化网络的管理控制。

14.2.1 配置 VLAN

介绍IR12000智能路由器设备上二层功能VLAN的配置。

1.VLAN的基本配置。

步骤	命令	功能
1	inspur(config)#**switchvlan-configuration**	进入swithvlan配置模式
2	inspur(config-swvlan)#**vlan** {<*vlan-id*>| **name** <*vlan-name*>}	创建VLAN或者是对VLAN进行配置
	inspur(config-swvlan)#**list** <*2-4094*>	批量创建VLAN
4	inspur(config-swvlan-sub-interface)#**name** <*vlan-name*>	指定VLAN的别名
5	inspur(config-swvlan-if-interface-name)#**switchport mode**{**access**| **trunk**| **hybrid** }	设置端口的VLAN链路类型

2.将以太网端口加入到指定VLAN。

Access端口只能加入到1个VLAN，Trunk端口和Hybrid端口可以加入到多个VLAN中。

步骤	命令	功能
1	inspur(config-swvlan-if-interface-name)#**switchport access vlan** {<*vlan-id*>|<*vlan-name*>}	将Access端口加入到指定VLAN
2	inspur(config-swvlan-if-interface-name)#**switchport trunk vlan** <*vlan-list*>	将Trunk端口加入到指定VLAN
3	inspur(config-swvlan-if-interface-name)#**switchport hybrid vlan** <*vlan-list*>[**tag**|**untag**]	将Hybrid端口加入到指定VLAN

3.设置以太网端口的Native VLAN（PVID）。

Access端口只属于1个VLAN，所以该端口的Native VLAN就是其所在的VLAN，不用设置。

Trunk端口和Hybrid端口属于多个VLAN，需要设置Native VLAN。如果设置了端口的Native VLAN，当端口接收到不带VLAN标签的帧时，则将该帧转发到属于这个Native VLAN的端口。默认情况下Trunk端口和Hybrid端口的Native VLAN为VLAN 1。

步骤	命令	功能
1	inspur(config-swvlan-if-interface-name)#**switchport trunk native vlan** {<*vlan-id*>|<*vlan-name*>}	设置Trunk端口的Native VLAN

步骤	命令	功能
2	inspur(config-swvlan-if-interface-name)#**switchport hybrid native vlan** {<*vlan-id*>|<*vlan-name*>}	设置Hybrid端口的Native VLAN

4.添加VLAN成员端口。

命令	功能
inspur(config-swvlan-sub-interface)#**switchport** {**pvid**|**tag**|**untag**}<*port-name*>	添加VLAN成员端口

switchport pvid对所有类型的端口（Access、Trunk、Hybrid）都有效，运行本配置后所有选定端口的PVID都变成指定VLAN的VLAN ID。

switchport tag对Trunk、Hybrid端口有效。

switchport untag对Hybrid端口有效。

5.创建VLAN三层接口。

要创建VLAN三层接口，先必须创建此VLAN。三层VLAN接口的配置和以太接口类似。

三层VLAN实现了跨VLAN之间的路由，具有路由器三层口的一些基本功能。

命令	功能
inspur(config)#**interface vlan** <*vlan-id*>	创建VLAN三层接口

6.验证配置结果。

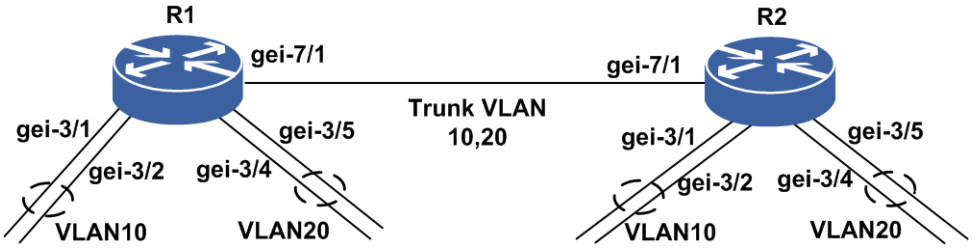
命令	功能
inspur(config)#**show running-config switchvlan**	查看二层功能的相关配置
inspur(config)#**show vlan** [**access**|**trunk**|**hybrid**|**id** <*vlan-id*>[**ifindex**]|**name** <*vlan-name*>[**ifindex**]]	查看VLAN的配置

14.2.2 VLAN 基本应用配置实例

配置说明

将IR12000智能路由器作为交换机使用，实现不同VLAN之间的隔离与相同VLAN之间的互通。如*图* **14-1**所示，图中所示接口为二层口。R1的端口gei-3/1、gei-3/2和R2的端口gei-3/1、gei-3/2属于VLAN 10；R1的端口gei-3/4、gei-3/5和R2的端口gei-3/4、gei-3/5属于VLAN 20，均为Access端口。R1和R2通过端口gei-7/1以Trunk方式连接，两端口为Trunk端口。

图 14-1 VLAN 典型组网图



配置思路

1.将三层接口切换为二层口。

2.将接口加入指定VLAN，并配置为access模式。

3.将R1和R2互联接口配置为trunk模式，并加入到多个指定VLAN。

配置过程

R1上的配置：

```
R1(config)#interface gei-3/1
R1(config-if-gei-3/1)#switch attribute enable
Would you change the L2/L3 attribute of the interface?[yes/no]:y
R1(config)#interface gei-3/2
R1(config-if-gei-3/2)#switch attribute enable
Would you change the L2/L3 attribute of the interface?[yes/no]:y
R1(config)#interface gei-3/4
R1(config-if-gei-3/4)#switch attribute enable
Would you change the L2/L3 attribute of the interface?[yes/no]:y
R1(config)#interface gei-3/5
R1(config-if-gei-3/5)#switch attribute enable
Would you change the L2/L3 attribute of the interface?[yes/no]:y

R1(config)#switchvlan-configuration
R1(config-swvlan)#interface gei-3/1
R1(config-swvlan-if-gei-3/1)#switchport access vlan 10
R1(config-swvlan-if-gei-3/1)#exit
R1(config-swvlan)#interface gei-3/2
R1(config-swvlan-if-gei-3/2)#switchport access vlan 10
R1(config-swvlan-if-gei-3/2)#exit
R1(config-swvlan)#interface gei-3/4
R1(config-swvlan-if-gei-3/4)#switchport access vlan 20
R1(config-swvlan-if-gei-3/4)#exit
R1(config-swvlan)#interface gei-3/5
R1(config-swvlan-if-gei-3/5)#switchport access vlan 20
R1(config-swvlan-if-gei-3/5)#exit
R1(config-swvlan)#interface gei-7/1
R1(config-swvlan-if-gei-7/1)#switchport trunk vlan 10,20
```

R2上的配置：

```
R2(config)#interface gei-3/1
R2(config-if-gei-3/1)#switch attribute enable
Would you change the L2/L3 attribute of the interface?[yes/no]:y
R2(config)#interface gei-3/2
R2(config-if-gei-3/2)#switch attribute enable
Would you change the L2/L3 attribute of the interface?[yes/no]:y
R2(config)#interface gei-3/4
R2(config-if-gei-3/4)#switch attribute enable
```

```
Would you change the L2/L3 attribute of the interface?[yes/no]:y
R2(config)#interface gei-3/5
R2(config-if-gei-3/5)#switch attribute enable
Would you change the L2/L3 attribute of the interface?[yes/no]:y

R2(config)#switchvlan-configuration
R2(config-swvlan)#interface gei-3/1
R2(config-swvlan-if-gei-3/1)#switchport access vlan 10
R2(config-swvlan-if-gei-3/1)#exit
R2(config-swvlan)#interface gei-3/2
R2(config-swvlan-if-gei-3/2)#switchport access vlan 10
R2(config-swvlan-if-gei-3/2)#exit
R2(config-swvlan)#interface gei-3/4
R2(config-swvlan-if-gei-3/4)#switchport access vlan 20
R2(config-swvlan-if-gei-3/4)#exit
R2(config-swvlan)#interface gei-3/5
R2(config-swvlan-if-gei-3/5)#switchport access vlan 20
R2(config-swvlan-if-gei-3/5)#exit
R2(config-swvlan)#interface gei-7/1
R2(config-swvlan-if-gei-7/1)#switchport trunk vlan 10,20
```

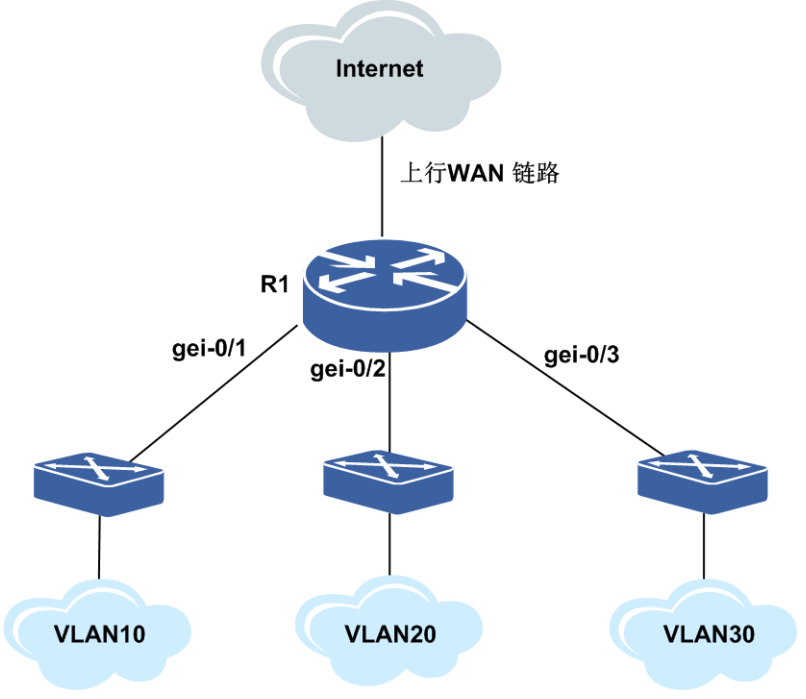
14.2.3 二层交换汇聚和三层网络接入配置实例

配置说明

IR12000智能路由器上集成了二层交换功能，可以完成二层交换的汇聚和三层网络的接入。

二层交换应用组网如*图 14-2*所示。

图 14-2 二层交换汇聚和三层网络接入组网图



配置思路

IR12000智能路由器设备作为交换机的汇聚层。该设备与交换机对接，配置二层接口，完成二层功能；同时在设备上配置三层VLAN接口，用于终结二层交换，开始三层转发。

配置过程

R1上的配置：

```
R1(config)#interface gei-0/1
R1(config-if-gei-0/1)#switch attribute enable
Would you change the L2/L3 attribute of the interface?[yes/no]:y
R1(config)#interface gei-0/2
R1(config-if-gei-0/2)#switch attribute enable
Would you change the L2/L3 attribute of the interface?[yes/no]:y
R1(config)#interface gei-0/3
R1(config-if-gei-0/3)#switch attribute enable
Would you change the L2/L3 attribute of the interface?[yes/no]:y

R1(config)#switchvlan-configuration
R1(config-swvlan)#interface gei-0/1
R1(config-swvlan-if-gei-0/1)#switchport access vlan 10
R1(config-swvlan-if-gei-0/1)#exit

R1(config-swvlan)#interface gei-0/2
R1(config-swvlan-if-gei-0/2)#switchport access vlan 20
R1(config-swvlan-if-gei-0/2)#exit

R1(config-swvlan)#interface gei-0/3
R1(config-swvlan-if-gei-0/3)#switchport access vlan 30
R1(config-swvlan-if-gei-0/3)#exit
R1(config-swvlan)#exit

/*R1配置三层VLAN用于终结二层报文*/
R1(config)#interface vlan10
R1(config-if-vlan10)#ip address 10.1.1.254 255.255.255.0
R1(config-if-vlan10)#exit

R1(config)#interface vlan20
R1(config-if-vlan20)#ip address 10.1.2.254 255.255.255.0
R1(config-if-vlan20)#exit

R1(config)#interface vlan30
R1(config-if-vlan30)#ip address 10.1.3.254 255.255.255.0
R1(config-if-vlan30)#exit
```

配置验证

```
R1#show running-config switchvlan
!<switchvlan>
switchvlan-configuration
 vlan 1
 $
 vlan 10
 $
 vlan 20
 $
 vlan 30
 $
 interface gei-0/1
```

```
   switchport access vlan 10
  $
 interface gei-0/2
   switchport access vlan 20
  $
 interface gei-0/3
   switchport access vlan 30
  $
$
```

查看**vlan**的命令：利用该命令可以查看所有VLAN、指定ID的VLAN、指定名称的VLAN的信息，还可以分别查看端口模式为Access、Trunk、Hybrid的VLAN信息。示例如下。

查看所有VLAN的配置信息：

```
inspur#show vlan
VLAN Name PvidPorts     UntagPorts     TagPorts
------------------------------------------------------------------------------
------
1  vlan0001
10 vlan0010 gei-0/1
20 vlan0020 gei-0/2
30 vlan0030 gei-0/3
```

14.3 MAC

MAC地址是网络设备的硬件标识，路由器根据MAC地址进行报文转发。MAC地址具有唯一性，这保证了报文的正确转发。

每个路由器都维护着一张MAC地址表。在这张表中，MAC地址和路由器的端口一一对应。当路由器收到数据帧时，根据MAC地址表来决定对该数据帧进行过滤还是转发到路由器的相应端口。MAC地址表是路由器实现快速转发的基础和前提。

路由器进行二层转发时，根据数据帧的目的MAC地址查找MAC地址表和VLAN表，得到需要将数据帧转发到哪个端口。

路由器进行三层快速转发时，当得到下一跳IP地址对应的MAC地址后，同样要通过查找MAC地址表得到需要将数据包转发到哪个端口。

初始状态下，路由器的MAC地址表是空的。为了实现快速转发，必须建立MAC地址表。同时，由于MAC地址表的容量有限，而网络上的设备变动比较频繁，路由器要及时删除旧的MAC地址表项，更新发生了变化的MAC地址表项。

14.3.1 配置 MAC 地址表

路由器的MAC地址表使用默认设置就能正常运行。而对MAC地址表进行一些适当的配置，可以提高网络的稳定性。

1.设置MAC地址老化时间。

MAC地址老化时间的设置会影响路由器的性能。

如果设置的MAC地址老化时间过短，路由器可能会删除许多有效的MAC地址表项，导致路由器广播大量找不到目的MAC地址的报文，占用路由器的带宽。

如果设置的MAC地址老化时间过长，路由器可能会保存许多过时的MAC地址表项，

从而耗尽MAC地址表资源，导致新的MAC地址无法添加到MAC地址表中，同样也会影响转发。

命令	功能
inspur(config-mac)#**aging-time** <*time*>	设置动态MAC地址老化时间

IR12000上MAC地址的老化时间默认为300s，可配置的范围是60s~630s。

2.端口绑定MAC地址。

在IR12000上通过配置向MAC地址表中添加永久的MAC地址，实现端口上MAC地址的绑定。绑定MAC地址后，MAC地址和端口的对应关系就按照配置的情况固定下来，该地址将不再被学习，直到手动删除该地址，这种绑定关系才会解除。

步骤	命令	功能
1	inspur(config-mac)#**add permanent** <*mac-address*> **interface**{<*interface-name*>|<*smartgroup-name*>}{[**vlan** <*vlan-id*>]|**all-owner-vlan**}	添加MAC地址
2	inspur(config-mac)#**delete** {<*mac-address*>|**interface**{<*interface-name*>|<*smartgroup-name*>}|[**vlan**<*vlan-id*>]}	删除MAC地址

3.MAC地址过滤。

在IR12000上通过配置MAC地址过滤来过滤某些已知报文。MAC地址过滤有三种过滤形式，分别为基于源MAC地址的过滤、基于目的MAC地址的过滤以及基于双向MAC地址的过滤。过滤MAC不会被学习。

步骤	命令	功能
1	inspur(config-mac)#**filter** { **source**| **destination**| **both** }<*mac-address*> **vlan**<*vlan-id*>	配置MAC地址过滤
2	inspur(config-mac)#**delete** <*mac-address*>[**vlan** <*vlan-id*>]	删除MAC地址过滤

4.查看MAC地址表。

可以通过以下命令查看MAC地址表项，显示的MAC地址包括动态学习到的和手动添加的：

命令	功能
inspur(config)#**show mac** { **count**| **l2-switch**| **table**| **vpls summary**| **move-dampening vpls**}	显示MAC地址表项

14.3.2 MAC 地址表配置实例

配置说明

可以使用命令添加MAC地址。

配置过程

```
inspur(config)#mac
inspur(config-mac)#add permanent 2222.2222.2222 interface gei-3/1 vlan 1
inspur(config-mac)#filter source 0000.0000.0001 vlan 1
inspur(config-mac)#exit
```

配置验证

通过**show mac table**命令查看MAC地址表配置信息：

```
inspur(config)#show mac table
Total MAC address : 2

Flags: Src--Source filter, Dst--Destination filter
      From:0,driver;1,config;2,VPN;3,802.1X;4,micro;5,DHCP;
          6,PBT;7,EVB;8,OTV;9,TRILL;10,ESADI;11,MC-LAG,
      Time--Day:Hour:Min:Sec

MAC           VLAN Outgoing Information        Attribute      From Time
--------------   ----   ----------------------------   --------------   ----
-----------
2222.2222.2222 1    gei-3/1                   Permanent      1    N/A
0000.0000.0001 1                             Filter(Src)    1    N/A

inspur(config-mac)#delete interface gei-3/1 ?
 XXXX.XXXX.XXXX MAC address
 vlan VLAN ID
 <cr>
inspur(config-mac)#delete interface gei-3/1

inspur(config-mac)#show mac table
Total MAC address : 1

Flags: Src--Source filter, Dst--Destination filter
      From:0,driver;1,config;2,VPN;3,802.1X;4,micro;5,DHCP;
          6,PBT;7,EVB;8,OTV;9,TRILL;10,ESADI;11,MC-LAG,
      Time--Day:Hour:Min:Sec

MAC           VLAN Outgoing Information        Attribute      From Time
--------------   ----   ----------------------------   --------------   ----
-----------
0000.0000.0001 1                             Filter(Src)    1    N/A
```

14.4 STP

STP协议可应用于环路网络，通过一定的算法阻断某些冗余路径，将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。

STP协议是通过在一个扩展的局域网中参与STP的所有设备之间交换BPDU（Bridge Protocol Data Unit）来实现的。通过交换BPDU消息可以完成以下操作：

·在稳定的生成树拓扑结构中选择一个根网桥。

·在每个交换网段选择一台指定设备。

·通过将冗余的设备端口置为Discarding来避免拓扑网络中的环路。

IR12000智能路由器的STP模块支持三种模式：SSTP、RSTP和MSTP，这三个模式分别遵循IEEE802.1d、IEEE802.1w、IEEE802.1s的标准要求。

14.4.1 配置 STP

本节介绍STP的配置步骤和命令。

1.进行STP的基本配置。

步骤	命令	功能
1	inspur(config)#**spantree**	进入STP配置模式
2	inspur(config-stp)#{**enable**|**disable**}	启用或者关闭STP协议
3	inspur(config-stp)#**mode** { **sstp**|**rstp**|**mstp** }	设置STP协议的模式

IR12000智能路由器默认的模式为MSTP。无论配置哪一种模式，都可以与其他两种模式完全兼容和互通。

2.配置STP协议的参数。

步骤	命令	功能
1	inspur(config-stp)#**hello-time** <*1-10*>	设置生成树协议的Hello间隔，默认2s
2	inspur(config-stp)#**forward-delay** <*4-30*>	设置生成树协议的转发延迟时间，默认15s
3	inspur(config-stp)#**max-age** <*6-40*>	设置BPDU包的最大有效时间，默认20s
4	inspur(config-stp)#**mst max-hops** <*1-40*>	设置BPDU包的最大有效跳数，默认20

hello-time ：用于控制BPDU包的发送时间间隔。

forward-delay ：在非状态快速迁移的条件下，此参数决定端口从Blocking状态进入Forwarding状态需要经历的延时间隔（2*forward-delay）。

max-age ：在CST网络生成树结构中，最新的BPDU包从Root设备沿CST生成树结构往叶节点设备传递。从Root设备发出的BPDU包中，message-age值为0，以后每经过一个中间节点设备，message-age值加1，max-age值不变。当BPDU包中message-age值大于max-age值时，此BPDU包无效。

max-hops：max-hops值由MST区域中某实例的区域根节点来决定，每经过一个区域中的设备节点，此值减1。当此参数值减为0时，此BPDU包无效。MST区域中BPDU报文的message-age和max-age值在整个区域传输过程中不改变。

提示：

在CST网络生成树结构中，所有设备的hello-time参数值都由Root设备来决定。Max-hops参数值只有在本节点作为MST区域内某实例的区域根节点时才会有效。

3.创建MST实例。

在MSTP模式中，用户可以通过创建或删除实例使相连的设备组成一个MST区域，这样可以实现整个网络的快速收敛和负载均衡。

步骤	命令	功能
1	inspur(config-stp)#**mst vlans** <*vlan-id*> **instance** <*instance*>	创建MST实例
2	inspur(config-stp)#**mst name** <*string*>	设置MST配置名称
3	inspur(config-stp)#**mst revision** <*version*>	设置MST配置版本号

4.进入MSTP配置模式。

步骤	命令	功能
1	inspur(config)#**spantree**	进入STP配置模式
2	inspur(config-stp)#{**enable**|**disable**}	启用或者关闭STP协议
3	inspur(config-stp)#**mode** { **sstp**|**rstp**|**mstp** }	设置STP协议的模式

IR12000在SSTP和RSTP模式下有且仅有一个实例0。在MSTP模式下，实例0默认存在，不能任意删除。

判断相互连接的设备是否在同一个MST区域内时，需要检查MST配置名称和配置版本号是否相同。

设备属于同一个MST区域需要以下四个条件，缺一不可：MST配置名称相同、MST配置版本号相同、INS-VLAN映射表相同、设备之间相互连接。

5.配置设备的优先级和端口优先级。

在整个生成树结构区域内，通过设置某个实例的网桥优先级来决定此设备在整个CST生成树结构中的位置（是否能够被选择为整个生成树的根）或在MST区域内的某个实例生成树结构中的位置（是否能够被选择为此实例的区域根）。

通过给网桥设置较小的优先级可以指定某个网桥作为生成树的根。

通过设定端口的优先级可以指定特定的端口包含在生成树内。一般情况下设置的值越小，端口的优先级就越高，该端口就越有可能包含在生成树内。如果网桥上所有的端口都设置了相同的优先级值，则端口的优先级高低就取决于该端口的索引号。

步骤	命令	功能
1	inspur(config-stp)#**mst priority** <*priority*> **instance** <*instance*>	设置某实例的网桥优先级
2	inspur(config-stp-if-interface)#**mst priority** <*priority*> **instance** <*instance*>	设置某实例的端口优先级

提示：

IR12000的网桥优先级和端口优先级必须在此实例已创建的条件下进行配置。

6.配置STP协议中某端口不参与生成树的计算。

在一些特定的环境中，可能要求某端口不参与生成树的计算，比如设备的上行口或连接PC机的端口。

命令	功能
inspur(config-stp-if-interface)#{**enable**|**disable**}	设置端口是否参与生成树计算

7.配置STP协议中某端口STP保护功能。

命令	功能
inspur(config-stp-if-interface)#**edged-port enable**	设置端口为边缘端口
inspur(config-stp-if-interface)#**bpdu-guard action**{**discard**| **shutdown**}	设置端口的BPDU保护
inspur(config-stp-if-interface)#**guard root instance**<*instance*>	设置端口的Root保护
inspur(config-stp-if-interface)#**guard loop instance**<*instance*>	设置端口的环路保护

边缘端口在由堵塞状态（N/A）向转发状态（forward）时，可以实现快速迁移，无需等待延迟时间。

- BPDU保护：端口接受到BPDU报文后，端口状态会变成discard状态或者shutdown。
- Root保护：端口会被blocking，状态为Discard*，从而不会被选为Root端口。
- 环路保护：端口在组网环境因某个交换机STP协议禁止而出现的环路情况时，能够保持discard状态，避免出现环路。

8.验证配置结果。

命令	功能
inspur(config)#**show spantree instance** <*instance*>	显示某个已创建实例的生成树详细信息
inspur(config)#**show spantree interface** <*port-name*>	显示指定端口的生成树信息

命令	功能
inspur(config)#**show spantree statistics** *<port-name>*	显示指定端口的BPDU包发送和接收统计信息

在以下三种情况中，即使启动设备的STP功能，也不能避免环路出现，配置时一定要注意。

- 两台设备对接多条平行链路，其中一台设备对这些端口配置聚合，另一台设备没有对这些端口配置聚合。
- 一台设备对多个端口配置聚合，但是聚合端口组中有一个端口与本设备的其他端口自环连接。
- 两台设备对接两条平行链路，由于未知原因使得双方接收不到对方所发的BPDU包。

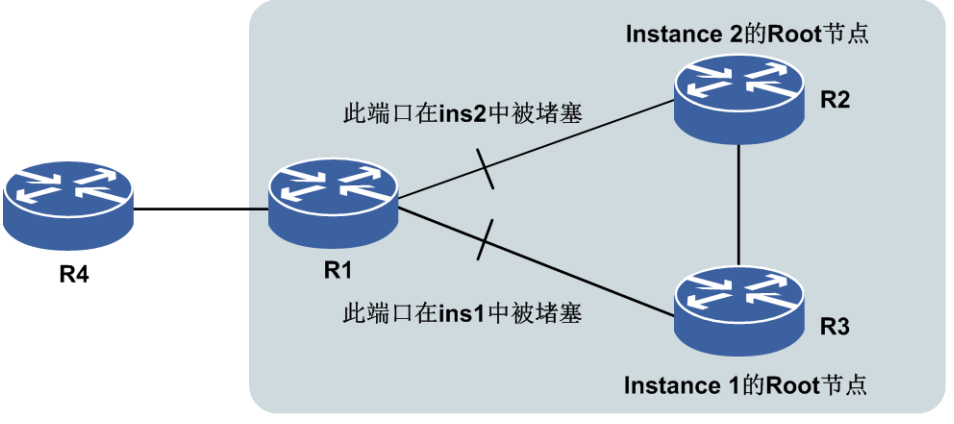
14.4.2 MSTP 配置实例一

配置说明

如*图 14-3*所示，在骨干网运行MSTP，MST域作为CST的根，即CIST根桥在MST区域内部。三台设备R1、R2、R3配置在同一个MST区域中，并且此区域在网络拓扑中的身份是CIST Root，其初始优先级均为32768，根据MAC地址确定CIST root和IST root。三台设备的MAC地址分别为：

- R1：000d.0df0.0101
- R2：000d.0df0.0102
- R3：000d.0df0.0103

图 14-3 MSTP 配置实例组网图 1



配置过程

R1上的配置：

```
/*配置MST区域*/
R1(config)#spantree
```

```
R1(config-stp)#mode mstp
R1(config-stp)#mst name inspur
R1(config-stp)#mst revision 2

/*将VLAN 1~10映射到instance 1中，VLAN 11~20映射到instance 2中*/
R1(config-stp)#mst vlans 1-10 instance 1
R1(config-stp)#mst vlans 11-20 instance 2
```

R2上的配置：

```
/*配置MST区域*/
R2(config)#spantree
R2(config-stp)#mode mstp
R2(config-stp)#mst name inspur
R2(config-stp)#mst revision 2

/*将VLAN 1~10映射到instance 1中，VLAN 11~20映射到instance 2中*/
R2(config-stp)#mst vlans 1-10 instance 1
R2(config-stp)#mst vlans 11-20 instance 2

/*改变R2在instance 2中的优先级，使之成为Instance 2的Root*/
R2(config-stp)#mst priority 4096 instance 2
```

R3上的配置：

```
/*配置MST区域*/
R3(config)#spantree
R3(config-stp)#mode mstp
R3(config-stp)#mst name inspur
R3(config-stp)#mst revision 2

/*将VLAN 1~10映射到instance 1中，VLAN 11~20映射到instance 2中*/
R3(config-stp)#mst vlans 1-10 instance 1
R3(config-stp)#mst vlans 11-20 instance 2

/*改变R3在instance 1中的优先级，使之成为Instance 1的Root*/
R3(config-stp)#mst priority 4096 instance 1
```

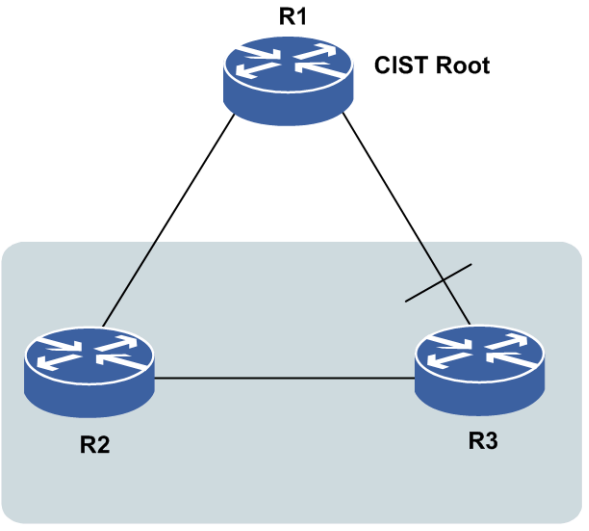
R4保留默认配置即可。

14.4.3 MSTP 配置实例二

配置说明

如*图 14-4*所示，设备R2、R3运行在一个区域中，CIST根桥R1在区域外部，设备R2或R3的一个边缘端口将被阻塞。

图 14-4 MSTP 配置实例组网图 2



本例与MSTP配置实例一的区别在于：

由于在一个区域中只存在一个能和外界通信的实例，边缘端口对所有的VLAN都是block或都是forward，因而不存在负载均衡，没有发挥MSTP模式的优点。*图 14-4*中，设备R3到R1的链路将对所有VLAN block，而设备R2到R1的链路将对所有VLAN forward。